

# ISC2 CISSP

## Study Guide

### Introduction

- **Introduction**

- Key Information and Concepts

- Overview of the CISSP Certification

- One of the most prestigious certifications in information security
      - Created and governed by the International Information System Security Certification Consortium (ISC2)
      - Demonstrates expertise in designing, implementing, and managing information security

- Audience Qualification

- Recommended 3-5 years of experience in cybersecurity or IT
    - Other certifications, such as CompTIA Security+, ISC2 SSCP, or equivalents, can be helpful
    - Not strictly required, as individuals from various professional backgrounds have succeeded

- CISSP Exam Structure

- Based on the Common Body of Knowledge (CBK) covering eight domains
    - The exam is computer-based and adaptive (CAT) with 100-150 questions over 4 hours

# ISC2 CISSP

## (Study Guide)

- The percentage of questions per domain varies, with Domain 1 holding the most weight
- The exam includes multiple-choice questions and other innovative test item types like drag-and-drop and hotspot questions
- CISSP Knowledge Domains
  - Domain 1
    - Security and Risk Management – 16% of exam questions
  - Domain 2
    - Asset Security – 10% of exam questions
  - Domain 3
    - Security Architecture and Engineering – 13% of exam questions
  - Domain 4
    - Communication and Network Security – 13% of exam questions
  - Domain 5
    - Identity and Access Management (IAM) – 13% of exam questions
  - Domain 6
    - Security Assessment and Testing – 12% of exam questions
  - Domain 7
  - Security Operations – 13% of exam questions
  - Domain 8
  - Software Development Security – 10% of exam questions
- CISSP Course Structure
  - Each domain and exam objective is clearly labeled in the video titles
  - The course organizes material in a way that groups related topics together for easier learning and understanding

# ISC2 CISSP

## (Study Guide)

- The material is designed to cover everything needed to pass the exam without the need for external resources
- CISSP Certification Importance
  - Validates applied knowledge of security concepts across various industries and technologies
  - Helps professionals advance in their careers and provides recognition in the cybersecurity industry
- Tips for Success
  - Use closed captions to enhance comprehension
  - Adjust playback speed to suit personal learning pace
  - Download the study guide for notes and reference
  - Take quizzes and practice exams seriously to assess readiness
  - Join online learning communities (Facebook, Discord) to connect with other learners and ask questions
- **Exam Tips**
  - Understand the Purpose of the CISSP Exam
    - Recognize it as a leadership-focused exam aiming at managing security risk, not just technical knowledge
    - The exam tests your ability to apply concepts to real-world scenarios
  - Learn and Understand vs. Memorizing
    - Focus on understanding concepts deeply rather than memorizing terms or acronyms
    - ISC2 exams spell out acronyms to challenge comprehension, not recall
  - Create a Structured Study Plan

# ISC2 CISSP

## (Study Guide)

- Plan your study time around your life commitments; about an hour a day is recommended
- Include rest days and review sessions to consolidate learning
- Limit Study Resources
  - Avoid information overload by sticking to a few trusted sources
  - Recommended resources include the official CISSP study guide and CISSP CBK books
- Use Practice Exams Properly
  - Practice exams are critical for getting used to the question format and testing your understanding
  - Focus on understanding why answers are correct or incorrect to identify knowledge gaps
- Manage Time During the Exam
  - Develop a strategy to allocate time appropriately across questions, aiming to spend no more than 1.5 minutes per question
- Prepare for Exam Day
  - Ensure rest the night before and arrive early at the testing center
  - Bring necessary identification and confirmation details, and manage stress and time during the test efficiently

## Security Management Concepts

### Objectives:

- 1.1 - Understand, adhere to, and promote professional ethics
- 1.2 - Understand and apply security concepts
- 1.3 - Evaluate and apply security governance principles
- 1.12 - Establish a security awareness program
  
- **Security Management Concepts**
  - Security Management Concepts
    - Fundamental for establishing a robust security foundation in organizations
    - Essential for both the CISSP exam and effective security management in real-world scenarios
  - Code of Ethics
    - Focus on the ISC2 Code of Ethics which guides security professionals' behavior
    - Emphasizes integrity, competence, and professionalism
  - Information Security Concepts
    - Core principles
    - Confidentiality, Integrity, Availability (CIA Triad), authenticity, and non-repudiation
    - Supports effective security controls and strategies

- Aligning Security and the Organization
  - Security measures should support and align with organizational goals, culture, and operations
  - Involves tailoring security strategies to meet specific business needs
- Organizational Roles and Responsibilities
  - Defines clear roles in security management to avoid conflicts and ensure effective security practices
  - Includes roles of senior executives, security managers, and end-users
- Security Awareness Training
  - Essential for mitigating risks associated with human error and social engineering
  - Focuses on educating employees about their roles in protecting assets
- Social Engineering
  - Techniques used by attackers to manipulate individuals into divulging confidential information
  - Requires a combination of technical measures and a vigilant organizational culture to defend against
- Personnel Security Policies
  - Manage risks associated with personnel throughout their employment lifecycle
  - Includes pre-employment screening and post-employment restrictions to safeguard sensitive information

- **Code of Ethics**

- Code Of Ethics (1.1)

- ISC2 requires all CISSP® holders to adhere to, and follow, the Code of Ethics (COE)
    - *Preamble*
    - “The safety and welfare of society and the common good, duty to our principles, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.” – isc2.org
    - “Therefore, strict adherence to this Code is a condition of certification.” – isc2.org

- *4 Canons of The Code of Ethics*

- Protect society, the common good, necessary public trust and confidence, and the infrastructure
    - Act honorably, honestly, justly, responsibly, and legally
    - Provide diligent and competent service to principals
    - Advance and protect the profession

- **Information Security Concepts**

- Confidentiality

- Ensure data/information is not disclosed to an unauthorized person or process (preventing people from seeing data they are not allowed to see)

Integrity

- Ensure data/information is not altered or changed by an unauthorized person or process (preventing people from changing data they are not allowed to change)
  - Availability
    - Ensure data/information is available for use by authorized persons or processes (making sure data is available when it is needed)
  - Authenticity
    - Make sure the data or action (whether it be the creation, modification, or deletion) came from a legitimate source
  - Non-repudiation
    - Proves that data or actions originated from a subject that cannot be disputed. Accomplished using cryptography
- **Aligning Security And The Organization**
  - Security Governance
    - Defines how to ethically align business objectives to laws, standards, or regulations
    - Sets the stage for how an organization's management will act in the best interest of the business stakeholders
  - Aligning Security
    - The security program must support the objectives, principles, and strategies of the organization
    - Security must be supported by senior management to be effective



- A top-down approach
- Top-down approach
  - Support for security starts with senior management, then middle management, then all other personnel
- Security Planning
  - Strategic plan (long-term)
  - Outlines the business goals and objectives over a 3–5-year period, and is typically updated annually
  - Tactical plan (mid-term)
  - Outlines the business goals and objectives over 1 year
  - Designed to meet the security objectives in the strategic plan
  - Operational plan (short-term)
  - Outlines business goals and objectives to meet the tactical and strategic plan objectives over a 1–3-month period
- Organizational Processes
  - Changes within the organizational structure must be evaluated to ensure it meets organizational policy
  - Security plans must be reviewed and updated upon any purchases, acquisitions, sales, and/or divestitures
- **Organizational Roles and Responsibilities**
  - Executive roles and responsibilities
    - Chief Executive Officer (CEO)
    - Responsible for everything relating to the organization

- Chief Financial Officer (CFO)
- Responsible for everything relating to organizational finances and assets
- Chief Information Officer (CIO)
- Responsible for the vision and strategy of the organization's information systems
- Chief Information Security Officer (CISO)
- Responsible for the vision and strategy of the organization's security program
- Boards And Committees
- Groups that are responsible for making key organizational decisions
- Security roles and responsibilities
  - Security Manager
  - Develops and manages the security program and security personnel involved
  - Security Officer
  - Implements and maintains the information security strategy or program
  - Security Analyst
  - Detects, analyzes, and responds to security threats and attacks
  - Security Engineer
  - Design, test, and implementation of security solutions
- Data roles and responsibilities
  - Data Owner
  - Responsible for the classification and protection of their data
  - Data Custodian
  - Responsible for implementing data protection.

- Data Steward
  - Provides subject matter expertise for specific data.
- System roles and responsibilities
  - Administrator
  - Responsible for implementing and maintaining the information system – privileged
  - Auditor
  - Responsible for auditing compliance with security policy
  - User
  - A subject with access to the information system
- **Security Awareness Training And Education**
  - Security Awareness Training and Education
    - Critical components of a security program designed to increase the overall security knowledge within an organization and ensure compliance with regulatory requirements.
  - CISSP Exam Objectives Related to Security Awareness Training
    - Establishment and maintenance of security awareness, education, and training programs
    - Methods for disseminating security awareness and training
    - Techniques for evaluating the effectiveness of these programs
  - Security Awareness
    - Objective
      - Increase employee understanding of company security policies and procedures

- Methods
  - Emails, posters, workshops, and regular updates on security protocols
- Security Training
  - Focus
    - Enhance skills to adhere to security policies
  - Approaches
    - Hands-on training sessions, simulations, and role-specific training
- Security Education
  - Goal
    - Provide comprehensive knowledge and skills beyond immediate job functions
  - Platforms
    - Formal courses, certifications, and advanced training programs
- Practical Applications and Scenarios
  - Administrative Security Controls
    - Implementation through policies and procedures distributed during employee onboarding and regular intervals
  - Regulatory Compliance
    - Adherence to standards such as PCI DSS, FISMA, and ISO 27001 through targeted training programs
  - Risk Reduction Strategies
    - Incorporation of findings from risk assessments into training materials

- Tailoring training to address specific security vulnerabilities and threats
  
- **Social Engineering**
  - Social Engineering
    - Psychological manipulation used to deceive individuals into divulging confidential or personal information, often for fraudulent purposes
  - Common Social Engineering Techniques
    - Pretexting
      - Creating a fabricated scenario to obtain information or persuade the target
    - Quid Pro Quo
      - An attacker provides something in exchange for information or access
    - Phishing
      - Fraudulent communications, usually via email, meant to lure individuals into revealing sensitive information
  - Phishing Variants
    - Spear Phishing
      - Targeted phishing aimed at specific individuals or groups.
    - Whaling
      - Phishing attacks targeted at high-profile or executive-level individuals
    - Vishing

- Voice phishing conducted over the phone
- Spit
  - Spam over internet telephony or pre-recorded calls
- Smishing
  - Phishing through SMS messages
- Spim
  - Spam over instant messaging, aimed at collecting data or tricking users
- Physical Social Engineering Tactics
  - Shoulder Surfing
    - Observing someone to gain information, such as passwords or PINs
  - Dumpster Diving
    - Sifting through trash to find sensitive information
  - Tailgating
    - Following someone through a secure door without their knowledge
  - Piggybacking
    - Gaining access by asking someone to hold the door, typically by pretending to be in need or using empathy
- Defense Against Social Engineering
  - Security Awareness Training
    - Educate personnel to recognize and respond to social engineering attempts
  - Identification and Authentication

# ISC2 CISSP

## (Study Guide)

- Require valid identification for all personnel and visitors; verify unknown individuals by contacting their associated company or team
- Verification of Visitors
  - Always check for identification and authorization, especially for vendors and visitors claiming to work for the organization
- Practical Applications and Scenarios
  - Example of Phishing
    - An email appears to be from Netflix, asking for updated payment information to prevent service interruption. Indicators include an incorrect email address and suspicious links
  - Example of Pretexting
    - A fake tech support call asking for user credentials to "resolve an urgent issue."
  - Scenario for Training
    - Role-playing exercises for employees to practice identifying phishing emails, suspicious phone calls, and tailgating attempts
- **Personnel Security Policies**
  - Objective
    - Implement security policies that govern the hiring, onboarding, managing, and termination of employees to mitigate security risks associated with personnel

- Key Security Controls for Personnel Management
  - Separation of Duties
    - Prevents any single person from having excessive control over critical functions
  - Least Privilege
    - Ensures personnel have only the minimum level of access required to perform their job functions
  - Need to Know
    - Restricts access to information solely to individuals who require it to perform their duties
- Hiring Process
  - Job Description
    - Clearly defines the role, responsibilities, and required qualifications to attract suitable candidates
  - Screening and Background Checks
    - Includes checks for criminal history, social media activities, previous employment, and educational qualifications to ensure candidates' suitability and trustworthiness
  - Interview Process
    - Structured interviews to assess candidates' skills, knowledge, and compatibility with the organization's security culture
- Employee Agreements and Policies
  - Non-Disclosure Agreement (NDA)
    - Binds employees to protect sensitive information both during and after their tenure



- Non-Compete Agreement
  - Prevents employees from joining competing firms for a specified period post-employment
- Acceptable Use Policy
  - Defines acceptable and secure ways employees can use company resources
- Onboarding Process
  - Security Training
    - Introduces new hires to the organization's security policies, tools, and expected behaviors
      - Access Authorization
    - Grants access to company resources based on the principle of least privilege
  - Policy Acknowledgement
    - Requires new hires to sign agreements acknowledging understanding and compliance with security policies
- Offboarding Process
  - Termination Procedures
    - Outlines steps to securely terminate access rights and retrieve company assets
  - Exit Interviews
    - Conducted to understand potential security concerns and reinforce confidentiality agreements
    - Access Revocation

- Ensures timely deactivation of all access rights once employment is terminated
  - Compliance and Legal Considerations
    - Regulatory Requirements
      - Ensures hiring practices comply with applicable laws and regulations
        - E.g., EEOC, GDPR
    - Documentation
      - Maintains records of all agreements, training, and policy acknowledgments for auditing and compliance purposes
- **Personnel Safety and Security**
  - Objective
    - To ensure the safety and security of personnel within the organization through effective policies and practices
  - Focus
    - Mitigate risks associated with travel, emergency situations, and potential duress scenarios that personnel may face during their duties
  - Key Components of Personnel Safety and Security
    - Travel Security
      - Ensure security measures are in place for personnel traveling on behalf of the organization
      - Implement endpoint security measures like host-based firewalls, anti-malware, and tracking software

# ISC2 CISSP

## (Study Guide)

- Use VPNs for secure remote access to organizational resources
- Remote Access Security
  - Enhance security protocols for remote network access
  - Regularly update and monitor the effectiveness of remote access solutions to prevent unauthorized access
- Emergency Communication
  - Establish clear protocols for personnel to report emergencies or security incidents.
  - Develop a comprehensive communication plan that includes emergency contact numbers and procedures
- Duress Situations
  - Train personnel on how to recognize and respond to duress situations
  - Implement security measures such as duress codes or silent alarms to alert security without escalating the situation
- Emergency Management
  - Develop and maintain an emergency management plan that includes procedures for different types of emergencies, such as natural disasters or on-site incidents
  - Ensure all personnel are familiar with emergency egress and ingress routes and have regular drills
- Training and Awareness
  - Objective
    - Equip personnel with the knowledge and skills to handle security situations effectively

- **Methods**
  - Regular training sessions on security policies and emergency procedures
  - Drills and simulations to prepare personnel for real-life scenarios
  - Awareness programs that focus on the importance of security in everyday operations.
- **Travel Safety Procedures**
  - **Policies for Secure Travel**
    - Guidelines for securing sensitive information and devices while traveling
    - Policies on the use of secure connections for accessing corporate networks
    - Procedures for reporting and responding to security incidents while away from the office
- **Handling Duress and Emergencies**
  - **Procedures for Reporting Duress**
    - Steps to take when experiencing or witnessing a duress situation.
    - Use of coded signals or words to discreetly inform security personnel.
  - **Emergency Response Protocols**
    - Specific actions to take in various emergency scenarios.
    - Roles and responsibilities defined for all personnel during an emergency.

## Security Governance and Compliance

### Objectives:

- 1.4 - Understand legal, regulatory, and compliance issues
- 1.6 - Develop, document, and implement security policy, standards, procedures, and guidelines
  
- **Security Governance and Compliance**
  - Security Governance and Compliance
    - Ensures organizational security practices align with legal and regulatory standards
    - Critical for protecting assets and responding appropriately to security incidents
  - Due Care and Due Diligence
    - Due care involves the responsibility to implement effective security measures
    - Due diligence refers to the ongoing effort to ensure these measures are continuously updated and effective
    - Understanding the distinction between these concepts is crucial for legal and regulatory compliance
  - Laws and Regulations

# ISC2 CISSP

## (Study Guide)

- GDPR (General Data Protection Regulation) for the EU and HIPAA (Health Insurance Portability and Accountability Act) for the US are key regulations
- Knowledge of both international and national regulations, as well as industry-specific laws, is essential for compliance
- Licensing and Property Rights
  - Understanding different software licenses and their legal implications
  - Managing software rights to avoid legal challenges and security vulnerabilities
- Export and Import Controls (EXIM)
  - Regulate the transfer of technology and sensitive information across borders
  - Important for organizations operating globally, especially regarding encryption software
- Cybercrime and Data Breaches
  - Includes activities like hacking, identity theft, and fraud
  - Understanding how to respond to data breaches and the legal requirements for reporting them is crucial
- Security Compliance Artifacts
  - Includes audit reports, risk assessments, and policy documents
  - Keeping these documents up to date is crucial for audits and demonstrating regulatory compliance

- **Due Care and Due Diligence**

- Objective

- Understand the legal and ethical standards for protecting organizational assets and information

- Focus

- Emphasize the importance of these standards in maintaining organizational security and compliance

- Definitions and Distinctions

- Due Care

- The reasonable efforts made by an organization to prevent harm to individuals or assets
      - Also known as the "Prudent Person Rule," which involves taking reasonable steps to protect the company from foreseeable risks
      - Key Concept
      - Responsibility to protect stakeholders and implement security measures aligning with industry best practices

- Due Diligence

- The continuous activities used to ensure compliance with due care
      - Focuses on avoiding liability and maintaining security practices by assessing and improving security measures to meet organizational standards
      - Key Concept
        - Ongoing assessment and validation of security practices to identify gaps and enforce improvements

- Legal and Ethical Implications

- Discuss the implications of not adhering to due care and due diligence, including potential legal liabilities and ethical breaches
- Emphasize the role of these principles in corporate governance and compliance frameworks
- Example
  - Illustrate with a scenario where a lack of due diligence led to a data breach and legal consequences
- Application in Security Governance
  - Requirement Identification
    - Recognize security requirements based on organizational, legal, and compliance needs
  - Implementation of Controls
    - Apply appropriate security controls to meet the identified requirements
  - Maintenance and Evaluation
    - Regularly review and update security controls to ensure they continue to meet the necessary standards
- Real-world Application
  - Provide examples of how due care and due diligence are applied in various industries, such as healthcare (HIPAA compliance) or financial services (SOX compliance)
  - Discuss case studies where failure to apply these principles led to significant financial and reputational damage



- **Important Laws and Regulations**

- Federal Trade Commission Act (FTC Act)
  - Protects consumers against unfair or deceptive acts that affect commerce
  - Includes protection of personally identifiable information (PII)
- Gramm-Leach-Bliley Act (GLBA)
  - Focuses on the privacy of financial data
  - Prohibits sharing of financial information without customer consent
- Electronic Communications Privacy Act
  - Governs the collection and disclosure of electronic communications
  - Limits how the US government can access electronic communications
- Health Insurance Portability and Accountability Act (HIPAA)
  - Establishes requirements for the protection of health-related information
- Health Information Technology for Economic and Clinical Health Act (HITECH)
  - Mandates protection of Protected Health Information (PHI) by entities covered under HIPAA
- Genetic Information Nondiscrimination Act (GINA)
  - Prohibits discrimination based on genetic information in health insurance and employment
- Sarbanes-Oxley Act (SOX)
  - Protects investors by improving the accuracy and reliability of corporate disclosures
- Payment Card Industry Data Security Standard (PCI DSS)
  - Sets security standards for companies that handle branded credit cards from the major card schemes

- Not a law but a standard enforced via fines or penalties by payment card companies
- General Data Protection Regulation (GDPR)
  - EU regulation that enhances and unifies data protection for individuals within the European Union
  - Applies to all entities that process personal data of EU residents
- Roles Defined by GDPR
  - Controller
    - Determines the purposes and means of processing personal data
  - Processor
    - Processes personal data on behalf of the controller
- Rights Under GDPR
  - Access
    - Subjects can access their personal data
  - Rectification
    - Subjects can update or correct their data
  - Erasure
    - Also known as the right to be forgotten
  - Restriction
    - Subjects can limit how their data is used
  - Data Portability
    - Subjects can reuse their data for their own purposes across different services
  - Object
    - Subjects can object to the processing of their personal data

- **Licensing and Property Rights**

- Intellectual Property (IP)

- Created by individuals, organizations, or companies from the human mind
- Includes product design ideas, unique names for products, catchphrases, slogans, books, articles, recipes, formulas, and other literary work
- Protected by law in most countries

- Intellectual Property Rights

- Rights that accompany intellectual property, granting ownership and protection against theft, misuse, or unauthorized access
- Due care and due diligence must be employed to maintain entitlement to intellectual property protection

- Key Intellectual Property Protections

- Patent

- Grants an inventor the exclusive legal right to use an invention
- Covers software code, hardware components, mechanical parts, etc.

- Trademark

- Identifies exclusive goods or services from an individual or organization
- Protects company names, slogans, logos, and symbols from unauthorized use

- Copyright

- Provides exclusive rights over artistic work like books, lyrics, videos, photographs, and paintings
- Valid for the author's life, plus 70 years in many jurisdictions

# ISC2 CISSP

## (Study Guide)

- Use of copyrighted material requires permission or attribution
- Trade Secret
  - Protects secret methods or processes that give an organization a competitive advantage
  - Can cover proprietary processes, recipes, designs, or algorithms
- License
  - Legal agreement outlining terms of use for a product or service
  - Grants permission to use products in a specified manner, including software, patents, or copyrighted/trademarked materials
- Types of Licenses
  - Perpetual License
    - Lifetime authorization to use the product
  - End User License Agreement (EULA)
    - Binding agreement between the user and the license issuer
  - Creative Commons (CC)
    - Free use license for copyrighted materials
- Corporate Espionage
  - Secretly acquiring protected information without the owner's permission
  - Goes beyond ethical competitive research and may involve criminal activity
  - Intellectual property protection is critical to defend against corporate espionage
- International Protection of Intellectual Property
  - World Intellectual Property Organization (WIPO)
    - Provides technical assistance for international IP protection

- World Trade Organization (WTO)
  - Offers a structured legal process for IP protection globally
- **Export and Import Controls**
  - Key Terms and Definitions
    - Export and Import Controls (EXIM)
      - Regulations governing the international trade of goods, services, and data to prevent sensitive technologies from reaching unauthorized nations
    - Transborder Data Flow
      - Movement of data across country borders, subject to legal jurisdictions and compliance requirements
  - Key Information
    - Many countries have laws controlling the export and import of technology, goods, services
    - Controls aim to prevent unauthorized access to trade secrets, controlled technologies, and sensitive data
    - Wassenaar Arrangement
      - Focuses on export controls for arms and dual-use goods and technologies
      - Prevents acquisition by terrorists
      - Includes 42 participating countries
      - Emphasizes on transparency and responsibility in international transfers
    - Category 5 of Wassenaar Arrangement
      - Part 1

# ISC2 CISSP

## (Study Guide)

- Telecommunications
- Part 2
  - Information Security, particularly cryptography and cyber weapons
- Examples
  - Encryption software exported to a country without proper compliance might violate Category 5 Part 2
  - Mechanical components that could be used in both civilian and military applications might fall under dual-use goods
- Security Controls
  - Administrative, technical, or logical, and physical controls are necessary to comply with export and import regulations
  - Security controls must cover the lifecycle of data and technology from creation to deletion, ensuring compliance with international laws
- Data Localization and Data Trading
  - Data Localization
    - Requires data to be processed within the country of origin to maintain control over its export and import
  - Data Trading
    - The buying and selling of data for various purposes, including marketing or malicious activities, necessitating strict compliance with data protection laws
- **Cybercrime And Data Breaches**
  - Key Information and Defined Terms
    - Cybercrime

# ISC2 CISSP

## (Study Guide)

- Defined as criminal acts carried out by means of computers or the internet
- Encompasses any crime that involves a computer and a network
- Data Breach
  - Occurs when information is accessed without authorization
  - Can happen on a local system, local area network, or involve large databases affecting millions
- Computer Fraud and Abuse Act (CFAA)
  - First major cybercrime legislation in the USA, established in 1984, updated in 1994
  - Focuses on fraud and related activities in connection with computers
- National Information Infrastructure Protection Act of 1996
  - Addresses the protection of critical information infrastructures
- Federal Information Security Modernization Act (FISMA)
  - Centralizes federal cybersecurity responsibilities within the Department of Homeland Security
- Types of Threat Actors
  - Attacker
    - Generally describes someone attempting unauthorized access to systems
  - Hacker
    - Uses computers to carry out attacks; traditionally meant a person intensely interested in the technicalities of computer systems and networks

# ISC2 CISSP

## (Study Guide)

- Script Kiddies
  - Individuals using existing computer scripts or codes to hack into computers, lacking sophisticated expertise
- Insider Threats
  - Employees who have access to the corporate networks and might exploit their access to steal information
- State Actors
  - Government-sponsored groups engaging in espionage and other cyber operations
- Types of Cyber Attacks
  - Active Attacks
    - Attempts to alter system resources or affect their operation
  - Passive Attacks
    - Attempts to learn or make use of information from the system without affecting system resources
  - Zero-Day Attack
    - Occurs when attackers exploit a previously unknown vulnerability in a computer application, one that developers have not had time to address and patch
- Cybercrime Classifications
  - Intentional Disruption Crime
    - Targets the availability of systems and networks
  - Destruction Crime
    - Focuses on the deliberate destruction of data or systems



- Hactivism
  - Attacks motivated by political or social objectives, often involving website defacement or data leaks
- Doxing
  - Publicly releasing private or identifying information about an individual or organization
- **Determine Compliance Requirements**
  - Compliance Requirements for Security Professionals
    - Security professionals must determine and understand compliance requirements for information systems
    - Compliance involves understanding contracts, legal matters, industry standards, and regulatory requirements
    - Essential to ensure that all applicable laws and regulations are followed in the organization's security practices
  - Importance of Compliance
    - Legal and regulatory requirements apply to every industry
      - E.g., financial, healthcare, government
    - Failing to comply with industry regulations can result in
      - Civil penalties
        - Monetary fines, legal costs, civil suits
      - Criminal penalties
        - Fines, imprisonment, and other legal consequences
  - Examples of Industry Regulations
    - Computer Fraud and Abuse Act (1986)

- Governs computer-related fraud and abuse
- Federal Privacy Act (1974)
  - Regulates personal information handled by federal agencies
- Computer Security Act (1987)
  - Establishes baseline security practices for federal agencies
- Federal Information Security Management Act (FISMA)
  - Establishes federal cybersecurity standards
- Economic Espionage Act (1996)
  - Protects against theft of trade secrets
- U.S. Patriot Act
  - Expands surveillance and investigatory powers
- Sarbanes-Oxley Act (SOX)
  - Governs financial disclosures for public companies
- Payment Card Industry Data Security Standard (PCI DSS)
  - Security standard for payment card transactions
- Gramm-Leach-Bliley Act (GLBA)
  - Regulates financial institutions' management of personal data
- Basel II Accord
  - International banking regulation standards
- Health Insurance Portability and Accountability Act (HIPAA)
  - Sets standards for medical data protection
- Personal Information Protection and Electronic Documents Act (PIPEDA)
  - Canadian privacy law for personal data
- General Data Protection Regulation (GDPR)
  - EU regulation for data privacy and protection

- Application of Compliance Standards
  - Security professionals must apply necessary security controls, safeguards, and countermeasures as required by regulations
  - Regulations usually focus on privacy and data protection
  - Compliance is demonstrated through
- Artifacts
  - Documents, plans, policies, and procedures
  - These artifacts are used to show adherence to security controls and regulatory requirements
- Cross-National Compliance Considerations
  - When contracting with organizations in different countries, consider laws and regulations from each jurisdiction
  - Laws vary between countries, requiring understanding of each applicable legal framework
- **Security Compliance Artifacts**
  - Key Information and Defined Terms
    - Security Documents
      - Define expectations for personnel behavior and actions, essential for compliance demonstration
    - Policy
      - High-level document stating organizational compliance with external requirements, such as laws or industry standards
    - Standard

# ISC2 CISSP

## (Study Guide)

- Specific requirements set to align with organizational policies, detailing compliance methods
- Procedure
  - Detailed, step-by-step instructions on how to implement standards
- Baseline
  - Minimum security controls required to meet standards, adjustable through formal change management processes
- Guideline
  - Recommendations or best practices used when standards or procedures are unclear or non-specific
- Types of Policies
  - Organizational Policy
    - Defines organizational security goals and responsibilities
    - Issue-Specific Policy
      - Offers guidance on handling specific security incidents or operational issues.
    - System-Specific Policy
      - Pertains to particular system components or devices
      - E.g., IoT or BYOD
- Compliance and Documentation Process
  - Documents must be regularly reviewed and updated to remain compliant with applicable laws and regulations
  - Using industry-standard templates ensures consistency and comprehension across different organizational and external entities.



# ISC2 CISSP

## (Study Guide)

- Documentation should include a clear process for managing exceptions and waivers to standard compliance requirements
- Development and revision of these documents must involve formal approval processes to align with organizational risk tolerance and ensure due diligence

## Risk Management

### Objectives:

- 1.9 - Understand and apply risk management concepts
- 7.2 - Conduct logging and monitoring activities
- 1.11 - Apply supply chain risk management concepts
  
- **Risk Management**
  - Risk Management
    - Essential to information security
    - Key for answering questions on the CISSP exam
    - Addresses risks including cyber threats and natural disasters
    - Drives security control implementations
    - Links to domains like asset security, network security, and security operations
  - Risk Management Concepts
    - Threats and vulnerabilities together create risk
    - Processes include identifying, assessing, and mitigating risks
  - Risk Response Strategies
    - Strategies include avoiding, transferring, and mitigating risk
    - Strategy selection based on organizational needs and risk nature
    - Importance of continuously assessing strategy effectiveness
  - Controls and Countermeasures

- Types include preventive, detective, compensating, or corrective
- Crucial for choosing the right control for specific scenarios
- Continuous Monitoring
  - Utilizes both technology and human oversight
  - Integral part of risk management
- Supply Chain Risk Management (SCRM)
  - Manages risks from the supply chain including vendors and geopolitical issues
  - Critical for ensuring operational resilience and security
  - Involves risk assessment and control implementation
- **Risk Management Concepts**
  - **Key Information and Defined Terms**
    - Risk Management
      - The process of identifying, assessing, and managing risks to an acceptable level
    - Threat
      - Potential for unwanted harm to occur to personnel or assets.
    - Vulnerability
      - A weakness or flaw in an organizational asset that can be exploited to cause harm
    - Risk Formula
      - $\text{Threats} \times \text{Vulnerabilities} = \text{Risk}$ ; emphasizes the interaction between threats and vulnerabilities to form a risk
  - Components of Risk Management

- Identifying Threats and Vulnerabilities
  - First step in risk management
    - Involves recognizing potential dangers and weaknesses within the organization
    - Conducting Risk Assessments
      - Analyzing organizational assets to discover potential risks
      - Led by senior management but involves input from various organizational levels
    - Risk Response
      - Deciding on how to address the identified risks
      - Involves choosing to accept, mitigate, transfer, or avoid the risks
    - Monitoring and Review
      - Ensuring that the risk responses remain effective over time
      - Includes adjustments based on new information or changes in the organizational context
- **Risk Response And Monitoring**
  - Key Information and Defined Terms
    - Risk Response
      - Decision-making process regarding how to address identified risks
    - Risk Monitoring
      - Continuous evaluation to ensure risk responses remain effective and compliant
  - Concepts Explained
    - Risk Mitigation
      - Most common risk response



# ISC2 CISSP

## (Study Guide)

- Involves reducing the risk to an acceptable level through various controls
- Risk Assignment
  - Transferring the responsibility and accountability of managing a risk to another party
    - E.g., insurance company, managed service provider
- Risk Deterrence
  - Implementing deterrent controls to decrease the likelihood or impact of a risk
- Risk Avoidance
  - Avoiding activities that introduce higher levels of risk
- Risk Acceptance
  - Acknowledging and accepting the level of residual risk after other responses have been applied
- Risk Monitoring Strategies
  - Verification of Effectiveness
    - Ensuring that risk management strategies and controls effectively mitigate risks to acceptable levels
  - Compliance Assurance
    - Confirming that risk responses adhere to relevant policies, laws, and regulations
  - Continuous Improvement
    - Regularly updating and refining risk responses based on operational feedback and changing conditions
- Risk Maturity Model

- Utilizes qualitative assessments to visualize risk levels over time, helping organizations monitor shifts in risk exposure and prioritize response
- **Controls and Countermeasures**
  - Security Controls
    - Purpose
      - To administratively, physically, or technically safeguard or counter security risks
    - Objective
      - Reduce or manage security risk by applying appropriate controls
  - Cost-Benefit Principle
    - Security control costs should not exceed the benefit or the asset value
    - Example
      - Protecting a \$10,000 web server should not cost more than \$10,000
  - Role of Controls in Organizations
    - Solve specific security problems within the organization
    - Ensure consistent protection, risk reduction, and compliance with governance
  - Applicability of Controls
    - Applicable to users, system components, services, protocols
  - Defense in Depth
    - Strategy involving multiple layers of security measures
    - Components
      - Functions, processes, personnel, and other assets
  - Categories of Controls

- Administrative Controls
  - Procedures and processes, also known as soft or process controls
- Technical and Logical Controls
  - Measures to protect assets technically and logically
- Physical Controls
  - Measures to protect assets physically
- Types of Controls
  - Deterrent Controls
    - Discourage unauthorized actions
  - Preventative Controls
    - Stop or prevent unauthorized actions
  - Detective Controls
    - Discover unauthorized actions
  - Corrective Controls
    - Correct or modify unauthorized actions
  - Compensating Controls
    - Support other controls
  - Directive Controls
    - Direct compliance with security policies
  - Recovery Controls
    - Recover from events
- Security Policy Role
  - Administrative, preventive, deterrent, and directive in nature
  - Example

- Policy sections specifying punishment for violations to deter non-compliance
  - Example Application of Controls to a Web Server
    - Physical Controls
      - Deterrent signs, alarm systems
    - Technical Controls
      - Warning banners, identity and access management, multi-factor authentication
    - Administrative Controls
      - Audit logs, configuration standards, employee reprimand
  - Effective Defense in Depth
    - Combination of administrative, technical, and physical controls for comprehensive security
- **Continuous Monitoring**
  - Definition and Purpose of Continuous Monitoring
    - Also known as Continuous Improvement
    - Objective
      - Maintain ongoing awareness of organizational risks and the security posture
    - Focuses on security control implementations, not just system monitoring
  - Difference from System Monitoring
    - Continuous Monitoring is not restricted to log file review or system status monitoring
    - Involves evaluating all types of controls
      - Administrative, logical, technical, and physical

- Importance in Security Operations
  - Regular evaluation of security controls against current threats and vulnerabilities
  - Ensures controls remain effective over time as threats evolve
- Due Diligence and Due Care
  - Due Care
    - Implementation of security controls
  - Due Diligence
    - Ongoing improvement of controls based on emerging threats and vulnerabilities
- Integration in Risk Management
  - Continuous monitoring data is crucial for security assessments, tests, and audits
  - Helps in understanding the effectiveness of controls and the security baseline
- Frameworks and Standards
  - NIST SP 800-137
    - Information Security Continuous Monitoring (ISCM)
  - ISO 27004
    - Monitoring, Measurement, Analysis, and Evaluation
  - Primary focus for CISSP exam
    - NIST SP 800-137
- Monitoring Strategy Components
  - Scope
    - Defines what assets, personnel, and controls are included

- Method
  - Describes how evaluations are performed, e.g., manual inspections, automated scans
- Frequency
  - Determines how often different controls are reviewed
- Metrics and Reporting
  - Metrics track success, failure, compliance, and non-compliance
  - Continuous monitoring findings are reported to senior management for decision-making
- Continuous Monitoring Plan
  - Document that outlines the monitoring strategy, scope, methods, frequency, and metrics
  - Adjusted periodically to align with organizational needs and governance requirements
- Tier Levels in Continuous Monitoring
  - Tier 1
    - Overall risk management strategies
  - Tier 2
    - Business processes or critical business functions
  - Tier 3
    - Security and privacy controls meeting business objectives
- **Supply Chain Risk Management**
  - Definition and Importance of Supply Chain Risk Management (SCRM)
    - SCRM addresses security risks in the supply chain of an organization acquiring goods and services

- Essential due to dependencies on external sources for operational components
- Frameworks and Standards
  - NIST IR7622
    - Notional Supply Chain Risk Management practices for Federal Information Systems
  - CNSS D505
    - Guidelines on Supply Chain Risk Management
  - ISO 28000
    - Specification for Security Management Systems for the Supply Chain
- Purpose of SCRM
  - To secure the supply chain against potential threats and vulnerabilities
  - Ensure compliance with laws and regulations requiring SCRM
- Risks in Supply Chain
  - Hardware Risks
    - Counterfeit components, spyware, lack of built-in security features
  - Software Risks
    - Vulnerabilities, malware, licensing issues
  - Service Risks
    - Exposure of sensitive data and intellectual property, security lapses by service providers
- Risk Analysis in SCRM
  - Analysis of each link in the supply chain to identify and mitigate risks
  - Consider the source and reputation of each vendor and supplier

- Due Care and Due Diligence in SCRM
  - Due Care
    - Initial assessment of supply chain risks
  - Due Diligence
    - Continuous monitoring and updating of the supply chain risk assessments
- Compliance and Unintentional Risks
  - Compliance with regulations that mandate SCRM
  - Addressing unintentional risks due to oversight or poor security practices
- Security Requirements and Acquisition Strategy
  - Establish minimum security requirements for all supplied goods and services
  - Develop an acquisition strategy to minimize risks introduced through new purchases
- Supply Chain Assessments
  - On-site supplier visits
  - Documentation reviews and compliance checks
  - Independent audits by third parties
- Service Level Agreements (SLAs)
  - Creation of SLAs with suppliers that define specific security requirements and acquisition policies



## Risk Frameworks

Objective 1.9: Understand and apply risk management concepts

- **Risk Frameworks Introduction**

- Introduction to Risk Frameworks
  - Overview of the importance of structured risk management frameworks
  - Essential for establishing consistent approaches to identifying, assessing, and responding to security threats
  - Crucial for CISSP exam success and practical security management
- NIST Cybersecurity Framework (CSF)
  - Describes the five core functions
    - Identify, Protect, Detect, Respond, and Recover
  - Adaptable across different industries and organizational sizes
  - Guides organizations in managing cybersecurity risks through a flexible framework
- ISO/IEC 27001
  - Focuses on the establishment and maintenance of an Information Security Management System (ISMS)
  - Encourages continuous improvement in security processes
  - Globally recognized for setting information security standards
- Payment Card Industry Data Security Standard (PCI DSS)
  - Essential for organizations handling credit card information

- Covers key security practices like maintaining secure networks and protecting cardholder data
- Highlights the importance of regular security monitoring and testing
- Sherwood Applied Business Security Architecture (SABSA)
  - Business-driven framework for developing risk management architectures
  - Aligns security strategies with business goals to support business needs
  - Offers a unique approach to developing security solutions tailored to specific risk environments
- **Risk Frameworks**
  - Risk Frameworks
    - Part of overall risk management involving assessment, control, monitoring, and auditing of organizational risks
  - NIST Special Publications 837 - RMF (Risk Management Framework)
    - Focus
      - Information systems and organizations
    - Provides a flexible 7-step process for managing security and privacy risks
    - Steps
      - Preparation, Categorization, Selection, Implementation, Assessment, Authorization, Monitoring
  - Importance of Preparations in RMF
    - Initial step involving identification of roles, business strategies, and control providers

- Involves inheriting controls such as physical security from external data centers
- Role of Categorization and Selection in RMF
  - Categorization based on data types and risk, influencing the selection of appropriate security controls
- Implementation and Assessment in RMF
  - Deployment of security controls followed by testing to ensure they meet compliance and organizational requirements
- Authorization and Continuous Monitoring in RMF
  - Authorization involves senior management reviewing remaining risks for acceptability
  - Continuous monitoring to evaluate and ensure effectiveness of security controls over time
- ISO 31000 Risk Management Framework
  - General framework applicable to various risks across industries
  - Emphasizes a structured, comprehensive, and dynamic approach to risk management
- COSO (Committee of Sponsoring Organizations)
  - Enterprise risk management framework used primarily for corporate governance and compliance with Sarbanes-Oxley
  - Components
    - Governance and Culture, Strategy and Objective Setting, Performance, Review and Revision, Information, Communication, and Reporting
- Due Care and Due Diligence in Risk Frameworks

- Due Care
    - Early stages of risk management including planning and selecting controls
  - Due Diligence
    - Continuous assessment, monitoring, and adaptation to changes in risk environment
- **NIST Cybersecurity Framework**
  - Definition and Purpose of NIST CSF
    - A voluntary framework for managing and reducing cybersecurity risk
    - Integrates existing standards, guidelines, and best practices from NIST and industry
  - Components of the CSF
    - Core
      - Consists of security activities and desired outcomes grouped into five functions—Identify, Protect, Detect, Respond, Recover
    - Tiers
      - Describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the CSF (Partial, Risk-Informed, Repeatable, Adaptive)
    - Profiles
      - Help organizations align their cybersecurity activities with business requirements, risk tolerances, and resources
  - Core Functions

- Identify
  - Develop an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities
- Protect
  - Implement appropriate safeguards to ensure delivery of critical infrastructure services
- Detect
  - Implement appropriate activities to identify the occurrence of a cybersecurity event
- Respond
  - Take action regarding a detected cybersecurity event
- Recover
  - Maintain plans for resilience and to restore any capabilities or services impaired due to a cybersecurity event
- Implementation of the CSF
  - Organizations apply the Core in a manner consistent with their risk management strategy and business needs
  - Profiles allow organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements, and reflects risk appetite
- Significance of Tiers
  - Provide context on how an organization views cybersecurity risk and the processes in place to manage that risk
  - Are not maturity indicators but help in assessing the rigor and sophistication of cybersecurity practices

- Usage of Profiles
  - Enable organizations to prioritize opportunities for improving cybersecurity posture by comparing a "Current" profile (the "as is" state) with a "Target" profile (the "to be" state)
  - Facilitate communication among internal and external stakeholders about cybersecurity risk and management
- **ISO/IEC 27001**
  - Overview of ISO IEC 27001
    - Internationally recognized standard for information security management systems (ISMS)
    - Provides guidance for establishing, implementing, maintaining, and improving an ISMS
    - Applicable to all types of organizations regardless of size or sector
  - Purpose of ISO IEC 27001
    - Helps organizations protect their information assets
    - Manages information security risks effectively
    - Ensures organizational compliance with laws and regulations related to information security
  - Key Principles of ISO IEC 27001
    - Based on the CIA triad
      - Confidentiality, Integrity, and Availability
    - Aims to safeguard sensitive information and ensure regulatory compliance

- Structure of the ISO IEC 27001 Standard
  - Clauses 0-3
    - Cover standard documentation and introductory material
      - E.g., scope, terms
  - Clause 4
    - Context of the Organization
      - Requires understanding the internal and external issues that influence information security management
  - Clause 5
    - Leadership
      - Focuses on management's commitment to information security, defining roles, and policy formulation
  - Clause 6
    - Planning
      - Involves setting information security objectives and planning to achieve them through risk assessments and risk treatment
  - Clause 7
    - Support
      - Allocates necessary resources, ensures adequate communication, and fosters staff competence and awareness
  - Clause 8
    - Operation

# ISC2 CISSP

## (Study Guide)

- Addresses the execution and management of the ISMS processes
  - Clause 9
    - Performance Evaluation
      - Involves monitoring, measurement, analysis, and evaluation of the information security performance
  - Clause 10
    - Improvement
      - Ensures continual improvement of the ISMS
- Implementation Guidance
  - Organizations should tailor the implementation of the standard to their specific needs, considering the context of their operations and the risks they face
  - The standard emphasizes the importance of leadership involvement and a clear commitment to information security
- **Understanding PCI DSS**
  - Introduction to PCI DSS
    - PCI DSS stands for Payment Card Industry Data Security Standard
    - It is a security standard designed to protect cardholder data from unauthorized access or disclosure
  - Nature of PCI DSS



- Not a legal requirement but treated with the rigor of law or regulation in the payment industry
- Mandatory for all entities processing payment card transactions to comply with PCI DSS
- Purpose of PCI DSS
  - To ensure that all organizations that process, store, or transmit credit card information maintain a secure environment
- PCI DSS Requirements
  - Aim to protect cardholder data
  - Ensure the maintenance of a secure network
  - Implement strong access control measures
  - Regularly monitor and test networks
  - Maintain an information security policy
- Key Components of PCI DSS
  - Cardholder Data (CHD)
    - Includes the account number, cardholder name, expiration date, and service code
  - Sensitive Authentication Data (SAD)
    - Includes full track data, card verification codes, and PINs
  - Cardholder Data Environment (CDE)
    - All system components involved in cardholder data processing, storage, or transmission
- PCI DSS Compliance Levels
  - Defined based on the volume of transactions over a 12-month period
  - Range from Level 1 (highest volume) to Level 4 (lowest volume)

- Compliance Requirements
  - Install and maintain a firewall configuration to protect data
  - Do not use vendor-supplied defaults for system passwords and other security parameters
  - Protect stored data
  - Encrypt transmission of cardholder data across open, public networks
  - Use and regularly update anti-virus software
  - Develop and maintain secure systems and applications
  - Restrict access to cardholder data by business need-to-know
  - Assign a unique ID to each person with computer access
  - Restrict physical access to cardholder data
  - Track and monitor all access to network resources and cardholder data
  - Regularly test security systems and processes
  - Maintain a policy that addresses information security
- **Understanding SABSA**
  - Overview of SABSA
    - SABSA stands for Sherwood Applied Business Security Architecture
    - It is a framework for developing business-driven, risk-focused security architectures at both enterprise and solutions levels
  - Purpose and Focus of SABSA
    - Aligns security architecture with business objectives, ensuring that security supports the business rather than constraining it

- Provides a structured approach to security architecture that is adaptable to various organizational needs
- Core Components of SABSA
  - Business Attributes Profiling
    - Understanding and aligning with business attributes to tailor security according to business needs
  - Risk Management
    - Integrates risk management practices into security architecture to identify, assess, and manage risks effectively
- SABSA Matrix
  - A tool for developing and visualizing security architecture.
  - Helps trace security decisions and practices back to business requirements
  - Organized into six layers (Contextual, Conceptual, Logical, Physical, Component, Operational), each addressing different aspects of security from high-level business goals to specific technical controls
- Integration with Other Frameworks
  - SABSA does not replace other frameworks but complements them by providing a security architecture overlay
  - Can be integrated with frameworks like TOGAF, ITIL, and ISO 27001 to enhance their security dimensions
- Usage in the Industry
  - Applied in various sectors for designing and implementing security that supports and enables business operations



# ISC2 CISSP

## (Study Guide)

- Useful in both enterprise-wide and more focused solution-specific contexts
- Exam Preparation Tips
  - Understand the purpose and unique attributes of SABSA
  - Familiarize yourself with the SABSA matrix and its application in security architecture
  - Learn how SABSA integrates with and complements other management and security frameworks

## Risk Assessment

Objectives:

- 1.9 - Understand and apply risk management concepts
- 1.10 - Understand and apply threat modeling concepts and methodologies
  
- **Risk Assessments**
  - Risk Assessments
    - Essential in risk management and threat modeling
    - Fundamental to cybersecurity roles
    - Involves identifying, evaluating, and addressing risks to reduce exposure and mitigate impact
  - Understanding Risk Assessments
    - Introduction to the foundational concepts of risk assessments
    - Involves identifying vulnerabilities, understanding threat impacts, and evaluating threat likelihood
  - Conducting Risk Assessments
    - Steps to perform a risk assessment
    - Discussion on tools and techniques for data gathering, risk evaluation, and mitigation strategy development
  - Control Assessments
    - Evaluation of security controls to mitigate identified risks
    - Continuous evaluation of control effectiveness against evolving threats

- Privacy Control Assessments
  - Focus on how well privacy-specific controls protect personal and sensitive data
  - Context of laws and regulations, including the General Data Protection Regulation (GDPR)
- PCI DSS Assessments
  - Assessment of compliance with the Payment Card Industry Data Security Standard
  - Focus on securing payment card information and aligning with risk management practices
- Threat Modeling Concepts
  - Threat modeling as a technique in risk assessment
  - Key concepts include identifying assets, analyzing threats, and understanding the attacker's perspective
- Threat Modeling Methodologies
  - Exploration of methodologies like STRIDE, PASTA, and DREAD
- **Understanding Risk Assessments**
  - Key Information and Defined Terms
    - Risk Analysis/Assessment
      - The process of researching and analyzing organizational assets to identify and evaluate potential risks
  - Concepts Explained
    - Purpose of Risk Assessment
      - Aids in making informed decisions regarding potential risks

# ISC2 CISSP

## (Study Guide)

- Identifies risk factors and their relationships to the organization
  - Analyzes and evaluates the validity and relevance of potential risks
- Risk Tolerance/Risk Appetite
  - Refers to the level of risk an organization is willing to accept
- Organizational Impacts
  - Evaluates the broader implications of identified risks within the organization
- NIST Special Publication 800-30 Risk Assessment Steps
  - Preparation
    - Define the purpose, scope, and approach of the risk assessment
    - Tailored to fit organizational uniqueness in purpose, scope, and methodology
  - Conducting the Assessment
    - Create a comprehensive list of security risks
    - Act upon identified risks based on their analysis
  - Reporting
    - Communicate findings to senior management in an understandable business language
    - Aimed at aiding decision-making processes
  - Maintaining/Monitoring
    - Ensures effective implementation and ongoing efficacy of risk responses
- Additional Details
  - Threat Identification
    - Focus on identifying potential threat sources and their intent

- Assess the likelihood of threats materializing
  - Vulnerability Analysis
    - Determine existing vulnerabilities and assess their severity
    - Evaluate the potential impact of vulnerabilities on the organization
- **Conducting Risk Assessments**
  - Key Information and Terms
    - Risk Management Concepts
      - Essential for performing a risk assessment or risk analysis
      - Involves applying research and analysis to organizational assets to discover potential risks
    - Quantitative Risk Assessment
      - Utilizes numerical values to determine asset values and projected losses
      - Focused on quantifiable metrics like monetary values to assess potential losses
    - Qualitative Risk Assessment
      - Employs subjective judgment to determine asset values and projected losses
      - Involves ranking risks using categories such as high, low, moderate, often utilizing color codes
    - Asset Value (AV)



# ISC2 CISSP

## (Study Guide)

- Total cost of an asset including purchase, maintenance, and operational costs
  - Critical in calculating potential losses in risk scenarios
- Exposure Factor (EF)
  - Represents the percentage of the asset value that could be lost in the event of a risk realization
  - Example
    - A 50% exposure factor implies half of the asset's value is at risk
- Single Loss Expectancy (SLE)
  - Expected monetary loss for a single occurrence of a risk event
  - Calculated by multiplying the asset value (AV) by the exposure factor (EF)
- Annualized Rate of Occurrence (ARO)
  - Estimated frequency at which a specific risk is expected to occur within a year
- Annualized Loss Expectancy (ALE)
  - Projected annual financial loss due to a specific risk
  - Calculated by multiplying the single loss expectancy (SLE) by the annualized rate of occurrence (ARO)
- Annual Cost of Safeguard
  - Expense incurred from implementing a countermeasure to protect an asset
  - Important for cost-benefit analysis in risk management
- Delphi Technique

- Method used in qualitative risk assessment to gather consensus among experts through anonymous feedback
  - Helps in making informed decisions without bias
- Hybrid Risk Assessment
  - Combines quantitative and qualitative approaches for a comprehensive risk analysis
  - Suitable for complex scenarios where both numerical data and expert judgment are required
- Control Assessments
  - Key Information and Terms
    - Control Assessments
      - Formal evaluations aimed at determining the effectiveness of security and privacy controls
      - Essential for verifying compliance and functionality before deployment and during operation
    - Security Control Assessment
      - Evaluates the security measures implemented to protect systems and ensure they meet objectives throughout the system development lifecycle
      - Involves continuous monitoring and regular assessments in operational environments
    - Privacy Impact Assessment
      - Focuses on evaluating privacy controls related to data protection laws

# ISC2 CISSP

## (Study Guide)

- Concerns itself with how personal data of subjects is handled and protected according to legal requirements
- Continuous Monitoring
  - Regular assessment of systems to ensure security controls remain effective post-deployment
  - Integral to maintaining long-term security and compliance
- Planning Assessments
  - Involves defining the purpose, scope, and criteria of the assessment
  - Determines necessary resources, personnel, and dependencies for successful execution
- Cost-Effectiveness of Controls
  - Controls should not cost more than the value of the asset they protect
  - Ensures that expenditure on security measures is justified by the asset's value
- Assessment Procedures
  - Encompasses examination, interviews, and testing to evaluate control effectiveness
  - Includes defining success and failure criteria for tests to gauge control efficacy accurately
- Documentation and Reporting
  - Documentation during assessments is crucial for capturing findings and ensuring repeatability

- Reporting communicates results to stakeholders and guides further actions based on the assessment outcomes
  
- **Privacy Control Assessments**
  - Key Information and Terms
    - Privacy Control Assessment
      - Evaluates organizational privacy controls to ensure compliance with regulations governing the protection of Personally Identifiable Information (PII)
      - Ensures practices and procedures adequately protect privacy as required by law
    - Important Regulations
      - GDPR (General Data Protection Regulation)
        - Focuses on privacy and data protection for individuals within the European Union
      - HIPAA (Health Insurance Portability and Accountability Act)
        - U.S. regulation that includes provisions for protecting Protected Health Information (PHI), which is a subset of PII
      - Privacy Act of 1988
        - Emphasizes the protection of personal information, demonstrating global concerns over privacy.
    - Privacy Threshold Analysis (PTA)
      - Initial step to determine if PII is involved in any new or existing system or process.

# ISC2 CISSP

## (Study Guide)

- Helps identify if a Privacy Impact Assessment (PIA) is needed based on potential risks to PII.
- Privacy Impact Assessment (PIA)
  - Conducted after a PTA if risks to PII are identified.
  - Analyzes how PII is collected, used, shared, and stored, assessing the risks and impacts to privacy
- NIST SP 800-53A
  - Provides guidelines for assessing the security and privacy controls in federal information systems and organizations.
  - A key resource for conducting structured privacy control assessments
- Steps in Privacy Control Assessment
  - Prepare
    - Define the objective, scope, and resources needed for the assessment
  - Develop
    - Document the controls and procedures to be assessed.
  - Conduct
    - Execute the assessment, identify risks and vulnerabilities
  - Analyze
    - Review findings, address deficiencies, and plan remediation
- **PCI DSS Assessments**
  - Key Information and Terms
    - PCI DSS Overview

# ISC2 CISSP

## (Study Guide)

- Payment Card Industry Data Security Standard (PCI DSS) focuses on protecting cardholder data (CHD) and sensitive authentication data (SAD) from unauthorized access and breaches
- Essential for organizations that handle branded credit cards from the major card schemes
- Importance of PCI DSS
  - Increasing relevance due to the growth in online payment processing
  - Ensures the security of card transactions and protects against data theft
- Assessment Steps as per PCI DSS
  - Assess
    - Identify and analyze all locations where cardholder data is stored, processed, or transmitted
  - Remediate
    - Address vulnerabilities to ensure cardholder data is adequately protected
  - Report
    - Document assessment findings and remediation actions, submit compliance reports
  - Monitor and Maintain
    - Continuously monitor security controls and maintain compliance over time
- Assessment Methods
  - Examine

# ISC2 CISSP

## (Study Guide)

- Review documents, configurations, and logs to validate compliance
- Observe
  - Conduct tests to see how systems respond under attack scenarios
- Interview
  - Discuss security practices and controls with system administrators and other stakeholders
- Reporting Requirements
  - Report on Compliance (ROC)
    - Required for large merchants (Level 1), involves detailed reporting of compliance status by a Qualified Security Assessor (QSA)
  - Self-Assessment Questionnaire (SAQ)
    - Used by smaller merchants (Levels 2-4) to self-report compliance
- Merchant Levels for PCI DSS Compliance
  - Level 1
    - More than 6 million transactions per year Requires ROC
  - Level 2
    - 1 to 6 million transactions per year Requires SAQ
  - Level 3
    - 20,000 to 1 million transactions per year Requires SAQ
  - Level 4
    - Less than 20,000 transactions per year Requires SAQ

- **Threat Modeling Concepts**

- Key Information and Terms

- Threat Modeling Overview

- Threat modeling is a type of risk assessment used to identify and analyze potential threats from both the attack and defense perspectives
    - It examines internal and external network perspectives, focusing on both incoming threats and system vulnerabilities

- Key Definitions

- Threat
      - The potential for unwanted harm to personnel or organizational assets
    - Vulnerability
      - A flaw or weakness that can be exploited by a threat to cause harm
    - Attack Surface
      - All possible points where an attacker can try to enter or extract data from an environment

- Threat Intelligence

- Involves gathering, analyzing, and using information about potential threats to make informed security decisions
    - Includes understanding known tactics, techniques, and procedures (TTPs)

- Approaches to Threat Modeling

- Proactive



# ISC2 CISSP

## (Study Guide)

- Involves predicting potential threats and designing security measures to minimize the attack surface before deployment
- Reactive
  - Focuses on responding to threats after they have been identified in an operational system
- Threat Modeling Questions
  - What are we working on
  - What can go wrong
  - What are we going to do about it
  - Did we do a good enough job
- Useful Tools and Frameworks
  - Red Canary
    - Used for threat hunting
  - MITRE ATT&CK Framework
    - Provides a comprehensive matrix of tactics and techniques used by threat actors
  - Cisco Talos
    - Offers threat intelligence and security insights
- **Threat Modeling Methodologies**
  - Key Information and Terms
    - Threat Modeling Methodologies Overview
      - Essential for identifying and analyzing potential threats from both attack and defense perspectives in various environments
    - STRIDE

# ISC2 CISSP

## (Study Guide)

- Developed by Microsoft, focuses on
  - Spoofing
    - Impersonating another user to gain unauthorized access
  - Tampering
    - Manipulating data to compromise integrity
  - Repudiation
    - Performing actions without leaving evidence
  - Information Disclosure
    - Exposing information to unauthorized parties
  - Denial of Service (DoS)
    - Disrupting service availability
  - Elevation of Privilege
    - Gaining higher access levels than authorized
- NIST SP800-154
  - Provides a framework for data-centric threat modeling
  - Steps include identifying data and characterizing threats, selecting and analyzing attack vectors, and evaluating security controls
- PASTA (Process for Attack Simulation and Threat Analysis)
  - A seven-stage process that integrates business objectives and technical requirements
  - Involves defining objectives, technical scope, threat analysis, vulnerability analysis, and risk analysis
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)
  - Focuses on organizational risk and security practices

# ISC2 CISSP

## (Study Guide)

- Steps include establishing drivers, creating profiles, identifying threats, and mitigating risks
- TRIKE
  - A risk management-driven methodology that utilizes a rigorous framework for defining security requirements and assessing risks
- VAST (Visual, Agile, and Simple Threat)
  - Designed for integration with agile development processes
  - Emphasizes a scalable approach for enterprise-level threat modeling

## Asset Security

### Objectives:

- 2.1 - Identify and classify information and assets
- 2.2 - Establish information and asset handling requirements
- 2.3 - Provision information and assets securely
- 2.4 - Manage data lifecycle
- 2.5 - Ensure appropriate asset retention
  - E.g., End of Life (EOL), End of Support
- 3.10 - Manage the information system lifecycle
  
- **Asset Security**
  - Asset Security
    - Asset Security is a critical concept within information security
    - CISSP exam dedicates an entire domain to managing and protecting assets, with a focus on data protection
    - Proper classification, handling, and lifecycle management of assets are key to maintaining an organization's security posture
  - Classifying Data and Assets (CISSP Exam Objective 2.1)
    - Identifying and classifying information and assets based on criticality, sensitivity, and value to the organization
    - Different data classification levels determine how data should be handled and secured

# ISC2 CISSP

## (Study Guide)

- E.g., public, internal, sensitive, top secret
- Aligning classification with business needs minimizes risks and strengthens security
- Information and Asset Handling Requirements (CISSP Exam Objective 2.2)
  - Establish procedures for proper storage, access control, transmission, and destruction of data
  - Understand how regulations like GDPR and HIPAA influence data handling practices
  - Ensure that assets are marked, labeled, and handled according to organizational and legal requirements
- Managing System Assets (CISSP Exam Objective 2.3)
  - Provision information and assets securely throughout their lifecycle
  - Importance of managing both digital and physical assets securely
  - Ensures that every hardware, software, and data asset is accounted for and protected
- Data Roles and Responsibilities (CISSP Exam Objective 2.4)
  - Data roles include
    - Data Owner
      - Determines classification levels and access rights
    - Data Custodian
      - Manages day-to-day data tasks (backups, maintenance)
    - Data Steward
      - Oversees data governance and ensures compliance
    - Allocating proper roles ensures data security and proper management throughout its lifecycle

- Managing the Data Lifecycle (CISSP Exam Objective 2.4)
  - Understanding the phases of the data lifecycle (creation, storage, usage, archive, destruction)
  - Applying security measures at each stage of the lifecycle to prevent unauthorized access and ensure secure data handling
- Information System Lifecycle (CISSP Exam Objective 3.10)
  - Part 1
    - Covers the early stages of the system lifecycle (initiation, development, acquisition)
    - Security should be planned from the beginning, integrated into system design and implementation
  - Part 2
    - Focuses on the later stages (operations, maintenance, decommissioning)
    - Importance of maintaining security controls, regular updates, patches, and secure disposal of systems when no longer needed
- **Classifying Data And Assets**
  - Key Concepts and Definitions
    - Data Classification
      - The process of analyzing the sensitivity of data and determining the level of protection required
    - Asset Identification
      - Understanding and documenting all assets within an organization, crucial for effective security and compliance

- Important Reference
  - NIST Special Publications 800-60
    - Essential for understanding data types and classification standards
- Data Classification
  - Identification of Data Types
    - Includes private, sensitive, regulated, and public data
    - Focus on both physical and digital formats
  - Importance of Inventory
    - Comprehensive listing of all data and assets within an organization
    - Helps in assessing criticality and impact on business operations
  - Governance, Regulation, and Compliance
    - Policies governing data creation, collection, management, and disposal
    - Ensures data quality, authenticity, and reliability
  - Sensitivity Assessment
    - Evaluating the data's need for protection based on its confidentiality, integrity, and availability
- Asset Classification
  - Understanding Asset Impacts
    - Determining how critical each asset is to the organization
    - Includes hardware, software, and other resources
  - Flow of Data
    - Tracking how data moves within and outside the organization

- Ensures appropriate security measures are in place during data transmission
- Security Controls
  - Application of security measures based on the sensitivity and flow of data
  - Protects data at all states
    - In use, in transit, and at rest
- Security Controls for External Data
  - Handling of Data Leaving the Organization
    - Assessing the value and sensitivity of data shared externally
    - Applying appropriate security controls before data is transmitted
- Data Policy Development
  - Creation and Management
    - Defines how data is handled within the organization
    - Aligns with legal and regulatory requirements to ensure compliance
- Types of Sensitive Data
  - Personally Identifiable Information (PII)
    - Data that can uniquely identify an individual
    - Subject to strict regulatory standards
  - Protected Health Information (PHI)
    - Health-related information that requires protection under laws like HIPAA
  - Proprietary Data



- Gives a business competitive advantage and requires high-level security
- Other Sensitive Data Types
  - National security information, sensitive business and user information, regulated information
- Data Categorization and Classification
  - Methodologies
    - Assigning sensitivity labels to data types based on potential impact
    - Utilizing frameworks like NIST SP 800-60 for guidance
  - Classification Levels
    - Top Secret
      - Extremely high impact on disclosure; significant damage potential
    - Secret
      - High impact; causes serious damage if disclosed
    - Confidential
      - Moderate impact; causes noticeable damage
    - Unclassified
      - Low or no impact; minimal value information
  - Asset Classification Tiers
    - Tier 0 (Essential)
      - Critical servers, databases, and network devices
    - Tier 1 (Important)
      - Development environments, backup systems
    - Tier 2 (Non-Essential)

- Workstations, mobile devices, printers
  - Significant Systems
    - Required to meet specific regulatory standards
  - Benefits of Proper Classification
    - Improved Security Awareness
      - Enhances understanding of potential risks and necessary protections
    - Compliance Assurance
      - Ensures data and assets are handled according to applicable laws and standards
    - Enhanced Planning
      - Aids in business continuity and disaster recovery planning
- **Information and Asset Handling Requirements**
  - Key Concepts and Definitions
    - Asset Handling
      - Involves the policies, processes, and procedures required to protect both physical and digital assets throughout their lifecycle
    - Data Owner Responsibilities
      - Classification and labeling of data
      - Managing how data is handled based on policies and procedures
  - Handling Mechanisms
    - Marking

# ISC2 CISSP

## (Study Guide)

- Physical identification of an asset with its appropriate sensitivity or classification level
- Example
  - Using cover sheets with security classifications (Secret, Confidential) clearly indicated
- Labeling
  - Digital or logical identification of an asset with its appropriate sensitivity or classification level
  - Implemented through metadata or digital watermarks indicating the confidentiality level
- Organizational Policies
  - Essential to define a consistent process for marking and labeling across the organization
  - Helps in routine handling and security awareness
- Handling Sensitive Data and Assets
  - Data States
    - Data in Use
      - Handling by authorized subjects
    - Data in Transit
      - Secure transmission requirements, possibly via VPN or encrypted channels
    - Data at Rest
      - Storage protocols, possibly involving encryption or secure archiving
  - Sensitive Asset Management

- Aligns with organizational governance for consistent handling procedures
  - Training on proper handling techniques according to established procedures
- Storage and Security Controls
  - Application of appropriate security measures based on data classification to prevent unauthorized access and mishandling
  - Management of copies and backups, ensuring they are also handled and stored according to the data's sensitivity
- Practical Examples
  - Marking Example
    - Physical tags or stickers on hardware indicating its security level
  - Labeling Example
    - Watermarks on digital documents or metadata tagging in digital files
- Importance of Consistent Processes
  - Ensures that all personnel handle data and assets correctly, minimizing risks of data breaches or asset misuse
  - Supports compliance with legal and regulatory requirements by documenting and enforcing handling procedures
- **Managing System Assets**
  - Overview
    - Topic
      - Secure provisioning and asset management
    - Focus

- Understanding how to provision resources securely, including asset ownership, inventory, and management
- Key Concepts
  - Provisioning
    - Involves creating, managing, and destroying assets throughout their lifecycle
  - Asset Lifecycle (NIST SP 1800-5)
    - Steps include strategy, planning, design, procurement, operation, maintenance, modification, and disposal
- Responsibilities
  - Senior Management
    - Accountable for overall asset management including IT assets, hardware, procurement, and asset disposal
  - Data Owners
    - Responsible for data-related assets, ensuring proper handling and security measures are in place
- Asset Management Components
  - Asset Inventory
    - Crucial for implementing change control and configuration management
    - Ensures all assets are accurately accounted for throughout their lifecycle
- What to Track
  - Hardware
    - Servers, switches, firewalls, gateways, proxies, IDS/IPS systems

- Software
  - Operating systems, firmware, applications
- Specific Details
  - Manufacturer, model, serial number, version, supply chain info, risk assessments, warranty details
- Operational Details
  - Purchase and installation dates, licensing, dependencies, updates, location, IP addresses, barcode info, network settings, compute metrics (CPU, memory), and baseline configurations
- Tools and Techniques for Asset Tracking
  - Manual Tracking
    - Spreadsheets, databases
  - Automated Discovery
    - Tools like Nessus, Nmap, OpenVAS for host discovery and operating system identification
- Organizational Policy and Management
  - Depth of Tracking
    - Determined by organizational policies which dictate the extent of asset tracking
  - Management Software
    - Utilize specialized software for tracking and managing inventory
  - Security and Integrity
    - Ensure inventory list security and integrity to restrict access and modifications to authorized personnel only
  - Updates and Change Control

- Manage updates through configuration management and change control protocols
  
- **Data Roles And Responsibilities**
  - Overview
    - Topic
      - Data roles, their responsibilities, and their importance in the data lifecycle
    - Focus
      - Understand key data roles including owners, controllers, custodians, processors, users, and subjects
  - Key Concepts
    - Data Roles Overview
      - Every role in data management defines accountability and responsibility
      - It's critical that someone is responsible for each data type and the protection of that data
  - Data Roles
    - Data Owner
      - Ultimately responsible for the data
      - Manages access, use, and protection of the data

# ISC2 CISSP

## (Study Guide)

- Typically specialized to handle certain types of data (e.g., financial, medical)
- Delegates responsibilities to data custodians
- Data Custodian
  - Implements physical, administrative, and logical controls on behalf of the data owner
  - Manages the technical protection of data
  - Works with the data owner to implement protection levels
- Data Steward
  - Subject matter expert for specific data types
  - Assists in classifying and categorizing the data
  - Works closely with both the data owner and custodian to ensure proper data management
- Data Subjects
  - Individuals who consume or interact with the data
  - Often referred to as "users" who operate information system resources
  - Subjects can also include non-human entities such as applications, scripts, or automated processes that access and use data
- Data Controllers and Processors (GDPR Focused)
  - Data Controller
    - Determines the purpose and means of processing personal data
    - The ultimate responsibility lies with the data controller under GDPR regulations
  - Data Processor



# ISC2 CISSP

## (Study Guide)

- Acts on behalf of the data controller to collect, process, and store data
- Liable for any breaches or issues that occur during data processing
- Practical Example of Roles in a Network
  - Data Ownership
    - Data owners are responsible for the security, use, and access of data stored on systems (e.g., storage servers)
    - They ensure encryption is applied to protect confidentiality and integrity
  - Data Custodianship
    - Custodians handle tasks such as applying encryption, monitoring access, and enforcing protection measures
  - Data Stewardship
    - Stewards provide expertise on specialized data types and assist with protection strategies
  - Data Subjects
    - The users or automated processes that interact with the system and data
      - E.g., accessing streaming services
  - Controllers and Processors
    - Data controllers decide what information to collect
    - Data processors handle the collection, processing, and management of the data on the controller's behalf

- **Managing The Data Lifecycle**

- Overview

- Topic

- Understanding the data life cycle and how to manage data at each stage

- Focus

- Key stages include data creation, classification, storage, use, archiving, and destruction

- Key Concepts

- Data Life Cycle Overview

- The data life cycle is a conceptual model; not a strict set of steps
      - It emphasizes protecting data throughout its entire life span, from creation to destruction
      - The responsibility to protect data remains constant until the data is destroyed

- Cradle to Grave Responsibility

- Data must be protected continuously from the moment it's created until it's destroyed
      - When data is no longer needed or relevant (e.g., for regulatory purposes), it must be securely destroyed

- Data Life Cycle Phases

- Data Creation

- Data is either created or collected
      - Must be in compliance with organizational policies and privacy laws

- Example
  - Automatically assigning default file permissions using UMASK on a Linux system
- Data Classification
  - After creation, data must be classified or categorized according to its sensitivity
  - Different data types (e.g., public web data vs. personal identifiable information) require different levels of protection
  - Ensures compliance with privacy laws and organizational standards
- Data Storage
  - Data is stored in hard drives, cloud environments, or other storage mediums while awaiting use or archiving
  - Storage can occur on-premises or off-premises
    - E.g., cloud
  - Security controls must be maintained regardless of where the data is stored
    - E.g., on-site vs. third-party cloud providers
- Data Use
  - Data is used or processed during this phase
  - Systems must track data usage, log activities, and ensure compliance with business objectives
  - Data sharing and transit must be secure
    - E.g., encryption in transit
- Data Archiving

# ISC2 CISSP

## (Study Guide)

- Data that is no longer needed regularly is moved into archive storage
- Access controls and encryption must be applied to protect archived data
- Archive storage can be driven by regulatory requirements or for organizational purposes
  - E.g., compliance, legal
- Data Destruction
  - Data that is no longer needed is securely deleted or destroyed
  - Destruction must follow organizational policies and legal/regulatory requirements
    - E.g., for sensitive data like PII, PHI
  - Secure destruction methods ensure that no sensitive data can be recovered by unauthorized parties
- Key Considerations
  - Data Value Over Time
    - The value of data may change over time, affecting its classification and protection needs
    - Example
      - World War II battle plans are now declassified, while the Coca-Cola recipe remains highly protected
    - The value of data can fluctuate based on organizational priorities or regulatory requirements
  - Emerging Threats and Compliance

# ISC2 CISSP

## (Study Guide)

- Emerging threats (e.g., new vulnerabilities or network changes) can alter the risks to data and require new protections
  - Changes in laws and regulations (e.g., GDPR replacing PrivacyShield) can also affect how data is managed
- 
- **The Information System Lifecycle - Part 1**
    - Overview
      - Topic
        - Information System Lifecycle Management
      - Focus
        - Overview and key phases of the information system lifecycle, aligned with CISSP exam objectives
    - Key Concepts
      - Lifecycle Phases
        - The lifecycle includes various phases from the initiation of a system to its disposal, emphasizing the integration of security from the start to the end
      - Security Integration
        - Core to lifecycle management is the integration of security considerations throughout all phases, ensuring secure operations and compliance
    - Phases of Information System Lifecycle
      - Initiation

# ISC2 CISSP

## (Study Guide)

- Involves identifying and engaging stakeholders who influence the system
- Stakeholders can include users, managers, customers, auditors, and senior leadership
- The phase focuses on understanding stakeholder requirements and the overall purpose of the information system
- Development and Acquisition
  - Addresses how systems are either developed in-house or acquired through third-party solutions
  - Important to decide whether to build or buy based on the capabilities and security needs
  - Involves setting up secure development practices if building internally or vetting third-party solutions for security if acquiring
- Implementation and Assessment
  - Involves the actual setup or installation of the system and ensuring it meets specified requirements
  - Assessment is critical to validate that the system is functioning as intended and meets all security standards
- Operations and Maintenance
  - The ongoing phase where the system is in use and needs continuous monitoring, regular updates, and maintenance
  - Security is crucial during this phase to handle emerging threats and to ensure compliance with evolving regulations
- Disposal

- The final phase involves the secure decommissioning and disposal of the system
  - Ensures that all data is securely erased and hardware is disposed of in a manner that prevents data recovery
- NIST Special Publication 800-64 Revision 2
  - Although retired, still referenced for foundational concepts in lifecycle management
  - Provides a structured approach to embedding security into the lifecycle of an information system
- Exam Preparation Focus
  - Understand Stakeholder Needs
    - How stakeholder needs drive the requirements and security measures throughout the lifecycle
  - Lifecycle Security Integration
    - How security is integrated at each phase, from planning through disposal, to protect the system and data
  - Regulatory Compliance
    - Importance of ensuring the system complies with relevant laws and industry standards throughout its lifecycle
- **The Information System Lifecycle - Part 2**
  - Overview
    - Topic
      - Information System Lifecycle Management (Part 2)

# ISC2 CISSP

## (Study Guide)

- Focus
  - Detailed exploration of the final stages of the information system lifecycle, emphasizing security integration
- Key Concepts
  - Lifecycle Continuation
    - Understanding the transition from development to operation and eventual disposal, with a focus on maintaining security at every step
  - Security Throughout Lifecycle
    - Emphasizes the need to integrate security measures from the initial phases through disposal to protect data and comply with regulations
- Phases of Information System Lifecycle (Continued)
  - Verification and Validation
    - Ensure all components meet specified requirements
    - Conduct rigorous testing and assessments to confirm system security and functionality
  - Transition and Deployment
    - Implement the new or updated system into an operational environment
    - Manage the transition carefully to ensure security settings are transferred and operational
  - Operations and Maintenance/Sustainment
    - Regularly update and maintain the system to address new security threats and ensure compliance



# ISC2 CISSP

## (Study Guide)

- Perform continuous monitoring to detect and respond to security incidents
- Retirement/Disposal
  - Securely decommission the system, ensuring all sensitive data is appropriately sanitized or destroyed
  - Follow legal and regulatory requirements for data retention and destruction
- Detailed Phase Descriptions
  - Verification and Validation
    - Involves checking that the system meets all technical, security, and user requirements before full-scale implementation
    - Uses methods like testing, code reviews, and security assessments
  - Transition and Deployment
    - The process of moving a system from development/testing environments to live production environments
    - Requires careful planning to avoid security breaches and data loss during the transition
  - Operations and Maintenance
    - Ongoing management of the system to ensure it continues to meet security requirements and operates effectively
    - Includes updates, patches, and modifications to address new security challenges and maintain compliance
  - Retirement/Disposal
    - Procedures for properly removing the system from service while ensuring that all data is securely handled



# ISC2 CISSP

## (Study Guide)

- Includes data destruction, hardware disposal, and ensuring no sensitive data remains accessible

## Data Security Controls

### Objectives

- 2.6 - Determine data security controls and compliance requirements
- 1.3 - Evaluate and apply security governance principles
- 3.3 - Select controls based upon systems security requirements
- 2.4 - Manage data lifecycle
  
- **Understanding Data States**
  - Data States Overview
    - Data can exist in three different states
      - In use, in transit, and at rest
    - Security needs to be applied in all states to protect data from threats and vulnerabilities
  - Data in Use
    - Data is actively being used by software, applications, or systems
    - Data in use typically resides in memory or is being processed
    - Most volatile state because changes during processing can impact data integrity
    - Requires security measures such as authentication, authorization, and monitoring to prevent unauthorized access
  - Data in Transit
    - Data is moving from one location to another
      - E.g., from a source to a destination

- Most at risk during transit because it is exposed to the network (wired or wireless)
- Confidentiality, integrity, and availability can be impacted while data is in transit
- Common protection mechanisms include encryption, secure routing, and digital certificates (SSL/TLS)
- Data at Rest
  - Data is inactive and stored on a device, in a cloud, or in archives
  - Data becomes a static target for attackers while stored
  - Data at rest is often targeted by persistent attackers using repeated attempts
  - Protection measures include full-disk encryption, trusted platform modules (TPM), and secure storage environments
- Security Considerations
  - Data in Use
    - Volatile, requires authentication, authorization, and accounting to maintain data integrity
  - Data in Transit
    - Most at risk, use encryption and mutual authentication to protect data in motion
  - Data at Rest
    - Static target, requires encryption and secure storage to defend against persistent attacks
- Examples and Use Cases
  - Data in Use

- Actively processed web server requests or displayed data on a screen
  - Transactions being performed by a system or application
- Data in Transit
  - Logs sent from a server to another location for analysis
  - Transferring data between a web server and a storage server using encryption and digital certificates
- Data at Rest
  - Archived system logs, compliance reports, or stored data in a database
  - Sensitive information stored on file servers or cloud storage
- **Security Control Frameworks**
  - Security Control Frameworks Overview
    - Provide a structured approach to implementing information security
    - Outline how to create policies, processes, and common security practices for governance and compliance
    - Facilitate assessments, audits, and compliance with legal and regulatory standards
  - COBIT (Control Objectives for Information and Related Technologies)
    - Designed for IT governance and improving IT efficiency and effectiveness
    - Provides guidelines for security implementation and auditing for compliance
    - Managed by ISACA (Information Systems Audit and Control Association)
    - Helps align IT with business needs and objectives
    - Ensures alignment between business and IT

# ISC2 CISSP

## (Study Guide)

- COBIT is derived from the COSO (Committee of Sponsoring Organizations) framework
- COSO is used to comply with Sarbanes Oxley (SOX) 404, focused on preventing fraudulent financial reporting
- COBIT Five Principles
  - Meeting Stakeholder Needs
    - Linking enterprise IT goals to stakeholders' needs
  - Covering the Enterprise End-to-End
    - Managing and governing all IT-related assets
  - Applying a Single Integrated Framework
    - Creating a unified governance framework for IT assets and resources
  - Enabling a Holistic Approach
    - Ensuring all parts of the organization work as intended
  - Separating Governance from Management
    - Keeping management out of the governance process to avoid conflicts of interest
- ISO/IEC 27002 (International Standard for Information Security)\*\*
  - Originated from British Standard 7799, later replaced by 17799 and now ISO/IEC 27002
  - International standard for security control frameworks
  - Broken into multiple control objectives, including policies, human resources, security, and cryptography
  - Focuses on objectives for maintaining international security standards
  - Widely adopted globally across industries

# ISC2 CISSP

## (Study Guide)

- NIST SP 800-53 (National Institute of Standards and Technology Special Publication 800-53)
  - Widely adopted in the U.S. government and U.S.-based organizations
  - Focuses on security and privacy controls for information systems and organizations
  - Required by FISMA (Federal Information Security Management Act)
  - Selection of controls depends on risk impact levels, data overlays, priority, and baseline allocation
  - Control families include categories like access control, training, audit, and accountability
  - Data overlays address specific controls for different data types (e.g., military, HR, financial)
- Important Terms
  - COBIT
    - IT governance framework
  - COSO
    - Framework for financial reporting compliance (drives SOX 404 compliance)
  - ISO/IEC 27002
    - International security standard with control objectives
  - NIST SP 800-53
    - U.S. federal security control framework with control families

- **Determining Security Controls**

- Security Controls Overview

- Safeguards or countermeasures implemented as administrative, physical, or technical methods
    - Aim to reduce or manage security risks and meet compliance requirements
    - Used in administrative controls
      - E.g., policies
    - Technical controls
      - E.g., firewalls
    - physical controls
      - E.g., gates, guards

- Types of Security Controls

- Administrative
      - Policies, procedures, standards
        - E.g., security awareness training, incident response plans
    - Physical
      - Locks, fences, guards
        - E.g., security personnel, CCTV systems
    - Technical
      - Software, hardware, and system configurations
        - E.g., encryption, firewalls

- Standards for Selecting Security Controls

- Controls should follow a trusted source, standard, or regulation relevant to the industry



- Health Industry
  - HIPAA compliance
- Government Industry
  - FISMA compliance
- Financial Industry
  - SOX compliance
- International Standards
  - ISO/IEC 27002
- Common Security Control Standards
  - NIST SP 800-53
    - Security and Privacy Controls for Information Systems and Organizations
    - Required by FISMA
    - Focuses on selecting controls based on risk levels, data sensitivity, and organizational needs
  - ISO/IEC 27002
    - International Code of Practice for Information Security Controls
    - An international standard for information security controls
  - COSO Framework
    - Committee of Sponsoring Organizations of the Treadway Commission
    - Commonly used with Sarbanes-Oxley (SOX) compliance
  - COBIT
    - Control Objectives for Information and Related Technologies
    - IT governance framework used for security and compliance

- Control Types within Defense in Depth Strategy
  - Preventative
    - Stop incidents from happening
      - E.g., firewalls, authentication
  - Detective
    - Identify incidents after they happen
      - E.g., log monitoring, intrusion detection systems
  - Corrective
    - Remedy an incident after detection
      - E.g., backup recovery, patch management
  - Compensating
    - Alternate measures when primary controls fail
      - E.g., using a second layer of encryption
  - Deterrent
    - Discourage incidents
      - E.g., security signage, warning banners
  - Directive
    - Mandate behaviors or actions
      - E.g., security policies, procedures
  - Recovery
    - Return systems to normal after an incident
      - E.g., disaster recovery plans
- Control Baseline and Tailoring
  - Baseline

# ISC2 CISSP

## (Study Guide)

- The minimum set of controls for safeguarding security and privacy, often selected from frameworks such as NIST SP 800-53 or ISO/IEC 27002
- Acts as a starting point for protection
- Adaptable based on the organization's needs
- Scoping
  - Selecting controls that apply specifically to an organization's environment
- Tailoring
  - Modifying the baseline by adding or removing controls to fit the organization's security needs
- Tailoring In
  - Adding additional controls based on new risks or data sensitivity
- Tailoring Out
  - Removing controls that are not relevant or applicable to the system
- Examples of Security Controls
  - NIST SP 800-53 REV 5 Example
    - Vulnerability Monitoring and Scanning
    - Use vulnerability monitoring tools to scan systems
    - Analyze reports and remediate legitimate vulnerabilities
    - Ensure monitoring tools are updated frequently
    - Share vulnerability information with designated teams
- Important Terms
  - High Watermark

- A principle that ensures the highest level of protection is applied to data across different types
- Baseline
  - The minimum set of controls required for security
- Scoping
  - Determining which controls are applicable based on the organization's structure
- Tailoring
  - Adjusting the baseline controls to fit specific organizational needs
- **Selecting Security Controls**
  - Security Controls Overview
    - Security controls are administrative, physical, or technical safeguards used to reduce or manage security risks
    - Privacy controls also exist, but the focus here is on security
    - Common frameworks help define and recommend security controls based on regulations, policies, or governance
  - Security Control Frameworks
    - NIST SP 800-37
      - Risk Management Framework (RMF) for information systems and organizations
      - Life cycle-based framework for implementing risk management in secure system development.
    - NIST SP 800-53

- Control catalog within the RMF that provides a set of security and privacy controls
- ISO 27001 Series
  - International standard for managing information security, providing a framework for risk management
- HITRUST (Health Information Trust Alliance)
  - Common security framework for health information
- Control Selection Process
  - Selection within the RMF
    - Selection is Step 3 in the RMF after preparing and categorizing the data
    - Controls must align with organizational and regulatory policies.
    - Controls are selected based on the level of risk and the protection needs of the information
    - Over-securing public systems is avoided; sensitive systems receive appropriate controls
  - Control Baselines
    - Frameworks
      - E.g., NIST, ISO, HITRUST often provide a baseline of minimum controls
    - Baselines are determined based on the system's sensitivity, such as co-mingled data (sensitive and public data on the same system)
    - Controls are designed to protect at the highest level of sensitivity
- Key Considerations for Selecting Controls
  - Risk Analysis

- Understand emerging threats, vulnerabilities, and factors specific to the data types
- Scoping
  - Determines whether controls apply to the system
- Tailoring
  - Modifying controls by adding (tailoring in) or removing (tailoring out) based on the system's needs and the recommended baseline
- Incidents
  - Security incidents can drive the need for reassessment, updating, or adding controls to address gaps or new vulnerabilities
- Emerging Threats and Vulnerabilities
  - New threats or zero-day vulnerabilities may require adjustments to security controls
- The Deming Cycle (PDCA)
  - Plan
    - Identify security objectives and determine appropriate controls
  - Do
    - Implement selected controls to meet objectives
  - Check
    - Assess the effectiveness of controls and ensure they meet security goals
  - Act
    - Address gaps in control effectiveness, especially after incidents or changes in the environment
- Important Terms

- NIST SP 800-37
  - Provides the Risk Management Framework (RMF) for information systems
- NIST SP 800-53
  - The control catalog within the RMF, offering a range of security and privacy controls
- Control Baseline
  - The minimum set of controls needed to safeguard the system, selected from a framework like NIST or ISO
- Scoping
  - Process of determining which controls apply to a specific system
- Tailoring
  - Adding or removing controls based on system-specific requirements
- Deming Cycle (PDCA)
  - Continuous improvement cycle for planning, implementing, assessing, and acting on security controls
- **Data Protection Methods**
  - Digital Rights Management (DRM)
    - Uses encryption to enforce copyright protection for digital media (movies, music, e-books)
    - Protects against copying, piracy, and unauthorized sharing of intellectual property

- DRM ensures that digital content can only be accessed when the device has the appropriate decryption key
- DRM Methods
  - HDCP (High-Bandwidth Digital Content Protection)
    - Protects digital displays like HDMI or DVI but has been compromised and is not widely used anymore
  - AACPS (Advanced Access Content System)
    - Protects Blu-ray discs, HD DVDs, and other media discs
  - ADEPT (Adobe Digital Experience Protection Technology)
    - Used by Adobe to protect e-books, PDFs, and other digital content
  - Blockchain-Based DRM
    - Uses cryptography to create immutable (unchangeable) records, providing a new method for DRM, although not widely adopted yet
- Data Loss Prevention (DLP)
  - Blocks unauthorized data exfiltration (egress monitoring)
  - Uses pattern matching to identify and take action against data (based on classifications like PII, PHI, etc.)
- Types of DLP
  - Network DLP
    - Scans outgoing data on the network to detect and block unauthorized data leaving the system
  - Endpoint DLP
    - Scans local file systems and monitors data leaving individual endpoints to detect and block unauthorized exfiltration



- DLP Process
  - Data must be labeled or classified to be detected by DLP software
  - DLP can be configured with policies to address different data protection needs
  - Regular updates are needed for optimal DLP performance
- Cloud Access Security Broker (CASB)
  - A security policy enforcement point between users and cloud services
  - Functions as a proxy between the user and the cloud, ensuring security controls are applied to cloud-based assets
  - CASB Functions
    - Provides data security, DLP, threat protection, real-time risk analysis, and URL filtering
    - Ensures compliance with security policies and provides threat intelligence in real-time
    - Can be used on-premises or off-premises (local or cloud-based)
  - CASB Capabilities
    - Enforces security policies
    - Protects data in the cloud
    - Detects and prevents threats with real-time monitoring and alerts.
    - Integrates services to evaluate web traffic, enforce DLP, and provide granular threat protection
- Important Terms
  - DRM
    - Technology used to protect digital content from unauthorized access and copying

- **HDCP**
  - Protection for digital display interfaces (e.g., HDMI) (now obsolete)
- **AACS**
  - Protects Blu-rays, HD DVDs, and similar media
- **ADEPT**
  - Adobe's DRM system for protecting digital content like e-books and PDFs
- **DLP**
  - Software and techniques designed to prevent the unauthorized transfer of sensitive data
- **CASB**
  - A security proxy that ensures proper security controls between users and cloud-based services
- **Data Retention Requirements**
  - Data Retention Overview
    - Data retention involves maintaining and protecting data throughout its entire lifecycle (creation, classification, storage, use, archiving, and destruction)
    - Organizational policy and regulatory requirements govern how long data should be retained and how it must be protected
    - Data must be retained securely and only for as long as it is necessary according to organizational policy and legal or regulatory requirements
  - Regulations Governing Data Retention
    - HIPAA

# ISC2 CISSP

## (Study Guide)

- Health Insurance Portability and Accountability Act (for healthcare data retention and protection)
- PCI DSS
  - Payment Card Industry Data Security Standard (for financial and payment data)
- FISMA
  - Federal Information Security Management Act (for government data protection)
- GDPR
  - General Data Protection Regulation (for data privacy and protection, particularly in the EU)
- SOX
  - Sarbanes-Oxley Act (for financial reporting data retention)
- GLBA
  - Gramm-Leach-Bliley Act (for financial institutions' customer data protection)
- Guidance on Data Retention
  - NIST SP 800-53
    - Provides security and privacy controls for information systems and organizations
  - ISO 15489
    - Focuses on records management, including concepts and principles of data retention
  - ISO 17799
    - Outlines the best practices for information security management

- Organizational Data Retention Policy
  - Policies must align with legal and regulatory requirements
  - Policies should define
    - Purpose, scope, and applicability of data retention
    - Type of data and assets covered
    - Retention periods or timelines
      - E.g., archive data for 1 year, destroy it on day 366
    - End-of-life and end-of-support requirements for assets (servers, hardware, software)
    - Important to destroy data once it is no longer needed to prevent legal liabilities or unauthorized disclosure in case of a breach
- Retention Best Practices
  - Retain data only for as long as it is necessary or legally required
  - End-of-Life (EOL)
    - When the asset (hardware, software) can no longer be used or the license expires
  - End-of-Support (EOS)
    - When the vendor no longer maintains or supports the hardware or software
  - Properly Destroy Data
    - Once no longer needed, data should be securely destroyed to prevent liability and reduce costs
  - Maintain administrative, logical/technical, and physical security controls over data while in storage
    - E.g., encryption, access control

- Asset Retention
  - Assets
    - E.g., servers, hardware, software) have finite lifespans
    - Regularly monitor for end-of-life and end-of-support statuses
    - Replace hardware based on mean time to failure to avoid availability issues
    - When assets are no longer supported, ensure they are replaced or removed to avoid security vulnerabilities
- Retention and Legal Proceedings
  - If data is involved in legal or security investigations, it must be retained until the case is concluded
  - Chain of custody must be maintained to ensure data integrity in legal contexts.
- Important Terms
  - Data Retention
    - Maintaining data securely for a specified period, as required by policies or regulations
  - End-of-Life (EOL)
    - The point at which an asset (hardware, software) is no longer usable or supported
  - End-of-Support (EOS)
    - When a vendor no longer provides updates or support for an asset
  - Chain of Custody
    - A documented process that tracks who has access to data, ensuring integrity in legal proceedings

- **Managing Data Remanence**

- Data Remnants

- Data remnants refer to leftover data that remains after an attempt to delete or remove it
    - Deleting data typically does not guarantee proper destruction; it often just moves data to a different location, such as a recycle bin
    - Proper destruction techniques are necessary to ensure data cannot be accessed by unauthorized users

- Importance of Data Destruction

- Confidentiality is the main focus when managing data remnants, ensuring that sensitive data is not disclosed to unauthorized individuals
    - Data must be securely erased or destroyed as part of the data lifecycle, which involves creation, classification, storage, use, archiving, and destruction
    - Proper data destruction ensures compliance with regulations and organizational policies

- Regulations and Guidelines

- NIST SP 800-88
      - Guidelines for Media Sanitization
    - ISO/IEC 27040
      - Storage security standards
      - Regulatory guidelines often require proof of data destruction to prevent data remnants and unauthorized disclosure

- Declassification Techniques

- De-identification

# ISC2 CISSP

## (Study Guide)

- Removal of personal identifiers from data to prevent linking to a specific subject
- Used to anonymize data
  - E.g., removing account numbers from medical records
- Pseudonymization
  - Replacing sensitive data with aliases or pseudonyms
  - Allows data to be masked, but still linked back to the original information through separate records
- Tokenization
  - Substitutes sensitive data with non-sensitive tokens that have no intrinsic value
  - The tokenized data must be mapped back to the original data for internal use but appears meaningless to unauthorized users
- Obfuscation
  - Concealing sensitive data by hiding or masking it
  - A common example is drawing a black box over text to prevent it from being read
- Data Destruction Techniques
  - Erasing
    - Deletes the data from the file system but does not remove it from the disk
    - Not effective against data remnants
  - Clearing
    - Overwriting data to make it unrecoverable

- More effective at preventing data remnants compared to simple erasing
- Purging
  - Repeated clearing to ensure data is completely unrecoverable
  - Often used in highly sensitive environments like government or medical sectors
- Sanitization
  - Complete removal of data to ensure the medium is as if it were brand new
  - Common in preparing devices for reuse or resale
- Data Sanitization Methods
  - Degaussing
    - Uses strong magnetic fields to scramble the data stored on magnetic media
      - E.g., backup tapes
    - Effective at making the data completely unrecoverable.
  - Zeroing
    - Overwrites the entire storage medium with zeros
    - Effective for simple data sanitization but can still leave traces in some cases
  - Overwriting
    - Replaces data with multiple passes of random 1s and 0s
    - More complex and thorough than zeroing, ensuring that data is irrecoverable



- Best Practices for Data Remnant Management
  - Ensure data is properly declassified or destroyed according to organizational policies and regulations
  - Use the appropriate sanitization method based on the medium
    - E.g., degaussing for tapes, overwriting for hard drives
  - Implement controls to guarantee that sensitive data is either anonymized or securely destroyed at the end of its lifecycle.
- Important Terms
  - Data Remnants
    - Leftover data that was not properly destroyed or erased
  - Clearing
    - Process of erasing data to make it unrecoverable
  - Purging
    - Repeated clearing to ensure data is permanently destroyed
  - Sanitization
    - Complete removal of data, restoring the medium to its original state
  - Degaussing
    - Magnetic destruction of data stored on tapes or similar media

## Secure Design Principles

### Objectives

- 3.5 - Assess and mitigate vulnerabilities in security architectures, designs, and solutions
- 3.1 - Implement and manage secure design principles
- 5.4 - Implement and manage authorization mechanisms
- 3.4 - Understand security capabilities of information systems
- 3.2 - Understand fundamental concepts of security models
  
- **Secure Design Principles**
  - Secure Design Principles
    - Essential for building secure systems, applications, and networks
    - Security should be integral to the design process, not an afterthought
  - Common System Designs
    - Types include open and closed systems, open source and closed source
  - Core Concepts of Secure Design
    - Bounds, confinement, transitive trust
  - Established Design Principles
    - Principle of least privilege, separation of duties, fail-safe defaults
  - Zero Trust
    - No inherent trust; continuous verification of users, devices, and systems
    - Moves away from traditional perimeter-based security models
  - Privacy by Design
    - Embedding privacy into the design and architecture of systems

- Adheres to regulations like GDPR
- Seven foundational principles include proactive privacy measures and transparency
- System Security Capabilities
  - Features like memory protection, Trusted Platform Module (TPM), hardware security modules
- Security Models
  - Bell-LaPadula, Biba, Clark-Wilson models
  - Key for maintaining data integrity, confidentiality, and availability
- **Understanding Secure Design**
  - Purpose of Secure Design
    - Involves selecting security controls and building systems to reduce security risk to an acceptable level
    - Applies to all components, including servers, networks, cloud systems, routers, and data storage methods
  - Core Terms in Secure Design
    - Object
      - Any system resource, such as a file, directory, service, or CPU, that can be accessed or used
    - Subject
      - Any system user or process that interacts with objects
  - Types of System Designs
    - Closed System

# ISC2 CISSP

## (Study Guide)

- Uses a single vendor, is not exposed to external networks, and relies on proprietary or closed-source products
  - E.g., Windows OS, Cisco IOS
- Easier to manage but harder to integrate and more difficult to detect vulnerabilities
- Open System
  - Integrates multiple vendors and open-source components, allowing public evaluation of source code for flaws and patches
  - Allows flexibility, integration, and public collaboration on security
- Trust and Secure Design
  - Transitive Trust
    - Inherited trust passed from one process to another without requiring verification; often risky without proper security
  - Trusted Systems
    - Security controls work collectively to create a secure system environment
  - Assurance
    - Provides confidence in the effectiveness of security measures for protecting against threats
- Secure Design Concepts
  - Confinement (Sandboxing)
    - Runs software in an isolated environment, restricting its access to system resources to avoid unintended interactions
  - Bounds

- Limits the memory resources available to a process, ensuring it operates within assigned limits and cannot impact other system areas
- Isolation
  - Separates software applications from the main OS; virtualization is a common method, providing isolation and controlled resource allocation
- Control Definitions in Secure Design
  - Defines how subjects and objects interact securely within the design framework
  - May include administrative, technical, logical, and physical controls to ensure comprehensive security measures
- **Secure Design Principles**
  - Purpose of Secure Design Principles
    - Guide system design to prevent security flaws and focus on data protection
    - Based on Saltzer and Schroeder's eight core principles from "The Protection of Information in Computer Systems" (1975), plus two suggested principles
  - Core Secure Design Principles
    - Economy of Mechanism
      - Design should be simple and small to reduce complexity and potential errors
    - Fail-Safe Defaults

# ISC2 CISSP

## (Study Guide)

- Default settings should deny access; components should fail securely (closed) rather than open
- Complete Mediation
  - Requires authorization each time a subject requests access to an object, preventing unauthorized access over time
- Open Design
  - System design should be open to external review; security relies on keeping cryptographic keys and passwords secret, not the design itself
- Separation of Privilege (Duties)
  - Critical functions require two or more subjects to execute, minimizing risks from single-user access to sensitive data or processes
- Least Privilege
  - Subjects should only have the minimum access required to perform their job functions
- Least Common Mechanism
  - Limit shared components and avoid transitive trust between processes to minimize cross-system vulnerabilities
- Psychological Acceptability
  - User experience should be simple to prevent misuse and reduce errors, ensuring security features are user-friendly
- Suggested Principles
  - Work Factor

- Evaluates the time and resources needed for an attacker to bypass a security control; adjusts controls to match asset value and risk level
- Compromise Recording
  - Uses detection mechanisms like audit logs, CCTV, IDS/IPS to track and detect potential attacks
- Design Verification Methods
  - Threat Modeling
    - Identifies and analyzes potential threats from both offensive (attack vectors) and defensive (security controls) perspectives
  - Risk Assessment (Analysis)
    - Analyzes organizational assets to assess risks and determine the level of investment for protection based on risk levels
  - Controls Assessment
    - Formal evaluation of security and privacy controls to ensure they meet governance, regulatory, and compliance requirements
- **Zero Trust Architecture**
  - Zero Trust Overview
    - Zero Trust Architecture (ZTA) does not inherently trust any entity inside or outside its network boundaries
    - Focuses on continuous authentication and real-time authorization for access to resources
  - Trust but Verify vs. Zero Trust
    - Trust but Verify
      - Allows initial trust, with verification upon access attempts

- Zero Trust
  - No implicit trust, continuous authentication, authorization, and least privilege enforced per request
- NIST SP 800-207 Zero Trust Principles
  - All data sources and computing services are resources
    - Treats all assets as resources, requiring verification for access
  - Secure communication regardless of network location
    - Encrypts all network traffic, even within internal, traditionally trusted networks
  - Access on a per-session basis
    - Authenticates and authorizes for each individual access attempt
  - Dynamic policies based on behavior and environment
    - Considers factors like location, device state, and activity to adapt access controls dynamically
  - Continuous monitoring of security posture
    - Regularly evaluates security measures and entity compliance within the system
  - Strictly enforced, real-time authentication and authorization
    - Applies updated policies immediately for consistent access control
  - Comprehensive data collection and analysis
    - Aggregates system logs, network data, and user behavior to enhance security and detect patterns
- Zero Trust in Network Design
  - No implicit trust of private networks



- Internal network traffic is not inherently trusted; Zero Trust protocols are applied
- Non-enterprise owned devices treated as untrusted
  - Personal and external devices must authenticate before accessing resources
- No automatic trust for any networked resource
  - Trust for any asset or device must be verified per interaction
- Remote connections viewed as potentially insecure
  - Assumes that local networks (especially remote access points) may be compromised
- Consistent security policy across enterprise boundaries
  - Extends security controls and policies to both on-premises and cloud resources for continuity
- Zero Trust Architecture Components
  - Policy Engine (PE)
    - Decides subject access authorization for resources, logs access decisions
  - Policy Administrator (PA)
    - Manages subject and resource communication, authentication, and authorization through token creation
  - Policy Enforcement Point (PEP)
    - Enforces access control between subjects and resources by acting as a gateway or intermediary
- Shared Responsibility Model
  - Inherits Controls

- Organization may inherit controls like physical security from cloud providers
- Shares Controls
  - Organization and third parties may share responsibilities for areas like patch management or authentication
- Common in Cloud Services
  - Seen in cloud platforms (AWS, Azure, Google Cloud) where clients and providers share security responsibilities
- **Privacy By Design**
  - Privacy by Design Overview
    - Concept that integrates privacy into the system architecture from the start
    - Ensures that data is collected, used, and protected according to privacy principles, legal standards, and regulations
  - Seven Foundational Principles of Privacy by Design
    - Proactive, Not Reactive
      - Focus on preventing unauthorized access by anticipating risks before they occur
      - Implement high security standards, aiming to go beyond compliance to strengthen privacy protections
      - Identify poor privacy design with assessments, such as Privacy Impact Assessments, and implement remedial actions
    - Privacy by Default
      - Set privacy protections as the default setting in all processes
      - Collect only necessary data, limiting purpose, scope, and retention

# ISC2 CISSP

## (Study Guide)

- Destroy data that is no longer needed to reduce risk and comply with data retention policies
- Privacy Embedded into Design
  - Integrate privacy protections at every stage of development and into all operational activities
  - Perform regular privacy impact assessments and update designs in response to emerging risks or regulatory changes
- Full Functionality – Positive-Sum, Not Zero-Sum
  - Ensure privacy protections do not impede organizational objectives or user experience
  - Maintain a balance where privacy measures support business processes without unnecessary restriction or impact
- End-to-End Security – Full Lifecycle Protection
  - Protect data throughout its entire lifecycle
    - Creation, processing, storage, and destruction
  - Maintain secure handling, storage, and transmission of data, ensuring compliance with applicable regulations
- Visibility and Transparency
  - Establish accountability through transparent privacy policies and make them accessible to all users
  - Publish privacy policies that comply with applicable regulations
    - E.g., PCI DSS, HIPAA, GDPR
- Respect for User Privacy – Keep it User-Centric
  - Respect users' ownership over their data, maintaining a user-focused approach in all privacy practices

- Ensure users have access to their data, can modify it, and can consent to its use, while protecting it as personal and sensitive information
- **System Security Capabilities**
  - System Security Capabilities Overview
    - Capabilities are system features that enforce technical or logical security controls
    - Built into various devices, these capabilities help maintain secure processes and limit unauthorized access
  - Memory Protection
    - Memory stores data for active processes on computing devices
    - Goal
      - Prevent processes in memory from interacting with each other to avoid data leaks and breaches
      - Allows multiple processes at different security levels to run independently in main memory
  - Virtualization
    - Emulation of physical devices through software, commonly applied to networks, servers, and workstations
    - Enables multiple computing environments on a single hardware component
    - Benefits
      - Centralized control, scalability, easy recovery, and useful in malware analysis within sandboxed environments
    - Common tools

- VirtualBox, VMware Workstation
- User Interfaces (Restricted or Constrained Interfaces)
  - Restricts what objects users can access based on privilege levels
  - Certain features are hidden or limited based on user roles, such as admin vs. general user
  - Implements least privilege by limiting functions accessible to unauthorized users
  - Example
    - Admin dashboard with features visible only to authorized users
- Trusted Platform Module (TPM)
  - Specialized motherboard chip providing cryptographic services to the computer
  - Follows ISO standard 11889
  - Functions include creating key pairs, signing data, and data encryption
  - TPM Components
    - Endorsement Key (EK)
      - Private key embedded by the hardware manufacturer, unalterable
    - Storage Root Key (SRK)
      - Secures TPM-stored keys
    - Platform Configuration Registers (PCR)
      - Tracks current software configuration
      - Attestation Identity Key (AIK)
        - Authenticates TPM with a trusted authority
    - Hardware Security Modules (HSM)

# ISC2 CISSP

## (Study Guide)

- Standalone cryptographic devices for encryption and decryption services
  - Encrypts data passing through interfaces and can be used in applications requiring high security for cryptographic keys
  - Example Devices
    - Smart Cards: Card-sized modules used for multifactor authentication and secure transactions (e.g., credit cards, PIV cards)
    - Bulk Encryptor: Processes large data flows, encrypting and decrypting data
- **Understanding Security Models**
  - Security Model Concepts
    - A security model is a concept for enforcing security or privacy policies within a system design
    - Provides guidance for mapping organizational requirements into a system design to enforce security rules effectively
    - Assists in meeting security objectives by simplifying security requirements for easier implementation in secure architecture
  - Building Security into the System
    - Identify security objectives aligned with business goals
    - Use security models to map controls to system design requirements
    - Employ multiple security models if necessary, especially for larger enterprise systems
  - Trusted Computing Base (TCB)

- Comprises system components and security controls that enforce security policies
- Encompasses all trusted elements within a system to form a secure computing environment
- Security Perimeter
  - Conceptual boundary defining trusted (inside) and untrusted (outside) areas within the system
  - Inside the perimeter, controls are managed and trusted, while anything outside is untrusted
- Reference Monitor
  - Verifies and enforces access requests between subjects
    - E.g., users
  - And objects
    - E.g., files
  - Ensures that only authorized access is allowed based on system policies
- Security Kernel
  - Core component of the TCB, encompassing both the TCB and the reference monitor
  - Handles access requests and maintains system security integrity
- Execution Domain
  - Isolated area where the TCB operates, free from interference by other system processes
  - Ensures TCB functions without external influence to maintain security
- Trusted Path

- Communication channel presumed secure and resistant to compromise by potential attackers
- Finite State Machine
  - Evaluates the current state of subjects and objects before allowing a transition to a new state
  - Assesses if an action (state transition) is permissible based on configured permissions and system policies
- Lattice Model
  - Establishes fixed security levels for subjects and objects, controlling access based on clearance levels
  - Subjects can access objects of equal or lower security levels, ensuring controlled information flow
  - Commonly used in environments requiring strict access control, such as mandatory access control systems
- Example of Finite State Machine
  - A user purchasing a course
    - System checks if discount or full price is authorized
    - If course is closed, the enrollment state is denied; if open, it's authorized
- Example of Lattice Model
  - User with a clearance of "Secret"
    - Can access information at "Confidential" or "Secret" levels
    - Access to "Top Secret" information is denied
- **Security Models - Part 1**
  - Non-Interference Model (Goguen-Meseguer Model)



- Ensures actions of one user cannot interfere with another user's actions, maintaining isolation
- Focused on separation between different security levels, such as private and public domains
- Changes made by one entity do not affect another, especially across different security classifications
- Access Control Matrix
  - Utilizes a table-like structure where subjects are mapped to objects with specific access rights
  - Columns
    - Objects
      - E.g., files, directories
  - Rows
    - Subjects
      - E.g., users, processes
  - Permissions granted per cell
    - E.g., Read, Write, Execute
  - Provides a flexible yet straightforward method to manage access control across multiple levels
- Information Flow Model
  - Controls how information flows between different security levels, focusing on preventing unauthorized transfer
  - Two Key Models
    - Bell-LaPadula Model
      - Focused on confidentiality

- Biba Model
  - Focused on integrity
- Bell-LaPadula Model
  - Designed for confidentiality, especially in military or government environments
  - State Machine Model
    - Monitors data flow between security classifications
  - Properties
    - Simple Security Rule
      - No read up (subjects cannot read data above their classification level)
    - Star Property Rule
      - No write down (subjects cannot write data to a lower classification level)
      - Ensures sensitive information does not flow to unauthorized levels
- Biba Model
  - Prioritizes integrity, ensuring the accuracy and consistency of data
  - Based on the Lattice Model
  - Properties
    - Simple Integrity Axiom
      - No read down (high-integrity users cannot read lower-integrity data)
    - Star Integrity Axiom

- No write up (lower-integrity users cannot write to higher-integrity data)
    - Protects high-integrity data like financial records, medical data, and other sensitive information
  - Take-Grant Model
    - Manages transitive trust and access rights between subjects and objects
    - Rules
      - Take Rule
        - A subject can take rights from an object
      - Grant Rule
        - A subject can grant rights to an object
      - Create Rule
        - A subject can create new rights
      - Remove Rule
        - A subject can remove rights
    - Supports scenarios where rights need to be assigned, inherited, or removed dynamically based on trust relationships
- **Security Models - Part 2**
  - Clark-Wilson Model
    - Focuses on data integrity in business and industrial applications
    - Uses Access Triple
      - Subjects, Programs, and Objects
    - Well-formed transactions

- Restrict subjects' ability to manipulate data directly, ensuring data modifications are authorized
- Separation of duties
  - Prevents a single user from accessing and modifying critical data without oversight
- Key Terms
  - Constrained Data Item (CDI)
    - Data that requires protection
  - Unconstrained Data Item (UDI)
    - Data that does not require protection
  - Transformation Procedures (TP)
    - Authorized methods to modify a CDI
  - Integrity Verification Procedures (IVP)
    - Verifies CDI integrity is maintained after modification
- Brewer-Nash Model (Chinese Wall Model)
  - Also known as Ethical Wall or Cone of Silence
  - Focuses on conflict of interest prevention
  - Prevents information flow between subjects and objects that could lead to conflicts of interest, ensuring individuals cannot access conflicting data
    - E.g., data from competing companies
- Graham-Denning Model
  - Focuses on secure interaction between subjects and objects with defined access rights
  - Utilizes an Access Control Matrix to manage subject-object interactions
  - Eight Primary Actions

- Create Object
  - Subjects can create new objects
- Delete Object
  - Subjects can delete existing objects
- Read Object
  - Subjects can read objects
- Grant Access
  - Subjects can grant others access to objects
- Delete Access
  - Subjects can revoke access to objects
- Transfer Access
  - Subjects can transfer access rights to others
- Create Subject
  - Subjects can create other subjects
- Delete Subject
  - Subjects can delete other subjects
- Sutherland Model
  - Also called the Non-Deducibility Model
  - Aims to prevent information leaks through covert channels by controlling information flow
  - Combines the Information Flow Model and State Machine Model
  - Defines system states and transitions to prevent unauthorized inferences about data

## Secure Architecture Design

Objective 3.5: Assess and mitigate vulnerabilities of security architectures, designs, and solution elements

- **Secure Architecture Design Introduction**
  - Secure Architecture Design
    - Fundamental to creating systems that resist cyber threats
    - Vital for ensuring system confidentiality, integrity, and availability
  - System Architectures
    - Examination of different types of system architectures
    - Application of best practices in system design to ensure security
  - Database Systems
    - Critical for protecting sensitive organizational information
    - Focus on database structures, vulnerabilities, and common security attacks
  - Common Criteria
    - Framework for evaluating the security of IT products and systems
    - Guides decision-making in selecting secure systems or components
  - Industrial Control Systems (ICS)
    - Essential in sectors like manufacturing, energy, and healthcare
    - Unique security challenges due to legacy systems not originally designed with security in mind
  - Secure Access Service Edge (SASE)

- Integrates network security and wide-area networking into a cloud-delivered service
- Supports zero-trust models, enhancing security for remote work and cloud services
- Internet of Things (IoT)
  - Expanding connectivity of devices, posing unique security challenges
  - Focus on securing IoT devices and managing associated risks
- Microservices Architecture
  - Breaks down applications into smaller, independent components
  - Security challenges include securing service communications and managing complexity
- Embedded Systems
  - Common in consumer electronics and industrial equipment
  - Challenges in implementing robust security measures due to limited processing power
- High-Performance Computing (HPC)
  - Used in applications requiring computing at scale
  - Security focus on data protection, parallel processing, and redundancy systems
- Edge Computing
  - Processing data closer to where it is generated
  - Security considerations for maintaining data integrity and security between edge devices and core network
- **System Architectures**
  - Distributed Systems

- Systems connected via a network that share resources to create an integrated, distributed system
- Example
  - Accessing cloud-based training from a remote device
- Risks
  - Vulnerable endpoints
    - E.g., laptops, mobile devices
  - Insecure network communications (especially public or shared networks)
  - Insufficient security awareness by users.
- Mitigation
  - Secure endpoints with antivirus, firewalls, and IDS
  - Enforce strong network security protocols
- Client-Based Systems
  - Systems that require an agent or client, like a web browser or app, installed on the user's device
  - Example
    - Using a company-specific app to access secured data
  - Key Considerations
    - Data Flow Security
      - Ensuring data exchanged between clients and servers is secure
  - Secure Protocols
    - Use HTTPS, SSH, etc., to protect communication
  - Validation



- Verify both subject and data before granting access
- Types of Clients
  - Thick Clients
    - Installed applications that work independently
      - E.g., Outlook
  - Thin Clients
    - Rely on remote servers
      - E.g., web browsers
  - Zero Clients
    - Depend entirely on servers for functionality
      - E.g., virtual desktops
- Best Practices for System Architecture Security
  - Patch Management
    - Regularly update all components within the architecture to prevent vulnerabilities
  - Minimize Services and Applications
    - Enable only essential apps, services, and protocols
  - Monitoring and Logging
    - Track system health, status, and activities for security and troubleshooting
  - Account Management
    - Remove unnecessary or outdated accounts
    - Change default passwords for any new or reset accounts
- Architectural Design Principles
  - Defense in Depth

- Layered security with administrative, technical, logical, and physical controls
- Deny by Default, Permit by Exception
  - Restrict all access except for explicitly approved services or resources
- Exam Tips
  - Understand Vulnerabilities
    - Distributed systems are highly reliant on secure endpoint and network management
    - Client-based systems need strict data flow and protocol validation
  - Types of Clients
    - Know differences between thick, thin, and zero clients, and their specific dependencies
- **Database Systems**
  - Structured Query Language (SQL)
    - Language for managing and manipulating data within relational databases
    - Functions
      - Allows querying, storing, modifying, and structuring data
  - Database Structure
    - Schema
      - Defines the organization and structure of a database
    - Tables
      - Core storage structure within a database
    - Columns (Attributes)

- Define data categories
- Rows (Tuples)
  - Represent individual records
- Keys
  - Primary Key
    - Unique identifier in a table
- Foreign Key
  - Establishes a relationship between two tables
- Data Relationships
  - Aggregation
    - Combining data from multiple tables
  - Inference
    - Drawing conclusions from data using multiple pieces of information
- Database Vulnerabilities
  - Aggregation Attacks
    - Gathering data from multiple tables to infer sensitive information
    - Example
      - Using employee ID and pay grades from different tables to infer salaries
  - Inference Attacks
    - Deducting hidden or sensitive information from accessible data
    - Example
      - Using publicly available tables to infer employee salaries or positions

- Polyinstantiation
  - Purpose
    - Enables multiple instances of the same primary key with different data sensitivity levels
  - Use
    - Provides different views of data based on access level
      - E.g., public vs. private data
- Data Collection and Analysis in Databases
  - Data Warehouse
    - Central storage for large volumes of data collected from multiple databases
  - Use
    - Allows for data mining and analytics
  - Data Mining
    - Analyzing data to find patterns and connections
  - Purpose
    - Often used for marketing, sales, and security analysis
  - Data Analytics
  - Analyzing raw data to extract actionable insights
  - Big Data
    - Extremely large datasets requiring advanced processing and analytics
    - Solution
      - Often managed through parallel data processing systems
- ACID Framework for Database Transactions

- Atomicity
  - Transactions are all-or-nothing. Either fully complete or fail entirely
- Consistency
  - Data must comply with defined rules and constraints
- Isolation
  - Ensures transactions are separate, preventing interference
- Durability
  - Completed transactions are permanently recorded, even after a system failure
- Database Security Best Practices
  - Enable Only Essential Components
    - Disable all unnecessary applications, services, and protocols
  - Account Management
    - Remove unneeded accounts
    - Change default passwords on database management systems
  - Set Permissions
    - Apply strict permissions to database directories, data stores, log files, and certificates
- **Common Criteria**
  - Common Criteria
    - An internationally recognized standard for IT security evaluation, providing a structured approach for evaluating the security features of products and systems

- Purpose
  - Evaluate and certify security features for international recognition
  - Standard
    - Established under ISO/IEC 15408
- Components of Common Criteria
  - Part 1
    - Introduction and General Model
      - Outlines basic concepts of security evaluations
  - Part 2
    - Security Functional Requirements (SFR)
      - Details the specific security functions a product or system must have
  - Part 3
    - Security Assurance Requirements (SAR)
      - Defines the evaluation assurance levels (EALs), providing confidence levels in security functionality
- Key Terms
  - Target of Evaluation (TOE)
    - The specific product, system, or component being evaluated
      - E.g., software, firmware, or hardware
  - Protection Profile (PP)
    - General security requirements and objectives a product should meet
  - Strict Conformance
    - All security requirements are mandatory

- Demonstrable Conformance
  - Demonstrates select security capabilities; not all requirements are mandatory
- Security Target (ST)
  - High-level security requirements and objectives for the TOE, specifying the desired protection outcomes
- Evaluation Assurance Levels (EALs)
  - Levels measure assurance of security functionality, from basic (EAL1) to highly secure (EAL7)
  - EAL1 - Functionally Tested
    - Assurance
      - Basic functionality confirmed; no extensive security focus.
  - EAL2 - Structurally Tested
    - Assurance
      - Full security target testing; documentation and commercial standard adherence
  - EAL3 - Methodically Tested and Checked
    - Assurance
      - Comprehensive security assurance with independent review
  - EAL4 - Methodically Designed, Tested, and Reviewed
    - Assurance
      - Commonly used for OSEs and applications, moderate to high assurance with independent evaluation
    - Note

# ISC2 CISSP

## (Study Guide)

- Changes above EAL4 require re-certification.
- EAL5 - Semi-Formally Designed and Tested
  - Assurance
    - Higher assurance for specialized applications, such as authentication systems
- EAL6 - Semi-Formally Verified, Designed, and Tested
  - Assurance
    - Used for high-assurance systems in government, energy, and transport
- EAL7 - Formally Verified, Designed, and Tested
  - Assurance
    - Highest security for critical systems where human safety is a factor
- Risks and Limitations of Common Criteria
  - Selective Evaluation
    - Manufacturers may control what features are evaluated
  - Focus on Product, Not Data
    - Certification applies only to product security, not data protection
  - Limited Physical and Personnel Security
    - Excludes considerations for personnel security controls
  - No Business Continuity Controls
    - Omits business continuity and disaster recovery measures
- Key Takeaways
  - Understand



# ISC2 CISSP

## (Study Guide)

- Parts 1-3 of Common Criteria, including TOE, PP, ST, and their purposes
- EALs Focus
  - Concentrate on EAL levels 3-5, as these are most applicable to commonly used systems
- Limitations
  - Recognize the flexibility manufacturers have in shaping evaluations and the Common Criteria's exclusion of data and business continuity protections
- **Industrial Control Systems**
  - Overview of ICS
    - Industrial Control Systems (ICS) manage industrial processes and machines, widely used across sectors like manufacturing, utilities, transportation, and more. ICS are fundamental in settings like
      - Manufacturing Plants
      - Product Handling Facilities
      - Energy Plants (Water, Electrical)
      - Transportation (Rail, Airport)
  - Components of ICS
    - Programmable Logic Controllers (PLC)
      - Type
        - Digital computers
      - Function

# ISC2 CISSP

## (Study Guide)

- Control automation and manage specific operations like valve regulation, temperature, and speed control
- Examples of Use
  - Lights, conveyor belts, sensors, and industrial valves
- Distributed Control Systems (DCS)
  - Type
    - Centralized system within a single facility
  - Function
    - Gather and distribute operational data, enabling centralized control across devices
  - Example
    - Temperature monitoring across different production stages within a single facility
- Supervisory Control and Data Acquisition (SCADA)
  - Type
    - Networked control system
  - Function
    - Enables centralized data acquisition and control over distributed assets, commonly used in critical infrastructure sectors
  - Examples of Use
    - Water treatment, electric grid management, and oil/gas pipelines
- SCADA System Components
  - Remote Terminal Unit (RTU)

# ISC2 CISSP

## (Study Guide)

- Purpose
  - Connects to sensors or controllers for data collection, often using radio frequency
- Also Known As
  - Remote telemetry unit
- Human-Machine Interface (HMI)
  - Purpose
    - Interface that allows human operators to interact with and control SCADA systems
- Distributed Network Protocol (DNP3)
  - Type
    - Open-standard protocol
  - Purpose
    - Used to connect RTUs with SCADA Master Control Stations (MCS) across sectors like energy and transportation
- Intelligent Electronic Device (IED)
  - Purpose
    - Collects data to send to RTUs, which then send the data to MCS
- Vulnerabilities in ICS
  - ICS are particularly vulnerable due to outdated technology and minimal built-in security
    - Legacy Systems
      - Older software often lacks built-in security, making updates and patches challenging

# ISC2 CISSP

## (Study Guide)

- Minimal Security Protocols
  - Often developed without modern security considerations, making ICS susceptible to attacks
- Limited Patch Options
  - Software updates may not address newly emerging threats
- Common ICS Vulnerabilities and Risks
  - Unauthenticated Access
    - Lack of strong authentication makes unauthorized access easier
  - Denial of Service (DoS)
    - Overloading systems can disrupt critical processes
  - Command Injection
    - Exploiting weak protocols to send unauthorized commands
- Impact of ICS Attacks
  - Attacks on ICS systems can disrupt essential services, including
    - Resource Destruction
      - Disruptions in energy or water supply
    - Chemical Hazards
      - Accidental release of hazardous substances, impacting public safety
    - Economic Impact
      - Production halts in manufacturing and other sectors
- Key Points for Exam Preparation
  - Understand the role and purpose of each ICS component
    - PLCs, DCS, and SCADA

- Familiarize with SCADA components (RTU, HMI, DNP3, IED) and how data is transmitted
  - Recognize vulnerabilities specific to ICS and their potential impacts on critical infrastructure
- 
- **Secure Access Service Edge**
    - Overview of SASE
      - Secure Access Service Edge, abbreviated as SASE, is a framework that consolidates network security functions and wide area networking into a unified cloud-based service
      - SASE centralizes control for consistent security policy enforcement across networks, enhancing remote and mobile access management
    - Purpose and Benefits of SASE
      - Consolidates multiple networking and security functions, reducing cost and complexity
      - Provides centralized control and orchestration of security policies and network access
      - Offers improved security for remote and mobile users with a unified security approach
      - Enhances visibility and management through centralization and integrated services
    - Components of SASE
      - Secure Service Edge (SSE)
      - Cloud-based security elements that exist within the cloud provider's infrastructure

- Moves security functions closer to user interactions, improving availability, performance, and reducing exposure of the internal network
- Access Layer
  - Manages user access to the SSE, primarily through the cloud, to enforce security controls at the network's edge
- Common SASE Features
  - Firewall as a Service (FWaaS)
    - Provides firewall functionality as a cloud-based service managed by the service provider
    - Service provider maintains configuration, rule sets, and access control lists based on customer requirements
  - Secure Web Gateway (SWG)
    - Handles web filtering, malware protection, and Data Loss Prevention (DLP)
    - Filters web traffic to block malicious content before it reaches users
  - Cloud Access Security Broker (CASB)
    - Offers visibility and control over cloud applications
    - Enforces security policies based on user access to cloud resources
    - Example
      - A CASB controls what users can do in cloud services and enforces policies like restricting access to sensitive data
  - Zero Trust Network Access (ZTNA)
    - Shifts from a traditional perimeter-based model to an identity-centric approach

- Enforces security policies based on verified identities rather than assumed trust based on network location
- Vendor Solutions for SASE
  - Cisco, Netskope, Palo Alto, Fortinet offer SASE solutions, defining SASE similarly as an architecture or methodology with consolidated security functions
- Considerations for SASE on the Exam
  - Recognize that SASE provides a security layer between users and cloud resources
  - Familiarize with common components
    - FWaaS, SWG, CASB, and ZTNA
- **Internet of Things**
  - Internet of Things (IoT)
    - IoT encompasses any device or technology capable of communication over the Internet
    - Examples include home appliances like refrigerators, dishwashers, washing machines, and dryers, as well as office and industrial devices like cameras, sensors, and medical devices
  - Purpose of IoT
    - Combines operational technology (OT) with information technology (IT)
    - Integrates diverse devices such as lights, cameras, sensors, and appliances, making them internet-capable
  - IoT Capabilities and Risks

- IoT devices provide functions such as data storage and network connectivity
- Technical capabilities of IoT devices introduce vulnerabilities and access points for potential intruders
- IoT devices lack traditional security controls, such as endpoint security, antivirus, and anti-malware
- Examples of IoT Devices
  - Household devices
    - Refrigerators, dishwashers, washing machines
  - Office and home security
    - CCTV cameras, lights, timers
  - Medical and industrial devices
    - Motorized wheelchairs, medical equipment
  - Vehicles and motorized equipment with remote control capabilities
- Challenges with IoT Security
  - IoT devices lack traditional management methods, such as SSH and VPNs, limiting remote management options
  - Security capabilities are often minimal, inefficient, and less effective than traditional technology
- Considerations for IoT Security
  - Threat Modeling
    - Identifying potential threats and vulnerabilities for each IoT device
    - Assessing attack vectors and defense mechanisms
  - Industry Standards



- Following standards like NIST and OWASP to ensure best practices and demonstrate due care and due diligence
- IoT Security Policy
  - Establishing policies that define usage and security protocols for IoT devices
- Default Account and Password Changes
  - Changing default accounts, passwords, and certificates before deployment in production environments
- Regular Software and Firmware Updates
  - Engaging with vendors for patch management to ensure frequent updates
- Security Architecture Integration
  - Incorporating IoT devices within a secure architecture and restricting exposure to the open internet
- Isolation and Segmentation
  - Isolating or segmenting IoT network traffic to prevent unnecessary access to other network devices
- Monitoring IoT Communications
  - Continuously monitoring IoT traffic to detect unusual patterns or potential security incidents
- **Microservices**
  - Microservices
    - Mini applications or services that work together to create a system
    - Perform specific functions with their own logic and adapters
  - Characteristics of Microservices

- Unlike monolithic applications, microservices consist of multiple endpoints that create a system
- Provide fine-grained control over application functions and services
- Commonly used for business functions, such as database access, messaging, user interface activities, and identification/authentication
- Frequently found in API-based communications (e.g., REST APIs), container-based infrastructures, and cloud-based deployments
- Benefits of Microservices
  - Simplify the information system, improve application performance, and reduce recovery times in disaster scenarios
  - Enhance control over communication traffic, allowing for better monitoring and load management
  - Enable automation and orchestration of services within an infrastructure
- API (Application Programming Interface)
  - Serves as a gateway to access microservices in the architecture
  - A software-level interface that allows users to connect to specific services
- Service Mesh
  - Dedicated infrastructure that simplifies service-to-service communications
  - Enhances resiliency and infrastructure support, particularly under heavy load
- API Gateway and Service Mesh Architecture
  - API Gateway
    - Acts as an entry point to access backend microservices

- Routes client requests to the appropriate microservices and performs protocol translations if necessary
- Provides service monitoring, health and status checks, security logging, and monitoring
- API Gateway Security Measures
  - API Keys
    - Used for non-sensitive microservice communications
  - Authentication Tokens
    - Implemented for sensitive communications
      - E.g., JSON Web Tokens, SAML, OpenID, OAuth
    - Example
      - A token translation service between gateways ensures secure authentication for sensitive microservice access
  - Monitoring Communications
    - Observes unknown or malicious activity in microservice traffic
- Service Mesh Architecture
  - Adds a data plane and control plane to manage and secure microservice communications
  - Data Plane
    - Moves application requests between microservices using sidecar proxies
  - Control Plane
    - Manages data plane policies and defines service mesh capabilities
    - Complements the API gateway with additional service and security capabilities

- Security Best Practices for Microservices
  - Access Control Policies
    - Enforce access control by default for all services in the service mesh
  - Privilege Management
    - Avoid configurations that require elevated privileges, preventing privilege escalation
    - Implement zero-trust principles by limiting privilege access (e.g., no root-level access for user accounts reaching into a microservice)
  - Network Segmentation
    - Segment networks for sensitive applications using microservices to control and monitor traffic for malicious activity
- **Embedded Systems**
  - Embedded Systems
    - Dedicated computing components within a larger device
    - Provide specific, focused functionality within devices like appliances, control systems, smartphones, automobiles, medical devices, and telecommunications
  - Characteristics of Embedded Systems
    - Often include computing components such as memory, processors, and circuit boards
    - Improve and extend functionality, efficiency, and convenience within larger systems
    - Act as microprocessors or microcontrollers for automated functions

- Example
  - A programmable logic controller in industrial control automates tasks like activating buttons or adjusting controls
- Risks and Vulnerabilities of Embedded Systems
  - Simplistic Firmware
    - Minimal complexity, easily manipulated
    - Designed primarily for functionality and automation, not security
    - Vulnerable to unauthorized control over components like processors, actuators, and valves
    - Safety and security become critical due to potential life-threatening implications
    - Example
      - In medical devices, a manipulated embedded system could lead to serious harm to patients
  - Common Attacks on Embedded Systems
    - User Interface Attack
      - Brute force or input manipulation to gain administrative or privileged access
    - Physical Attack
      - Manipulate inputs or remove the system from the device entirely
    - Sensor Attack
      - Tricks the system into sensing an action or input that wasn't actually performed
      - Example

- Manipulating a vending machine to dispense items without payment
- Output Attack
  - Manipulates components to alter the output, such as opening an electronic door lock
- Processor Attack
  - Direct or indirect targeting of memory or processor components
- Firmware Attack
  - Exploits vulnerabilities in firmware or installs rogue firmware on the embedded system
- Defense Strategies for Embedded Systems
  - Threat Modeling
    - Identify attack vectors, surfaces, and potential threats
    - Essential for understanding vulnerabilities in embedded systems
  - Traffic Isolation and Segmentation
    - Segregate embedded system traffic to avoid interference with other network devices
  - Application Firewall
    - Install on hosting devices (if applicable) to monitor and control communication with the embedded system
  - Defense in Depth
    - Layer physical, logical, and administrative controls to protect embedded systems
    - Example

- Use of physical security, such as enclosures, alongside network controls
- Wrapping or Encapsulation
  - Adds security features not natively supported by the embedded system
  - Example
    - Using TCP wrappers for additional control over data flow
- Manual Updates and Digital Signatures
  - Prevent untested or untrusted updates by manually verifying and using digitally signed firmware or updates
- Redundancy and Diversity Control
  - Ensure redundancy as part of business continuity and limit the diversity of embedded systems
  - Consistency aids in implementing effective policies and defense strategies
- Continuous Monitoring
  - Track status changes, unusual communications, and policy violations for timely identification of security concerns
- **High-Performance Computing**
  - High Performance Computing Systems (HPC)
    - Supercomputers that operate in parallel to solve complex mathematical and scientific problems
    - Typically designed for dedicated functions and high-volume data processing tasks
    - Utilized in advanced fields such as big data, data analytics, data mining, cryptocurrency, and medical imaging

- Often used in atmospheric research, applied physics, nuclear science, bioscience, and other fields requiring rapid calculations
- Example
  - High-performance computers are found in web search engines, healthcare, and energy sectors
- Purpose of HPC
  - Designed to handle millions of simultaneous tasks with advanced processors and parallel simulations
  - Commonly used in data centers and for research in areas such as seismology, pharmaceutical design, and cyber security
- Key Components of HPC
  - Requires extensive use of Graphics Processing Units (GPUs) for processing and rendering complex tasks
  - Equipped with numerous CPUs, often requiring large physical space and significant energy resources
- Challenges in Securing HPC
  - Large Footprint
    - Requires substantial space in server rooms or data centers for high-performance infrastructure
  - Energy Consumption
    - High electricity demands require system resiliency, including generators, UPS, and batteries
  - Data Separation
    - Sensitive research data requires extensive isolation and segmented access controls



- Geographical Dispersion
  - Users are often distributed globally, complicating identity and access management
- Confidentiality Risks
  - Open research and development activities create challenges with data confidentiality and unauthorized code use
- Compliance Issues
  - Import/export laws and regulatory factors may affect data handling and access control
- Unreviewed Code in R&D
  - Experimental code from research may cause system issues, such as denial-of-service attacks
- Security Measures for HPC
  - Threat Modeling
    - Essential to identify potential threats and vulnerabilities specific to HPC environments
  - Data Management
    - Data isolation and segmentation necessary due to vast amounts of sensitive data
  - Hardware Security Features
    - Implement security features on HPC servers to enforce trusted code execution
  - Multi-Factor Authentication (MFA)
    - Enhances identity verification, especially for geographically dispersed users

- Identity Management Policies
  - Effective policy for user identity and role management can reduce insider threats
- Compliance with Standards
  - Adhere to standards like NIST and OWASP for secure HPC architecture design
- Edge Computing Systems
  - Edge Computing Systems Overview
    - Provides computing and analytics resources close to the data source, also known as fog computing in cloud-based contexts
    - Found in sectors like energy, pharmaceuticals, food/beverage production, transportation, retail, and infrastructure
  - Purpose and Functionality
    - Moves computing resources closer to users or applications needing real-time access to data
    - Increases data availability and scalability by minimizing the need for traditional data centers
    - Relies on edge servers to provide computing infrastructure and serve data locally rather than via central servers
  - Edge Devices
    - Vary in purpose and terminology; may include mobile devices, routers, switches, and IoT devices
    - Examples include smart devices, medical devices, video cameras, and programmable interfaces
    - Example

- Edge devices may include sensors, smart watches, and smart glasses accessing data through edge servers
- Edge Computing Architecture
  - Edge devices connect to edge servers, which then link to cloud-based resources
  - Moves data processing closer to the user to improve interaction efficiency between devices and servers
  - Sometimes called Fog Nodes, Fog Servers, or Fog Computing when implemented in the cloud
- Benefits of Edge Computing
  - Increased Data Availability
  - Locally processes data, enhancing cloud-based resource performance
  - Improved Network Performance
  - Reduces bandwidth and network demands by caching data locally and sending data in chunks
  - Enhanced Data Protection
  - Minimizes the volume of data shared over the internet
- Risks of Edge Computing
  - Physical tampering and poor security in sensors and IoT devices
  - Different devices may require various levels of security controls, complicating baseline security measures
  - Limited remote management capabilities as devices often lack SSH or direct remote access
- Security Challenges

- Limited availability of standard endpoint security features (e.g., anti-malware, antivirus) in edge devices
- Potential attack vectors as edge devices can provide entry points into protected systems
- Security Best Practices for Edge Computing
  - Follow industry standards like NIST and OWASP for edge architecture guidance
  - Establish edge computing security policies, detailing device usage and security requirements
  - Change default accounts, passwords, and certificates on edge devices before deployment
  - Regularly update firmware and software to maintain security with vendor patches
  - Remove unnecessary protocols and services to minimize attack surface on edge servers
  - Segment edge computing traffic, using VLANs to separate it from Ops and Prod traffic

## Virtualization and Cloud Computing

Objectives:

- 3.5 - Assess and mitigate the vulnerabilities of security architectures, designs, and solutions
- 4.1 - Apply secure design principles in network architectures
  
- **Virtualization and Cloud Computing**
  - Virtualization and Cloud Computing
    - Critical for modern IT infrastructures, enhancing flexibility, scalability, and cost-efficiency
    - Introduces unique security risks that need careful management
  - Foundational Concepts of Virtualization
    - Includes virtual machines (VMs), hypervisors, and the support of cloud infrastructures
  - Containerization
    - Offers greater flexibility than VMs in deploying applications
    - Focus on security practices for container images and runtime
  - Cloud Deployment Models
    - Types include public, private, community, and hybrid clouds
    - Each model presents specific security challenges and use cases
  - Cloud Service Models
    - Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS)
    - Different security approaches required for each service model

- Shared Responsibility Model
  - Defines the security obligations of cloud providers and customers
  - Essential for choosing cloud services based on security needs
- Virtual Private Clouds (VPCs)
  - Private cloud within a public cloud, offering enhanced control and security
  - Discussion on VPC configuration and security measures
- Serverless Computing
  - Runs code without managing servers, simplifying operations but introducing security challenges
  - Focus on permission management, securing APIs, and other security practices
- **Virtualized Systems**
  - Virtualized Systems
    - Creation of software-based representations of physical components like servers, storage, applications, and networks
    - Enables resource optimization, centralized control, improved productivity, and scalability
  - Features of Virtualization
    - Virtual Machine (VM)
      - Software-created computers or components
    - Elasticity
      - Enables dynamic scaling of resources like CPU, memory, and storage based on demand
    - Hypervisor

- Connects virtual and physical components, enabling VM creation and management
- Types of Hypervisors
  - Type 1 Hypervisor
    - Installed directly on hardware (bare metal), acting as the primary OS with minimal attack surface. Often used in data centers
      - E.g., ESXi, vSphere
  - Type 2 Hypervisor
    - Runs on an OS (e.g., Windows, MacOS) as an application, allowing flexibility but with a larger attack surface
      - E.g., VMware Workstation, VirtualBox
- Use Cases for Hypervisor Types
  - Type 1
    - Ideal for data centers, providing high efficiency and security with dedicated hardware
  - Type 2
    - Commonly used for software testing, sandboxing, and skill development in isolated environments
- Drawbacks and Risks
  - Hardware Vulnerabilities
    - Defects or vulnerabilities in hardware affect both virtualized components and the hypervisor
  - Hypervisor Vulnerabilities
    - Unpatched hypervisors or VMs may compromise the entire virtual environment

- VM Escaping
  - Risk in Type 2 environments where a user can bypass the guest OS, potentially accessing and controlling the host OS
- Protection Mechanisms
  - Host critical functions on physical machines where feasible
  - Maintain updated virtual software and conduct regular monitoring of the virtual environment for threats
- **Containerization**
  - Purpose of Containerization
    - Provides a software-based representation of packaged files, libraries, and dependencies for hosted applications
    - Enables OS-level virtualization, isolating applications within containers that use the resources of the host OS through a container engine
    - Commonly used in microservices architectures for efficient resource sharing and deployment
  - Benefits of Containers
    - Consistent configuration for speed, efficiency, flexibility, and scalability
    - Isolation from other infrastructure, making them lightweight, fast, portable, and minimally impactful on OS resources
    - Supports reusable images for portability across various environments
  - Containers vs. Virtual Machines
    - Containers
      - Use a container engine for OS-level virtualization
      - Share the host OS resources and rely on the host's configuration, increasing efficiency



- Example
  - Docker, AWS Elastic Container Service (ECS), Google Kubernetes Engine
- Virtual Machines
  - Use a hypervisor to provide isolated resources to each VM instance, requiring an OS per VM
  - Higher resource demands due to separate OS installations for each VM
- Key Containerization Components
  - Container Engine
    - Facilitates container operation, allowing apps to share OS resources while managing isolation
  - Common Container Software
    - Docker (popular containerization platform)
    - Kubernetes (container orchestration)
    - ECS (AWS's container service)
- Containerization Risks
  - Vulnerabilities in hosted applications, including malware or unprotected embedded data
  - Risks from inter-container communications and identification/authentication weaknesses
  - Inherited vulnerabilities from the host OS or engine, increasing susceptibility to attacks
  - Unpatched software and outdated configurations leading to security issues
- Security Considerations for Containers

- Group sensitive containers separately to avoid data exposure with non-sensitive containers
  - Implement hardware protections, like Trusted Platform Module (TPM) for hardware-level security
  - Reduce the host OS attack surface by minimizing unnecessary services and applications
  - Employ robust access controls and authentication mechanisms for both containers and host OS
  - Secure registry keys, APIs, and network communications with encryption
  - Ensure regular patching and updates for the container engine, host OS, and containerized applications
- **Cloud Deployment Models**
    - Cloud Computing Overview
      - Collection of scalable resources and services accessible over a network
      - Provides computing resources from nearly any location with internet access
      - Reduces on-site hardware needs, increasing scalability, performance, and data accessibility
    - On-Premise (On-Prem) and Off-Premise (Off-Prem) Deployments
      - On-Prem
        - Cloud infrastructure and software hosted and maintained locally by the organization's administrators
        - Resources are accessible only within the organization's premises
      - Off-Prem
        - Cloud infrastructure hosted by third-party providers

- E.g., AWS, Google Cloud, Microsoft Azure
- Users and administrators access resources over the internet, often through secure connections like VPN
- Cloud Deployment Models
  - Public Cloud
    - Cloud-based services available to any customer over an external network, typically the internet
    - Examples
      - Public storage services, Google Drive, Dropbox, and Office 365
  - Private Cloud
    - Services available only to a single organization, not exposed to the public
    - Can be on-prem or off-prem, depending on whether the organization or a third party hosts it
  - Community Cloud
    - Shared services used by two or more organizations, typically with shared goals or requirements
    - Often includes a service level agreement (SLA) between organizations
  - Hybrid Cloud
    - Combination of two or more deployment models, most commonly a mix of public and private cloud services
    - Example

- An organization uses a private cloud for sensitive data and a public cloud for less sensitive applications
- Security and Risk Considerations for Cloud Models
  - Data Privacy
    - Ensure governance, regulatory, and compliance standards are maintained for data types in the cloud
  - Attack Surface
    - Private Cloud
      - Limited to internal threats and requires focus on internal security controls
  - Public Cloud
    - Increased attack surface due to exposure to external internet threats
  - Hybrid Cloud
    - Combines both internal and external threat models, requiring detailed security configurations
  - Community Cloud
    - Includes both external and internal threats, often shared among organizations with common objectives
- Resource and Capability Requirements
  - Determine resources needed, such as API dependencies or external services, to decide between public and private cloud
  - Establish security requirements and build security controls to align with system, business, and security objectives
- **Cloud Service Models**

- Cloud Computing Overview
  - Provides system services and resources over a network, accessible globally
  - Enhances scalability, data accessibility, and performance, while reducing physical hardware needs
- Service Models in Cloud Computing
  - Integrated into deployment models (public, private, hybrid, community) to create an infrastructure for specific services
- Infrastructure as a Service (IaaS)
  - Provider Responsibility
    - Manages and maintains hardware, networking, storage, and often the hypervisor
  - Customer Responsibility
    - Manages the operating system, applications, data protection, and access controls
    - Example
      - Leasing virtual machines and storage space from Amazon Web Services or Google Cloud Platform
- Platform as a Service (PaaS)
  - Provider Responsibility
    - Manages hardware, hypervisor, networking, and operating system
  - Customer Responsibility
    - Manages applications, access controls, and data
    - Example

- Using Google App Engine for application development without managing underlying OS
- Software as a Service (SaaS)
  - Provider Responsibility
    - Manages entire infrastructure from hardware to application
  - Customer Responsibility
    - Manages data and access controls
    - Example
      - Using software applications like Google Drive, Office 365, or streaming platforms where data is uploaded and accessed by end users
- Security as a Service (SECaaS)
  - Provides security services directly from the cloud
    - Examples include LifeLock identity protection, cloud-based malware scanners, and real-time threat monitoring services
- Cloud Access Security Broker (CASB)
  - Sits between the cloud user and cloud services to enforce security policies and protect cloud assets
  - Functions as a proxy, enforcing security in areas such as
    - Data security and data loss prevention
    - Compliance with governance, regulations, and control standards
  - Threat protection and security integration
    - Example
      - CASB may filter incoming and outgoing data traffic to prevent unauthorized access to sensitive data

- **Shared Responsibility Model**

- Purpose of the Shared Responsibility Model
  - Establishes clear guidelines for responsibilities between customer and cloud service provider (CSP)
  - Primarily used in cloud environments such as AWS, Azure, Google Cloud Platform, VMware, and IBM
  - Ensures both parties know their roles and responsibilities in securing the cloud infrastructure and services through a service level agreement (SLA)
- Key Components of the Shared Responsibility Model
  - Security of the Cloud (Provider's Responsibility)
    - CSP maintains and protects the infrastructure, including hardware, networking, and data centers
  - Security in the Cloud (Customer's Responsibility)
    - Customer responsibilities vary by service model (IaaS, PaaS, SaaS), defining the scope of responsibility for securing data and other cloud configurations
- Service Models and Customer Responsibilities
  - Infrastructure as a Service (IaaS)
    - Customer Responsibilities
      - Operating systems, applications, access controls, data security, client-side encryption
    - CSP Responsibilities
      - Compute, storage, networking infrastructure, physical security
  - Platform as a Service (PaaS)

- Customer Responsibilities
  - Applications, identity and access management, data encryption as needed
- CSP Responsibilities
  - OS, networking, platform security
- Software as a Service (SaaS)
  - Customer Responsibilities
    - Data security, access control
  - CSP Responsibilities
    - Entire stack, from application down to physical infrastructure
- Types of Service Level Agreements (SLAs)
  - Customer-Level SLA
    - Agreement covering services used by a single customer
    - Common for customized or proprietary cloud services
  - Service-Level SLA
    - Agreement detailing services shared by multiple clients
    - Example
      - SLA covering general use of a SaaS product accessible to multiple customers
- Exam Focus for Shared Responsibility Model
  - Understanding responsibilities for each service model
    - IaaS, PaaS, SaaS
  - Knowing the differences between customer-level SLA and service-level SLA



- Recognizing the need for SLAs to document shared responsibilities between CSP and customer
- **Virtual Private Cloud**
  - Purpose of Virtual Private Cloud (VPC)
    - A logically isolated virtual network within a public cloud environment
    - Provides a private, secure area within the cloud, isolated from the public cloud
    - Allows businesses to perform cloud operations with enhanced control and security
  - Features of VPCs
    - Regions and Availability Zones (AZs)
      - Regions are geographical locations, and AZs are isolated areas within each region
      - Supports high availability by isolating VPCs across multiple AZs
    - Subnets
      - Logically isolate resources within the VPC, supporting different levels of security and segmentation
    - Route Tables
      - Defines routing paths for network traffic within the VPC, facilitating controlled communication between subnets
    - Gateways and Endpoints
      - Used to control access to the VPC, including internet gateways, VPN gateways, and NAT gateways for secure connectivity
    - Security Groups and Network Access Control Lists (NACLs)

- Security groups act as virtual firewalls controlling traffic to and from resources within the VPC
- NACLs provide network-level access controls, filtering traffic between subnets and external connections
- Connection Methods for VPCs
  - Direct Connect
    - A high-speed, dedicated connection between on-premises and VPC, typically used by data centers
  - VPC Peering
    - Allows connectivity between two VPCs, enabling resource sharing under a single AWS or cloud account
  - VPN Connection
    - Uses a VPN gateway for secure, encrypted connectivity between the VPC and on-premise networks over the internet
- Benefits of Using VPCs
  - Enhanced Security
    - Logical isolation from the public cloud, enabling better control over network traffic and security
  - Scalability and Flexibility
    - Dynamic adjustment of resources to meet demand, helping optimize costs
  - Customizable Networking
    - Control over subnetting, IP addressing, routing, and network configurations
  - Cost Efficiency

- Costs vary based on resources used, allowing businesses to optimize based on specific needs
- Best Practices for VPCs
  - Network Segmentation
    - Use subnets and security groups to create isolated environments for different applications or user groups
  - Least Privilege
    - Limit access to resources within the VPC based on role and function to reduce security risks
  - Strong Access Controls
    - Implement robust authentication and access controls to prevent unauthorized access
  - Encryption
    - Encrypt data both at rest (e.g., in S3 storage) and in transit to protect sensitive information
  - Monitoring and Logging
    - Utilize tools like CloudWatch, or a Security Information and Event Management (SIEM) solution for real-time monitoring, incident detection, and response
  - Regular Audits
    - Conduct regular security assessments, compliance checks, and performance reviews to ensure continuous improvement and adherence to regulations
- **Serverless Computing**
  - Purpose of Serverless Computing

- Provides computing resources on an as-needed or on-demand basis, eliminating the need for infrastructure management
- Enables faster application development by shifting infrastructure responsibilities to the cloud service provider
- Reduces costs, as users pay only for the resources they use
- Also known as Function as a Service (FaaS), where cloud providers manage the execution environment
- Benefits of Serverless Computing
  - Scalability
    - Resources are automatically scaled up or down based on demand
  - Cost-Effectiveness
    - Only pay for the resources utilized during execution, minimizing idle infrastructure costs
  - Speed of Development
    - Removes the need for infrastructure management, allowing developers to focus on application development
  - Reduced Infrastructure Management
    - Provider manages servers, execution, and resource allocation
- Risks and Vulnerabilities in Serverless Computing
  - Expanded Attack Surface
    - Attack surface spans the provider's infrastructure, introducing potential unknown vulnerabilities
    - Some attack vectors may vary or be harder to detect due to lack of visibility into the provider's infrastructure
  - Incompatibility with Traditional Security Solutions

- Traditional security measures may not work due to limitations in access controls, network monitoring, and filtering capabilities in a serverless architecture
- Performance and Availability Concerns
  - If functions are infrequently used, there may be delays or timeouts due to resources spinning up, impacting availability
- Reduced Control Over Environment
  - Limited access to underlying infrastructure can reduce the ability to fully secure and configure the environment
- Data Security Challenges
  - Sensitive data may be exposed if stored or processed without sufficient control within the serverless environment
- Mitigations for Serverless Computing Security
  - Clear Responsibility
    - Define and document security responsibilities between the organization and the cloud service provider, ideally within a service level agreement (SLA)
  - Minimize Code and Microservices
    - Use smaller codebases and efficient microservices to improve performance and control while maintaining security within the application
  - Limit Sensitive Data Use
    - Avoid or minimize processing and storage of sensitive data in serverless environments to reduce exposure risks
  - Architecture Design for Security



# ISC2 CISSP

## (Study Guide)

- Include robust design considerations for confidentiality, integrity, and availability when planning serverless deployments

## Cryptographic Solutions

Objective 3.6: Select and determine cryptographic solutions

- Cryptographic Solutions
  - Cryptographic Solutions
    - Essential for ensuring confidentiality, integrity, and authenticity of data
    - Plays a crucial role in securing communication and data storage
  - Foundational Cryptography Concepts
    - Encryption, decryption, and goals of cryptography
      - Confidentiality, integrity, authentication, non-repudiation
  - Cryptographic Methods
    - Symmetric and asymmetric encryption, hashing, digital signatures
    - Application in real-world scenarios to mitigate risks like data breaches and unauthorized access
  - Symmetric Ciphers
    - Use the same key for both encryption and decryption
    - Discussion on strengths, weaknesses, and appropriate use cases
  - Asymmetric Ciphers (Public-Key Cryptography)
    - Uses two keys
      - A public key for encryption and a private key for decryption
    - Used for secure key exchange, digital signatures, and authentication
  - Quantum Cryptography
    - Adaptation of cryptography in the context of quantum computing
    - Basics of how quantum cryptography works and its implications

- Hash Functions
  - Use of hashing to verify data integrity
  - Common hash functions like Message Digest and Secure Hash Algorithm
- Cryptographic Key Management
  - Importance of managing cryptographic keys securely
  - Key lifecycle management, differences between manual and automated key management
- Digital Signatures and Certificates
  - Use of digital signatures to verify authenticity and integrity of data
  - Role of certificates and certificate authorities in establishing trust
- Public Key Infrastructure (PKI)
  - Framework for managing digital certificates and public keys
  - Components include certificates, certificate authorities, certificate revocation lists (CRLs)
- **Understanding Cryptography**
  - Purpose of Cryptography
    - Protect sensitive information in three data states
      - Data in use, data in transit, and data at rest
    - Guarantees confidentiality and integrity
    - Does not provide availability
    - Provides additional services such as authentication and non-repudiation
  - Non-repudiation
    - Ensures that actions or data origination cannot be denied by a subject
    - Provides undeniable proof that data actions were performed by a specific entity



- Key Cryptographic Terms
  - Algorithm
    - Mathematical calculations used to encrypt and decrypt messages
  - Cipher
    - Specific type or brand of algorithm for encryption and decryption
    - Types of Ciphers
      - Substitution Cipher
        - Replaces one character with another
      - Transposition Cipher
        - Rearranges characters or blocks of characters into a different order
  - Key
    - Information used to encrypt and decrypt messages, such as a passphrase or password
  - Encryption and Decryption
    - Encryption converts plain text to ciphertext for secure transmission
    - Decryption converts ciphertext back to readable plain text using the same key and cipher
- Concepts in Encryption
  - Confusion
    - Ensures the key cannot be discovered by analyzing plaintext and ciphertext
  - Diffusion

- Alters ciphertext significantly when plaintext changes, making key discovery harder
- Concealment Cipher
  - Hides a message within another message, file, or image
- Steganography
  - Conceals a message within a media file, such as an image or photograph
- Digital Watermarking
  - Embeds visible or invisible text, message, or images into digital content, often for copyright protection
- Cryptographic Life Cycle Steps
  - Select Method
    - Choose cryptography type
      - E.g., shared key or public key
  - Select Cipher
    - Choose algorithm based on security needs, industry standards, and chosen method
  - Select Key and Key Length
    - Longer keys enhance security but may impact performance
  - Select Mode (if applicable)
    - Operating mode of the cipher for additional security functions, where available
- Cryptography Security Principles
  - Finite Life of Ciphers and Keys

# ISC2 CISSP

## (Study Guide)

- Ciphers and keys become insecure over time due to advances in computational power (Moore's Law)
  - Regular key rotation and cipher updates ensure security
  - Kerckhoff's Principle
    - Security should remain intact even if everything about the cryptosystem except the key is public knowledge
    - Emphasizes that security should not rely on secrecy of the system's design, only the key
- **Cryptographic Methods**
  - Symmetric Cryptography
    - Uses a single shared key for both encryption and decryption
    - Known as secret key cryptography and is commonly used today
    - Example
      - Accessing a wireless network with a pre-shared key like a passphrase or password
    - Encrypts and decrypts messages using the same key for both plaintext and ciphertext
  - Types of Symmetric Ciphers
    - Block Cipher
      - Encrypts specified blocks or chunks of data, typically in 64 or 128-bit blocks
      - Uses rounds of encryption for each block
    - Stream Cipher

# ISC2 CISSP

## (Study Guide)

- Encrypts each character in the message individually, creating a continuous stream
- Synchronous Stream Cipher requires perfect synchronization between sender and receiver
- Self-Synchronizing Stream Cipher can automatically sync with sender after processing a set number of ciphertext characters
- Substitution vs. Transposition Ciphers
  - Substitution Cipher
    - Swaps one character for another
  - Transposition Cipher
    - Rearranges characters or blocks of characters
    - Monoalphabetic Approach uses one cipher alphabet and fixed substitutions
    - Polyalphabetic Approach uses multiple cipher alphabets and substitutions
  - One-time Pad
    - Uses unique substitution alphabets for each plaintext character
    - Requires key as long as the message itself for security
    - Common examples include Caesar, Vigenère, and Vernam ciphers
- Operating Modes of Block Ciphers
  - Electronic Codebook (ECB) Mode
    - Simplest and least secure mode
    - Produces identical ciphertext blocks for identical plaintext blocks, making patterns easy to detect
  - Cipher Block Chaining (CBC) Mode

# ISC2 CISSP

## (Study Guide)

- Uses an initialization vector (IV) for the first block to avoid repeated patterns
- Each plaintext block is XORed with the previous ciphertext block
- Cipher Feedback (CFB) Mode
  - A streaming version of CBC, processing data in real time using memory buffer blocks
- Output Feedback (OFB) Mode
  - Similar to CFB but uses a seed value instead of previous ciphertext blocks
  - Reduces pattern propagation in ciphertext
- Counter (CTR) Mode
  - Uses an incrementing counter for each plaintext block
    - No chaining or dependency, offering higher security and better performance
- Asymmetric Cryptography
  - Also known as public key cryptography
  - Uses a public-private key pair for encryption and decryption
  - Eliminates the need to protect a shared single key
  - Public key is openly available; private key must be kept secure and not shared
  - Example
    - Encrypts with the private key and decrypts with the public key, or vice versa
- Important Cryptographic Terms
  - Algorithm

- The mathematical calculation used to encrypt and decrypt messages
- Cipher
  - Specific type of algorithm for encryption and decryption
- One-time Pad
  - Encryption with a unique key for each plaintext character
- Initialization Vector (IV)
  - Block of random bits used in some modes to ensure unique encryption output
- **Symmetric Ciphers**
  - Symmetric Key Cryptography Overview
    - Uses a single shared key between parties for encryption and decryption
    - Also known as secret key cryptography
  - Data Encryption Standard (DES)
    - Developed from IBM's Lucifer cipher
    - Uses predefined substitution and transposition functions to create 64-bit ciphertext blocks
    - Operates with a 56-bit key and 16 rounds of encryption
    - Supports all five operating modes (ECB, CBC, CFB, OFB, CTR)
    - Considered weak and outdated; not recommended for use
  - Triple DES (3DES) or Triple Data Encryption Algorithm (TDEA)
    - Applies DES encryption three times to each plaintext block (48 rounds of encryption)
    - Key sizes
      - 168-bit, 112-bit, or 56-bit with 64-bit block size

- Modes
  - Triple E
    - Encrypts data three times
  - Triple EDE
    - Encrypts, decrypts, and re-encrypts data
  - Triple E2 and EDE2
    - Uses two keys (first and third round with the same key, second with a different key)
  - Triple E3 and EDE3
    - Uses three different encryption keys
- International Data Encryption Algorithm (IDEA)
  - Operates on 64-bit blocks and uses a 128-bit key
  - Divides the key into 52 subkeys for encryption operations
  - Supports all five operating modes
  - Commonly used in Pretty Good Privacy (PGP)
- Blowfish
  - 64-bit block cipher designed as a DES replacement
  - Key sizes range from 32 to 448 bits with 16 encryption rounds
  - Open-source, freely accessible algorithm widely used globally
- Advanced Encryption Standard (AES)
  - Based on the Rijndael cipher and developed by NIST in 2001
  - Supports key and block sizes of 128, 192, and 256 bits
    - 128-bit
      - 10 rounds of encryption
    - 192-bit

# ISC2 CISSP

## (Study Guide)

- 12 rounds of encryption
  - 256-bit
    - 14 rounds of encryption
  - Mandated by FIPS 197 for U.S. government use for data protection above unclassified levels
  - Approved for encryption of sensitive data up to top secret levels in the U.S. government
- Rivest Ciphers (RC or ARC)
  - RC2
    - 64-bit block cipher with 8 to 1024-bit keys and 16 encryption rounds
  - RC4
    - Stream cipher with variable key lengths (48 to 2048 bits) and one encryption round
    - Originally a trade secret algorithm, leaked in the mid-1990s
  - RC5
    - Supports 32, 64, or 128-bit blocks with keys from 0 to 2040 bits; recommended key strength is 64 bits
  - RC6
    - Uses a 128-bit block size and key lengths of 128, 192, and 256 bits; 128-bit key recommended
- Key Takeaways
  - Familiarize with DES, 3DES, IDEA, Blowfish, AES, and Rivest ciphers
  - Know key sizes, block sizes, and number of encryption rounds where specified



- Recognize which algorithms and modes are outdated and discouraged for use
- **Asymmetric Ciphers**
  - Asymmetric Key Cryptography Overview
    - Utilizes a public and private key pair for encryption and decryption
    - Also known as public key cryptography
    - The private key is always protected and not shared
  - Diffie-Hellman Key Exchange
    - An asymmetric cipher that enables secure key exchange
    - Complements symmetric ciphers by securely sharing symmetric keys
    - Does not provide encryption, only facilitates key exchange
    - Uses forward secrecy
      - Generates unique session keys for each session, discarding keys after use
  - Mathematics
    - Uses two prime numbers to generate private keys for both ends
    - Private keys are used to create public keys, which are then exchanged
    - Public keys are used to create a shared secret key for secure sessions
  - Rivest-Shamir-Adleman (RSA)
    - Public key algorithm that enables key encryption, decryption, authentication, and digital signatures
    - Created in 1977, renowned for its secure nature
    - Strength relies on the use of two large prime numbers (non-discrete logarithms)
    - RSA remains unbroken and secure due to its use of prime numbers

- Elliptic Curve Cryptography (ECC)
  - Used for encryption, digital signatures, and key exchange
  - Known for its efficiency and high security with shorter key lengths
  - A 1024-bit RSA key strength can be achieved with only a 168-bit ECC key
  - Provides superior performance and security efficiency compared to RSA
- ElGamal Algorithm
  - Based on the Diffie-Hellman key exchange, used for encryption, digital signatures, and key exchange
  - Adds additional security to Diffie-Hellman by publicly exchanging secret keys
  - Drawback
    - Doubles message size with encryption, causing network latency
  - Example
    - A 500-bit message encrypted with ElGamal becomes 1000 bits
- Key Takeaways
  - Know each asymmetric cipher and their primary functions (encryption, key exchange, digital signatures)
  - Understand the strengths, weaknesses, and key characteristics of Diffie-Hellman, RSA, ECC, and ElGamal
- **Quantum Cryptography**
  - Overview of Quantum Cryptography
    - Based on the theory of quantum computing, applying quantum mechanics to perform complex computations

- Quantum mechanics studies properties at the atomic and subatomic particle level, analyzing information at the most basic level
- Quantum cryptography uses quantum computing's powerful capabilities to break current cryptographic algorithms
- Quantum supremacy
  - Quantum computers can solve problems that classical computers cannot
- Quantum Computers
  - Quantum computers operate using quantum bits, or qubits, as the basic unit of measurement in quantum information science
  - Qubits hold twice as much information as traditional binary bits, using superpositions that place one bit over another
  - Quantum computers have immense computational power compared to traditional computers
- Impact of Quantum Cryptography on Current Cryptography
  - Quantum cryptography will replace classical algorithms (e.g., RSA, ElGamal, ECC, AES) as they will become obsolete with quantum computing advancements
  - NIST is working on quantum-resistant algorithms for a post-quantum world to secure key establishment schemes, digital signatures, and key exchanges
- Key Features in Quantum Cryptography
  - Key Distribution (QKD)
    - Facilitates the sharing of secret keys, similar to symmetric key cryptography

- Quantum Coin Flipping (OCF)
- Establishes a trusted communication path between untrusted parties, similar to Diffie-Hellman Key Exchange
- Focuses on the probability to prevent either side from maliciously influencing the outcome of the communication channel setup
- Exam Focus Points
  - Quantum cryptography is grounded in quantum mechanics
  - Quantum cryptography aims to replace classical cryptographic algorithms with quantum-resistant alternatives
  - Familiarize with key distribution (QKD) and quantum coin flipping (OCF) as they relate to secure key exchange and communication
- **Hash Functions**
  - Overview of Hash Functions
    - Hashing creates a unique value (message digest) from a block of data using a hash algorithm
    - Produces a fixed-size data output from any input size
    - Common hash sizes
      - 160 bits or 256 bits, depending on the function used
    - Message digests verify data integrity by allowing comparisons of the hash values before and after data processing
  - Hashing Process
    - Data is run through a hash function to produce a message digest (also called a hash, hash value, or hash digest)
    - Even minor changes in data will generate a different hash value, indicating modification

- Common Hash Algorithms
  - SHA (Secure Hash Algorithm)
    - Found in FIPS publication 180-4 for Secure Hash Standards
    - Generates fixed-length hashes from variable-length inputs
  - Variants
    - SHA-1
      - 160-bit digest, 512-bit block size
    - SHA-224
      - 224-bit digest, 512-bit block size
    - SHA-256
      - 256-bit digest, 512-bit block size
    - SHA-384
      - 384-bit digest, 1024-bit block size
    - SHA-512
      - 512-bit digest, 1024-bit block size
    - SHA-512/224 and SHA-512/256
      - Use 512-bit block size but reduce digest to 224 or 256 bits, respectively
- MD (Message Digest)
  - Variants
    - MD2
      - 128-bit digest, 128-bit blocks
    - MD4
      - 128-bit digest, 512-bit blocks, fewer rounds of processing than MD5

- MD5
  - 128-bit digest, 512-bit blocks, performs three rounds of processing for enhanced security
- HAVAL (Hash of Variable Length)
  - Based on MD5 but uses 1024-bit blocks instead of 512-bit
  - Digest can vary between 128, 160, 192, 224, or 256 bits
- RIPEMD (Race Integrity Primitives Evaluation Message Digest)
  - Created as an alternative to SHA and MD for additional security
  - RIPEMD-128
    - 128-bit digest
  - RIPEMD-160
    - 160-bit digest, improved version for stronger hashing
- Key Terms
  - Message Digest
    - The output of a hash function, providing a unique representation of input data
  - Integrity Verification
    - Detects changes by comparing hash values before and after any data manipulation
  - Forward Secrecy
    - Used in cryptographic algorithms like Diffie-Hellman to ensure keys are unique to each session and cannot be reused
- **Cryptographic Key Management**
  - Crypto Policy and Crypto Period

# ISC2 CISSP

## (Study Guide)

- Define a cryptographic life cycle (Crypto period) to outline key validity
- Duration of key validity depends on organizational needs
  - E.g., 30 days, one year, two years
- Follow any regulatory or industry standards for key management based on industry (financial, medical, government)
- Key Creation and Security
  - Key must be long enough to protect the information but not unnecessarily long
  - Example
    - AES 128-bit key is sufficient for most industries, but AES 256-bit is required for top secret information in the U.S. government
  - Longer keys increase encryption and decryption time, affecting availability
  - Automate key generation to reduce errors
- Key Distribution
  - Symmetric keys should be distributed offline or using a secure key distribution algorithm
    - E.g., Diffie-Hellman Key Exchange
  - Use encrypted communication channels or trusted paths for key distribution
- Key Storage
  - Ensure keys are accessible when needed and protected at the same level as the data they secure
  - Encrypt keys in storage and protect them based on data classification
    - E.g., confidential, top secret

- Store keys offline or in a Key Escrow for best protection
- Cryptographic keys must be included in business continuity and disaster recovery plans
- Key Escrow
  - Third-party service storing backup copies of keys, digital signatures, and certificates
  - Account for emergency recovery needs to access keys quickly
- Split Knowledge
  - Uses multiple parties to manage access, ensuring no single party has full control over a cryptographic function
  - Similar to separation of duties, two-person integrity
- Key Rotation
  - Cryptographic keys, signatures, etc., should have a finite crypto period
  - Rotate keys frequently, especially those exposed externally or used for sensitive data
  - General guidance
    - Rotate keys annually, but high-sensitivity keys may require more frequent rotation
- Key Revocation and Destruction
  - Policy should define revocation process for keys no longer needed or compromised
  - Emergency Revocation
    - Account for scenarios requiring immediate revocation
  - Destruction
    - Destroy keys per industry or regulatory standards



- Keep accurate records of destroyed keys for legal or investigative purposes
- **Digital Signatures and Certificates**
  - Digital Signatures
    - Goal is to replicate a physical signature using cryptography
    - Provides
      - Authentication
        - Verifies the message originated from a specific subject
      - Non-repudiation
        - Proof that the signer cannot deny their signature
      - Integrity
        - Ensures data was not modified after signing through hashing
    - Standards to know
      - FIPS 186-4
        - Specifies U.S. government-approved algorithms for digital signatures
      - DSA
        - Digital Signature Algorithm, based on ElGamal Cipher, specified in FIPS 186-4
      - RSA DSA
        - Uses RSA, detailed in ANSI X9.31, supports encryption, key distribution, and digital signatures
      - ECDSA

# ISC2 CISSP

## (Study Guide)

- Elliptic Curve Digital Signature Algorithm, a variant of DSA, specified in ANSI X9.60, more efficient with shorter keys than RSA and DSA
- Hashed Message Authentication Code (HMAC)
  - Uses a hash and shared secret key to create a partial digital signature
  - Provides integrity but not non-repudiation
  - Used with SHA-2 and SHA-3 for faster performance in scenarios where non-repudiation is not required
  - Shared secret key prevents HMAC from achieving non-repudiation
- Creating and Verifying Digital Signatures
  - Creating
    - Data is hashed to create a message digest
    - Digest is sent through an asymmetric algorithm with the private key, creating the digital signature
  - Verifying
    - Data is re-hashed and compared with a decrypted hash from the digital signature
    - Sender's public key is used in the asymmetric algorithm
    - Matching hashes confirm authenticity; mismatched hashes indicate forgery
- Digital Certificates
  - Electronic document that validates identity of the certificate holder
  - Signed by a Certificate Authority (CA) to confirm the certificate holder's identity
  - Used within Public Key Infrastructure (PKI)

- X.509 defines standard attributes and requirements for digital certificates
  - Issuer details, serial number, version, signature algorithm, key length, validity period, subject's name, and public key
- Certificate Signing Request (CSR)
  - Information provided to the CA to issue the certificate
- Drawbacks and Mitigations
  - Hash Collision
    - When two different messages produce the same hash, compromising integrity
  - Mitigation
    - Use modern hash algorithms (SHA-2, SHA-3) proven to resist collisions
  - Key Disclosure
    - If the private key is exposed, messages can be forged
  - Mitigation
    - Protect the private key, use it only for digital signatures, avoid use for general encryption
  - Compromised CA
    - If an attacker spoofs the CA, certificates can be forged
  - Mitigation
    - Use a proven and trusted CA with a reputation for secure certificate issuance
- **Public Key Infrastructure (PKI)**
  - PKI Purpose
    - Provides assurance of a claimed identity through digital certificates

- Offers authentication, integrity, and non-repudiation
- Digital Certificate
  - Electronic document with certificate holder's information and digital signature of the issuer
  - Includes
    - Integrity from the hash
    - Non-repudiation from the digital signature
- PKI Components
  - Certificate Authority (CA)
    - Trusted third-party entity for both sender and receiver
    - Manages all PKI certificates by issuing, revoking, and providing certificate status
    - Requires proof of identity before issuing a digital certificate
  - Registration Authority (RA)
    - Trusted entity assisting the CA with identification verification
    - Processes identification requests on behalf of the CA
  - Certificate Signing Request (CSR)
    - Contains identity information and subject's name
    - Signed with the subject's private key to prove identity
    - Provided to the CA for certificate creation in X.509 format
- PKI Certificate Creation Process
  - Step 1
    - Subject creates a CSR and signs it with a private key
  - Step 2
    - CSR and public key provided to CA

- Step 3
  - CA verifies identity (or passes to RA for verification)
- Step 4
  - CA creates a digital signature using the subject's public key and CA's private key
- Step 5
  - PKI certificate created in PKCS #10 format and issued to subject
- Certificate Validation and Verification
  - Certificate must be validated by the CA each time it is used to ensure it remains current and not revoked
  - Methods of Verification
    - Certificate Revocation List (CRL)
    - Lists all certificates revoked by the CA
    - Downloaded and kept offline; must be updated regularly
  - Online Certificate Status Protocol (OCSP)
    - Real-time verification through OCSP client and OCSP responder on the CA

## Cryptanalytic Attacks

### Objectives:

- 3.5 - Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements
- 3.7 - Understand methods of cryptanalytic attacks
- **Cryptanalytic Attacks**
  - Cryptanalytic Attacks
    - Exploits vulnerabilities within cryptographic systems
    - Essential knowledge for information security professionals and the CISSP exam
  - Vulnerabilities in Cryptographic Systems
    - Weaknesses that can compromise the security of cryptographic systems
    - Examples include improper key generation and weak random number generators
  - Types of Cryptanalytic Attacks
    - Brute-force Attacks
      - Systematically trying every possible key until the correct one is found
    - Known Plaintext Attacks
      - Attacker has access to both plaintext and ciphertext, which can help deduce the encryption key

- Ciphertext-only Attacks
  - Attacker attempts to decrypt information with only access to encrypted data
- Implementation Attacks
  - Exploit weaknesses in how encryption is implemented, not in the algorithm itself
- Side-channel and Timing Attacks
  - Target the environment around the encryption process, bypassing traditional cryptographic defenses
- **Vulnerabilities in Cryptographic Systems**
  - General Cryptography Risks
    - Inherent Threats
      - Present throughout the encryption-decryption process
    - Plaintext, Cipher, and Ciphertext Risks
      - Weak ciphers and algorithms make plaintext easier to compromise
      - Short, non-random keys increase vulnerability
      - Attacks on ciphertext can lead to plaintext compromise
    - Algorithm Choice
      - Use industry-standard, open algorithms rigorously tested by experts
  - Key Risks
    - Algorithm Aging
      - Advances in processing power make old algorithms breakable
    - Moore's Law

- Microchip processing power doubles every two years, reducing security lifespan
- Quantum Computing
  - Expected to break modern cryptographic algorithms eventually
- Protocol Vulnerabilities
  - Strong algorithms can be weakened by flawed protocols
  - Example
    - SSH and HTTPS rely on underlying encryption (e.g., OpenSSL) which may have vulnerabilities
- Implementation Weaknesses
  - Lifecycle Maintenance
    - Protections weaken over time, requiring regular lifecycle checks
  - Key Management Automation
    - Automate creation and distribution of keys to reduce human error
  - Consistent Updates
    - Regularly revisit cryptographic implementations for sufficient data protection
- Key Management Risks
  - Key Strength
    - Use long, random keys to ensure security and unpredictability
  - Secure Key Storage & Usage
    - Prevent key reuse and rotate keys periodically
  - Key Lifecycle Management
    - Destroy expired keys to avoid misuse or replay attacks
    - Match key protection level to the data's sensitivity



- E.g., Confidential data needs confidential-level key protection
  - Bottom Line for Exam
  - Understand Weaknesses
    - Know vulnerabilities in algorithms, protocols, and implementation
  - Comprehend Key Risks
    - Recognize the importance of strong key management and regular lifecycle review
- **Cryptanalytic Attacks - Part 1**
  - Purpose of Cryptanalytic Attacks
    - Goal
      - Compromise cryptographic systems to uncover the key
    - Focus Area
      - Plaintext, ciphertext, key, and potentially the algorithm/cipher
  - Key Attack Types and Their Mechanisms
    - Known Plaintext Attack
      - Attempt to uncover the key by analyzing known plaintext and its ciphertext
    - Attack types
      - Brute Force Attack
        - Attempt every possible key or password combination
    - Linear Cryptanalysis
      - Uses linear math equations for statistical analysis of a cipher

- Focuses on the relationship between plaintext and ciphertext to approximate the key
- Meet in the Middle Attack
  - Encrypts and decrypts data using all possible key combinations
  - Effective against ciphers with multiple rounds of encryption
- Chosen Plaintext Attack
  - Attacker selects specific plaintext, encrypts it, and analyzes the resulting ciphertext
  - Benefit
    - Narrows down the focus to a portion of the message, saving time and resources
  - Attack types
    - Differential Cryptanalysis
      - Analyzes differences in ciphertext produced by slight changes in plaintext or key
      - Commonly used on a smaller portion of the plaintext to identify variations that could lead to discovering the key
- Summary of Key Attacks
  - Brute Force
    - Trial of all combinations; guaranteed success given time and resources
  - Linear Cryptanalysis
    - Uses mathematical relationships for statistical analysis of the cipher
  - Meet in the Middle

- Tests all key combinations in ciphers with multiple encryption rounds
- Differential Cryptanalysis
  - Analyzes slight differences by changing bits in plaintext or key
- Mind Map of Attacks
  - Known Plaintext
    - Whole Message
      - Brute Force, Linear Cryptanalysis, Meet in the Middle
    - Chosen Portion
      - Differential Cryptanalysis (on a small portion to identify key variations)
    - Differential Cryptanalysis Use Case
      - Preferably with chosen plaintext to isolate manageable variations in output
- **Cryptanalytic Attacks - Part 2**
  - Ciphertext-Only Attacks
    - Goal
      - Attempt to discover the cryptographic key by analyzing ciphertext alone
    - Related Key Attack
      - Compares ciphertexts generated with different but mathematically related keys
      - Relies on poor cryptographic standards implementation or weak key selection
    - Chosen Ciphertext Attack

# ISC2 CISSP

## (Study Guide)

- Analyzes specific ciphertext portions and their decrypted outputs
- Looks for differences or patterns to infer the key or cipher used
- Techniques
  - Differential Cryptanalysis
    - Examines differences between plaintext and ciphertext outputs, especially by varying key lengths or values
  - Frequency Analysis
    - Observes frequency of characters or sequences within the ciphertext, helping identify potential ciphers or key characteristics
  - Hash-Based Attacks
    - Pass the Hash
      - Uses stolen password hashes directly for authentication rather than plaintext passwords
      - Often targets Windows systems vulnerable to Landman (LM) and NTLM authentication methods
    - Kerberoasting
      - Targets Kerberos authentication by harvesting and attempting to crack password hashes
      - Key focus
        - Exploit Ticket Granting Ticket (TGT) (Golden Ticket) or Ticket Granting Service (TGS) (Silver Ticket) for single sign-on compromise
    - Birthday Attack

- Based on the Birthday Paradox, which calculates the likelihood of two identical hashes (hash collision)
- Exploits the chance of hash collisions to bypass integrity controls, particularly in systems with weaker hash algorithms
- Rainbow Table Attack
  - Uses precomputed tables of hash values for common passwords to quickly find matches
  - If a captured hash matches a value in the rainbow table, the corresponding plaintext password is identified
- Summary of Attacks
  - Ciphertext-Only Attacks
    - Related Key Attack
      - Compares ciphertexts with related keys
    - Chosen Ciphertext Attack
      - Targets specific ciphertext segments for analysis
    - Differential Cryptanalysis
      - Examines changes by adjusting key parameters
    - Frequency Analysis
      - Identifies repeating patterns to deduce encryption details
  - Hash-Based Attacks
    - Pass the Hash
      - Uses hash directly for authentication
    - Kerberoasting
      - Cracks Kerberos tickets to gain unauthorized access
    - Birthday Attack

- Finds hash collisions by exploiting probabilistic properties
  - Rainbow Table Attack
    - Matches captured hashes to known password hashes
- **Cryptanalytic Attacks - Part 3**
  - Attacking the Cryptosystem
    - Goal
      - Exploit vulnerabilities in the cryptographic algorithm, cipher, or protocol implementation
  - Key Concepts and Techniques
    - Work Factor
      - Measures the time, effort, and resources required to break a cryptosystem
      - Helps attackers assess the feasibility of targeting a specific cipher or algorithm
    - Weaknesses in Ciphers, Applications, and Protocols
      - Older algorithms like DES are more vulnerable due to shorter keys and weaker encryption
      - Protocol flaws in encryption standards (e.g., SSL, SSH) can expose sensitive data if misconfigured
    - Fault Injection Attack
      - Injects errors or invalid data to see how a system responds
      - Identifies vulnerabilities in how a cryptographic system handles unexpected inputs

- **Replay Attack**
  - Intercepts an encrypted message and reuses it to gain unauthorized access
  - Countermeasure
    - Use of timestamps, expiration periods, or timeouts
- **Side Channel Attack**
  - Targets the operational characteristics of the cryptographic process, like power consumption or timing
  - Timing Attack
    - Analyzes the time required to complete cryptographic operations, revealing clues about the algorithm used
- **Attacking the User**
  - **Goal**
    - Exploit weaknesses in the human element of the cryptographic process
- **Key Techniques**
  - **Man-in-the-Middle Attack**
    - Places the attacker between two parties, intercepting and possibly altering communications
    - Tools
      - Protocol analyzers or network sniffers to capture sensitive data, like keys or plaintext
  - **Ransomware Attack**
    - Encrypts the victim's data and demands payment to release the key

- Effective due to the difficulty in breaking encryption without the correct key
- Social Engineering
  - Trick the user into revealing the cryptographic key or sensitive information
  - Often involves pretending to be an authority figure (e.g., IT support) needing access
- Summary
  - Cryptosystem Attacks
    - Work Factor
      - Estimates resources needed for an attack
    - Fault Injection
      - Tests how the system handles errors
    - Replay Attack
      - Reuses captured encrypted messages
    - Side Channel Attack
      - Focuses on timing, power, and other process attributes
  - User Attacks
    - Man-in-the-Middle
      - Intercepts and monitors communication
    - Ransomware
      - Encrypts data to demand ransom
    - Social Engineering
      - Deceives users into giving up critical information



## Physical Security

Objectives:

- 3.8 - Apply security principles to site and facility design
- 3.9 - Design site and facility security controls
- 7.14 - Implement and manage physical security
  
- **Physical Security**
  - Physical Security
    - First line of defense in protecting sensitive data, systems, and personnel
    - Essential for both CISSP exam and real-world security operations
  - Site Design Principles
    - Focus on the geographic location, layout, and proximity to hazards
    - Impact of surrounding environment on physical security
  - Facility Design
    - Architectural decisions enhancing security, including placement of walls, doors, and windows
  - Facility Security Controls
    - Physical barriers (fences, gates, locks) and advanced controls (biometric readers, security badges)
  - Facility Infrastructure Security
    - Protection of key facility systems
      - Power, heating, cooling, telecommunications
  - Fire Prevention, Detection, and Suppression

- Types of fire detection systems (smoke detectors, heat sensors)
  - Fire suppression systems (sprinklers, gas-based systems)
  - Physical Security Controls
    - Surveillance cameras, security guards, environmental controls
    - Comprehensive application of physical security measures
- **Site Design Principles**
  - Overview of Site Design for Security
    - Site design in security involves establishing administrative, technical, and logical controls to ensure physical security for facilities
    - Goal
      - Create a secure facility using defense-in-depth principles to safeguard critical assets and support dependencies
  - Key Components of Site Design
    - Critical Path Analysis
      - Analyze relationships between critical assets and dependencies like electricity, environmental controls, water, and waste services
      - Identify risks, such as water leaks, which could impact asset availability
    - Site Selection Considerations
      - Location
        - Assess for high crime areas, natural disaster zones, and response times for emergency services
      - Environmental Risks

# ISC2 CISSP

## (Study Guide)

- Consider potential natural threats, such as earthquakes, floods, fires, etc.
- Nearby Businesses and Traffic
  - High foot traffic can increase crime potential; review surrounding businesses for risk factors
- Infrastructure Access
  - Ensure availability of essential services like power, gas, waste, and telecommunications
- Crime Prevention Through Environmental Design (CPTED)
  - A strategy focused on designing the environment to influence behavior and deter crime
  - Key Elements of CPTED
    - Natural Access Control
      - Limit access points naturally, such as with landscape features.
    - Natural Surveillance
      - Ensure visibility of surroundings to deter criminal activities
        - E.g., elevated views, clear sightlines
    - Natural Territorial Reinforcement
      - Use physical features (e.g., landscaping, barriers) to reinforce ownership and deter intrusion.
- Example of CPTED Principles in Action
  - Fort Knox (Kentucky, USA)
    - Surrounding area is clear and elevated, allowing for clear visibility and surveillance

# ISC2 CISSP

## (Study Guide)

- Only one access point for controlled entry and exit
    - Trees are cleared, offering visibility for cameras and patrol routes
    - Open terrain for natural surveillance and deterrence
  - Key Exam Points
    - Understand
      - The role of critical path analysis in identifying facility dependencies
    - Recognize
      - Site selection factors such as crime rates, natural disasters, and emergency response times
    - Identify
      - The purpose of CPTED in reducing crime through environmental influence
    - Apply
      - Principles of natural access control, surveillance, and territorial reinforcement in site design
  - Site Design Principles create a layered, defense-in-depth approach, blending natural environmental elements with security controls to safeguard facilities and deter crime effectively
- 
- **Facility Design Principles**
    - Overview of Facility Design Principles for Security
      - Purpose
        - Identify and implement physical security controls within facility design to deter, deny, detect, and delay potential security threats

- Components
  - Incorporate administrative, technical, and logical controls to ensure physical security aligned with the organization's needs
- Types of Physical Security Controls
  - Deterrence
    - Discourages potential security violations
  - Fencing
    - 3-4 feet
      - Deters casual passersby
    - 6-7 feet
      - Deters most intruders
    - 8+ feet with barbed wire
      - Maximum deterrence for determined intruders
    - Lighting
      - Use two-foot candle power in critical areas for clear visibility
    - Landscaping
      - Use natural barriers like thorn bushes or water features (similar to a moat) to create obstacles
    - Denial
      - Prevents access to restricted areas
    - Turnstiles
      - Limits entry to one person at a time, authenticates identity
    - Mantraps

# ISC2 CISSP

## (Study Guide)

- Two sets of doors that isolate a subject for identity verification; prevents piggybacking (intentional following) and tailgating (unintentional following)

### ■ Detection

- Identifies potential security violations.
- Cameras
  - Clear line of sight to entrances, exits, and key areas.
  - Use PTZ (Pan, Tilt, Zoom) cameras for a full 360-degree field of view
- Detection Sensors
  - Infrared Detectors
    - Detects changes in infrared light
  - Wave Pattern Detectors
    - Detects motion through ultrasonic or microwave signals
  - Heat and Temperature Sensors
    - Detects sudden temperature changes
  - Photoelectric Detectors
    - Detects motion or changes in light
  - Audio Detectors
    - Detects specific sounds, such as breaking glass
  - Capacitance Detectors
    - Detects changes in electrical or magnetic fields
  - Passive Infrared (PIR)
    - Detects changes in heat, indicating presence

- Delay
  - Slows down potential intruders
  - Fence Enhancements
    - Barbed wire and other modifications to slow intruder access
  - Locks
    - Can be bypassed by methods like lock picking, skeleton keys, or shimmying
  - Bollards
    - Prevent vehicles from ramming into sensitive areas
- Decision-Making
  - Utilizes physical access control systems to monitor and respond to security incidents
  - Physical Access Control System (PACS)
    - Integrates controls to allow real-time situational awareness
  - FIPS Publication 201
    - Governs PACS requirements
  - ID Badges
    - Personal Identity Verification (PIV) cards or Common Access Cards (CAC) authenticate users
- Crime Prevention Through Environmental Design (CPTED)
  - Uses environmental design to influence human behavior and deter crime.
  - Applications
    - Natural Access Control

- Restrict access points naturally
- Natural Surveillance
  - Use elevation or clear sightlines for better observation
- Natural Territorial Reinforcement
  - Use barriers to convey ownership and deter entry
- Examples of Facility Security Applications
  - Example of Deterrence
    - Fort Knox uses dual high fences with barbed wire, security guards, and surveillance as visual deterrents
  - Example of Delay
    - Use of bollards to prevent vehicle access to sensitive areas, barbed wire on fences to slow intruders, and locked gates
- Key Exam Points
  - Understand
    - The role of controls in deterring, denying, detecting, delaying, and deciding responses to potential threats
  - Recognize
    - Importance of CPTED in design to reduce crime
  - Identify
    - Use cases of detection sensors, cameras, and access control systems to monitor and respond to facility security incidents
- Facility Design Principles ensure physical security by combining deterrence, denial, detection, and delay mechanisms in a layered defense-in-depth strategy



- **Facility Security Controls**

- Facility Security Areas Overview

- Wiring Closets

- Purpose

- Houses network and telecommunications infrastructure, supporting facility IT services

- Contents

- Modems, routers, switches, patch panels, networking cables

- Protection Needs

- Ventilation

- Prevents equipment overheating; add fans or cooling systems

- Physical Security

- Locking mechanisms, cameras, and sensors

- Cleanliness

- No storage of flammable materials

- Access Control

- Limit entry to authorized personnel only

- Server Rooms

- Purpose

- Contains critical IT infrastructure like routers, firewalls, switches, intrusion detection systems

- Protection Needs

- Location

# ISC2 CISSP

## (Study Guide)

- Preferably in the middle of the facility, away from top and bottom floors to avoid flood risks and natural disaster exposure
- Climate Control
  - Maintain air conditioning with Computer Room Air Conditioning (CRAC) units and humidity control
- Access Control
  - Limited entry points, cameras, sensors, and monitoring for ingress and egress
- Organizational Standards
  - No storage of flammable materials; maintain cleanliness and limited personnel traffic
- Data Centers
  - Purpose
    - Enterprise-level server room with extensive servers, typically used by large organizations
  - Types
    - Local Data Center
      - On-premise; server room within the organization's facility
    - Remote Data Center
      - Off-premise; typically operated by third-party providers (e.g., cloud services)
  - Protection Needs
    - Access Control

# ISC2 CISSP

## (Study Guide)

- One primary entry point and an emergency exit
  - Environmental Controls
    - Temperature (60-75°F / 15-23°C) and humidity (40-60%) to prevent overheating, static, and corrosion
  - Emergency Power
    - Generators and Uninterruptible Power Supplies (UPS) for backup
  - Centralized Monitoring
    - Secure access control systems, CCTV, and alarms
- Storage Areas
  - Purpose
    - Dedicated areas for physical asset storage, backups, media, and evidence
  - Protection Needs
    - Organization
      - Use dedicated space for organized storage, not as random overflow
  - Evidence Storage
    - If used, maintain chain of custody documentation and restrict access
  - Access Controls
    - Strict policies, sensor monitoring, alarm systems, and CCTV surveillance
- Types of Facility Security Controls

- Deterrence
  - Prevents potential security breaches through visible security measures
  - Examples
    - Fencing, lighting, signage, CCTV cameras
- Denial
  - Restricts access to unauthorized individuals.
  - Examples
    - Locked doors, turnstiles, mantraps, limited entry points
- Detection
  - Identifies unauthorized access or potential breaches
  - Examples
    - Cameras, intrusion sensors, access control logs, environmental monitors (for temperature and humidity)
- Delay
  - Slows down potential intruders, giving security personnel time to respond
  - Examples
    - Barbed wire on fences, locked doors, bollards
- Response
  - Actions taken to address detected security threats
  - Examples
    - Security guards, automated alerts, emergency plans
- Environmental Controls
  - Temperature

- 60-75°F (15-23°C)
- Humidity
  - 40-60% to prevent static electricity and corrosion
- Ventilation
  - Ensure separate HVAC for server rooms/data centers from the rest of the facility
- Key Exam Points
  - Understand
    - The purpose and protection needs of wiring closets, server rooms, data centers, and storage areas
  - Recognize
    - Types of physical security controls (deterrence, denial, detection, delay, response)
  - Apply
    - Environmental controls effectively in facility design to maintain equipment integrity and availability
- Facility Security Controls ensure secure design and operation of wiring closets, server rooms, and data centers, prioritizing access control, environmental controls, and structured response measures
- **Facility Infrastructure Security**
  - Facility Infrastructure Security Components
    - Work areas

# ISC2 CISSP

## (Study Guide)

- Security priority to reduce risk to personnel and protect confidentiality, integrity, and availability (CIA) of organizational resources
- Limit access to only those who require it
- Apply least privilege and need-to-know principles
- Require two-person control in restricted areas
- Two-person control means two people must access the area, ensuring no person is alone
- Layer security controls to control, monitor, and grant access
- May be required by governance regulations and compliance
  - E.g., GDPR, HIPAA, PCI DSS
- Compliance may dictate work area design, access, and data handling practices
- Environmental considerations
  - Assess area vulnerability to natural disasters
    - E.g., earthquakes, tornadoes, hurricanes, wildfires
  - Design facility to reduce vulnerabilities (e.g., fire resistance, flood protection)
- Facility utilities
  - Follow strict procedures for utilities (e.g., water, steam, gas, electricity, sewage) near data centers, server rooms, or work areas
  - Water leaks, gas leaks, and electrical shortages can impact computing resources
  - Install water detectors in ceilings and under floors
- HVAC (Heating, Ventilation, and Air Conditioning) Considerations

# ISC2 CISSP

## (Study Guide)

- Maintain work area temperature at 65-75°F or 18-23°C for personnel and equipment comfort
- Use computer room air conditioning (CRAC) for server rooms
- Maintain equipment at 60-75°F or 15-23°C
- Control temperature, static electricity, and humidity levels
- Maintain humidity around 50% to prevent corrosion and static electricity
- Less humidity causes static electricity
- More humidity causes metal corrosion
- Secure HVAC ducts
  - Lock, monitor, and add sensors to ducts as they may be vulnerable to intrusion
- Facility Power Considerations
  - Recognize electricity vulnerability to faults, failures, fluctuations, and interruptions
  - Implement power protection through backup or redundant power sources
  - Data center tiers
    - Four tiers exist, each with different uptime and redundancy levels
    - Tier 1
      - Lowest level, single path for cooling, no redundancy
    - Tier 2
      - 16 hours maximum downtime
    - Tier 3
      - Multiple paths for cooling, improved redundancy
    - Tier 4

- Full redundancy, highest uptime, most expensive
- Example of Tier uptimes
  - Tier 1
    - Up to 28-29 hours of downtime per year
  - Tier 4
    - 99.995% uptime, maximum of 26 minutes downtime per year
- Power Issues
  - Power issues that can affect facility and equipment
  - Fault
    - Temporary power loss
  - Blackout
    - Complete power loss
  - Sag
    - Temporary low power voltage
  - Brownout
    - Extended period of low power voltage
  - Spike
    - Temporary high voltage
  - Surge
    - Extended period of high voltage
  - Inrush
    - Initial surge of power when devices start up
  - Noise
    - Power fluctuation or EMI



- Transient
  - Temporary noise on the line
- EMI (Electromagnetic Interference)
  - Often causes noise and transient issues
- RFI (Radio Frequency Interference)
  - Comes from lights and electrical cables
- Power Backup and Redundancy
  - Uninterruptible Power Supplies (UPS)
    - Provides uninterrupted power for a short duration
  - Double Conversion UPS
    - Stores power in a battery, providing consistent, clean power to devices
  - Line Interactive UPS
    - Contains surge protection and voltage regulation between power source and battery
  - Generators
    - Motor-operated machines creating large amounts of electricity for backup
    - Require fuel, maintenance, and regular operation for reliability
- **Fire Prevention, Detection, and Suppression**
  - Primary Fire Safety Focus
    - Protect health and lives by enabling safe facility exit
    - Protect organizational personnel as the top priority
    - Protect system assets as the secondary priority

- Understand fire risks
  - Smoke, excessive heat, and hazardous effects
- Key Fire Safety Principles
  - Detection
    - Discover the presence of smoke or fire
  - Suppression
    - Use water, inert gas, or chemical agents to eliminate fire
  - Prevention
    - Reduce or prevent the fire from spreading
- Fire Triangle Components
  - Oxygen source
  - Heat source
  - Fuel source
  - Removing any component disrupts the fire
- Fire Classes
  - Class A
    - Common combustibles (wood, paper, clothing, plastics)
  - Class B
    - Flammable liquids (gasoline, petrol)
  - Class C
    - Electrical equipment fires (circuit boards, motors, appliances)
  - Class D
    - Combustible metals (magnesium, titanium, lithium)
  - Class K
    - Commercial kitchen fires (fats, greases, oils)

- Fire Detection Methods
  - Smoke Detectors
    - Ionization smoke detector
      - Uses radioactive material, triggers on electrical plate disruption
    - Photoelectric smoke detector
      - Common in buildings, triggers on light source disruption
  - Fixed Temperature Detector
    - Activates upon significant temperature change
  - Rate of Rise Detector
    - Activates with rapid temperature increase
- Fire Extinguisher Classes and Materials
  - Class A
    - Common combustibles, use water or soda acid
  - Class B
    - Flammable liquids, use carbon dioxide, halon substitute, or soda acid
  - Class C
    - Electrical fires, use carbon dioxide or halon substitute
  - Class D
    - Metal fires, use only dry powder
- Facility-Level Fire Suppression Systems
  - Wet Pipe System
    - Water-filled at all times, releases water upon activation
    - Also called a closed head system

- Dry Pipe System
  - Contains compressed air, fills with water upon activation
- Deluge System
  - Dry pipe system that releases a large water amount quickly
  - Not recommended for electronics or machinery areas
- Pre-Action System
  - Combination of dry and wet pipe; pipes fill with water when heat or smoke detected
  - Requires two activation mechanisms, suitable for computer rooms and data centers
- Gas Suppression Systems
  - Inert Gas Discharge Systems
  - Formerly Halon; banned due to environmental harm
  - FM 200
    - Effective Halon replacement, also known as HFC 227EA
    - Other substitutes
      - CEA 410 or 308, HCFC Blend A (NAF S 3), HCFC 23, IG55, IG01, IG541, AeroCase
- Fire Prevention Techniques
  - Use non-combustible and fire-resistant materials in facility design
  - Reduces fire spread risk in server rooms and data centers
  - Protect combustible materials from heat sources
  - Example
    - Store documents away from heat sources
  - Use solid-core, fire-rated doors in data centers and server rooms

- Conduct regular fire safety training
- Train personnel on evacuation procedures and emergency services notification
- Teach usage of alarms and suppression systems
- Personnel Fire Safety Knowledge
  - Know location of exits and alternate exits in case of blockage
  - Know location of fire extinguishers in work areas, data centers, and server rooms
  - Understand how to activate or disable HVAC and fire suppression systems
  - Know how to manually activate fire suppression and shut off electricity if necessary
- Exam Preparation Key Points
  - Differences between fire detection, suppression, and prevention
  - Types and classes of fires and fire extinguishers
  - Suppression systems used in facilities
  - Steps for fire prevention and essential personnel knowledge
- **Physical Security Controls**
  - Physical Security Control Types
    - Deterrent Controls
      - Discourage potential security violations
    - Denial Controls
      - Prevent potential security violations
    - Detection Controls
      - Identify security violations

- Delay Controls
  - Slow down potential security violations
- Determine Controls
  - Find the cause of security violations
- Decision Controls
  - Address the security violations
- Recovery Controls
  - Enable recovery from security violations
- Facility Security Controls
  - Perimeter Controls
    - Track and control access to the exterior facility areas
    - Examples
      - Fences, guard patrols, security cameras
  - Internal Security Controls
    - Track and control access to restricted facility areas
    - Examples
      - Turnstiles, mantraps, access control systems
- Restricted Areas
  - Designated to allow only authorized access
  - Protect sensitive data, operations, or personnel
  - Examples
    - Security operation centers (SOC), network operation centers (NOC), R&D departments
- Perimeter Security Examples
  - Fencing

# ISC2 CISSP

## (Study Guide)

- Multiple layers, often 12 feet high, may include razor wire
- Deterrent signage
  - Warnings such as "Deadly Force Authorized"
  - Guard patrols and guard dogs
  - CCTV and sensors
- Access Control Examples
  - Turnstiles
    - Require credentials for entry, deny access without authorization
  - Mantraps
    - Isolated entry area with dual locking doors, requiring proper credentials for access
  - Access control system
    - Monitors and detects failed access attempts, alerts security personnel
- Detection and Surveillance
  - CCTV Cameras
    - Closed-circuit television used to monitor for potential violations
  - Types of Cameras
    - Fixed CCTV
      - Monitors a specific area constantly
    - Pan, Tilt, Zoom (PTZ) Camera
      - Provides 360-degree field of view, remote-controlled for flexibility in monitoring
- Intrusion Detection Sensors
  - Active Infrared

- Detects motion based on changes in infrared light patterns
- Passive Infrared
  - Detects motion based on changes in ambient temperature
- Wave Pattern
  - Detects motion through changes in ultrasonic or microwave signals
- Capacitance Motion Detectors (Proximity Sensors)
  - Detect changes in magnetic/electric fields
- Photoelectric
  - Monitors changes in visible light levels
- Passive Audio
  - Detects sound changes, used for glass break detection
- Intrusion Alarms
  - Notification Alarms (Silent Alarms)
    - Notify an alarm station without audible alert
  - Repellent Alarms
    - Activate loud sirens or lights to deter intruders
  - Deterrent Alarms
    - Engage barriers like gates or locks to prevent further access
  - Examples of Alarm Systems
    - Local Alarm System
      - Audible alarm only heard locally
    - Central Station System
      - Silent alarm remotely monitored by security
    - Auxiliary Station Alarm



- Directly alerts emergency services and law enforcement
- Alarm Verification Types
  - Single Verification
    - Monitor point alerts to a potential intrusion
  - Secondary Verification
    - Uses additional mechanism, such as CCTV, to confirm a real threat
- Exam Preparation Focus
  - Understand the types and purposes of intrusion sensors and alarms
  - Know how CCTV and other monitoring methods work as secondary alarm verification methods

## Network Components

Objectives:

- 4.1 - Apply secure design principles in network architectures
- 4.2 - Secure network components
- **Network Components**
  - Network Components
    - Essential building blocks of network environments, including physical hardware, infrastructure, and media
    - Crucial for CISSP exam and security operations
  - Hardware Operations
    - Covers physical devices like routers, switches, firewalls, and servers
    - Focus on device functions, integration into network architectures, and security implications
  - Network Infrastructure Operations
    - Involves redundancy, high availability, vendor support, and end-of-life issues
    - Critical for minimizing downtime and maintaining continuous network security
  - Transmission Media
    - Selection based on network topology, data transfer speeds, and physical device locations
    - Includes types like coaxial cable, twisted pair cable, and fiber optic cables

- Examines each type's function, security implications, and effective deployment
- Network Monitoring
  - Tools and techniques for real-time threat detection and network traffic analysis
  - Use of Simple Network Management Protocol (SNMP) for network management and monitoring
  - Acts as an early warning system for potential security breaches
- **Hardware Operations**
  - Repeater
    - Used to re-energize electrical signals to increase transmission distance
    - Also referred to as an amplifier or concentrator
    - Found integrated in modern network devices like switches, routers, firewalls
  - Modem
    - Modulates and demodulates analog carrier signals for data processing
    - Facilitates communication between digital and analog systems, such as in DSL systems
  - Hub
    - Connects multiple computers to the same network segment without routing or addressing
    - Operates by flooding; transmits all incoming traffic out all other ports
  - Bridge

- Connects two network segments together using the same network protocol
- Considered a Layer 2 device
- Now largely replaced by multiport bridges known as switches
- Switch
  - More advanced than hubs; directs data to appropriate port based on MAC addresses
  - Can perform both Layer 2 and Layer 3 (multilayer switching) functions
- Router
  - Manages communications between different networks using logical (IP) addresses
  - Determines the best path for data packets based on various metrics (hop count, speed)
  - Maintains route information in a route table or applies route policies
- Brouter
  - Combination of a bridge and a router
  - Routes using Layer 3 when possible, defaults to Layer 2 otherwise
- Gateway
  - Connects network segments that use different protocols
  - Functions as a protocol translator, facilitating communication between different systems
- Proxy
  - Mediates requests between two systems while maintaining security by verifying and forwarding requests
  - Does not alter protocols or port numbers

- Common implementation includes Network Address Translation (NAT)
- LAN Extender
  - Used to connect remote network segments over WAN links
  - Typically employed for remote access purposes
- Wireless Access Points (WAP)
  - Physical devices that connect wireless devices to a network
  - Can operate on Layer 2 or Layer 3 depending on functionality
- Multiplexer (MUX)
  - Combines multiple signal types for transmission over a single medium
  - Used in telecommunications for data, voice, and video
- Endpoints
  - Devices that originate or terminate communications
  - Examples include computers, mobile devices, printers, and IoT devices
- **Network Infrastructure Operations**
  - Network Infrastructure
    - Defined as hardware, software, and other components that enable network connectivity and communication
    - Key components include users, devices, apps, and internet connectivity
  - Redundant Power
    - Essential for ensuring continuous operations of network infrastructure
    - Includes uninterruptible power supplies (UPS) and backup generators
    - UPS provide short-term power; generators provide long-term power solution

- Uninterruptible Power Supply (UPS)
  - Provides continuous battery power to IT infrastructure during electrical outages
  - Types include
- Standby (Offline) UPS
  - Basic protection, most cost-effective
- Line Interactive UPS
  - Includes AVR for stabilizing power fluctuations
- Online (Double Conversion) UPS
  - Offers the cleanest and most stable power, protecting against all power anomalies
- Generators
  - Motor operated machines that provide uninterrupted power
  - Essential for long-term power supply during outages
  - Require steady fuel supply and regular maintenance
- Vendor Warranty
  - Covers repairs and replacements of hardware within a specified period
  - Ensures timely resolution of hardware issues
- Vendor Support
  - Provides technical assistance for setting up and maintaining network infrastructure
  - Includes access to software updates, bug fixes, and vendor documentation
- End of Service (EOS)
  - Termination of vendor support and updates for a product or service

- Important to renew service agreements to continue receiving support
- End of Life (EOL)
  - Point at which a product is no longer supported or maintained by the vendor
  - Use of product beyond EOL is at the user's risk
  - No further support or updates provided
- **Transmission Media - Part 1**
  - Transmission Media
    - Pathway for data to travel from one point to another
    - Can be physical (wired) or digital (wireless)
  - Key Factors in Choosing Transmission Media
    - Network Topology
      - Arrangement of network elements impacts transmission media selection
    - Location of Computing Services
      - Determines if wired or wireless connectivity is needed
    - Data Transfer Rates (Throughput)
      - Speed requirement from point A to point B
    - Cost and Equipment
      - Equipment compatibility and budget influence media selection
  - Network Topologies
    - Ring Topology
      - Only one host can communicate at a time
      - Data is passed using a token in a circular pattern

- Bus Topology
  - Central backbone cable connects all devices
- Star Topology
  - Devices connected through a central network device (common in small networks)
- Mesh Topology
  - High availability setup, each device is connected to multiple others
- Network Types
  - Wide Area Network (WAN)
    - Spans large geographical areas
      - E.g., the internet
  - Metropolitan Area Network (MAN)
    - Covers a city or metropolitan area
      - E.g., city-wide Wi-Fi
  - Local Area Network (LAN)
    - Small geographical area
      - E.g., office or home network
  - Personal Area Network (PAN)
    - Limited to an individual's immediate area, e.g., mobile device hotspot or Bluetooth
- Data Rates
  - Bit
    - Binary unit of information
  - Byte



- 8 bits
- Megabit (Mb)
  - 1,000 bits
- Gigabit (Gb)
  - 1,000 megabits
- Types of Communications
  - Baseband
    - Digital signals on a single frequency (used in Ethernet)
  - Broadband
    - Analog signals on multiple frequencies
      - E.g., DSL
- Ethernet Technology
  - Based on IEEE 802.3 standard
  - OSI Layer 2 protocol using frames for communication
  - Supports full duplex communication
  - Uses twisted pair cabling
- Ethernet Components
  - Data Terminal Equipment (DTE)
    - Endpoints in Ethernet technology
      - E.g., computers
  - Data Communication Equipment (DCE)
    - Transfers Ethernet frames
      - E.g., Layer 2 switches
- Ethernet Data Rates
  - Fast Ethernet

- 100 Mbps
  - Gigabit Ethernet
    - 1,000 Mbps (1 Gbps)
  - 10 Gig Ethernet (10 Gig E)
    - 10 Gbps
- **Transmission Media - Part 2**
  - Transmission Medium
    - Pathway for transferring data from point A to point B
    - Can be wired
  - E.g., cabling
    - Or wireless
      - E.g., radio frequency
  - Coaxial Cable
    - Composed of a copper wire, shielding, and grounding to prevent electromagnetic interference (EMI)
    - Used for digital subscriber line (DSL), CCTV cameras, and other communications
  - Twisted Pair Cables
    - Comprises pairs of copper wires twisted together to reduce interference
    - Types include
      - Unshielded Twisted Pair (UTP)
  - Shielded Twisted Pair (STP)
    - Commonly used with category cables
  - Cat5

- Supports up to 100 Mbps (100BASE-TX)
- Cat6
  - Supports up to 1 Gbps
- Cat7
  - Supports up to 10 Gbps
- Effective distance limitation is 100 meters for Cat5 and Cat6, and 55 meters for Cat7
- Fiber Optic Cabling
  - Utilizes a glass core to transmit data using light and lasers
  - Types include
- Single Mode
  - For long-distance applications, uses a small core (8.3 microns)
- Multi Mode
  - Suitable for shorter distances (up to 2 kilometers), uses a larger core (50 or 62.5 microns)
  - Wireless Media
    - Enables device communication without physical cables through radio frequency
    - Main challenges include range and coverage interference from other electronic devices
- Common Cable
  - Dielectric Insulation
  - Insulates the copper core in coaxial cables from shielding
- Plenum Rated Cable

- Non-toxic jacket material used for cables in airflow spaces to prevent toxic fumes in case of fire
- TIA 568 Standard
  - Standard for the color-coding and positioning of wires within twisted pair cables for connectivity
  - Common configurations
  - 568A
  - 568B (most prevalent)
- **Network Monitoring**
  - Network Monitoring
    - Practice and techniques to identify, track, and analyze network performance and operations
    - Utilized to manage, troubleshoot, and ensure health and status of network infrastructure
  - Purposes of Network Monitoring
    - Focuses on network performance to enhance security
    - Detects anomalies, threats such as DDoS attacks, malware propagation, and unauthorized access
  - Monitoring Protocols
    - Simple Network Management Protocol (SNMP)
    - Monitors system status and configuration of devices like switches, printers, and computers
  - Internet Control Message Protocol (ICMP)

- Used to send operational information and generate error messages for device failures
- Tools and Platforms for Network Monitoring
  - Cisco Discovery Protocol
  - Older protocol used for discovering information about directly connected Cisco devices
  - ThousandEyes Synthetics
  - Synthetic monitoring solution by Cisco for tracking application performance and network health
  - CloudFlare Magic Network Monitoring
  - Provides end-to-end visibility for traffic within internal and external network environments
  - Amazon CloudWatch
  - Monitors AWS resources and applications, usable for both cloud and on-premises environments
- Process of Network Monitoring
  - Collection
    - Gathering data from various sources like SNMP, ICMP, or client-generated metrics
  - Monitoring
    - Analyzing collected data to visualize and determine network health
  - Detection
    - Identifying anomalies or issues within the network traffic or performance

- Action
  - Responding to issues detected to mitigate potential impacts or rectify anomalies
- Key Benefits of Network Monitoring
  - Enhances the ability to respond to network issues and maintain operational continuity
  - Supports security by identifying potential threats and enabling proactive responses

## Networking Concepts

Objectives:

- 4.1 - Apply secure design principles in network architectures
- 4.3 - Implement secure communication channels according to design
  
- **Networking Concepts**
  - Networking Concepts
    - Fundamental for secure and reliable communication across networks
    - Critical component of the CISSP exam
  - TCP/IP and OSI Models
    - Frameworks that explain how communications occur across networks
    - TCP/IP and OSI layers help in segmenting network processes and applying security measures
  - IP Networking
    - Involves IP addressing and subnetting
    - Essential for organizing how devices communicate within networks
  - Local Area Network (LAN) Communications
    - Focuses on networking within a limited area such as a building or campus
    - Critical for defending organizational information systems
  - Communication Protocols
    - Enable devices to exchange data and communicate effectively
    - Knowledge of protocols is essential for securing day-to-day operations
  - Multilayer Protocols

- Operate across multiple layers of the OSI and TCP/IP models
- Important for applying security measures at different communication stages
- Converged Protocols
  - Combine different types of network traffic (voice, data, video) over a single network
  - Security strategies for converged protocols, including VoIP and other technologies
- Data Communications
  - Mechanisms that enable data movement across networks
  - Focus on encryption and securing protocols to protect data in transit
- Virtualized Networks
  - Increasing use of virtualization in networking
  - Security implications and measures for virtualized network environments
- **TCP/IP and OSI Models**
  - TCPIP
    - Collection of protocols and services used for network communications
    - Referred to as TCPIP suite or TCPIP stack
    - Most common method of network communication
  - Important TCPIP Terms
    - Port
      - Logical endpoint for communication
    - Protocol
      - Set of rules for computer communication
        - E.g., FTP, HTTP



- Service
  - Function provided by protocol using a port
    - E.g., FTP for file transfer
- OSI Model Layers
  - Layer 1 - Physical Layer
    - Handles bits, converts frames into bits for physical transmission
    - Examples
      - Cabling, wireless signals
  - Layer 2 - Data Link Layer
    - Contains hardware source and destination information, like MAC addresses
      - Sub-layers
        - Logical Link Control (error handling) and MAC sub-layer (addressing)
  - Layer 3 - Network Layer
    - Manages routing and addressing for packet transfer
    - Protocols
      - IP, ICMP, OSPF
  - Layer 4 - Transport Layer
    - Controls logical connections between computers (TCP - connection-oriented, UDP - connectionless)
  - Layer 5 - Session Layer
    - Establishes, maintains, and terminates communication sessions
  - Layer 6 - Presentation Layer
    - Transforms data into standard format

- Eg., encryption and decryption
- Layer 7 - Application Layer
  - Provides an interface for human interaction
    - E.g., HTTP, FTP, SNMP
- Protocol Data Unit (PDU)
  - Layer-specific format for data transfer
  - Transport Layer
    - Segment
  - Network Layer
    - Packet
  - Data Link Layer
    - Frame
  - Physical Layer
    - Bits
- Encapsulation Process
  - Adds headers and information to data as it moves from application to physical layer
  - Each OSI layer adds information, forming segments, packets, frames, and bits
- TCP Three-Way Handshake
  - SYN
    - Initiates connection with synchronization request
  - SYN-ACK
    - Acknowledges request and readiness to communicate
  - ACK

- Confirms connection, initiating data transfer
- Additional TCP Flags
  - URG
    - Urgent, priority traffic
  - RST
    - Reset, used to restart a connection
  - FIN
    - Finalize, used to terminate connection
- TCPIP Model Layers
  - Link Layer
    - Physical and Data Link layers (OSI layers 1 and 2)
  - Internet Layer
    - Network layer functions (OSI layer 3)
  - Transport Layer
    - Responsible for data transmission (OSI layer 4)
  - Application Layer
    - Merges OSI layers 5, 6, and 7
- **IP Networking**
  - IP Networking
    - Method of network communication using TCP/IP protocols
    - Facilitates communications over the Internet and intranets
  - Key IP Networking Terms
    - MAC Address
      - Physical, permanent address of a device (Layer 2)

- IP Address
  - Logical, dynamic address that corresponds to MAC address (Layer 3)
- Domain Name
  - Human-readable address of a device or server
- Fully Qualified Domain Name (FQDN)
  - Complete domain name for specific device within the network hierarchy
- Communication Methods
  - Simplex
    - One-directional communication
  - Half Duplex
    - Bi-directional but not simultaneous
  - Full Duplex
    - Bi-directional simultaneous communication (standard today)
- IP Addressing Overview
  - IPv4
    - 32-bit decimal address
      - E.g., 192.168.1.15
    - Limited to ~4.3 billion addresses
  - IPv6
    - 128-bit hexadecimal address
      - E.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334
    - Allows 340 trillion addresses

- Built-in auto-configuration, eliminating the need for DHCP and NAT
- Uses scoped addresses for network grouping and filtering
- IPv4 Classes
  - Class A
    - Range 1.0.0.0 - 126.0.0.0, Default Subnet Mask: 255.0.0.0 (/8)
  - Class B
    - Range 128.0.0.0 - 191.255.0.0, Default Subnet Mask: 255.255.0.0 (/16)
  - Class C
    - Range 192.0.0.0 - 223.255.255.0, Default Subnet Mask: 255.255.255.0 (/24)
  - Class D
    - Reserved for multicasting, Range 224.0.0.0 - 239.255.255.255
  - Class E
    - Reserved for experimental purposes, Range 240.0.0.0 - 255.255.255.255
- IPv4 Private Address Ranges (RFC 1918)
  - Class A
    - 10.0.0.0 - 10.255.255.255
  - Class B
    - 172.16.0.0 - 172.31.255.255
  - Class C
    - 192.168.0.0 - 192.168.255.255

- Network Address Translation (NAT)
  - Converts private IP addresses to public IP addresses for Internet routing
  - Static NAT
    - One-to-one mapping between private and public IP
  - Dynamic NAT
    - Pool of public IPs shared among private devices
  - Port Address Translation (PAT)
    - Maps multiple private IPs to one public IP using unique port numbers
- CIDR Notation for Subnet Masks
  - Class A - /8 (255.0.0.0)
  - Class B - /16 (255.255.0.0)
  - Class C - /24 (255.255.255.0)
- Benefits of IPv6
  - Eliminates need for NAT and DHCP through built-in configuration
  - Scoped addresses for efficient traffic grouping and filtering
  - Quality of Service (QoS) for traffic management based on priority
- Summary for Exam Preparation
  - Know IPv4 ranges and default CIDR notation
  - Understand IPv6 benefits and configuration features
  - Know NAT and PAT functionalities for private-public IP translation
- **LAN Communications**
  - IP Networking Communication Types
    - IP networking allows TCP/IP-based communication

- Types of Networks
  - Wide Area Network (WAN)
    - Spans large geographical areas
      - E.g., across countries or continents
  - Local Area Network (LAN)
    - Limited to a small geographical area; not intended for long-distance communication
  - Metropolitan Area Network (MAN)
    - Covers city-sized areas, often used by city governments
  - Personal Area Network (PAN)
    - Limited to an individual's immediate area
      - E.g., Bluetooth, ZigBee
  - Campus Area Network (CAN)
    - Covers large campuses, like universities; LANs within CANs can connect locally
- Network Domains
  - Broadcast Domain
    - A logical grouping of network devices that receive network broadcasts
    - Broadcasts can be for various purposes, like updates or general information sharing
  - Collision Domain
    - A grouping of devices to reduce data collisions
    - Collisions occur when multiple devices send data simultaneously on the same network segment

- Layer 2 (Data Link Layer) creates collision domains, typically managed by switches
- Broadcasts occur on Layer 3 (Network Layer), managed by routers or Layer 3 switches
- Collision Management
  - CSMA/CD (Carrier Sense Multiple Access with Collision Detection)
    - Used in Ethernet and wired networks
    - Waits a short, random time after a collision before retransmitting
  - CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)
    - Used in wireless networks to avoid collisions
    - Allows only one device to communicate at a time, preventing collisions
- Types of Routes
  - Static Routes
    - Manually configured; direct traffic to specified paths
  - Dynamic Routes
    - Automatically determined using routing protocols, sharing information with neighboring routers
- Routing Protocol Types
  - Distance Vector Protocols
    - Determine paths based on distance (hop count) and direction
  - Link State Protocols
    - Calculate paths based on the overall state of the network, selecting the most reliable, fastest routes
- Types of Routing Protocols



- Interior Gateway Protocols (IGPs)
  - Exchange routing data within the same system or autonomous system
- Exterior Gateway Protocols (EGPs)
  - Share routing information between different systems or autonomous systems
- Autonomous System (AS)
  - A collection of network devices managed under a single routing policy
- Key Routing Protocols
  - Distance Vector Protocols
    - RIP (Routing Information Protocol)
      - Uses hop count to determine best path (maximum of 15 hops; 16+ considered unreachable)
      - RIP Version 1
        - No subnet support
      - RIP Version 2
        - Supports subnetting with CIDR (Classless Inter-Domain Routing)
    - BGP (Border Gateway Protocol)
      - Exterior protocol, used on the internet to find shortest paths between autonomous systems
    - IGRP (Interior Gateway Routing Protocol)
      - Cisco proprietary protocol for local AS communication
  - EIGRP (Enhanced IGRP)

# ISC2 CISSP

## (Study Guide)

- An open protocol with added Variable Length Subnet Masks (VLSM) for more subnet control
- Link State Protocols
  - OSPF (Open Shortest Path First)
    - Commonly used in LANs, uses Dijkstra algorithm for shortest path calculation
    - Utilizes areas to divide networks within an AS, allowing efficient load balancing and alternative route selection
  - IS-IS (Intermediate System to Intermediate System)
    - Primarily used in large service provider networks
- Bottom Line for the Exam
  - Understand different network types
    - WAN, LAN, MAN, CAN, and PAN
  - Know network domains
    - Broadcast and Collision
  - Be familiar with routing types, protocols, and how they operate within autonomous systems
- **Communication Protocols**
  - Protocol Basics
    - Protocol
      - Set of agreed rules for computer communication
    - Unsecure Protocols
      - No encryption; all data in plain text
    - Secure Protocols

- Built-in security features
  - E.g., encryption
- Layer 7 - Application Layer Protocols
  - HTTP (Port 80)
    - Unsecure web-based communication
  - HTTPS (Port 443)
    - Secure web-based communication with SSL/TLS encryption
  - FTP (Ports 20, 21)
    - Unsecure file transfer; Port 20 for data, Port 21 for control
  - SMTP (Port 25)
    - Unsecure email message routing
  - SNMP (Ports 161, 162)
    - Network device monitoring; Port 161 unsecure, Port 162 for TRAPS
  - DNS (Port 53)
    - Resolves domain names to IP addresses
  - DHCP (Ports 67, 68)
    - Assigns dynamic IP addresses to devices
  - NTP (Port 123)
    - Synchronizes system clocks
  - ICMP
    - Provides communication status, used for PING and Traceroute (no assigned port)
  - Telnet (Port 23)
    - Unsecure remote access

- SSH (Port 22)
  - Secure remote access with encryption
- POP3 (Port 110)
  - Retrieves emails; option for secure Kerberos (Port 1109)
- IMAP (Port 143)
  - Manages emails with SSL/TLS security option (Port 993)
- Layer 6 - Presentation Layer Protocols
  - ASCII
    - Text encoding standard
  - JPEG
    - Digital image file format
  - PNG
    - Digital image file format
  - MPEG
    - Audio/video digital file format
- Layer 5 - Session Layer Protocols
  - NFS (Port 2049)
    - File sharing across networks
  - SQL
    - Relational database management
  - RPC (Port 111)
    - Calls routines and functions on remote systems
- Layer 4 - Transport Layer Protocols
  - TCP
    - Connection-oriented protocol with handshake

- UDP
  - Connectionless, fast transmission without handshake
- SSL
  - Original protocol for secure network communication (replaced by TLS)
- TLS
  - Secure communications with better security than SSL
- Layer 3 - Network Layer Protocols
  - IP
    - Connectionless routing for network communication
  - ICMP
    - Communication status and error messages
      - E.g., PING, Traceroute
  - OSPF
    - Dynamic routing protocol for path selection
  - IPSec
    - Secure VPN communications using encryption
  - NAT
    - Converts private IPs to public IPs for internet communication
- Layer 2 - Data Link Layer Protocols
  - ARP
    - Maps MAC addresses to IP addresses
  - RARP
    - Maps IP addresses to MAC addresses
  - L2TP

- Layer 2 tunneling for VPN; requires IPSec for encryption
    - PPTP
      - Point-to-Point tunneling for secure PPP communication
  - Layer 1 - Physical Layer Protocols
    - SONNET
      - Optical digital communications
    - HSSI
      - High-speed serial communications over WAN
    - RS-232, RS-449
      - Standards for serial communications
  - Exam Focus
    - Differentiate between secure and unsecure protocols
    - Identify purposes and functions of key protocols
- **Multilayer Protocols**
    - Multi-Layer Protocols
      - Protocols that span multiple layers of the TCP/IP stack
      - Example
        - A protocol that operates at Layer 2 and Layer 3, or Layer 3 and Layer 4
    - Key Points for Multi-Layer Protocols
      - Protocol Layer Limits
        - Not all protocols span multiple layers; some stop at specific layers
      - Example
        - IP packets stop at Layer 3 and do not continue beyond that layer

- Benefits
  - Multi-layer protocols support higher-level OSI model functions
  - Efficient processing by network and security components
  - Encryption can be applied at different layers for added security
- Risks
  - Encapsulation Challenges
    - If a packet is encrypted, additional information cannot be added
    - May bypass switches, routers, and endpoint security if not designed to detect multi-layer protocols
  - Network Segmentation
    - Difficult to identify multi-layer protocol traffic for segmentation at Layer 3 or Layer 2
    - Secure protocols like SSH or HTTPS aid in segmentation, whereas non-segmentable protocols pose a risk
  - Covert Channels
    - Covert channels (storage and timing) can leverage encapsulation to disguise malicious traffic as legitimate
    - These covert channels may bypass detection in security mechanisms
- Important Protocol to Know for the Exam
  - DNP3 (Distributed Network Protocol version 3)
    - An open standard protocol commonly used in industrial control systems
    - Applications include electric, water, wastewater, transportation, oil, and gas industries

- Primary function
  - Connects remote terminal units to SCADA master control stations
- Bottom Line
  - Understand both benefits and risks of multi-layer protocols
  - Familiarize with DNP3 and its role in industrial control systems
- **Converged Protocols**
  - Converged Protocols
    - Protocols that combine a specialized protocol with a standard protocol
    - Example
      - Combining Fibre Channel with Ethernet to create Fibre Channel over Ethernet (FCoE)
    - Purpose
      - Provides specific functions not supported by traditional protocols, reducing costs by leveraging existing infrastructure rather than developing new protocols and equipment
  - Key Converged Protocols
    - Fibre Channel over Ethernet (FCoE)
      - Allows Fibre Channel communications (used in Storage Area Networks) over Ethernet
      - Reduces infrastructure costs by using Ethernet instead of specialized Fibre Channel hardware
    - Internet Small Computer System Interface (iSCSI)



# ISC2 CISSP

## (Study Guide)

- An internet-based standard that enables storage access over IP networks
- Merges SCSI with IP networking to allow remote storage access
- Multi-Protocol Label Switching (MPLS)
  - Uses labels to transfer data quickly based on a predetermined path
  - Works with various protocols, including ATM, SONNET, and DSL, enabling flexibility beyond just TCP/IP
- Voice over IP (VoIP)
  - Encapsulates voice and multimedia communications over IP networks
  - Reduces costs by utilizing existing network infrastructure (e.g., Cat5/6 cabling) rather than dedicated PBX systems
  - Used in applications like Skype and Google Meet for voice communication over IP
- Software-Defined Networking (SDN)
  - Combines virtualized network resources to create a unified, converged network
  - Reduces dependence on specific platforms, vendors, or hardware, offering flexibility across network environments
- Security Risks and Considerations
  - Protocol Security
    - Must secure both the specialized and standard protocol components
      - E.g., VoIP requires security for both voice and IP protocols

- New and Undefined Standards
  - Some converged protocols lack established security standards, leading to potential vulnerabilities
- Tunneling Risks
  - Tunneling can obscure or hide communication data, making it challenging for security tools to detect intrusions or sniff traffic
- Testing Requirements
  - Important to test converged protocols against security mechanisms to ensure effective protection in production environments
- Bottom Line
  - Understand the purpose and advantages of converged protocols
  - Familiarize with key converged protocols
    - E.g., FCoE, iSCSI, MPLS, VoIP, SDN
  - Recognize security implications and the need for thorough testing
- **Data Communications**
  - Purpose of Secure Data Communications
    - Ensures data protection as it transmits from source to destination
    - Focus on maintaining data integrity and security throughout the transmission process
  - Key Communication Security Concepts
    - Transparency
      - Security mechanisms operate in the background without impacting user experience

# ISC2 CISSP

## (Study Guide)

- Aim
  - To avoid user frustration while keeping data safe
- Integrity
  - Data remains unaltered or uncorrupted during transmission
  - Uses hash functions and checksums to verify data authenticity upon arrival
- Transmission Logging and Error Correction
  - Enables accountability and error detection in data transmission
  - Supports high availability and redundancy
- Communication Control Implementation
  - Understand architecture and data flows
- Permit by Exception (Whitelisting)
  - Allow known, trusted communications and block all others (fail secure)
- Deny by Exception (Blacklisting)
  - Deny specific communications; requires high maintenance
- Emanation Security (EMSEC)
  - Protects against signal leaks that could be intercepted by attackers
  - Common with copper, radio, and wireless transmissions
  - Countermeasures
    - Faraday Cage
      - Blocks electromagnetic signals using a fully enclosed area with a metal mesh
    - White Noise
      - Generates alternate signals to mask sensitive emanations

- Control Zones
  - Specific areas protected by Faraday cages or white noise for targeted security
- Port Security
  - Restricts device connections based on configuration policies to prevent unauthorized access
  - MAC Filtering
    - Configures switches to permit only authorized MAC addresses on the network
    - Used in both wired and wireless networks
  - Secure Protocols
    - Preferred over insecure ones to ensure safe communication
      - E.g., SSH instead of Telnet, HTTPS instead of HTTP
  - Circuit Encryption
    - Link Encryption
      - Protects the entire communication channel (all content in tunnel is encrypted)
    - End-to-End Encryption
      - Encrypts data only, leaving header information (e.g., IP addresses) unencrypted for routing
- Virtual Private Network (VPN) Encryption Modes
  - Link Encryption (Tunnel Mode)
    - Encrypts all data between two points in the communication path, such as between VPN concentrators
    - Risk

- Data may be exposed after leaving the VPN concentrator
  - End-to-End Encryption (Transport Mode)
    - Encrypts all data between two specific endpoints (e.g., computer-to-computer), with routing info unencrypted
  - VPN Components
    - VPN Concentrator/Gateway
      - Creates a secure tunnel over public or untrusted networks (usually the internet)
      - Often paired with Layer 2 Tunneling Protocol (L2TP) for Layer 2 protection, complementing Layer 3 IPsec encryption
  - Bottom Line
    - Understand communication security's purpose, EMSEC and Tempest standards, and circuit encryption techniques
- **Virtualized Networks**
  - Purpose of Virtualized Networks
    - Virtualized networks create a software-based representation of physical network components or services
    - Enable virtualization of routers, switches, firewalls, proxies, gateways, load balancers, etc.
  - Virtual Local Area Networks (VLANs)
    - Software-created LAN segments for segmentation and isolation
    - Implemented using 802.1Q Tagging (Q Tagging/Q Trunking)
    - Open standard for tagging Ethernet frames, enabling VLAN management by routers

- VLAN Security Risk
  - VLAN Hopping Attack
    - Attackers use double encapsulation to insert unauthorized VLAN tags
      - E.g., inserting VLAN 20 and VLAN 10 tags
    - By removing the outer VLAN tag, the switch processes unauthorized traffic on an unintended VLAN
- VLAN Hopping Prevention
  - Set all switch ports for computers to Access Mode
  - Use trunks only between switches
  - Change native VLAN from default (e.g., VLAN 1) to another number (e.g., VLAN 999)
  - Enforce native VLANs for trunk ports
- Types of VLANs
  - Private VLAN (PVLAN)
    - Limits communication within VLAN or to PVLAN's uplink port (also called port isolation)
  - Virtual Extensible LAN (VXLAN)
    - Tunnels Layer 2 frames over Layer 3, mainly used in cloud-based networks
- Software-Defined Networking (SDN)
  - Purpose
    - Uses virtualized network resources to eliminate platform/vendor dependencies and create a converged network
  - SDN Layers

- Infrastructure Layer
  - Provides network infrastructure and data forwarding
- Control Layer
  - Manages data flow between application and infrastructure layers
- Application Layer
  - Hosts services and applications
- Communication Directions
  - Northbound and Southbound
    - Ingress (northbound) and egress (southbound)
  - East-West
    - Lateral movement across networks
- Software-Defined Everything (SDX)
  - Virtualizes various components, enabling hardware-independent systems
  - Examples of SDX include containerization, serverless computing, infrastructure as code, and security as code
- Virtual Desktop Infrastructure (VDI)
  - Centralized hosting of virtual machines accessible by users remotely
  - Examples
    - VMware Horizon, Amazon WorkSpaces
- Virtual Mobile Infrastructure (VMI)
  - Centralized hosting of mobile operating systems, accessed remotely (common in BYOD environments)
  - Example
    - Parallels RAS (Remote Application Server)



# ISC2 CISSP

## (Study Guide)

- Bottom Line
  - Understand the role of virtualized networks, VLANs, PVLANS, and VLAN hopping
  - Know the fundamentals of SDN, SDX, VDI, and VMI



## Network Architectures

Objective 4.1: Apply secure design principles in network architectures

- **Content Distribution Networks**

- Content Distribution Networks (CDN) Overview
  - A CDN consists of multiple resources deployed in various locations accessible via the internet
  - Aims to provide high availability and efficient delivery of hosted content
  - Also referred to as a Content Delivery Network
- Purpose of a CDN
  - Ensures fast access to content for users globally
    - E.g., streaming services like Netflix, Amazon, Facebook
  - Reduces latency and load times for users by using multiple data centers
  - Handles high traffic by distributing requests across various servers
  - Supports various types of content: voice, data, music, documents, software licensing, and updates
- Architecture of CDNs
  - Predominantly a client-server relationship
  - Can also be deployed as peer-to-peer networks
    - E.g., BitTorrent, LimeWire, Napster
  - Example
    - A web browser (client) accessing content from a CDN server
- Security Considerations for CDNs

- Importance of securing hosted content with proper controls and protections
- Need for Service Level Agreements (SLA) to ensure performance and infrastructure provisioning
- Particularly crucial for cloud computing resources
- Defines performance metrics
  - E.g., 99.9% uptime
- Encryption and Authentication
  - Use of encryption to protect client-server communications
  - Implementation of mutual authentication
    - Client authenticates to the server
    - Server authenticates back to the client
    - Ensures confidentiality and integrity of the data transmitted over the CDN
- Key Points to Remember
  - Understand the primary purpose of CDNs
    - Enhancing availability and performance of content delivery
    - Familiarize with security measures that protect content and ensure reliable service through SLAs
    - Recognize the architecture and how client-server interactions occur in a CDN environment
- **Software Defined Networks**
  - Software Defined Networks (SDN) Overview
    - SDN is an architectural approach that separates various network functions and planes for better management

- It enables centralized control of the network, allowing for easier automation, orchestration, and policy enforcement
- Key Components of SDN Architecture
  - Controller
    - Central management element controlling network devices, automating tasks, and enforcing policies
  - Application Plane
    - Hosts applications for network automation, traffic optimization, and policy implementation
  - Data Plane
    - Comprises the network devices (routers, switches, access points) that execute the policies set by the controller
  - Northbound API
    - Interface that allows communication between the controller and applications
  - Southbound API
    - Interface that allows the controller to communicate with the data plane elements
- SDN Features
  - Enables real-time monitoring and traffic shaping.
  - Supports various applications like load balancing, intrusion detection/prevention systems (IDS/IDPS), and network orchestration
  - Facilitates scalability and flexibility within network operations

- SD-WAN (Software Defined Wide Area Network)
  - Extends the principles of SDN to wide area networks, allowing for simplified management and optimization of WAN traffic
  - Operates using similar concepts, focusing on abstraction and centralized control at a broader scale
- Security Considerations in SDN
  - Single Point of Failure
    - The SDN controller represents a critical vulnerability; if compromised, it can disrupt the entire network
  - API Vulnerabilities
    - Increasing the number of APIs expands the attack surface, necessitating strong access controls and security assessments
- Best Practices for Securing SDN
  - Implement network segmentation and isolation to mitigate the impact of breaches and lateral movement
  - Use strong authentication mechanisms, including multi-factor authentication (MFA), for network access
  - Monitor and log activities in real-time to detect and respond to security incidents promptly.
  - Conduct regular audits and assessments to identify vulnerabilities, misconfigurations, and compliance issues
- Key Points to Remember for the Exam
  - Understand the purpose and architecture of SDN and SD-WAN
  - Familiarize with the roles of the controller, application plane, and data plane

- Be aware of the security risks associated with SDN and the best practices to mitigate them
- **Application Programming Interfaces (API)**
  - Definition of API
    - Set of rules and protocols allowing different software applications to communicate and interact
    - Enables communication and data exchange between applications
  - Purpose of APIs
    - Facilitates application integration, data sharing, and third-party development
    - Essential for mobile apps and web services to access data from servers
  - Types of APIs
    - SOAP (Simple Object Access Protocol)
      - Uses XML for data exchange
      - Structured information exchange
    - RPC (Remote Procedure Call)
      - Executes code on a remote server as if local
      - Simplifies distributed computing
    - WebSocket API
      - Enables interaction between web applications and services
      - Uses HTTP/HTTPS protocols, transmits data types like JSON and XML
    - REST (Representational State Transfer)
      - Architectural style for network applications

- Emphasizes resource-based interactions using HTTP methods (GET, POST, PUT, DELETE)
- Stateless communication (servers do not save client data)
  - GraphQL
    - Query language for APIs allowing clients to request specific data
    - Offers flexible and efficient data retrieval
- API Deployment Methods
  - Private APIs
    - Reserved for internal users within an organization
  - Public APIs
    - Available to external users; increases attack surface
  - Partner APIs
    - Also known as shared APIs, for limited external access
  - Composite APIs
    - Hybrid approach combining two or more APIs for enhanced functionality
- API Gateways
  - Central interface for all API requests
  - Enforces security policies and facilitates access control
- Security Considerations
  - Implement mutual authentication for secure communication
  - Monitor API usage to detect anomalies
  - Ensure compliance with service level agreements (SLAs)

- Resources
  - RapidAPI Hub
    - Repository for numerous APIs available for integration
- Exam Focus Areas
  - Understand the different API types (SOAP, REST, RPC, WebSocket, GraphQL)
  - Be able to identify deployment methods and their implications
  - Recognize security measures associated with API usage
  - Know the role of API gateways and their importance in architecture
- **Network Functions Virtualization**
  - *Network Functions Virtualization (NFV)*
    - Technology that virtualizes network functions traditionally performed by dedicated hardware
    - Transforms traditional network management and configuration into a software-based approach
    - Increases scalability and flexibility, reduces costs, simplifies network operations
  - Components of NFV
    - *VNF (Virtualized Network Functions)*
    - Software applications that run network functions like firewalls, routers, and load balancers
    - *NFVI (Network Functions Virtualization Infrastructure)*
  - Hardware and software components that support the execution of VNFs
    - Includes compute, storage, and network resources

- *MANO (Management and Orchestration)*
- Framework that manages and orchestrates VNFs across NFVI
  - Automates deployment, scaling, and lifecycle management of network services
- Role in Software-Defined Networks (SDN)
  - NFV often works in conjunction with SDN, although they are distinct technologies
  - NFV focuses on the management of network functions, while SDN concentrates on network flows and decision-making processes
- Applications of NFV
  - Examples
  - Running network functions as virtual machines, replacing traditional hardware like routers and switches with software solutions
  - Use Cases
  - Data centers, enterprise networks, and as part of cloud services to enhance resource allocation and operational efficiency
- Security Considerations
  - Physical Security
  - Ensures that the physical infrastructure supporting NFV is protected
  - Cybersecurity Measures
  - Includes malware protection, isolation of network services, and robust access controls
  - Encryption
  - Essential for protecting data flows within and outside the NFV environment



- Challenges and Risks
  - Complexity
  - Managing an NFV environment can be complex due to the integration of multiple functional blocks
  - Visibility
  - Network traffic in virtualized environments may be less transparent, complicating monitoring and management
  - Segmentation
  - Essential for isolating network functions to prevent the spread of malware and enhance performance

## Secure Network Design

Objective 4.1: Apply secure design principles in network architectures

- **Transport Architecture**

- Transport Architecture

- The design and structure of networks that enable data transmission between endpoints, facilitating communication across various network setups including WAN, enterprise networks, and cloud services
    - Critical for ensuring effective network performance, scalability, security, and resilience

- Network Topologies

- Point-to-Point

- Direct connection between two devices
      - Ideal for simple, secure, and direct data transfer but lacks scalability

- Multi-Point

- Multiple devices connected, allowing simultaneous data transmissions
      - Used in most business and cloud networks for its flexibility

- Bus Topology

- All devices connected to a single central cable
      - Cost-effective and easy to set up but limited by bandwidth sharing and high failure susceptibility

- Star Topology
  - Devices connected to a central hub, typically a switch
  - Enhances performance management but central hub failure can disrupt the entire network
- Ring Topology
  - Each device connects to two others, forming a ring
  - Facilitates data token passing with improved fault tolerance but can be disrupted by a single link failure
- Mesh Topology
  - Every device connects to every other device
  - Offers high reliability and multiple paths for data transmission, though it can be complex and expensive to implement
- Architecture Planes
  - Data Plane
    - Manages the actual data transmission between devices
  - Control Plane
    - Controls routing and switching, making decisions about data paths based on configured routes and logic
  - Management Plane
    - Handles network management, configuration, and monitoring
- Security and Network Resilience
  - Encryption and Access Controls
    - Essential for protecting data in transit and ensuring only authorized access to network resources
  - Fault Tolerance

- Strategies like redundant systems and automatic failover mechanisms to maintain network operations during hardware or software failures
- Considerations for Network Design
  - Scalability
    - Ability to grow and expand the network without significant redesign
  - Bandwidth Optimization
    - Ensuring adequate bandwidth for all network activities to avoid bottlenecks and performance issues
  - Security Measures
    - Implementing robust security protocols to safeguard data and prevent unauthorized access
- **Performance Metrics**
  - Introduction to Performance Metrics
    - Purpose
      - Measure and evaluate the system or network performance using key performance indicators (KPIs)
    - Application
      - Establish a baseline for normal behavior to facilitate anomaly detection and optimize network operations
  - Key Performance Metrics
    - Throughput
      - Measures the actual amount of data transmitted or received over a network in a given time frame, usually in bits per second (bps)

- Influenced by factors like bandwidth, latency, and packet loss
- Bandwidth
  - The maximum data transmission capacity of a network, typically measured in megabits per second (Mbps) or gigabits per second (Gbps)
  - It defines the total available or required capacity for network traffic
- Latency
  - Time delay experienced in data transmission from one point to another, measured in milliseconds (ms)
  - Critical for real-time applications; affected by distance, network congestion, and routing
- Jitter
  - Variation in time delay in packet delivery over a network, affecting real-time communications like VoIP and video streaming
  - It's important for ensuring smooth transmission without delays or packet loss
- Signal to Noise Ratio (SNR)
  - Compares the level of the desired signal to the level of background noise, expressed in decibels (dB)
  - Higher SNR values indicate a clearer signal with less interference
- Impact on Network Architecture
  - Security Enhancements

- Utilization of performance metrics can help in strengthening network security by allowing timely detection and response to anomalies
- Optimization of Network Design
  - Metrics such as bandwidth and throughput guide the scaling and structuring of network resources to meet demand efficiently
- Tools for Monitoring Network Performance
  - SolarWinds
    - Offers features for network monitoring, SNMP monitoring, and network performance testing, among others
  - Nagios
    - Known for its robust IT infrastructure monitoring capabilities, helping in network management and anomaly detection
- Practical Applications
  - Network Baseline Establishment
    - Use metrics to define what normal network behavior looks like to quickly identify deviations that may indicate issues or attacks
  - Quality of Service (QoS)
    - Adjust policies and configurations based on performance analysis to prioritize traffic and ensure critical applications have necessary resources
- Real-World Examples
  - Throughput Testing
    - Demonstration using speed tests to measure actual data transfer rates compared to the maximum bandwidth available

- Latency Implications
  - Discussion on how latency affects user experience, particularly in real-time applications
- **Network Traffic Flows**
  - Throughput
    - The actual amount of data successfully transmitted or received across a network, typically measured in bits per second (bps)
    - Influenced by bandwidth, latency, and packet loss; essential for evaluating the capacity and efficiency of data transfer within the network
  - Bandwidth
    - The maximum rate of data transfer across a network path, usually measured in megabits or gigabits per second
    - Acts as the upper limit of throughput; critical for planning network capacity and ensuring sufficient resources for network traffic
  - Latency
    - The delay before a transfer of data begins following an instruction for its transfer, measured in milliseconds
    - Affects real-time applications significantly; high latency can degrade performance and user experience
  - Jitter
    - The variation in delay of received packets on a network, causing erratic and unpredictable network performance.

- Particularly problematic for voice over IP (VoIP) and real-time communications, leading to poor audio and video quality
- Signal to Noise Ratio (SNR)
  - A measure of signal strength relative to background noise, expressed in decibels (dB)
  - Higher SNR values indicate a clearer signal, which is crucial for wireless networks to minimize errors and improve reliability
- **Physical Network Segmentation**
  - Physical Network Segmentation
    - Enhances security, performance, and management by physically separating network segments
    - Methods
      - Dedicated physical infrastructure
      - Distinctive routing and switching configurations
      - Isolated network paths for sensitive data
  - Types of Physical Segmentation
    - In-Band Networks
      - Utilizes the same network infrastructure for both data and management traffic
      - Security Level
        - Least secure
      - Use Case
        - Cost-effective for smaller networks with limited resources



- Out-of-Band Networks (OOBN)
  - Employs a separate, dedicated network for management traffic, distinct from the data traffic network
  - Security Level
    - More secure than in-band networks
  - Benefits
    - Provides robust control for network management, allowing for maintenance or recovery without depending on the primary network's status
- Air-Gapped Networks
  - Represents the highest level of security through complete physical isolation from other networks and the internet
  - Security Level
    - Most secure
  - Application
    - Ideal for environments requiring stringent security measures to protect against external threats, such as military or critical infrastructure systems
- Applications and Implications
  - Segmentation Techniques
    - Physical isolation using different hardware
    - Use of security controls like firewalls and access lists to regulate traffic between segments
    - Implementing VLANs (though technically a logical segmentation technique, often coupled with physical strategies)

- Challenges and Considerations
  - Cost implications due to additional hardware and infrastructure
  - Maintenance complexity might increase due to the segmented environment
  - Balancing between security needs and operational efficiency
- **Logical Network Segmentation**
  - Logical Network Segmentation
    - Purpose
      - Enhances security, performance, and management by logically dividing a network into isolated segments
    - Advantages
      - Improved security through isolation of network segments
      - Enhanced network performance and management
      - Flexibility in network configuration and scalability
  - Key Logical Segmentation Techniques
    - VLANs (Virtual Local Area Networks)
      - Most common method for logical segmentation, used to group devices on different LAN segments that are configured to communicate as if on the same wire
      - Benefits
        - Flexibility, cost-effectiveness, and ease of setup
    - VPNs (Virtual Private Networks)
      - Purpose

# ISC2 CISSP

## (Study Guide)

- Securely connects remote users and sites over the internet
- Functionality
  - Encrypts data and uses tunneling protocols to secure communications over public networks
- VRFs (Virtual Routing and Forwarding)
  - Function
    - Allows multiple routing tables to coexist within the same router simultaneously
  - Use Cases
    - Ideal for multi-tenant environments, enhancing security and network path isolation
- VDOMs (Virtual Domains)
  - Application
    - Enables creation of multiple logical routers within a single physical device
  - Capabilities
    - Each VDOM operates independently with its own configuration, security policies, and routing
- Applications and Implications
  - VLANs
    - Simplifies network design and enhances security
    - Allows for efficient management of network resources
  - VPNs
    - Essential for secure remote access
    - Extends networks over geographically dispersed areas

- VRFs
  - Useful in environments where multiple users or tenants need to be isolated within a shared infrastructure
- VDOMs
  - Offers robust security and isolation in environments requiring rigorous compartmentalization of network resources
- **Micro-Segmentation**
  - Micro-Segmentation
    - The process of dividing a network into smaller, distinct security segments down to the individual workload level within data centers and cloud environments
    - Purpose
      - Enhances security by isolating workloads, applications, and services into secure zones, reducing the attack surface, and limiting lateral movement of attackers within the network
  - Benefits of Micro-Segmentation
    - Enhanced Security
      - Each segment or zone is secured separately, reducing the potential impact of breaches and attacks
    - Reduced Attack Surface
      - Limits the points of entry for attackers, making targeted attacks more difficult
    - Containment of Threats
      - Prevents the spread of breaches across segments, containing potential damage

- Key Technologies in Micro-Segmentation
  - VXLANs (Virtual Extensible LANs)
    - Extends the capabilities of traditional VLANs by allowing for up to 16 million unique network identifiers
    - Facilitates the creation of large-scale isolated networks over a physical network infrastructure
  - SDN (Software Defined Networking)
    - Provides centralized control over network traffic flow through programmable interfaces
    - Separates the control plane from the forwarding plane, enhancing flexibility and scalability
  - SD-WAN (Software Defined Wide Area Network)
    - Optimizes the performance of wide area networks, improving cloud application performance
    - Supports multiple connection types and offers dynamic path selection for efficiency and reliability
- Implementation Considerations
  - Zero Trust Model
    - Micro-segmentation is a core component of the zero trust security model, which assumes no implicit trust and verifies each request as though it originates from an open network
  - Policy Management
    - Requires careful management of security policies to ensure correct isolation and protection of network segments

- Technology Integration
  - Effective micro-segmentation often involves integrating multiple technologies like VXLAN, SDN, and SD-WAN to achieve comprehensive coverage and security
- Security Policies and Controls
  - Ensures that each segment can enforce its security policies independently
  - Facilitates rapid response and containment in case of security incidents within a segment
  - Use Case Scenarios
    - Data Centers
      - Protecting critical data and systems by isolating them into different segments based on sensitivity and function
  - Cloud Environments
    - Securing multi-tenant environments where customers' data and workloads must be isolated from each other
- Edge Networks
  - Edge Networks
    - Edge networks involve computing infrastructure placed at the boundary of a network, close to end-users for optimal performance and reduced latency
    - Purpose
      - Facilitates faster processing and response by bringing resources closer to the data source or user, enhancing application performance and user experience

- Key Components and Concepts
  - Ingress and Egress Traffic
    - Ingress (Southbound Traffic)
      - Data entering a network
    - Egress (Northbound Traffic)
      - Data leaving a network
    - These terms help define how data moves into and out of edge networks, crucial for understanding network flows and security implications
  - Network Peering
    - Establishes direct network connections that enhance data exchange efficiency and reduce reliance on third-party intermediaries
    - Common in scenarios involving virtual networks within the same region or across different cloud platforms, improving direct communication and reducing latency
- Benefits of Edge Networks
  - Reduced Latency
    - By minimizing the distance data must travel, edge networks reduce latency, which is critical for real-time applications
  - Improved Performance
    - Local processing of data ensures faster response times and better overall system performance

- Enhanced Security
  - By segmenting network traffic at the edge, there's better control over data flow, which can enhance security measures and reduce the attack surface
- Implementation Considerations
  - Infrastructure Design
    - Requires thoughtful design to ensure that edge nodes and related infrastructure are optimally placed to serve user needs without compromising security
  - Security Measures
    - While edge networks can improve performance, they also require robust security protocols to protect against potential vulnerabilities introduced by broader network access points



## Network Security and Attacks

### Objectives:

- 4.1 - Apply secure design principles in network architectures
- 4.2 - Secure network components
- 7.7 - Operate and maintain detection and preventative measures
  
- **Firewalls Concepts**
  - Firewall
    - Primarily software solutions designed to prevent unauthorized communications between networks by inspecting and filtering traffic based on predetermined security rules
    - Functionality
      - They control inbound and outbound traffic based on source and destination IP addresses, port numbers, protocols, and sometimes packet content
  - Types of Firewalls
    - Host-Based Firewalls
      - Installed directly on a server or computer
      - Protects the individual system by monitoring incoming and outgoing connections
      - Example tools include IPTables for Linux, Windows Firewall for Windows

- Network-Based Firewalls
  - Positioned at strategic points within the network to inspect all traffic passing through
  - Can be deployed as hardware appliances or virtualized solutions
  - Commonly used in corporate environments to enforce broad network security policies
- Web Application Firewalls (WAF)
  - Specialized type of firewall that focuses on web applications
  - Protects web apps by filtering and monitoring HTTP traffic between web applications and the Internet
  - Helps to prevent attacks such as SQL injection, cross-site scripting (XSS), and other web-based threats
- Deployment Strategies
  - Hardware (Appliance-Based) Firewalls
    - Deployed on dedicated hardware, offering robust performance due to dedicated resources
  - Virtual Firewalls
    - Deployed in virtual environments; flexibility allows for scaling and integration in cloud infrastructures
  - Software Firewalls
    - Can be integrated into other software systems or provided as standalone applications on operating systems
- Configuration and Policy
  - Firewalls operate using sets of rules defined in access control lists (ACLs), which permit or deny traffic based on specified conditions

- Rules are evaluated sequentially, and typically, a default deny (implicit deny) rule is set at the end of the list to block any traffic not explicitly allowed
- Traffic Inspection
  - Firewalls inspect different elements of network packets including source and destination IP addresses, port numbers, and the protocol used
  - Advanced firewalls can inspect packet payloads for deep packet inspection, enhancing detection capabilities for malicious activities
- Important Considerations for CSSP
  - Understanding the difference between host-based and network-based firewall implementations and their respective benefits and challenges
  - Recognizing the need for specific types of firewalls, like WAFs, in protecting web applications
  - The importance of properly configuring firewalls to effectively manage the traffic flow and enforce the network security policy
- **Types of Firewalls**
  - Static Packet Filtering Firewall
    - Function
      - Filters traffic based solely on source and destination IP addresses, protocols, and port numbers
    - Layer
      - Operates at the Network layer (Layer 3 of the OSI model)

- Characteristics
  - Known for being fast due to minimal processing overhead It does not track the state of network connections, hence referred to as "stateless"
- Common Deployment
  - Often implemented on routers and basic network gateways
- Proxy Firewall
  - Function
    - Acts as an intermediary between users and the internet, making network requests on behalf of devices
  - Types
    - Circuit-level Gateway
    - Establishes network sessions on behalf of clients, useful for hiding internal IP addresses
  - Application-level Gateway (Proxy)
    - Filters traffic based on application data besides IP addresses, offering detailed content filtering capabilities
    - Layer
      - Functions at the Application layer (Layer 7 of the OSI model)
    - Characteristics
      - Can inspect and manage application data, enhancing security but potentially reducing performance due to increased processing

### ■ Stateful Inspection Firewall

- Function
  - Monitors the state of active connections to make more informed decisions about which packets to allow or block
- Layer
  - Examines both the Network (Layer 3) and Transport (Layer 4) layers
- Characteristics
  - Tracks each connection's state, making it more secure than stateless firewalls but also more resource-intensive

### ■ Next Generation Firewall (NGFW)

- Function
  - Incorporates features of traditional and application-level firewalls with additional capabilities like intrusion prevention, deep packet inspection, and advanced threat protection
- Characteristics
  - Provides comprehensive security features that go beyond simple packet filtering, including application awareness, full-stack visibility, and threat intelligence
- Deployment
  - Common in environments requiring robust security measures where application-level inspection, user identity-based controls, and threat detection are critical

- Deployment Considerations
  - Static Packet Filtering and Proxy Firewalls
    - Are simpler in function and are often used in less complex environments or specific use cases where high throughput and basic filtering are sufficient
  - Stateful and Next Generation Firewalls
    - Are suited for environments where security needs are greater, including protecting sensitive data or supporting complex, dynamic applications
- Practical Insights
  - Firewalls, whether they operate at a basic network level or perform deep packet inspections, form the first line of defense in network security
  - The evolution from simple packet filters to advanced NGFWs reflects the growing complexity of cyber threats and the need for more sophisticated security measures
  - Understanding the operational specifics of each firewall type helps in designing appropriate security architectures and ensuring adequate protection against various cyber threats
- **Firewall Architecture**
  - Multi-Homed Firewalls
    - A multi-homed firewall has multiple network interfaces, often categorized as external (untrusted) and internal (trusted)

- Purpose
  - It serves as a gatekeeper by managing traffic between trusted internal networks and untrusted external sources
- Bastion Host
  - A special-purpose computer on a network specifically designed and configured to withstand attacks
  - Purpose
    - Acts as a fortified barrier, preventing unauthorized access from external threats while allowing legitimate external communications
  - Deployment
    - Typically placed in a network's DMZ to provide a secure and monitored node for external users accessing internal non-public services
- Screened Host
  - Incorporates a screening router (firewall) that handles network traffic filtering combined with a host behind the firewall that performs additional inspections
  - Purpose
    - Enhances security by providing a secondary layer of filtering and inspection beyond the primary firewall protection
  - Deployment
    - Used within the internal security boundary, offering an additional screening layer for incoming traffic before it reaches critical internal resources

- Screened Subnet (DMZ)
  - Involves two firewalls
    - One facing the external network and one protecting the internal network, with a DMZ positioned between them
  - Purpose
    - Increases security by segregating external-facing services from the internal network, reducing the risk of an attacker reaching internal systems
  - Deployment
    - Commonly used for public-facing applications like web servers, where the DMZ acts as a buffer zone offering services without exposing the internal network
- Deployment Considerations
  - Redundancy and High Availability
    - Firewalls are often deployed in pairs to ensure continuity and resilience, maintaining network security even if one firewall fails
  - Layered Security
    - By placing firewalls at different network layers and using diverse architectures (like bastion hosts and screened subnets), organizations can create a robust defense-in-depth strategy that enhances overall security
- Practical Applications
  - Corporate Networks



- Utilize multi-homed firewalls to segregate traffic between company resources and the internet, enhancing security and network performance
- Cloud Environments
  - Deploy bastion hosts to secure cloud-based resources, ensuring only authorized access while maintaining high security
- Complex Network Structures
  - Implement screened subnets for networks with high traffic demands or sensitive information, providing a buffer zone that filters harmful traffic before reaching the core network
- **IP Security**
  - IPsec
    - Primarily used to secure communications over untrusted networks by creating secure and trusted communication channels through tunneling
    - This involves encapsulating unsecure protocols within a secure protocol
    - Common Use Cases
      - The most prevalent application of IPsec is in Virtual Private Networks (VPNs), which provide a secure connection over the public internet by creating a private network connection
    - Cryptography
      - IPsec supports both symmetric (secret key) and asymmetric (public key) cryptography, enabling flexible security arrangements depending on the requirements of the communication scenario

- VPN Concentrators and Gateways
  - Essential for establishing VPN tunnels, these devices or software applications manage the creation and maintenance of IPsec tunnels
- L2TP and IPsec Combination
  - Often used together in VPNs, where L2TP handles the tunneling of Layer 2 data without encryption, and IPsec secures the IP traffic at Layer 3 with encryption and integrity checks
- IPsec Operational Modes
  - Transport Mode
    - Encrypts only the payload of the IP packet, leaving the header unencrypted
    - This mode is less secure as it exposes metadata about the communication but is more efficient
  - Tunnel Mode
    - Encrypts both the payload and the header of the IP packet, providing complete security but at the cost of higher resource consumption
- Security Associations and ISAKMP
  - Security Associations (SAs)
    - Dictate the security protocols and algorithms used in an IPsec connection, including key management
    - SAs are crucial for defining the terms of the encryption and authentication used

- ISAKMP
  - Handles the creation, negotiation, modification, and deletion of Security Associations
  - It is important for managing the keys and security protocols that IPsec will use
- Components of IPsec
  - Authentication Header (AH)
    - Provides integrity, authentication, and non-repudiation
    - It is crucial for protecting against replay attacks but does not encrypt data
  - Encapsulating Security Payload (ESP)
    - Provides confidentiality, integrity, and authentication of the data
    - It is used to encrypt the data and ensure that it has not been tampered with in transit
- Practical Deployment
  - VPN Implementation
    - IPsec can be configured directly on devices through client software or managed via concentrators/gateways that handle the encryption and decryption processes in a network
  - Efficiency vs. Security
    - Choosing between transport and tunnel mode involves balancing the need for efficiency against the requirement for security
    - Transport mode is more efficient but less secure as it exposes IP packet headers, while tunnel mode is more secure as it encrypts the entire packet

- **Endpoint Security**

- Endpoint Security

- Focuses on securing endpoints or nodes in a network where communications originate or terminate, such as computers, servers, and mobile devices
    - The goal is to eliminate single points of failure found in traditional network-based defenses like network intrusion detection systems (NIDS) and intrusion prevention systems (NIPS)

- Challenges with Network-Based Defenses

- Network-based systems like NIDS and NIPS may not catch traffic directly exchanged between endpoints, bypassing the network layer where these systems operate

- Strategies for Enhancing Endpoint Security

- Host-Based Firewalls

- Install on all endpoints capable of supporting them
      - Control both inbound and outbound communications to prevent unauthorized data exchanges

- Antivirus and Anti-Malware Software

- Essential for detecting and removing malicious software
      - Helps prevent the spread of malware across the network

- Host-Based IDS (HIDS) and IPS (HIPS)

- HIDS monitors for policy violations but does not take action, providing alerts for detected issues
      - HIPS actively responds to policy violations by taking pre-defined actions to mitigate threats

- Data Loss Prevention (DLP)
  - Monitors and controls data being transferred out of endpoints to prevent unauthorized data exfiltration
- Virtual Private Network (VPN)
  - VPN clients on endpoints can secure data communications over public networks by creating an encrypted tunnel to a VPN gateway
- Regular Patching and Updates
  - Keeping the operating system, applications, and security software up-to-date is crucial for closing vulnerabilities that could be exploited
- System Hardening
  - Minimizes the attack surface by disabling unnecessary services, applying the principle of least privilege, and enforcing strong access controls
- Practical Application and Benefits
  - Implementing these strategies creates multiple layers of security around each endpoint, significantly enhancing the overall security posture and reducing the risk of breaches
  - By securing each endpoint individually, organizations can ensure that even if the network perimeter is breached, the integrity and security of internal resources remain intact
- Endpoint Security in Action
  - Consider a scenario where a mobile device, computer, and server are all connected to the internet

- Each device should have a host-based firewall, intrusion detection/prevention systems, antivirus/anti-malware software, and other security measures configured according to best practices
  - This multi-layered approach ensures that even if one security measure fails, others still provide protection, embodying the defense-in-depth principle
- **Network Access Control**
    - Network Access Control (NAC)
      - Integrates various technologies to control and minimize access to a private network, focusing on enforcing strict security policies
      - Core Functions
        - Authentication
          - Confirms the identity of users and devices
        - Authorization
          - Grants access based on verified credentials
        - Accounting
          - Tracks user activities and resource usage
    - Key Technologies and Protocols
      - IEEE 802.1X
        - Often referred to as Port-Based NAC (PNAC), it manages network access at the point of entry, ensuring mutual authentication between devices and the network

- Role in BYOD and IoT
  - NAC ensures that devices meet security standards before accessing network resources, crucial for environments with diverse and numerous endpoint devices
- Types of NAC Implementations
  - Pre-Admission NAC
    - Validates device compliance with security policies before allowing network access, suitable for environments requiring high security like corporate networks
  - Post-Admission NAC
    - Allows devices network access but monitors them for policy violations, ideal for less restrictive environments like guest networks
- Deployment Models
  - Agent-Based NAC
    - Involves software installed on devices to monitor compliance and communicate with the NAC system
  - Agentless NAC
    - Monitors and controls devices remotely through the network, reducing the need for installed software but potentially less responsive than agent-based solutions
- Remediation Strategies
  - Quarantine Networks
    - Non-compliant devices are restricted to a separate network segment with limited access until compliance issues are resolved

- Captive Portals
  - Used primarily in guest networks to control access through a web-based login page that can enforce terms of service and basic credential checks
- In-Line vs. Out-of-Band
  - In-Line NAC
    - Positioned directly in the network traffic flow, actively monitoring and controlling all data passing through
  - Out-of-Band NAC
    - Operates alongside the network, monitoring access and applying policies without disrupting traffic flow
- Practical Application Scenario
  - Wired and Wireless Access
    - Demonstrates how NAC can manage both wired and wireless connections to ensure all devices adhere to the network's security policies
  - Use of Remediation Networks
    - Illustrates how non-compliant devices are handled, emphasizing the importance of keeping security risks isolated from the main network resources
- Conclusion
  - Importance of NAC
    - Ensures that all devices on a network, regardless of connection type, adhere to strict security standards to protect network integrity and data security



- **Adaptation and Flexibility**
  - Highlights the adaptability of NAC solutions in various environments, showcasing their crucial role in modern network security frameworks
- **Reconnaissance Attacks**
  - **Passive Reconnaissance (OSINT)**
    - Involves gathering information without direct interaction with the target
    - Utilizes publicly available data sources and aims to avoid detection
    - Common methods include web searching and social media analysis
  - **Active Reconnaissance**
    - Involves direct interaction with the target to gather more detailed information
    - Tools such as Nmap, Angry IP Scanner, and Nessus are typically used for ping sweeps and port scans
    - More likely to be detected by network security systems
  - **Types of Active Reconnaissance Attacks**
    - **Ping Sweep**
      - Identifies live hosts on a network by sending ICMP requests.
    - **Port Scan**
      - Determines open ports on network hosts, potentially identifying vulnerable services
    - **Banner Grabbing**
      - Gathers information about specific network services running on open ports

- SYN Scan
  - A type of port scan that checks for responsive ports using the SYN flag of the TCP protocol
- Defensive Measures
  - Restricting ICMP traffic and other protocols used in scanning to minimize the effectiveness of these reconnaissance methods
  - Implementing network segmentation and strict firewall rules to limit the scope of what an attacker can discover
  - Continuous monitoring and updating of network security measures to address vulnerabilities that may be exploited during reconnaissance
- **Spoofing and Poisoning Attacks**
  - Understanding Spoofing and Poisoning
    - Spoofing
      - Involves masquerading as a legitimate entity to deceive systems or individuals, usually by altering source addresses in network packets (IP or MAC addresses)
    - Poisoning
      - Involves injecting malicious data into otherwise trustworthy systems or processes, such as ARP caches or DNS records, to reroute or hijack sessions

- Key Attack Methods
  - IP Spoofing
    - Manipulates the IP address in packet headers to appear as if packets are coming from a trusted source, undermining network security measures
  - MAC Spoofing
    - Changes the media access control address to bypass access controls tied to specific hardware addresses
  - ARP Spoofing/Poisoning
    - Misleads network devices about the actual MAC address associated with an IP address, enabling man-in-the-middle attacks
  - DNS Spoofing/Poisoning
    - Alters DNS records to redirect traffic to malicious sites, facilitating phishing and data theft
- Defensive Measures
  - Port Security and MAC Filtering
    - Restricts network access to authorized devices only, reducing the risk of spoofing at the data link layer
  - Network Segmentation
    - Separates critical network segments to limit the spread of spoofed or poisoned packets
  - DNS Security Enhancements (DNSSEC)
    - Provides authentication for DNS responses to prevent DNS spoofing
  - Regular Monitoring and Updating

- Ensures that security devices and software are up-to-date and monitoring for unusual activities indicative of spoofing or poisoning
  - Implications for Security Architecture
    - Security teams must design networks with these threats in mind, ensuring that protective measures are integrated at all layers of the OSI model, particularly at the data link and network layers
    - Training and awareness for staff on recognizing and responding to spoofing and poisoning can prevent successful attacks
- **Denial of Service Attacks**
  - Types of DoS Attacks
    - Distributed Denial of Service (DDoS)
      - Uses a network of compromised devices (botnets) to flood a target with overwhelming traffic, making it inaccessible
    - SYN Flood
      - Exploits the TCP handshake by sending numerous SYN packets to a target, exhausting server resources by leaving connections half-open
    - Ping Flood
      - Involves inundating the target with ICMP Echo Request (ping) packets to consume its bandwidth and processing capacity
    - Buffer Overflow
      - Sends more data than a buffer can handle, potentially leading to system crashes or unauthorized access

- Reflection and Amplification Attacks
  - Smurf Attack (ICMP Echo)
    - Spoofs the victim's IP address and broadcasts large numbers of ICMP packets to network devices, which reply to the victim
  - Fraggle Attack (UDP Echo)
    - Similar to the Smurf attack but uses UDP echo packets instead, causing a flood of responses to the victim
- Legacy Attacks
  - Ping of Death
    - Sends malformed or oversized packets that exceed the MTU, which some systems can't handle, leading to crashes
  - Teardrop Attack
    - Sends fragmented packets that, when reassembled, cause crashes due to overlapping payloads
  - Land Attack
    - Sends SYN packets with the target's own IP address as both sender and receiver, causing the machine to attempt to open a connection to itself
- Protection Strategies
  - Implement rate limiting and traffic analysis to detect and mitigate unusual traffic patterns
  - Use firewalls and intrusion detection systems (IDS) to block known attack signatures and manage traffic flows

- Employ network redundancy and load balancing to distribute traffic evenly across multiple servers, reducing the impact of an attack on a single point
- Maintain up-to-date security patches and configurations to mitigate known vulnerabilities that could be exploited in DoS attacks
- Educational and Preventive Measures
  - Train staff to recognize the signs of a DoS attack and respond according to an established incident response plan
  - Conduct regular security audits and penetration testing to identify and address vulnerabilities in the network infrastructure that could be exploited in a DoS attack

## Secure Communications

Objective 4.3: Implement secure communication channels according to design

- **Remote Access Security**

- Nature of Remote Access

- Remote access enables users to connect to organizational resources from external locations, which introduces various security challenges. This includes teleworkers, contractors, and other external entities needing access to the network

- Security Concerns

- The primary concern with remote access is ensuring the integrity and security of data transmitted across potentially insecure networks like the internet
    - Devices used for remote access may not always comply with organizational security policies, especially personal devices in a BYOD (Bring Your Own Device) scenario

- Access Mechanisms

- Specific Service Access

- Grants users access to specific applications or services, limiting broader network exposure

- Application Portals

- Provide centralized access to multiple applications, enhancing user convenience while centralizing security controls

- Tunneling (VPNs)

# ISC2 CISSP

## (Study Guide)

- Secures data transmissions by encrypting data sent over public networks, crucial for protecting sensitive information
- Remote Control and Desktop Sharing
  - Facilitates direct or indirect control over remote systems, essential for support and remote work scenarios
- Authentication Methods
  - Robust authentication mechanisms are vital. Use of RADIUS (Remote Authentication Dial-In User Service) and TACACS (Terminal Access Controller Access Control System) for AAA services (Authentication, Authorization, Accounting) helps ensure that only authorized users gain access
  - Implementing multi-factor authentication (MFA) enhances security by requiring multiple proofs of identity
- Defensive Strategies
  - Logging and Auditing
    - Continuously monitor and log all remote access sessions to detect and respond to potential security incidents promptly
  - Secure Configuration
    - Ensure remote devices adhere to security policies and standards, including up-to-date antivirus protection, firewall enforcement, and necessary security patches
  - Encryption
    - Utilize strong encryption for data at rest and in transit to protect against interception and unauthorized access



- Network Segmentation
  - Use dedicated network segments for remote access, reducing the risk of lateral movement within the network if a remote system is compromised
- Contractual Agreements
  - Establish clear terms regarding remote access policies and security expectations with all third parties
  - This includes SLAs and MOUs to formalize the security requirements and responsibilities
- Best Practices
  - Regularly update and patch all systems involved in remote access to mitigate vulnerabilities
  - Provide training and support for remote users to ensure compliance with security policies and practices
  - Continuously evaluate and adjust remote access policies and controls based on emerging threats and changes in the organizational environment
- **Multimedia Collaboration**
  - Multimedia Collaboration
    - Facilitates real-time interaction among team members using various digital platforms and tools such as emails, instant messaging, video conferencing, and collaborative editing platforms
  - Common Tools
    - Tools include email, instant messaging apps, video conferencing software like Zoom, and cloud-based project management applications

- These tools support a range of functions from simple text communication to complex project planning and execution
- Security Challenges
  - The main security concerns revolve around ensuring the integrity and confidentiality of the data exchanged during multimedia interactions
  - This includes safeguarding sensitive communications in remote meetings, protecting files transferred via instant messaging, and securing access to collaborative workspaces
- Critical Security Measures
  - Authentication and Authorization
    - Strong user authentication processes are crucial to ensure that only authorized personnel have access to collaborative tools and sensitive data
  - Encryption
    - Implementing end-to-end encryption for all forms of communication within multimedia tools to protect data from interception during transmission
  - Data Control and Management
    - Managing data egress and ingress effectively to prevent data leaks and ensure that data shared through these platforms does not violate organizational security policies
  - Antivirus and Anti-malware Solutions
    - Integrating robust antivirus and anti-malware solutions to scan and filter out malicious content from files being shared through these platforms

- Access Controls
  - Setting stringent access controls and permissions within collaborative tools to limit user access based on roles, ensuring that sensitive information is only accessible to those who need it
- Data Protection and Retention
  - After collaboration sessions, it's vital to securely store and manage session records, including chat logs, shared files, and video recordings
  - Implement policies for the retention and deletion of such data to comply with data protection regulations
- Physical and Environmental Security
  - Be mindful of the physical environments from which participants join multimedia sessions
  - Sensitive information displayed on screens or audible in the background should be controlled to avoid accidental data exposure
- Social Engineering Defenses
  - Educate and train users on the risks of social engineering attacks through these platforms
  - Users should be aware of the tactics that might be used by attackers to gain unauthorized access to information or systems
- Legal and Regulatory Compliance
  - Ensure all multimedia collaboration practices comply with relevant laws and industry regulations, particularly those concerning data protection and privacy
  - This includes the General Data Protection Regulation (GDPR) for organizations operating in or dealing with data from the European Union

- **Voice Communications**

- Overview of Voice Communications

- Private Branch Exchange (PBX)

- A local telephone system used within organizations
      - It connects to the Public Switched Telephone Network (PSTN) to facilitate external calls

- Public Switched Telephone Network (PSTN)

- Also known as Plain Old Telephone Service (POTS), this network interconnects different telecommunication networks, enabling phone communications globally

- Security Vulnerabilities

- Eavesdropping

- Both PBX and PSTN are susceptible to wiretapping, where unauthorized individuals can intercept and listen to voice communications

- Phreaking

- Techniques like blue box and red box attacks manipulate telephone systems to access services without payment
      - Modern systems have mostly mitigated these risks

- *Voice over Internet Protocol (VoIP)*

- VoIP technology allows voice communications over internet protocol networks, integrating with the existing data network infrastructure

- Protocols

- Real-time Transport Protocol (RTP)

- Manages the transmission of audio and video over IP networks
- Secure RTP (SRTP)
  - Enhances RTP by adding encryption, message authentication, and integrity checks
- ZRTP
  - Combines the Diffie-Hellman key exchange with SRTP for secure VoIP communications
- Advantages
  - Reduces infrastructure needs by leveraging existing network equipment and cables
- Security Attacks and Defenses
  - Vishing
    - Social engineering attacks via VoIP, where attackers manipulate callers into divulging sensitive information
  - SPIT (Spam over Internet Telephony)
    - Unsolicited pre-recorded calls that may be used for phishing or spreading misinformation
  - VoIP Hopping
    - Attackers exploit vulnerabilities to access unauthorized network segments or data
  - Man-in-the-Middle Attacks
    - Attackers intercept VoIP communications, potentially leading to data breaches or eavesdropping

- Security Recommendations
  - Encryption
    - Encrypt all VoIP communications to protect against eavesdropping and interception
  - Network Segmentation
    - Use VLANs to separate voice traffic from regular data traffic, enhancing security and performance
  - Strong Authentication
    - Implement robust authentication mechanisms to ensure only authorized devices and users can access the VoIP system
  - Regular Audits
    - Conduct regular security audits and updates to VoIP infrastructure to address vulnerabilities and ensure compliance with security policies
- Email Security
  - Key Concepts and Protocols
    - Email Protocols
      - SMTP (Simple Mail Transfer Protocol)
        - Used for sending emails
        - Operates on port 25 and is unsecure by default
      - POP3 (Post Office Protocol version 3)
        - Used for retrieving emails from a server
        - Typically unsecure but can implement Kerberos for enhanced security
      - IMAP (Internet Message Access Protocol)

- Allows management of emails on a server
  - Supports TLS on port 993 for secure connections
- Email Client-Server Architecture
  - Clients use SMTP to send and POP3 or IMAP to retrieve emails
  - Integration with other systems like ITU X.400 for global message handling standards
- Security Risks and Threats
  - Common Threats
    - Spamming
      - Unsolicited messages that may lead to more severe attacks
    - Phishing
      - Deceptive emails attempting to acquire sensitive data
    - Masquerading and Spoofing
      - Sending emails from a forged source to trick recipients
  - Specific Attacks
    - Open Relay
      - SMTP servers that relay emails without proper authentication, posing a significant security risk
- Security Techniques and Standards
  - Encryption and Authentication Protocols
    - MOSS (MIME Object Security Services)
      - Utilizes cryptographic hash functions and encryption algorithms like MD5 and DES for securing email messages
    - PEM (Privacy Enhanced Mail)

# ISC2 CISSP

## (Study Guide)

- Implements encryption and digital certificates for comprehensive email security
- PGP (Pretty Good Privacy)
  - Secures emails by encrypting message contents, widely recognized for its robustness
- S/MIME (Secure/Multipurpose Internet Mail Extensions)
  - Uses digital certificates to ensure email authenticity, confidentiality, and integrity
- Domain and Sender Verification
  - DKIM (DomainKeys Identified Mail)
    - Helps verify the domain of the sender to prevent email spoofing
  - SPF (Sender Policy Framework)
    - Validates email senders to combat spam and spoofing by verifying sender IP addresses against DNS records
- Best Practices for Email Security Management
  - Policies and Procedures
    - Establish strong email security policies that define acceptable use and outline measures against misuse
    - Implement robust access controls to safeguard email accounts and data
  - Technical Safeguards
    - Use endpoint security solutions to protect against malicious code in email attachments



- Regularly update and patch email systems to guard against vulnerabilities
  - Employ email filtering techniques to block spam and potentially harmful messages
  - Data Protection and Compliance
    - Ensure that email backups and data retention align with organizational policies and compliance requirements
    - Implement strong encryption for data at rest and in transit to protect sensitive information contained in emails
- **Backhaul Networks**
  - Backhaul Network
    - Defined as the backbone for connecting access networks to core networks
    - Utilizes backhaul links to connect smaller access networks or devices to a larger central core network
    - Provides bandwidth and connectivity to support data communications between remote locations and central network infrastructure
  - Backhaul Link
    - Serves to establish network connectivity between the access and core layers of a network
    - Acts as uplinks from the access to the core
  - Security Best Practices for Backhaul Networks
    - Encryption
      - Essential to protect data in transit and ensure confidentiality
      - Examples of encryption include AES and TLS

# ISC2 CISSP

## (Study Guide)

- Access Controls
  - Enforce strict access controls to restrict unauthorized access to backhaul network components and critical infrastructure
- Authentication
  - Implement multi-factor authentication wherever possible
  - Ensure strong single-factor authentication where necessary
- Network Segmentation
  - Isolate traffic and applications to limit data breaches, prevent lateral movement, and reduce congestion
  - Techniques include using VLANs and secure zones
- Monitoring and Intrusion Detection
  - Deploy real-time monitoring to detect unusual network behavior, unauthorized access attempts, and security incidents
  - Implement Intrusion Detection and Prevention Systems (IDPS) to provide a deeper analysis of potential threats
- Additional Considerations
  - Regular assessments and demonstrating due care and diligence in network security practices are crucial

## Wireless Networking Introduction

### Objectives:

- 3.5 - Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements
- 4.1 - Apply secure design principles in network architectures
- **Wireless Networks**
  - Wireless Networks
    - Enable communications without the need for physical cable medium
    - Uses radio frequency (RF) to transmit data
    - Frequencies range from 3 Hz to 300 GHz
    - Common frequencies
      - 900 MHz, 2.4 GHz, 5 GHz
  - Modulation
    - Technique of changing information on the radio frequency
    - Varies properties of the signal such as amplitude, frequency, phase
  - Spread Spectrum
    - Transmits communications over multiple frequencies to increase performance
    - Types
      - Frequency Hopping Spread Spectrum (FHSS)
        - Randomly changes frequencies to minimize interference and improve security against eavesdropping

- Direct Sequence Spread Spectrum (DSSS)
  - Divides data among multiple frequencies transmitted simultaneously, using a chipping code to reduce signal interference
- Orthogonal Frequency Division Multiplexing (OFDM)
  - Divides data into multiple substreams transmitted over separate channels
  - Reduces transmission bandwidth while increasing throughput
- Wireless Local Area Network (WLAN)
  - Common form of wireless networking encountered in both the exam and practice
  - Governed by IEEE 802.11 standards which define hardware and physical requirements
  - Standards include amendments A, B, G, N, AC with varying speeds and frequencies
- Broadcast Channels
  - Divide RF signal into subfrequencies
  - Types
    - Public Channels
      - Shared and can overlap, increasing risk of interference and eavesdropping
    - Private Channels
      - Exclusive to an organization, offering more controlled use
- Light Fidelity (Li-Fi)
  - Introduced in 2011 for optical wireless communications using visible, infrared, or ultraviolet light

- Transmits data by modulating light intensity, similar to fiber optic communications but through air
- ZigBee
  - Open standard for creating personal area networks using IEEE 802.15.4
  - Utilizes low power wireless signals suitable for IoT and mobile devices
  - Security features include 128-bit AES encryption
  - Vulnerable to physical access, key attacks, and replay or injection attacks
- **Wireless Network Modes**
  - Wireless Network Modes
    - Modes essential for CISSP exam understanding
    - Types
      - Ad hoc mode
        - Decentralized, peer-to-peer mode without a network intermediary
      - Infrastructure mode
        - Involves wireless access points like routers or extenders
  - Sub-Modes of Infrastructure Mode
    - Standalone mode
      - Connects wireless devices without linking to a physical network
    - Wired Extension mode
      - Connects wireless devices to a physical network, allowing access to external networks
    - Enterprise Extended Mode

- Utilizes multiple access points with the same network identifier to facilitate network access across different points
- Bridge Mode
  - Connects two physical networks via a wireless connection
- Service Set Identifiers (SSID)
  - Basic SSID (BSSID)
    - Used in ad hoc mode for unique identification of wireless networks
  - Extended SSID (ESSID)
    - Employed in infrastructure mode for network identification
- Network Access and Management
  - Antenna Placement
    - Centralize antennas to ensure even coverage and avoid signal obstructions like walls and electrical equipment
  - Defines wireless coverage area as "cell" to optimize signal distribution and minimize interference
- Bluetooth Technology
  - Personal area network technology prevalent in mobile devices
  - Involves pairing devices, typically with a 4-digit PIN transmitted in clear text
  - Governed by IEEE 802.15 standard, focusing on pairing protocols and security implications
- Cellular Networks
  - Utilize radio frequencies for wide geographical coverage
  - Comprise cell sites or base stations for transmitting voice, video, and data

- Essential for understanding the broad application of wireless technology beyond local networks

- **Wireless Network Security**

- Wireless Network Security Concepts
  - Importance for CISSP exam
  - Wireless communications do not require physical media but are susceptible to security vulnerabilities
- Wi-Fi Protected Setup (WPS)
  - Simplifies and secures wireless network access
  - Utilizes two four-digit PINs for authentication
  - Not recommended for use due to security concerns
- Encryption Protocols
  - Wired Equivalent Privacy (WEP)
    - Provides 64-bit and 128-bit encryption using the RC4 cipher, known for its vulnerabilities
  - Wi-Fi Protected Access (WPA)
    - Improves on WEP's weaknesses using Temporal Key Integrity Protocol (TKIP) and Lightweight Extensible Authentication Protocol (LEAP)
  - Wi-Fi Protected Access II (WPA2)
    - Enhances security over WPA using Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) based on AES
  - Wi-Fi Protected Access III (WPA3)

- Uses 192-bit AES encryption in enterprise mode and 128-bit AES in personal mode, including Secure Authentication of Equals (SAE) for secure key exchange
- Key Wireless Network Attacks
  - CRACK (Key Reinstallation Attack)
    - Exploits vulnerabilities in WPA2's four-way handshake to reuse encryption keys
  - Signal Jamming
    - Denial of Service (DoS) attack that disrupts wireless communications
  - Rogue Access Points
    - Unauthorized access points connected to the network that bypass security controls
  - Evil Twin Attacks
    - Fake wireless access points created to capture valid credentials
  - Replay Attacks
    - Reuse previously authenticated communications to bypass security measures
  - War Driving
    - Identifying and exploiting vulnerable wireless networks by moving around an area
  - War Chalking
    - Marking locations with open or vulnerable wireless networks for others to exploit



- Bluetooth Security Threats
  - Bluejacking
    - Sending unsolicited messages to collect data from a device
  - BlueSnarfing
    - Forcing a Bluetooth connection to access stored data
  - BlueBugging
    - Gaining control of a device to execute commands without the user's knowledge
- General Wi-Fi Security Measures
  - Change default passwords and SSIDs on wireless devices to prevent unauthorized access
  - Consider SSID broadcast options (visible or hidden)
  - Implement MAC address filtering to control device connections
  - Use advanced encryption standards like WPA2 or WPA3
  - Manage physical access and employ network access controls like 802.1X
  - Apply a defense-in-depth strategy to protect the wireless network
- **Mobile Device Management**
  - Delegated Identity Management
    - Delegated Identity Management involves outsourcing identity management responsibilities to a third-party provider
    - Part of Federated Identity Management, focusing on delegating authentication services
    - Also known as Identity as a Service (IDaaS)
  - Key Providers and Uses

# ISC2 CISSP

## (Study Guide)

- Major providers include Google, Oracle, Microsoft, Apple, Facebook, Amazon, LinkedIn, OneLogin
- Common in sectors lacking infrastructure for Active Directory or LDAP
- Utilized extensively in information security and technology sectors
- Benefits
  - Time and cost-efficient, reducing the need for in-house identity management systems
  - Provides consistent and reliable management of identification and authentication
  - Facilitates business continuity and disaster recovery
  - Simplifies credential management across multiple sites
- Implementation Types
  - On-Premise
    - Local authentication mechanisms installed within the facility
  - Off-Premise
    - Authentication mechanisms hosted externally, typically in the cloud
  - Hybrid
    - Combines on-premise and off-premise solutions for flexibility and redundancy
- Integration with Enterprise Systems
  - Commonly integrated with enterprise single sign-on systems to provide seamless access across various facilities
  - Often adopted to minimize infrastructure and administrative overhead
- Example of Usage

- Users may log into platforms using their Google, Facebook, or LinkedIn credentials
- This process illustrates how delegated identity management simplifies access by utilizing third-party credentials
- Considerations for Implementation
  - High Availability
    - Ensuring that the third-party service is reliable and available without significant downtime
  - Credential Protection
    - Must meet or exceed organizational policies and regulatory standards
  - Account Management
    - Planning out roles and privileges to minimize changes and disruptions
- Security and Compliance
  - Essential to ensure that the third-party provider complies with relevant industry standards and regulations
  - Organizations remain responsible for the security and privacy of the delegated identities

## Identity Management Introduction

### Objectives:

- 5.2 - Design identification and authentication strategy
  - E.g., people, devices, and services
- 5.3 - Federated identity with a third-party service
- 5.5 - Manage the identity and access provisioning lifecycle
- 5.6 - Implement authentication systems
  
- **Establishing Identity**
  - Introduction to Identity Management
    - Identity pertains to both individuals and entities such as computers, servers, and applications
    - Key components include hostnames, IP addresses, and MAC addresses, which serve as forms of identity
  - Registration and Identity Creation
    - Identity creation requires a registration process
    - Involves adding the applicant's identity into a registration system often part of an identification and authentication management system
  - Credential Service Provider (CSP)
    - CSP performs the identity proofing process
    - Confirms the applicant's identity by processing and affirming evidence based on set assurance levels

- Methods of Identification
  - Identification can be achieved using IDs such as driver's licenses, passports, and birth certificates
  - Identification processes can be conducted in person or remotely, dependent on the desired assurance level
- Assurance Levels
  - Level 1
    - Self-asserted attributes without validation, suitable for low-security access
  - Level 2
    - Requires evidence supporting the existence of the claimed identity, preferred to be done in person
  - Level 3
    - Physical presence required, suitable for high-security roles such as system administrators
- Identity Proofing Process
  - Initiated by the applicant providing necessary information and evidence to the CSP
  - Consists of the steps of resolution, validation, and verification
    - Resolution
      - Collection and initial assessment of applicant's attributes and evidence
    - Validation
      - Authentication of the evidence's authenticity and accuracy
    - Verification

- Confirmation of the claimed identity's real-life existence
- Proofing Process Steps
  - Applicant Request
    - Individual requests identity establishment
  - Resolution
    - Gathering and assessment of evidence to affirm uniqueness
  - Validation
    - Ensuring authenticity and accuracy of provided information
  - Verification
    - Linkage of the claimed identity with real-life existence
  - Enrollment
    - Applicant becomes a recognized user or subscriber upon successful verification
- Security and Privacy Considerations
  - Handling of personally identifiable information (PII) must adhere to stringent security policies
  - Validation often involves checking official documents against authoritative sources
  - Protecting applicant data during interactions with third parties or government agencies is crucial
- Enrollment and Completion
  - Enrollment process should be user-friendly and clearly communicate data collection purposes and protection measures
  - Final step involves the applicant confirming their enrollment and receiving credentials for system access

- **Identity Management**

- Identity
  - Is the assertion by a subject of who or what they are
  - It encompasses both individuals (users) and entities (computers, applications, servers), characterized by attributes like hostnames, IP addresses, and MAC addresses
- Provisioning and Deprovisioning
  - Provisioning
    - Process of creating identity and authentication credentials for a subject
  - Deprovisioning
    - Removal or expiration of identity and its associated credentials
- Authentication
  - The process of verifying or confirming a claimed identity
  - Example
    - Verifying if a person claiming to be a drummer in a band truly holds that identity by checking if they appear with the band in shows or photos
- Authorization
  - Determines if a subject has permission to access a specific object, such as determining if a person is allowed to play drums for a band on stage
- Access Controls
  - Manage how subjects can interact with objects, determining the level of interaction permissible

- Identity and Authentication Management
  - Involves managing access through verification of identities (username) and authentication credentials (password)
  - Once identity and authentication are validated, access controls dictate the level of interaction with the website or system
- Centralized vs. Decentralized Access Control
  - Centralized Access Control
    - Uses a single entity (e.g., Active Directory, LDAP, RADIUS) to handle identification, authentication, and authorization
  - Decentralized Access Control
    - Each host or object has its own identity and access management, often referred to as local authentication
- Distributed Access Controls
  - Combines centralized and decentralized approaches where centralized handles regular user access, and decentralized manages high-privilege access (administrator, root)
  - Provides a fallback mechanism if centralized authentication fail
- **Federated Identity Management**
  - Federated Identity Management (FIM)
    - Enables use of single sign-on (SSO) credentials across multiple different technologies
    - Digital identities are created, including attributes that define the subject and their access privileges



- Allows digital identity usage outside of the originating organization, facilitating inter-organizational access and authorization
- Security Assertion Markup Language (SAML)
  - An open standard for identity management maintained by OASIS (Organization for the Advancement of Structured Information Standards)
  - Built upon XML and uses SOAP for messaging requests and assertions
  - Provides a structured format for exchanging authentication and authorization data
  - Key components
    - Identity Provider
      - Authenticates the identity of the subject
    - Service Provider
      - Provides services or resources based on authentication from the Identity Provider
    - Principal (Subject)
      - The entity requesting access to a service/resource
- SAML Assertions, Protocols, and Bindings
  - Assertions
    - Statements made by the Identity Provider about a subject's authentication, attributes, and authorization
  - Protocol
    - Defines how requests for identities are made and how information is exchanged
  - Bindings

- Specifies how SAML protocol is transported within existing protocols like HTTP or SOAP
- Service Provisioning Markup Language (SPML)
  - Used for exchanging user, resource, and service provisioning information
  - XML-based protocol that automates identity creation and access provisioning within organizations
  - Related to Directory Service Markup Language (DSML), which formats directory service information into XML
- Extensible Access Control Markup Language (XACML)
  - Used with SAML in federated systems to enforce consistent access control policies
  - Determines access based on the attributes of the subject, the resource, and the action involved
- Operational Flow of SAML
  - The subject authenticates to the service provider
  - The service provider verifies the subject's identity with the Identity Provider
  - Once confirmed, the subject is granted access based on the assertions received
- Practical Applications
  - FIM allows subjects to use single credentials across platforms when collaborating with external organizations
  - SAML facilitates seamless authentication and authorization across web-based applications, enhancing user experience and security for federated identities

- **Delegated Identity Management**

- Overview of Delegated Identity Management
  - Delegation of identity management tasks to a third party
  - Also known as Identity as a Service (IDaaS)
  - Examples of providers include Google, Oracle, Microsoft, Apple, Facebook, Amazon, LinkedIn, and OneLogin
- Benefits of Delegated Identity Management
  - Cost-effective
    - Reduces the need for in-house infrastructure and expertise.
  - Efficiency
    - Streamlines the management of identity and authentication
  - Business Continuity
    - Facilitates easier access across locations, enhancing disaster recovery and business continuity plans
- Implementation Types
  - On-Premise
    - Identity management systems are installed locally within the organization's facilities
  - Off-Premise
    - Identity management is handled externally, typically through cloud-based services
  - Hybrid
    - Combines both on-premise and off-premise solutions for identity management

- Operational Considerations
  - High Availability
    - Ensuring the third-party service is reliable and adheres to agreed service levels to prevent downtime
  - Credential Protection
    - Ensuring that the third-party service meets or exceeds organizational security policies and relevant regulations
  - Planning and Role Management
    - Planning account requirements and roles thoroughly to minimize the need for frequent changes
- Responsibilities
  - Despite delegation, the organization remains accountable for ensuring the protection of user data as per compliance and regulatory standards
  - Transparency with users about the use of third-party identity management services and the security measures in place
- **Identity and Access Lifecycle**
  - Identity and Access Provisioning Lifecycle
    - Involves the creation, management, and revocation of an identity
    - Key processes
      - Provisioning, managing, and revocation of access and credentials
  - Provisioning
    - Creation of identity and authentication credentials for a subject
    - Occurs at the beginning of the lifecycle

# ISC2 CISSP

## (Study Guide)

- Involves registering or enrolling the subject to establish their identity and access requirements
- Deprovisioning
  - Opposite of provisioning; involves removing or disabling authentication credentials
  - Necessary when a subject no longer requires access or leaves the organization
- Lifecycle Steps
  - Provisioning
    - Starts with enrollment or registration
    - Requires solid justification for the identity's creation based on organizational policies
    - Involves collecting evidence of identity such as photo ID, driver's license, or other documents
    - May include background checks and security awareness training
    - Creation of a unique username and authentication credentials
    - Access is granted based on defined roles and privileges, adhering to least privilege and need-to-know principles
  - Review
    - Periodic review of accounts to ensure access privileges are current and appropriate
    - Can be triggered by audits, assessments, or personnel changes
    - Goal is to adjust privileges to prevent privilege creep and ensure compliance with organizational policies
  - Revocation

# ISC2 CISSP

## (Study Guide)

- Disabling or removing access when no longer needed
  - Triggered by employment termination, role changes, or policy violations
  - Accounts should be disabled, not deleted, to preserve the ability to decrypt data or for audit purposes
- Key Considerations
    - Ensure provisioning processes are automated and secure
    - Regularly review and adjust access to prevent unauthorized use
    - Quickly revoke access when necessary to minimize security risks

## Authentication Mechanisms

Objectives:

- 5.2 - Design identification and authentication strategy
  - E.g., people, devices, and services
- 5.4 - Implement and manage authorization mechanisms
- 5.6 - Implement authentication systems
- **Authentication Systems**
  - Key Concepts
    - Authentication System
      - A system designed to store information about a subject's identity and authentication credentials
      - It can be centralized (a single repository like LDAP or Active Directory) or decentralized (local authentication at multiple points)
  - Directory Services
    - Directory Service
      - A database that contains and manages user identification, authentication, authorization, and access control functions
    - X.500 Standard
      - The most common form of directory services used for storing subject information
  - Protocols
    - LDAP (Lightweight Directory Access Protocol)

- The most commonly used directory service protocol over IP-based networks, running on port 389 (unencrypted) or 636 (encrypted)
- DNS (Domain Name System)
  - Also acts as a directory service
- NIS (Network Information Service)
- An older protocol that is rarely used today
- LDAP (Lightweight Directory Access Protocol)
  - LDAP
    - An open-standard directory services protocol, used for accessing and maintaining distributed directory information over IP networks
  - Common Ports
    - Port 389 (TCP)
      - Unsecured
    - Port 636 (TCP)
      - Secured (LDAP over SSL)
  - Data Formats in LDAP
  - Distinguished Name (DN)
    - Uniquely identifies a subject using multiple fields
  - Common Name (CN)
    - Represents the user's full name or an account name
  - Domain Component (DC)
    - Represents the domain
      - E.g., example.com
  - Organizational Unit (OU)



- Represents user groups or departments
- LDAP Example
  - CN
    - B Spencer (Common Name)
  - OU
    - Security (Organizational Unit)
  - DC
    - Example (Domain Component)
  - DN
    - Full representation combining all attributes (CN, OU, DC)
- AAA (Authentication, Authorization, and Accounting)
  - AAA Framework
    - Used in network-based devices for authentication and access control. Provides
      - Identification
        - Claiming an identity
      - Authentication
        - Proving that identity
      - Authorization
        - Defining what actions are allowed
      - Auditing
        - Logging actions taken by the user
      - Accounting
        - Reviewing logs and holding users accountable
  - AAA Protocols

- RADIUS (Remote Authentication Dial-In User Service)
  - Centralized authentication system for remote users
  - Uses UDP port 1812 for authorization and UDP port 1813 for accounting
  - Encrypts passwords, but other session data remains unencrypted
- TACACS+ (Terminal Access Controller Access-Control System Plus)
  - A more secure AAA protocol than RADIUS
  - Uses TCP port 49
  - Encrypts the entire communication session
- Diameter
  - Enhanced version of RADIUS, providing greater flexibility and improved security for modern communication
  - Uses TCP port 3868 or SCTP for transport
  - Does not natively encrypt, but can use IPSec or SSL/TLS for encryption
- Key Terms to Know
  - Distinguished Name (DN)
    - A collection of LDAP fields representing the full identity of a subject
  - RADIUS
    - An AAA protocol used primarily for remote access authentication. Encrypts only the password

- TACACS+
  - An enhanced AAA protocol that encrypts the entire communication session, used in more complex authentication scenarios
- Diameter
  - A flexible protocol improving upon RADIUS, commonly used in modern communication networks
- Best Practices and Considerations
  - Use LDAP Secure (LDAPS) (Port 636) instead of LDAP (Port 389) to prevent plaintext credentials from being intercepted
  - RADIUS is ideal for simple password-based authentication but should be paired with additional security measures for session data
  - TACACS+ offers stronger encryption for both authentication and authorization communication and is recommended for complex environments requiring fine-grained control
  - Diameter is highly flexible and suited for modern infrastructures, but additional encryption measures (e.g., IPSec, SSL/TLS) may be needed
- **Authentication Factors**
  - Key Concepts
    - Authentication
      - The validation of a claimed identity. The process of confirming that a subject (user, device, etc.) is who they claim to be
    - Common login screen

- A username identifies the subject, while a password is used for authentication
- Types of Authentication Factors
  - Single Factor Authentication (SFA)
    - Single Factor Authentication
      - Uses one factor to authenticate a subject's identity
    - Example
      - Username and password (something you know)
    - This is also called one-to-one authentication (one subject, one authentication factor)
  - Two Factor Authentication (2FA)
    - Two Factor Authentication
      - Requires two different factors for authentication
    - Commonly uses a combination of something you know (password) and something you have (token)
    - Example
      - Username, password, and a one-time password (OTP) delivered via a token or app
  - Multi-Factor Authentication (MFA)
    - Multi-Factor Authentication
    - Involves more than one authentication factor, typically two or more
    - MFA can include something you know (password), something you have (token), and something you are (biometric)

- Often used interchangeably with 2FA, but MFA may involve more than two factors
- Important for the exam
  - When given a choice between two-factor authentication and multi-factor authentication, select the more specific answer (2FA when applicable)
- Authentication Factor Types (Know for the Exam)
  - Type 1
    - Something You Know (Knowledge-based)
      - This is information the user knows, such as a password, PIN, or passphrase
      - Example
        - Username and password
  - Type 2
    - Something You Have (Ownership-based)
      - This is something the user physically possesses, such as a token, smart card, or mobile device
      - Example
        - Token-generated one-time password (OTP) or a smart card.
  - Type 3
    - Something You Are (Biometric-based)
      - Biometric-based authentication uses physical characteristics to verify identity
      - Example

- Fingerprint scan, iris scan, facial recognition, palm scan
- Authentication Process Examples
  - Single-Factor Authentication (SFA)
    - A user enters a username (identity) and password (authentication) to access a system
    - The system checks the credentials against a directory service (e.g., LDAP or Active Directory)
  - Multi-Factor Authentication (MFA)
    - After entering the username and password, the user is prompted for an additional factor such as a one-time password (OTP) from a token or mobile app
    - Example
      - Logging in with a password (Type 1) and verifying with an OTP (Type 2)
- Context-Based Authentication
  - Consider additional factors such as behavior, location, or device attributes.
  - Something you do
    - Behavior-based biometrics, such as how you type (keystroke dynamics) or your signature (signature dynamics)
  - Somewhere you are
    - Based on geographical location or IP address
    - Device or network in use

- Based on device identifiers (MAC address, IP address)
- Can be used to replace or supplement traditional password-based authentication
- Behavior-Based Biometrics
  - Part of context-based authentication
- Speech recognition
  - Identifies users based on how they speak
- Keystroke dynamics
  - Analyzes typing patterns to authenticate the user
- Signature dynamics
  - Analyzes the way a user signs their name
- Key Exam Tips
  - Single Factor Authentication (SFA)
    - Uses one factor for authentication
    - E.g., password only
  - Two Factor Authentication (2FA)
    - Combines two distinct authentication factors (e.g., password + token)
  - Multi-Factor Authentication (MFA)
    - Involves more than one authentication factor and is often used interchangeably with 2FA
  - Context-Based Authentication
    - Factors such as behavior, location, and device/network attributes play a role in authenticating users

- **Biometric Authentication**

- Biometric Authentication

- Validates a claimed identity using genetic or behavioral data
    - Rarely used as a single authentication factor, typically paired with Type 1 or Type 2 authentication
    - Common forms include fingerprints and facial recognition

- Types of Biometric Attributes

- Physiological Attributes (Physical Attributes)
    - Fingerprints
      - Unique visible ridges on fingertips
    - Palm Scans
      - Analyzes blood vessels and patterns on the palm
    - Retina Scans
      - Evaluates unique blood vessel patterns in the back of the eye
      - Extremely accurate
      - Can differentiate identical twins
    - Iris Scans
      - Analyzes colored part of the eye with unique patterns and rings
      - Rarely changes over a lifetime
    - Hand Geometry
      - Measures physical shape and dimensions of the hand
    - Facial Recognition
      - Analyzes facial features such as shape and position of eyes, nose, chin, and forehead



- Behavioral Attributes
  - Signature Dynamics
    - Analyzes writing speed, pressure, and stroke length
  - Keystroke Dynamics
    - Measures typing patterns, keypress duration, and time between keypresses
  - Voice Pattern Recognition
    - Analyzes speech patterns, pauses, and emphasis
  - Heart Rate Patterns
    - Analyzes pulse and heart behavior
- Biometric System Errors
  - Type 1 Error (False Rejection Rate - FRR)
    - Occurs when an authorized subject is mistakenly rejected by the system
    - Failure in system recognition
  - Type 2 Error (False Acceptance Rate - FAR)
    - Occurs when an unauthorized subject is mistakenly accepted by the system
    - Represents a security violation
- Crossover Error Rate (CER)
  - The point where false rejection rate (FRR) and false acceptance rate (FAR) are equal
  - Also known as the Equal Error Rate (EER)
  - Used to tune biometric systems for balanced accuracy and security

- Biometric Enrollment Process
  - Involves collecting and storing biometric data as hash values in an authentication database
  - Enrollment should take two minutes or less for user convenience
  - Potentially invasive, may capture sensitive health information
  - Requires appropriate security controls to protect stored biometric data and hash values
- **Single Sign On**
  - Single Sign-On (SSO)
    - Single set of credentials used to identify and authenticate a subject throughout a system
    - Allows subjects to authenticate once and access multiple systems using the same credentials
    - Reduces the security risk of multiple passwords as users only need to remember one password
    - Simplifies user experience by eliminating the need for repeated logins across authorized applications
  - How SSO Works
    - Subjects authenticate to an SSO service
    - SSO service creates a token representing identification and authentication
    - Token is passed to authorized applications to validate user access
  - SSO Drawbacks
    - Compromised Credentials

- If credentials or tokens are compromised, attackers gain access across SSO-enabled systems
- Integration Challenges
  - Variety of technologies in systems may complicate SSO implementation
- Example
  - Kerberos is primarily Windows-focused and may not integrate with Linux or other systems
- Expense
  - Can be costly for large organizations to implement token-based authentication across numerous applications
- Single Target
  - SSO server holding all credentials becomes an attractive and static target for attackers
- Common SSO Technologies
  - Kerberos
    - Ticket-based authentication service
    - Provides identification and authentication
    - Primarily designed for Windows environments
  - Security Assertion Markup Language (SAML)
    - Open standard for exchanging authentication and authorization information
    - Primarily used for web-based applications
    - Facilitates information exchange between an identity provider and a service provider

- OpenID
  - Allows the use of existing accounts to sign into multiple websites using pre-existing passwords
  - OpenID Connect (OIDC)
    - Extension of OpenID providing additional information about authenticated sessions and users
- **OAuth and OIDC**
  - OAuth (Open Authorization)
  - An open standard authorization protocol used to delegate access to a third party
  - Allows applications to access resources without requiring authentication credentials
  - Utilizes access tokens to authorize requests
  - Defined by RFC 6749 (OAuth 2.0)
  - OAuth 2.0 is not backward compatible with OAuth 1.0, requiring a choice between the versions
  - Example Use Case
    - Authorizing a social media app to access contacts on a mobile device
- OAuth Components
  - Resource Owner
    - Whitelists who can access specific resources
  - Authorization Server
    - Issues access tokens upon request

- Resource Server
  - Uses presented tokens to grant access to resources
- OAuth Workflow
  - Resource Owner whitelists access permissions
  - Authorization token presented to Authorization Server, which provides an access token
  - Client uses access token on Resource Server to access protected resources
- OpenID
  - An open standard authentication protocol allowing single sign-on for multiple websites
  - Authentication credentials managed by a third-party OpenID provider
  - Enables users to access multiple websites with a single set of credentials
- OpenID Connect
  - Identity layer built on top of OAuth 2.0
  - Uses REST and JSON messages for cross-site authentication
  - REST (Representational State Transfer)
    - Message format for web service communications
  - JSON (JavaScript Object Notation)
    - Lightweight data format for structured data exchange
  - JSON Web Tokens (JWT)
    - Used to provide authentication and profile information across sites

- Common Use
  - Allows single sign-on using providers like Google, LinkedIn, and Facebook on various websites
- **Kerberos**
  - Kerberos
    - A single sign-on (SSO) system and ticket-based authentication protocol
    - Primarily used in Windows environments, developed by MIT under Project Athena (1983-1991)
    - Named after the "Hound of Hades," the three-headed guard dog in Greek mythology
    - Current Version
      - Kerberos Version 5
    - Uses a Key Distribution Center (KDC) for identity and authentication verification
    - Employs Advanced Encryption Standard (AES) for message encryption to ensure privacy
  - Key Components of Kerberos
    - Key Distribution Center (KDC)
      - Trusted third-party server issuing and storing secret session keys for authentication
    - Authentication Server (AS)
      - Authenticates a subject's account using the Ticket Granting Ticket (TGT), also known as the "Golden Ticket"
    - Ticket Granting Service (TGS)

- Verifies the TGT, provides Service Tickets (also called the "Silver Ticket") and session keys for authorization
- Tickets
  - Ticket Granting Ticket (TGT) / Golden Ticket
    - Verifies initial authentication to the KDC and is essential for initiating single sign-on
  - Service Ticket / Silver Ticket
    - Provides encrypted evidence of the subject's authorization to access specific resources or services
- Kerberos Operation Flow
  - Client Authenticates
    - The client authenticates to the Authentication Server (AS) with their credentials
  - TGT Issued
    - Upon verification, the AS provides a Ticket Granting Ticket (TGT) to the client
  - TGT Presented to TGS
    - The client presents the TGT to the Ticket Granting Service (TGS)
  - Service Ticket Issued
    - The TGS provides a Service Ticket and session keys for accessing services
  - Access Granted
    - The client uses the Service Ticket to authenticate to the Kerberos-enabled service, enabling access

- Risks of Using Kerberos
  - Vulnerable to dictionary and brute-force attacks on passwords
  - Single Point of Failure
    - If the KDC is compromised, all access is denied as Kerberos fails secure
  - Time Synchronization Dependency
    - All services must synchronize with a reliable time source to avoid access issues
  - Secret Key Protection
    - Secret keys used in encryption must be securely protected
- Kerberoasting Attack
  - Extracts password hashes from Active Directory to crack passwords, allowing attackers to spoof identities and access the TGT and Service Tickets for unauthorized access
- **Credential Management Systems**
  - Credential Management Systems (CMS)
    - Systems designed to store a subject's authentication credentials
    - Often referred to as "password managers"
    - Used to store usernames, passwords, and other sensitive information
    - Common formats include standalone applications, web browser plugins, and endpoint security software
  - Types of Credential Management Systems
    - Standalone Applications
      - Examples include KeePass, Keeper



- Browser Plugins
  - Examples include LastPass, RoboForm
- Endpoint Security Software
  - Examples include Norton, Symantec, Kaspersky, Bitdefender
- Risk Management Software
  - Credential management can be embedded within tools like Nessus, OpenVAS for credential-based scans
- Operating Systems
  - Credential management is often integrated into OS features, such as Windows and Google account managers
- Examples of Popular CMS Solutions
  - Enable
  - LastPass
  - RoboForm
  - Windows Credential Manager
  - Google Password Manager
  - KeePass
  - Keeper
- Attributes Stored in Credential Management Systems
  - Identification credentials
    - Username, account number, ID number
  - Authentication credentials
    - Passwords, tokens, certificates
  - Biometric information

- Credential Vault
  - Encrypted storage area in a CMS, commonly called a “vault”
  - Vault encryption is typically managed by advanced cryptography
    - E.g., AES, RSA) to secure sensitive data
- CMS Security Considerations
  - Encryption Standards
    - Ensure vaults use modern, compliant cryptographic algorithms, such as AES and RSA
  - Acceptable Applications
    - Identify acceptable CMS applications, research vulnerabilities, and list approved applications in policy
  - Master Password Requirements
    - Define strong and complex password policies for the master password accessing the vault
  - Password Storage Policies
    - Specify which types of passwords can be stored in the CMS, especially concerning administrator or privileged accounts
  - Protection of Recovery Keys and Backups
    - Define protection requirements for CMS recovery keys, vault backups, and other related data
- **Just-In-Time Access**
  - Just in Time (JIT) Access
    - Purpose is to reduce the attack surface of a system

- Attack surface refers to possible points of entry for an attacker, not to be confused with attack vector, which is the method or path taken by an attacker
- Focused on limiting privileged access to the system and reducing the amount of time privileged accounts are active
- Provides on-demand privileged access to perform specific tasks, enhancing security through time-limited access
- Privileged Access Management (PAM)
  - PAM is necessary for managing and monitoring privileged access to system resources
  - Reduces the time that privileged accounts exist on a system, which decreases the attack surface
  - Instead of static privileged accounts, JIT provides ephemeral access, creating privileges only when necessary
- Components of JIT Access
  - Ephemeral Accounts
    - Used once for access, then removed after execution, reducing availability for attacks
  - Temporary Elevation
    - Provides temporary privileges to execute specific commands, revoked once the session ends
      - E.g., `sudo` in Linux
- Implementation and Best Practices
  - Fine-grained Access Policies

- Define specifically which subjects can access which objects and how, enforcing least privilege
  - Temporary Elevation for Privileged Commands
    - Ideal for users who need limited, task-specific privileges, such as developers or system administrators
  - Continuous Auditing
    - Track privileged activity to assess effectiveness of JIT, ensure policy compliance, and identify potential security violations
  - Bottom Line for the Exam
    - Understand the purpose and functioning of JIT
    - Know the components of ephemeral accounts and temporary elevation
    - Familiarize with best practices, including fine-grained access policies, temporary elevation, and continuous auditing
- **Access Control Models - Part 1**
  - Access Control Models Overview
    - Purpose is to control how a subject (user, device) interacts with an object (file, service, or function)
    - Models include discretionary, mandatory, and rule-based access controls
  - Discretionary Access Control (DAC)
    - Access is based on the subject's identity
    - Object owner determines access rights for subjects
    - Uses an Access Control List (ACL) to track privileges
    - Known for its flexibility with minimal complexity overhead
    - Security risk is higher as it lacks fine-grained control over access

- Process
  - Object owner assigns access permissions
  - Subject requests access
  - Operating system checks the ACL for permissions and grants or denies access
- Non-Discretionary Access Control
  - Access rights are predetermined by a central authority or policy, not by the object owner
  - Central management enforces permissions through security policies
  - Used in environments requiring strict access control, e.g., highly sensitive data protection
- Mandatory Access Control (MAC)
  - A type of non-discretionary access control
  - Uses security labels on subjects and objects to define access
  - Classification levels (e.g., Confidential, Secret, Top Secret) control access based on subject's clearance level
  - Common in environments with sensitive data, such as PII, PHI, and national security
  - Process
    - Subject requests access to labeled object
    - Access control checks if subject's clearance matches or exceeds the object's label
    - Access is granted or denied based on clearance and classification compatibility
- Rule-Based Access Control

- Access is controlled based on predefined rules or restrictions
- Frequently used in network security devices such as firewalls and intrusion prevention systems
- Allows or denies access based on rules, such as port number and protocol
- Process
  - Subject
    - E.g., a computer
  - Requests access based on specific parameters
    - E.g., HTTP port 80
  - Device checks if rules allow the requested interaction
  - Access is granted or denied depending on rule compliance
- Exam Focus
  - Understand the differences between DAC, MAC, and rule-based access control models
  - Familiarize with the roles of subjects, objects, and access control lists
- **Access Control Models - Part 2**
  - Access Control Overview Recap
    - Controls the interaction between a subject and an object
    - Defines how a subject is authorized to access an object
  - Role-Based Access Control (RBAC)
    - Access control based on group membership and privileges
    - Commonly used in organizations to streamline administration and enforce least privilege
    - Controls access by grouping subjects by roles or functions

- E.g., administrator, analyst, manager
- Helps reduce privilege creep by assigning access based on specific roles
- Effective for environments with high staff turnover
- Enforces need-to-know and least privilege by applying access rights to the entire group
- Example
  - Subject requests access to an object based on group membership
  - Access is granted if subject's role matches the security label of the object
  - Access is denied if roles or labels are undefined or mismatched
- Attribute-Based Access Control (ABAC)
  - Controls access rights based on multiple attributes
    - E.g., clearance level, department, physical location
  - Provides fine-grained control by filtering based on object attributes rather than subject roles
  - Often referred to as Policy-Based Access Control (PBAC)
  - Utilizes Extensible Access Control Markup Language (XACML) for defining policies
  - Attributes used for access control can include
    - Subject attributes
      - Roles, clearances, organizational affiliation
    - Action attributes
      - Read, write, execute permissions
    - Object attributes
      - Sensitivity, ownership, object type

- Environmental attributes
  - Date, time, IP address, MAC address
- Risk-Based Access Control
  - Dynamically grants or denies access based on a calculated risk level
  - Uses contextual data, such as device type, network attributes, geolocation, and object sensitivity
  - Also known as Risk-Adaptable Access Control (RAdAC)
  - Access decisions are adapted to the calculated risk level of the access request
  - Example
    - Low-risk scenario
      - User logs in from a known IP address and trusted device, access may be granted with single-factor authentication
    - Moderate-risk scenario
      - Privileged user attempting access with single-factor authentication may be denied or require additional factors
    - High-risk scenario
      - Unknown IP address or untrusted subnet triggers multi-factor authentication requirement or denial
- Exam Focus
  - Understand RBAC, ABAC, and risk-based access control models and their key attributes
  - Familiarize with the distinctions in how each model handles subject and object attributes



## Access and Authorization

### Objectives:

- 5.1 - Control physical and logical access to assets
- 5.2 - Design identification and authentication strategy (e.g., people, devices, and services)
- 5.4 - Implement and manage authorization mechanisms
  
- **Accountability**
  - Accountability
    - Ensures subjects are held accountable for their actions within the system
    - Goal
      - To track and verify actions performed by subjects interacting with objects and resources
    - Key Outcome
      - Supports non-repudiation, ensuring subjects cannot deny actions they performed
  - Examples of Accountability in Action
    - Accessing and reading sensitive files
      - racks who accessed a file and verifies if access was authorized
    - Modification of directory or folder permissions
      - Ensures that changes to permissions are intentional and prevent unauthorized access
    - Destruction of sensitive data

- Identifies who accessed and deleted data, addressing potential availability violations
- Creation of unauthorized system accounts
  - Tracks account creation to prevent unauthorized access by rogue users or administrators
- Implementing Accountability
  - System Logging
    - Logs actions to track and audit subject activities
  - Auditing Features
    - Ensures all platforms can record and monitor user actions
  - Protection Against Tampering
    - Secures logs and critical information from unauthorized access or destruction
  - Strong Access Controls
    - Enforces least privilege, strong authentication, and access controls on sensitive files and logs
- Key Benefits
  - Supports Non-Repudiation
    - Prevents subjects from denying actions by linking actions to authenticated subjects
  - Identifies Design Vulnerabilities
    - Accountability can reveal gaps in system design that allow for unauthorized actions

- **Access Authorization**

- Authorization

- Access granted to an object for an authorized subject

- Key Function

- Deciding if a subject can create, modify, execute, or delete resources (files, VMs, network interfaces)

- Key Terms in Authorization

- Permissions

- Subject's ability to access an object
        - Typically for objects only, e.g., read or write

- Rights

- Subject's authority to conduct specific actions
        - E.g., modify accounts, configure systems

- Privileges

- Combination of a subject's permissions and rights

- Core Concepts in Authorization

- Implicit Deny

- Access is denied by default unless explicitly granted

- Concept

- "Permit by exception, deny by default"

- Access Control Matrix

- Tracks subjects, objects, and privileges (object-focused)

- Capability Table

- Lists subject capabilities in relation to objects (subject-focused)

- Constrained Interface

- Limits the interface's actions based on the subject's privilege level
    - E.g., non-admin users have restricted interface access
  - Content-Dependent vs. Context-Dependent Controls
    - Content-Dependent Controls
      - Limits access based on the type of object
        - E.g., sensitive files
    - Context-Dependent Controls
      - Requires a specific action to grant access
        - E.g., pre-approval step
  - Authorization Principles
    - Separation of Duties
      - Dividing critical tasks among multiple individuals to prevent excessive control
    - Least Privilege
      - Providing only necessary access rights for subjects to perform their roles
    - Need to Know
      - Grants access to information solely required for a subject's duties; often enforced with least privilege and discretionary access controls
- **Controlling Logical Access**
  - Key Concepts
    - Logical Access Control

# ISC2 CISSP

## (Study Guide)

- Manages privileges to open, modify, execute, or delete data, ensuring confidentiality, integrity, and availability
  - Confidentiality
    - Data isn't accessed by unauthorized subjects
  - Integrity
    - Data isn't altered by unauthorized subjects
  - Availability
    - Data is available to only authorized subjects
- Information, Systems, Devices, Facilities, and Applications
  - Information
    - Data
      - E.g., documents, files
  - Systems
    - Hardware and software that process or interact with information.
  - Devices
    - Physical components
      - E.g., servers, mobile devices, IoT devices
  - Facilities
    - Locations housing systems and device
    - E.g., data centers, equipment rooms
  - Applications
    - Programs designed to perform specific functions within systems
- Subjects and Objects in Logical Access
  - Subjects
    - Entities that access an object

- E.g., users, programs, scripts, services
- Objects
  - Entities providing information or resources to a subject
- Example
  - User accesses a website
    - User = Subject, Website = Object
    - Website accesses the web server
      - Website = Subject, Web Server Data = Object
    - Web server returns data to website
      - Web Server = Subject, Website = Object
- Key takeaway
  - Subject and object roles interchange based on the nature of access
- Goals in Controlling Access
  - Prevent unauthorized disclosure of information
  - Maintain data integrity by ensuring only authorized changes
  - Ensure availability of data for authorized subjects
- Exam Focus
  - Definitions
    - Access, subject, object, and logical access concepts
  - Understanding the flow of access between subjects and objects in various scenarios
  - Purpose of Controlling Access
    - Protect information and systems by defining who can access what and how they can interact with it

- **Session Management**

- Session

- A session is a temporary, active connection between two entities, often using protocols like UDP or TCP
    - It enables an exchange of data, functions, or services.

- Types of Sessions

- User-to-computer
      - E.g., logging into a workstation
    - Computer-to-application
      - E.g., accessing a web app

- Session Management Basics

- Session IDs
      - Bind user credentials to active sessions and are critical for session initiation, management, and termination
    - Session Timeout
      - Automatically ends a session after a set period of inactivity
        - E.g., 5–15 minutes
      - Requires re-authentication to start a new session after timeout
    - Screen Savers
      - Help protect sensitive on-screen data by locking the session after a period of inactivity, requiring re-authentication to regain access

- Session Attacks

- Session Hijacking (Sidejacking)

- Attackers capture session tokens or cookies, often through man-in-the-middle (MITM) tactics, to impersonate the legitimate user
- Session Fixation
  - Attackers plant an insecure token or cookie in the user's browser, then use it to impersonate the user in a replay attack
- Session Management Security Controls
  - Session Timeout Configuration
    - Set timeouts on devices and network configurations to terminate idle sessions.
  - Logout Features
    - Provide visible and accessible logout options to allow users to manually terminate sessions.
  - Account Lockouts
    - Limit incorrect login attempts
      - E.g., 3-5 tries to prevent brute force and session replay attacks
  - Concurrent Session Limiting
    - Restrict simultaneous sessions per user (typically 1-3) to prevent denial-of-service and session replay risks
  - Session Encryption
    - Encrypt session traffic
      - E.g., HTTPS to prevent interception by unauthorized parties



- Exam Focus
  - Understand Key Session Terms
    - Session timeout, session ID, screen saver, session hijacking, and session fixation
  - Know the Types of Session Attacks
    - Differentiate between session hijacking and session fixation, and understand man-in-the-middle concepts
  - Key Session Security Measures
    - Remember the importance of session timeouts, logout features, account lockouts, concurrent session limits, and encryption for session integrity
- Password Attacks
  - Key Concepts of Passwords
    - A password is a confidential character or code combination used to authenticate an identity, tied to the user's username
  - Types of Passwords
    - Standard Passwords
      - Secret character codes, PINs, or phrases
    - Cognitive Passwords (Security Questions)
      - Questions like "What's your pet's name?" used for password recovery
  - Types of Password Attacks
    - Brute Force Attack

- Attempts every possible character combination to guess a password
- Dictionary Attack
  - Uses common words or known password lists to guess passwords, often using tools like Hashcat or John the Ripper
- Password Spraying
  - Uses a single password across multiple usernames to avoid account lockouts
- Credential Stuffing
  - Uses stolen credentials in bulk to gain unauthorized access, often through automated tools
- Birthday Attack
  - Leverages hash collisions to find matching hashes and potentially guess passwords, based on the birthday paradox concept
- Social Engineering
  - Manipulates users into revealing passwords, often through impersonation or deception
- Common Password Cracking Tools
  - Cain and Abel
    - Focused on cracking Windows credentials
  - John the Ripper
    - Multi-platform support (Windows, Unix/Linux)
  - Mimikatz
    - Primarily targets Windows credentials
  - Hashcat

- Multi-platform, used for comparing hashes
- Aircrack
  - Specializes in cracking wireless passwords (WEP, WPA)
- Hydra
  - Focuses on network-based service passwords (HTTP, FTP)
- Rainbowcrack, Loftcrack, and Offcrack
  - Primarily target Windows-based credentials
- Defense Against Password Attacks
  - Strong Password Policies
    - Complexity Requirements
      - At least 8 characters (preferably 16–24); include uppercase, lowercase, numbers, and special characters
    - Length
      - The longer the password, the more difficult it is to crack
  - Example of a Strong Password
    - P@ssw0rd!2023
  - Password Aging Policies
    - Minimum Age
      - Prevents frequent reuse by setting a minimum duration.
    - Maximum Age
      - Requires regular password changes
    - Password History
      - Limits password reuse by maintaining a record of previous passwords
  - Session Timeout and Logout Mechanisms

# ISC2 CISSP

## (Study Guide)

- Ensure that sessions are terminated upon inactivity to prevent hijacking attempts
- Limit Login Attempts
  - Lock accounts after a set number of failed login attempts to mitigate brute-force attacks
- Multi-Factor Authentication
  - Adds a secondary authentication layer, enhancing security even if a password is compromised
- Exam Focus
  - Recognize Types of Password Attacks
    - Understand the differences between brute force, dictionary, spraying, and credential stuffing attacks
  - Understand Password Management Techniques
    - Know how strong passwords, aging policies, and history settings prevent unauthorized access
  - Familiarize with Common Cracking Tools
    - Recognize the use cases for tools like Cain and Abel, Mimikatz, and Hydra for password cracking

## Security Test and Assessment

### Objectives:

- 6.1 - Design and validate assessment, test, and audit strategies
- 6.3 - Collect security process data (e.g., technical and administrative)
- 6.5 - Conduct or facilitate security audits
- **Security Test and Assessment Planning**
  - Security Test and Assessment Overview
    - Designed to verify that security controls provide the proper level of security protection
    - Terms test, assessment, and audit are often used interchangeably
    - Focused on ensuring the proper function, risk level, and effectiveness of security controls
  - Security Test
    - Ensures that a specific security control is functioning as designed
    - Conducted at regular intervals to test control performance and effectiveness
    - Example
      - Testing network interface cards (NICs) or APIs for specific control flaws or vulnerabilities
  - Security Assessment
    - Analyzes the security risk of a system component, application, or function
    - Evaluates the overall security posture with organizational policy
    - Generates a report for senior management or stakeholders

- Security Audit
  - An independent assessment using an impartial body to verify security controls and effectiveness
  - Often focused on compliance with governance, regulations, and security posture
  - Includes compliance status and perceived risk impact in the report
- Types of Security Audits
  - Internal Audit
    - Performed by internal personnel and reported directly to senior management
    - Example
      - Self-audit by the company before an external audit for an objective view
  - External Audit
    - Conducted by an outside organization specializing in security audits
    - Provides an unbiased perspective and reports to executive officers
  - Third-Party Audit
    - An outside team performs the audit on behalf of another organization
    - Results are reported directly to the outside organization, often for compliance or acquisition purposes
- Security Test and Assessment Strategy
  - Define the Scope
    - Determine whether a security test or assessment is needed

- Identify if the scope involves compliance, risk management, or control verification
  - Evaluate the Impact of Control Failure
    - Assess if failed controls impact critical business functions or assets
  - Identify Resources and Personnel
    - Determine the personnel and resources necessary, such as administrators, engineers, or tools
  - Define Test Criteria
    - Establish success and failure parameters for the test or assessment procedure
    - Create a documented plan to align with time, money, and effort considerations
- **Performance and Risk Indicators**
  - Indicators Overview
    - Identify measurements for potential success or failure in security performance
    - Key Performance Indicators (KPIs) measure security performance levels
    - Key Risk Indicators (KRIs) measure known security risks and control ineffectiveness
  - Key Performance Indicators (KPIs)
    - Measurement of security performance within the organization
    - Examples
      - Patch level compliance
      - Frequency and effectiveness of risk assessment and analysis

- Identification and resolution of security vulnerabilities
- Key Risk Indicators (KRIs)
  - Measurement of potential failure or ineffectiveness in security controls
  - Examples
    - Findings from security incident reports
    - Unresolved vulnerabilities from vulnerability assessments
    - Unaddressed stale accounts or delayed account deprovisioning after terminations
- Sources of Measurement Data
  - Risk assessment and analysis results (qualitative and quantitative)
  - Vulnerability assessment outcomes, categorized by severity
    - E.g., critical, high, moderate, low
  - Security incident responses and recovery timelines
  - Real-time data from Security Information and Event Management (SIEM) tools like Splunk or AlienVault
  - Dashboards for tracking SLAs, login attempts, threats, vulnerabilities, and other metrics
- Measurement Standards and Guides
  - NIST Special Publication 800-55
    - Performance measurement guide for information security
  - ISO 27004
    - Guidance for monitoring, measurement, analysis, and evaluation of security metrics
    - ITIL (Information Technology Infrastructure Library)



- Provides frameworks for security management and performance indicators
- **Collecting Security Data**
  - Importance of Data Collection
    - Collect data from all security controls to support tests, assessments, and audits
    - Use collected data to present evidence for management approval based on results
    - Success of tests, assessments, and audits depends on the quality of input data
  - Impact of Scope, Time, and Cost on Quality (Triple Constraint)
    - Quality depends on
      - Scope of what is being tested
      - Time available for the test
      - Cost associated with testing
      - Any change to one factor (scope, time, or cost) impacts the other two, thus affecting quality
      - Balance between scope, time, and cost is necessary for effective data collection and quality testing
  - Types of Data to Collect
    - Administrative Data
      - Gather policies, processes, and procedures documentation
      - Include records, logs, archived data, and previous assessments to verify security controls

- Example
  - Collect relevant information from departments like finance and human resources
- Technical Data
  - Collect system logs, software code, configuration files, change management records
  - Review system diagrams and data flow diagrams to understand system operations and expected outcomes
- Management Approval and Support
  - Obtain approval and support from senior managers to allocate resources for tests and assessments
  - Example
    - Administrators, engineers, architects may be required
    - Communicate the purpose and scope of the tests to ensure proper resources are available
  - Formal documentation is necessary for approval, including
    - Expected outcomes, schedule, scope, start/end dates and times, and any risk exceptions
  - Methodical planning and documented management approval are essential for successful testing
- **Account Management Data**
  - Purpose of Account Management Data in Security Assessment
    - Used to ensure authorized subjects maintain proper privilege levels
    - Prevents authorization or privilege creep

- Consists of user identity and authenticators
- Account Management Lifecycle
  - Creation of Accounts
  - Acquire a list of system accounts from centralized authentication services such as Active Directory, LDAP, RADIUS, TACACS, or local authentication services
  - Review lists to identify authorized and unauthorized accounts, including admin, root, and emergency accounts
  - Example
    - Reviewing system logs to detect account creation patterns or identify potential insider threats
  - Modification of Accounts
    - Review log files to confirm account actions, including privilege provisioning and deprovisioning, are captured correctly
    - Ensure logging captures any changes in privileges or permissions to support compliance
  - Auditing of Accounts
    - Verify that each account is assigned the correct privilege levels
    - Conduct audits regularly, based on policy; generally, at least annually, though industry regulations may require monthly, quarterly, or semi-annual audits
    - Identify and address any non-compliant accounts, such as inactive accounts not marked for disablement

- Deleting Accounts
  - Recommend accounts for access revocation, deprovisioning, or deletion based on audit findings
  - Adhere to industry regulations regarding retention timelines, typically requiring maintenance for three, five, or seven years, after which deletion is recommended
  - Aim to maintain account data only as long as necessary per governance and compliance requirements
- **Verifying Training and Awareness**
  - Purpose of Training and Awareness in Security Assessment
    - Raises personnel awareness of foundational security practices and responsibilities within the organization
    - Ensures personnel understand and can securely perform their duties
    - Integral to administrative controls and data collection in security assessments
  - Training Data Collection and Compliance
    - Gather personnel training records that align with specific training objectives
    - Example
      - High phishing incidents prompt training focused on recognizing and responding to phishing emails
    - Assess training effectiveness through key risk indicators (KRIs) and key performance indicators (KPIs)

- Ensure compliance with regulatory requirements for each training objective, handling data securely without identifiable information
- Assessing Training Objectives and Emerging Risks
  - Review training objectives to determine if security goals are being met
  - Identify and include emerging threats, vulnerabilities, or risks in training materials
  - Maintain due care by creating the training program and due diligence by updating it as new risks emerge
- Tracking Compliance and Addressing Non-compliance
  - Verify personnel attendance and completion of training programs
  - Identify non-compliant personnel and frequent policy violators
  - Provide remedial training options, including make-up sessions or on-demand training
  - Consider revoking or removing access privileges for personnel who do not comply with training requirements until they fulfill them
- **Disaster Recovery and Business Continuity Data**
  - Purpose of Business Continuity (BC) and Disaster Recovery (DR)
    - BC aims to assess and minimize risks to critical business processes during a disruption
    - DR involves processes and procedures to recover critical business processes after a disruption
    - BC focuses on critical business functions, while DR focuses on information technology
  - Key Elements for Security Assessment in BC and DR

- Gather and review copies of BC and DR plans, if they exist
- Verify the results from the latest BC or DR test events, such as parallel tests or simulation tests
- Note any outdated results, which may indicate areas for remediation
- Conduct a disaster recovery test alongside a security assessment if necessary
- Disaster Recovery Test Types and Considerations
  - Checklist Test (Read-through Test)
    - Team members receive and review checklists for comments and feedback
  - Structured Walkthrough Test (Tabletop Exercise)
    - Team members review the DR plan together in a meeting to identify potential issues
  - Simulation Test
    - Structured walkthrough for specific scenarios (e.g., natural or man-made disasters)
    - Evaluate results and corrective actions taken
  - Parallel Test
    - Procedures and processes are executed without impacting live operations
    - Example
      - Testing a recovery site by spinning up its resources without affecting current operations
  - Full Interruption Test

# ISC2 CISSP

## (Study Guide)

- Operations are impacted, and production moves to an off-premises or cloud-based backup site
- Examine if all controls and processes are effective under full interruption conditions
- Backup Data Testing and Verification
  - Gather backup data records, tapes, drives, etc., for testing and verification
  - Ensure retention, encryption, and proper archiving of backup data
  - Review backup data logs to ensure they are done per organizational policy and encryption standards
- Backup Types and Testing Requirements
  - Full Backups
    - Complete copies of system data, including all objects and user data
    - Test if the full backup can restore all critical data
  - Differential Backups
    - Copies of data modified since the last full backup
    - Ensure recovery from differential backups captures recent changes since the last full backup
  - Incremental Backups
    - Copies data modified since the last full or incremental backup
    - Verify the incremental backup includes all incremental changes and can recover the latest data

## Conduct Security Testing

### Objectives:

- 6.2 - Conduct security control testing
- 6.4 - Analyze test output and generate report
- **Vulnerability Assessments**
  - Purpose of Vulnerability Assessments
    - Identify and categorize security flaws and weaknesses
    - Understand security risks associated with identified vulnerabilities
    - Prioritize responses to discovered flaws, vulnerabilities, and weaknesses
  - Process of Identifying Vulnerabilities
    - Accurate System Inventory
      - Maintain details on hardware, software, firmware, and versions
      - Reference inventory to assess whether a specific vulnerability applies
  - Vulnerability Management Process Steps
    - Detection
      - Identify potential vulnerabilities
    - Validation
      - Confirm impact on assets
    - Remediation
      - Fix or reduce the identified vulnerability
    - Objective



- Rule out false positives and ensure vulnerabilities are correctly identified to avoid false negatives
- Sources for Vulnerability Information
  - National Vulnerability Database (NVD)
    - Managed by NIST
  - MITRE CVE Database
    - Common Vulnerabilities and Exposures
  - US CERT
    - United States Computer Emergency Readiness Team
  - Vendor Resources
    - Microsoft, Cisco, Amazon, Google, VMware, etc.
- Security Content Automation Protocol (SCAP)
  - Created by NIST to standardize vulnerability reporting
    - Includes community input for common specifications and system configurations
- Key SCAP Components
  - XCCDF (Extensible Configuration Checklist Description Format)
    - Provides security checklists and benchmark results
  - OVAL (Open Vulnerability and Assessment Language)
    - Configuration information, machine states, and assessment reporting
  - OCIL (Open Checklist Interactive Language)
    - Information exchange format, less commonly used
- SCAP Identification Schemes
  - CPE (Common Platform Enumeration)

- Identifies hardware, OS, applications
  - SWID (Software Identification Tag)
    - Identifies software with metadata
  - CCE (Common Configuration Enumeration)
    - Provides unique identifiers for configuration issues
  - CVE (Common Vulnerabilities and Exposures)
    - Identifies software flaws
- Common Vulnerability Scoring System (CVSS)
  - Provides a relative severity score for security flaws based on factors like attack vector, complexity, privilege requirements, and confidentiality/integrity/availability impacts
- SCAP-Compatible Tools
  - OpenSCAP
    - For Unix/Linux-based systems
  - Tripwire
    - Compliance and security automation tool
  - Nessus
    - Vulnerability scanning tool supporting XCCDF and OVAL
  - InsightVM (Rapid7)
    - Vulnerability management and scanning tool
- **Vulnerability Scanning**
  - Definition and Purpose
    - Uses automated tools to identify and categorize security flaws and weaknesses

- I.e., vulnerabilities
- Helps maintain system security and reduce risk exposure
- Popular Vulnerability Scanning Tools
  - Nessus
    - Widely used for network vulnerabilities
  - InsightVM
    - From Rapid7, focuses on risk prioritization
  - OpenVAS
    - Open-source scanner
  - Nmap
    - Primarily a network discovery tool but can perform basic vulnerability scans
  - Qualys
    - Cloud-based security and vulnerability management
  - Nikto
    - Web server vulnerability scanner
  - Tripwire
    - File integrity monitoring and vulnerability assessment
- Types of Scans
  - Non-Credentialed Scan
    - Only checks general settings, configurations, and communications
    - Provides read-only access and faster results but with limited depth
  - Credentialed (Authenticated) Scan
    - Requires privileged access to log in as a root/admin user, providing deeper scanning

- Shows patch levels, detailed configurations, and other privileged insights
- Discovery Scan
  - Targets an IP address, range, or subnet to detect active hosts
  - Useful for maintaining an inventory of active hosts within a network
  - Usually done using a SYN scan (half-open scan) which identifies listening hosts on specified ports
- Port Status Results in Discovery Scans
  - Open
    - Host is actively communicating on the port
  - Closed
    - Host is live, but not communicating on that specific port
  - Unknown/Filtered
    - Communication blocked by firewall or security mechanism; port status is unclear
- Types of Packet Scans in Vulnerability Scanning
  - SYN Scan
    - Half-open scan that sends SYN packets and waits for SYN-ACK responses to identify active hosts
  - TCP Connect Scan
    - Completes the full TCP handshake to open the session and conduct a full vulnerability scan
  - ACK Scan
    - Sends ACK packets to identify firewall presence and assess statefulness

- XMAS Scan
  - Sends PUSH, URGENT, and FINISH flags to test responses for vulnerable configurations
- UDP Scan
  - Used to check active UDP services; lacks handshakes due to connectionless nature
- Vulnerability Scanning Process
  - Signature-Based Scan
    - Uses a signature database to detect vulnerabilities in patch levels, configuration, and open communication ports
  - Tools like Nessus
    - Provides categorized findings with severity ratings (critical, high, medium, informational)
  - Reporting
    - Findings must be analyzed, prioritized, and approved for remediation
- Best Practices for Vulnerability Scanning
  - Plan and Schedule Scans
    - Communicate scan times, scan in off-hours or during low activity to minimize impact on operations
  - Use Updated Scanners
    - Ensure the scanner has the latest vulnerability signatures
  - Incremental Scanning
    - Scan small host groups or subnets (e.g., /24 networks) instead of large networks at once

- Pre-Testing
  - Run test scans in development or sandbox environments to verify configurations
- Avoid Automatic Remediation
  - Manual approval is needed to avoid unapproved changes in production environments
- **Penetration Testing**
  - Penetration Testing Purpose
    - Simulates a system attack to exploit and identify vulnerabilities
    - Can target both logical (e.g., network and software systems) and physical (e.g., locks, cameras) controls
    - Provides insights into system vulnerabilities and helps determine the actual risks.
  - Rules of Engagement
    - An agreement that defines scope, methods, and objectives of the penetration test
    - Establishes legal cover and authorizations to ensure testers can ethically and legally perform the test
  - Types of Penetration Tests
    - White Box (Full Knowledge)
      - Testers have all relevant system details; typically more cost-effective
    - Black Box (No Knowledge)

- Testers have no prior knowledge; usually more costly due to discovery requirements
- Grey Box (Partial Knowledge)
  - A combination, providing testers with some information while keeping certain elements hidden
- Testing Teams
  - Red Team
    - Simulates the attacker role
  - Blue Team
    - Defends against simulated attacks
  - Purple Team
    - Combines Red and Blue teams to improve overall security posture
- Breach and Attack Simulation (BAS)
  - Automated testing to validate if security controls detect and respond to threats effectively
  - Helps assess security posture and identify areas for remediation
- Popular Tools/Distributions for Penetration Testing
  - Kali Linux, Parrot OS, BlackArch, Core Impact, and BackBox
- Key knowledge for the exam
  - Understand the purpose and structure of penetration testing
  - Know the rules of engagement and their significance
  - Be familiar with testing types, Team roles, and the purpose of breach simulations

- **Penetration Testing Phases**

- Phases of Penetration Testing

- Discovery (Reconnaissance) Phase

- Focuses on passive reconnaissance to collect information without interacting with the system
      - Involves using Open Source Intelligence (OSINT) and footprinting to identify potential targets

- Scanning (Active Reconnaissance) Phase

- Involves active reconnaissance by interacting with the system
      - Includes techniques like ping sweeps, port scans, banner grabbing, and vulnerability scans
      - Aims to identify weaknesses in the system

- Exploitation Phase

- Attempts to bypass security controls using manual methods or tools like Metasploit
      - Focuses on executing attacks while avoiding Indicators of Compromise (IOCs) to stay undetected

- Post-Exploitation Phase

- Uses information from exploitation to move laterally within the system
      - Includes maintaining access for ongoing exploitation and evading detection
      - Involves covering tracks by removing log files, scripts, and other evidence



- Reporting Phase
  - Documents all findings, vulnerabilities, and remediation recommendations
  - Includes an executive summary and a technical report for different audiences
  - Maps findings to rules of engagement and details each attack attempt and its results
- Post-Test Cleanup
  - Recover affected hosts, remove scripts/tools, and return the system to its original state
- For the exam, remember
  - Purpose and actions for each penetration testing phase
  - The need to document findings and results in detail during the reporting phase
- Log Reviews
  - Overview of Log Reviews
    - Logs are chronological records of system-related events, capturing actions like creations, modifications, and deletions
    - Often called audit logs or audit trails, they are essential for tracking and auditing system activities
  - Key Concepts
    - Syslog
      - A standardized format for collecting and transferring log data

# ISC2 CISSP

## (Study Guide)

- Contains facility codes for log types (e.g., Auth = 4, AuthPriv = 10) and severity levels (0 = most detailed, 7 = least detailed)
- Commonly configured at levels 5 (notice) or 6 (information) to meet regulatory standards
- No authentication mechanism, so security measures should be considered when configuring Syslog
- Clock Synchronization (Network Time Protocol, NTP)
  - Essential for accurate timestamps and reliable chronological event sequences
  - NTP runs on port 123 (UDP) and synchronizes time using Stratum clocks
  - Stratum 0 and 1 clocks are most accurate and preferred for logging, while Stratum 2 clocks are less reliable
- Log Protection and Security Best Practices
  - Store log data on remote servers to avoid tampering and ensure integrity.
  - Use file and directory permissions to allow read-only access, preventing unauthorized modifications
  - Hash logs periodically to verify data integrity
  - Conduct periodic log assessments to meet policy and compliance requirements
- For the CISSP exam, remember
  - Purpose of logs for tracking system events and audit trails
  - The function of Syslog for standardized logging and NTP for time synchronization

- Best practices for log protection, including secure storage and periodic reviews
- **Software Testing Methods**
  - Overview of Software Testing
    - Purpose
      - To verify software functionality, configuration, and performance, identifying flaws, vulnerabilities, and security risks
    - Three Main Testing Types
      - White Box Testing
        - Full knowledge; internal testers
      - Black Box Testing
        - No knowledge; external testers
      - Gray Box Testing
        - Some knowledge; mixed testing from both perspectives
  - Types of Software Tests
    - System Testing
      - Verifies software meets functional and security requirements
      - Also called Acceptance Testing or Reasonableness Check
    - Unit Testing
      - Focused on specific applications, scripts, or components
      - Assesses security, privacy, performance, or usability of a targeted feature
    - Integration Testing
      - Tests how two or more technologies work together

- E.g., protocols or different OS versions
- Regression Testing
  - Ensures changes haven't impacted existing functionality
- Sanity Check
  - Quick validation of a feature's viability early in development
- Smoke Testing
  - Assesses basic functionality after a build, often called a Verification Test
- Fuzz Testing
  - Sends invalid data to discover vulnerabilities or performance issues
- Mutation Fuzzing (Dumb Fuzzing)
  - Modifies valid operational data to create invalid inputs
- Generational Fuzzing (Smart Fuzzing)
  - Creates synthetic data using an input model to generate invalid inputs
- Key Points for CISSP
  - Know the difference between system, unit, integration, regression, sanity, and smoke tests
  - Understand fuzz testing types (mutation and generational)
- **Software Code Reviews**
  - Overview of Code Reviews
    - A code review is an analysis of developed software code aimed at identifying flaws, defects, vulnerabilities, and security risks before deployment

- Static Testing
  - Static Application Security Testing (SAST)
    - Analyzes code without running it
      - E.g., reviewing code in a text editor
  - Dynamic Testing
    - Dynamic Application Security Testing (DAST)
      - Analyzes code while it's running in a production environment, often when code cannot be taken out of production
- Fagan Inspection Process (Phased Code Review Process)
  - Planning
    - Organize and prepare for the review
  - Overview
    - Define the scope of the review and establish roles and expected outcomes.
  - Inspection
    - Examine the code for potential flaws and vulnerabilities
  - Rework
    - Collaborate with developers to remediate identified flaws
  - Follow-up
    - Verify that remediation was successfully implemented
- Key Points for the CISSP Exam
  - Understand the differences between static and dynamic testing methods
  - Know the steps of the Fagan inspection process and their purpose within a code review

- **Misuse Testing**

- Overview of Misuse Testing

- Misuse testing simulates improper or malicious use of software or systems from an attacker's or user's perspective
    - Also known as abuse case testing, it aims to uncover how a system might respond to misuse and identify potential vulnerabilities

- Key Steps in Misuse Testing

- Identify Critical Assets

- Determine critical business functions, applications, or services.
      - Prioritize assets based on their importance to the organization.

- Define Security Goals

- Set expected outcomes for the test and identify which aspects require protection.

- Identify Threats

- Identify and analyze risks to each critical asset, often through threat modeling or risk analysis.

- Define Security Requirements

- Outline specific security needs, recognizing the need to prioritize due to resource constraints.

- Misuse Test Visualization - UML Diagram

- Unified Modeling Language (UML) diagrams help map user and attacker interactions with the system
    - Shows legitimate user activities and potential misuse by attackers, highlighting vulnerabilities and potential security requirements

- Application of Misuse Testing
  - Often conducted alongside risk analysis, security assessments, threat modeling, and penetration testing to fully understand possible attack vectors
- Key Points for the CISSP Exam
  - Know the purpose and process of misuse testing, including steps for planning and execution
  - Understand how to use UML diagrams to visually map potential misuse scenarios and threats
- **Interface Testing**
  - Overview of Interface Testing
    - Interface testing evaluates the connections between different components or systems, focusing on how data is exchanged
  - Common interfaces include
    - Application Programming Interface (API)
      - Used for software-to-software communication
    - User Interface (UI)
      - How users interact with applications and systems.
    - Physical Interfaces
      - Physical connections between hardware components (cables, wireless, etc.)
  - Purpose and Focus of Interface Testing
    - Validates data exchange to ensure security and functionality across interfaces

- Ensures secure information flow by testing for confidentiality, integrity, and availability
- Tests how the system responds to valid and invalid inputs, errors, and failures to prevent potential security issues
- Key Areas for Interface Testing
  - Error Handling
    - How does the system react to unexpected inputs or failures?
  - Security Controls
    - Are appropriate security measures in place to protect data flow across interfaces?
  - Session Management
    - Are sessions timed out securely if left inactive?
  - Recovery and Resilience
    - Does the system recover securely from a failure?
- Testing Scenarios
  - Used during system development, security assessments, and audits to ensure interfaces function as expected and securely handle data exchanges
- Key Takeaways for the CISSP Exam
  - Understand the different interface types and their unique testing requirements
  - Know the importance of testing both ends of each interface to ensure security and stability



- **Compliance Testing**

- Overview of Compliance Testing

- Purpose

- Ensures adherence to standards, helping identify vulnerabilities and demonstrate data protection (due care) and ongoing compliance (due diligence)

- Approach

- Involves security assessments and audits, both internally and externally, to verify proper control implementation

- Key Standards for Compliance

- SSAE 18 & SOC Reports

- SSAE 18

- A standard for audit reporting in financial services

- SOC 1, 2, 3

- Different SOC reports assess financial and security control standards. SOC 1 focuses on financial controls; SOC 2 covers security and privacy controls; SOC 3 is a high-level summary for public use

- PCI DSS Compliance

- Merchant Levels

- PCI DSS requirements vary by transaction volume. Level 1 (over 6 million transactions) requires a Report on Compliance (ROC) by a Qualified Security Assessor (QSA), while Levels 2-4 may only need a Self-Assessment Questionnaire (SAQ)

- CSA STAR (Cloud Security Alliance Security Trust Assurance and Risk)
  - Level 1
    - Self-assessment for low-risk data environments
  - Level 2
    - Requires third-party auditing for regulated or higher-risk data environments
- CISSP Exam Focus
  - Understand SOC reports
    - Types and purposes, especially SOC 1 (financial), SOC 2 (security), and SOC 3 (public)
  - Know PCI DSS levels
    - Requirements by merchant level, especially ROC for Level 1
  - CSA STAR Levels
    - Self-assessment for low-risk vs. third-party audits for high-risk environments
- **Test Coverage Analysis**
  - Test Coverage Analysis
    - Estimating the level of testing performed on a product
    - Relation between actual testing and possible testing
    - Calculation-based approach
  - Test Coverage Calculation
    - Test coverage is the number of executed test cases divided by the total possible test cases
    - Provides a level of confidence in the tested product

- Coverage Criteria (Code Criteria)
  - Defines test requirements for the product or component
  - Ensures that critical areas and functions are tested to a certain degree of confidence
- Coverage Examples
  - Example
    - 100 test cases are possible for a system component, and 50 are executed
  - Confidence level in testing is 50%
- Branch Coverage
  - Ensures each decision branch in the code has been tested
  - Involves version control and change control to enforce changes on branches
  - Enables parallel software development and branch check-ins/outs
- Condition Coverage
  - Ensures all logical conditions within routines, subroutines, and procedures are tested
- Functional Coverage (Function Coverage)
  - Ensures each program function is tested for verification
- Loop Coverage
  - Ensures all loop statements are tested
  - Loops repeat code until reaching a certain criteria
    - E.g., end of record
  - Essential to prevent service outages caused by continuous loops
- Statement Coverage

- Ensures each code statement is tested for verification of functionality
- Coverage Levels
  - Determined by the criticality of the application and the sensitivity of processed data
  - Example
    - An application for compliance purposes, such as financial systems, requires a higher coverage level
- Safety and Security
  - Prioritized for all coverage analyses
  - Safety and security considerations define the depth of coverage
- **Analyzing Test Results**
  - Test Result Outputs
    - Data generated from tools and test procedures after conducting security assessments
    - Includes errors, lessons learned, and potential system crashes
  - Report Structure
    - Clear definition of actions taken, expected outcomes, and a high-level summary of events
    - Consideration of target audience (senior management, system owners, security managers)
  - Information for Target Audiences
    - Senior management requires high-level information with business impacts

- Technical staff (system administrators, network administrators) need detailed technical information
- Balancing report details ensures effective communication without overloading or under-informing
- Types of Reports
  - Assessment Report
    - Outlines approach and findings of security tests or assessments
    - Includes control tests or assessments such as Privacy Impact Assessment (PIA)
  - Audit Report
    - Outlines approach and findings for compliance-related tests or assessments
    - Generated for self-assessments or third-party audits
- Ethical Disclosure
  - Requirement to disclose vulnerabilities, security problems, or other issues identified
  - Ensures transparency and adherence to the Code of Ethics
- Executive Summary
  - Briefly summarizes test outcomes, assessments, reviews, and audits
  - Provides critical findings, recommendations, and remediation options
  - Targeted at senior management, focusing on business impacts
- Key Report Components
  - Threats and Vulnerabilities
    - Include all discovered threats, regardless of perceived importance
  - Criticality and Likelihood

- Document importance of findings and likelihood of occurrence
- Exposure Factor
  - Potential impact if exploit occurs
    - E.g., percentage of asset loss
- Remediation Recommendations
  - Suggested corrective actions such as updates, patches, and security controls
  - Exceptions
    - Known non-compliant items or issues excluded from testing due to prior disclosures
- Remediation Process
  - Recommendations to fix or apply security controls to address findings
  - Authorized personnel must implement any changes to avoid configuration or compliance issues
- Handling Exceptions
  - Exceptions are known issues excluded from testing due to planned remediation timelines
  - Reduces unnecessary testing and focuses efforts on new findings
  - Listing exceptions saves time, energy, and cost
- Key Principles for CSSP Exam
  - Process test output information correctly
  - Adhere to ethical disclosure
  - Understand important report contents and appropriate remediation/exception handling

## Detective And Preventative Measures

### Objectives:

- 7.2 - Conduct logging and monitoring activities
  - 7.4 - Apply foundational security operations concepts
  - 7.7 - Operate and maintain detection and preventative measures
- 
- **Detective And Preventative Measures**
    - Key Concepts
      - Security Operation Concepts
        - Defense in Depth
          - Multiple layers of security controls used to protect information assets
          - Reduces the likelihood of a single point of failure
        - Least Privilege
          - Users and systems are granted the minimum level of access necessary to perform their duties
        - Separation of Duties
          - Dividing tasks and privileges among multiple people or systems to prevent fraud or error
        - Logging and Monitoring
          - Systems and applications should record relevant events for review

- Helps detect suspicious activity and prevent threats
- Detective and Preventative Measures
  - Detection
    - Involves identifying potential security threats and vulnerabilities
  - Prevention
    - Involves stopping security threats before they can cause harm
  - Intrusion Detection Systems (IDS)
    - Monitors network traffic and alerts administrators to potential threats
    - Passive system that does not actively block threats
  - Intrusion Prevention Systems (IPS)
    - Monitors network traffic and actively blocks identified threats
    - Takes preventive action to stop malicious activities
  - Honeypots
    - Decoy systems set up to attract attackers
    - Used to monitor and gather intelligence on attacker behavior
  - Honeynets
    - Networks of honeypots designed to look like real environments
    - Provides insights into the methods used by attackers
  - Anti-Malware Tools
    - Used to detect and remove malicious software from systems
    - Includes tools like antivirus software and advanced malware detection solutions
  - Artificial Intelligence (AI) in Detection and Prevention
    - AI helps automate threat detection processes



- Analyzes large amounts of data to detect potential vulnerabilities and anomalies
- Malicious Software (Malware)
  - Virus
    - A type of malware that attaches to files and spreads when executed
  - Worm
    - Self-replicating malware that spreads across networks without user interaction
  - Ransomware
    - Malware that encrypts data and demands a ransom for its release
  - Spyware
    - Malware designed to gather information about a user without their knowledge
  - Signature-based Detection
    - Identifies malware by comparing file signatures to a known database of threats
  - Heuristic Analysis
    - Detects malware by analyzing behavior and code patterns that resemble known threats
- End of Life (EOL) and End of Support (EOS)
  - End of Life (EOL)
    - Indicates when a product or software is no longer sold or upgraded
  - End of Support (EOS)

# ISC2 CISSP

## (Study Guide)

- Refers to the point when a vendor stops providing patches and updates
- Regression Testing
  - Used to ensure changes in software or security patches do not introduce new vulnerabilities or break existing functionality
  - Validates that all features, functionalities, and security measures remain intact after updates
- **Security Operation Concepts**
  - Security Operations
    - Ensures secure operation and maintenance of systems in production or operational environments
    - Maintains a secure baseline and effective controls throughout the system's lifecycle
  - Need to Know
    - Grants access only to information necessary to perform job duties or tasks
    - Decision made by the data owner, implementing discretionary access control (DAC)
    - Often managed using
      - Role-based access controls (RBAC)
      - Clearance levels or mandatory access controls (MAC)
      - Compartmentalization and data isolation for unauthorized users
  - Least Privilege

# ISC2 CISSP

## (Study Guide)

- Provides access only to functions or permissions needed to perform specific job roles
- Focuses on functional access rather than data access
- Typically enforced using RBAC and supports need to know and separation of duties
- Requires clear definition of job roles and functions to prevent unnecessary access
- Separation or Segregation of Duties
  - Requires multiple individuals to complete a sensitive or critical task to prevent abuse of power
  - Segregates responsibilities to avoid conflict of interest and security risks
  - Prevents any one individual from compromising security controls
  - May involve collusion, where multiple people would need to work together to bypass security
- Privileged Account Management
  - Controls the use of privileged or elevated accounts
    - E.g., admin, root, sudo, domain accounts
  - Limits access to sensitive functions and configurations that could impact system integrity
  - Protects accounts used for actions like credentialed vulnerability scans and log access
- Job Rotation
  - Rotates individuals in roles to detect internal or external threats and identify single points of failure

- Helps prevent privilege creep, where individuals retain excess permissions over time
- Acts as
  - Preventative by limiting exposure to sensitive functions
  - Detective by identifying inconsistencies or security issues
  - Deterrent by reducing excessive control of one individual
- Service Level Agreement (SLA)
  - A formal agreement with an external provider defining service terms and conditions
  - SLAs include cloud hosting, security services, and website hosting terms
  - Must include
    - Defined, agreed-upon metrics to measure service
      - E.g., uptime
    - Consequences for SLA violations
      - E.g., financial penalties or dispute resolutions
- **Detective and Preventative Concepts**
  - Security Operations Goals
    - Operate technical mechanisms to discover or prevent security policy violations
    - Use controls such as log analysis, network monitoring, and vulnerability scanning to detect potential issues
  - Detective Controls
    - Aim to discover current or previous security policy violations
    - Examples include

- Host-based Intrusion Detection Systems (HIDS)
  - Data Loss Prevention (DLP)
  - Anti-malware solutions
  - Host-based firewalls
- Send alerts to Security Information and Event Management (SIEM) systems for real-time monitoring
- Preventative Controls
  - Designed to prevent security violations from occurring
  - Examples include
    - Whitelisting and Blacklisting
    - Access Control Lists (ACLs)
    - Encryption
- Whitelisting
  - Permits specific actions or functions, denying everything else by default
  - Known as "permit by exception"
  - Offers stricter security as only specified actions are allowed
  - Reduces risk by strictly controlling access and functionality
- Blacklisting
  - Denies specific actions or functions, allowing everything else by default
  - Less secure but enhances availability
  - Known as "deny by exception"
- Access Control List (ACL)
  - Configurable as either whitelist or blacklist on network devices like firewalls or switches

- Used to permit or deny traffic based on criteria such as source, destination, and port
- Sandboxing
  - A confined, virtualized test environment for applications to prevent interaction with external systems
  - Also called confinement
  - Use cases include
    - Malware analysis
    - Testing configurations or code
    - Example
      - Type 2 hypervisors (e.g., VirtualBox, VMware Workstation Player) creating virtual machines isolated from the main system
- Third-Party Security Services
  - Utilize external providers for security expertise, tools, or analysis
  - Important considerations
    - Vetting of third-party background, tools, and supply chain
    - Compliance with governance and regulation requirements
    - Must have well-defined Service Level Agreements (SLAs) and Non-Disclosure Agreements (NDAs) in place
    - SLAs define expected services and metrics for performance
    - NDAs protect sensitive information, ensuring confidentiality
- Third-Party Involvement in Incident Response
  - Should be integrated into the incident response plan
  - Consider roles in both detection and prevention of incidents

- Ensure clear, professional handling of sensitive data and incidents
- Key Takeaways for Exam
  - Understand detective vs. preventative measures
  - Know whitelisting and blacklisting purposes
  - Recognize the role of sandboxes in secure testing
  - Comprehend the importance of third-party security services in incident response and regulatory compliance
- **IDS/IPS Systems**
  - Purpose of IDS and IPS
    - Intrusion Detection (IDS)
      - Listens and reports on unauthorized access attempts, circumventing security or privacy controls
    - Passive
      - Monitors activity without taking action
      - Methods include packet inspection, log analysis
    - Intrusion Prevention (IPS)
      - Actively detects and responds to security incidents
      - Also known as active IDS
      - Takes action to block attacks by altering device configurations
  - NIST and ISO Standards for IDS and IPS
    - NIST Special Publication 800-94
      - Guide to Intrusion Detection and Prevention Systems
    - ISO/IEC 27039
      - Selection, deployment, and operations of IDS and IPS

- Detection Types
  - Knowledge-Based Detection (Signature-Based)
    - Compares monitored events with known attack signatures (signature files or database required)
    - Requires constant updates to detect emerging threats
    - Also called pattern matching detection
  - Behavior-Based Detection (Anomaly-Based)
    - Compares current activity against profiles of normal activity
    - Requires a learning period to establish baseline behaviors
    - Prone to false positives due to unexpected but legitimate activity
    - Also known as heuristic-based or statistical intrusion detection
  - Stateful Protocol Analysis
    - Analyzes events against current communication protocol states
    - Uses vendor-provided signature profiles to detect protocol anomalies
  - IDS and IPS Deployment Types
    - Network-Based IDS (NIDS) and Network-Based IPS (NIPS)
      - Monitors and analyzes network-wide activity
      - Network IPS must be in line with network traffic to prevent attacks effectively
  - Host-Based IDS (HIDS) and Host-Based IPS (HIPS)
    - Monitors specific host activity for violations
    - Cannot analyze network-level threats or misconfigurations
  - Wireless IDS and Wireless IPS
    - Monitors wireless network traffic for protocol-related anomalies
  - Network Behavior Analysis



- Examines network traffic for unusual communication patterns, often combined with stateful protocol analysis
- Deployment Setup
  - IDS
    - Installed with a SPAN, monitor, or promiscuous port; traffic bypasses IDS as it is listen-only
  - IPS
    - Must be in line with traffic to intercept and take action on attacks; potential for network latency issues
  - Host-Level Deployment
    - Host-based IDS or IPS installed on each endpoint as an additional layer of defense
- Key Takeaways for Exam
  - Differentiate between IDS (passive detection) and IPS (active prevention)
  - Know detection types (knowledge-based, behavior-based, stateful protocol analysis)
  - Recognize network-based, host-based, and wireless deployment differences and use cases
- **Honeypots and Honeynets**
  - Purpose of Honeypots and Honeynets
    - Honeypot
      - A vulnerable system set up intentionally to lure attackers away from valuable assets

# ISC2 CISSP

## (Study Guide)

- Configured with vulnerabilities and often includes false data to attract intruders
- No sensitive information is stored on honeypots
- Can use missing patches, misconfigurations, and open services (e.g., Telnet, FTP) to appear more appealing
- Alerts when accessed to detect intrusion attempts
- Honeynet
  - A network of multiple honeypots designed to create a more realistic, vulnerable network environment
  - Used to simulate a full network, making it more believable for attackers
  - Deploys unused IP addresses to enhance believability
  - Containment strategy to keep attackers within a simulated network, reducing risk to real assets
- Advanced Honeypot Deployment
  - Padded Cell
    - Functions similarly to a honeypot but isolates attackers upon access to prevent damage to real systems
    - Simulates a realistic network environment with pseudo data to keep attackers engaged
    - Resource-intensive and typically used in large enterprise environments
    - Often monitored by a Security Operations Center (SOC)
  - Deployment Strategy for Honeypots and Honeynets
    - DMZ Deployment

- Place honeypots in the DMZ to attract attackers away from critical servers and infrastructure
- Internal Network Deployment
  - Deploy additional honeypots within the internal network to redirect attackers who breach further
- HoneyNet Setup
  - Multiple honeypots linked together to simulate a network, deterring attackers from critical assets
- Detection and Alerts
  - Honeypots and honeynets should send alerts to a Security Information and Event Management (SIEM) system when accessed to enable timely response
- Key Takeaways for Exam
  - Understand the purpose of honeypots, honeynets, and padded cells
  - Recognize the differences in setup and function between honeypots (single vulnerable system), honeynets (network of honeypots), and padded cells (isolated pseudo network)
- **Malicious Software**
  - Malware
    - Malicious software designed to harm or exploit computer systems
    - Includes software and malicious code (malcode) or scripts targeting specific harmful functions
    - Purpose includes causing damage, stealing data, exfiltrating data, or extorting money

- Types of Malware
  - Worms
    - Self-contained, replicate independently without human intervention
  - Logic Bombs
    - Activate under specific conditions
      - E.g., timer, file opening
  - Trojan Horses
    - Disguised as legitimate applications; install malware upon execution
  - Remote Access Trojans (RATs)
    - Create backdoor access for attackers
  - Ransomware
    - Encrypts data and demands ransom for decryption key
  - Keyloggers
    - Record keystrokes to capture sensitive information
  - Zero-Day Malware
    - Exploits vulnerabilities with no available defense or patch
- Additional Malware Types
  - Spyware
    - Monitors and collects data (e.g., credentials) from remote computers
    - Techniques include keylogging, screen scraping, screen capture
  - Adware
    - Collects user interest data, can expose personal information

- Bots
  - Malware-infected computers controlled by attackers
    - E.g., for DDoS attacks
- Botnet
  - Network of bots controlled by a Botmaster using a command-and-control server
- Viruses
  - Attach to legitimate applications, designed to infect and spread widely
  - Over 300 million types globally
- Virus Types by Infection Method
  - Master Boot Record Virus
    - Infects first boot sector, loaded upon device startup
  - File Infector Virus
    - Infects files and activates upon file execution
  - Macro Virus
    - Infects Microsoft Office products using Visual Basic for Applications (VBA)
  - Service Injection Virus
    - Infects trusted system services to evade detection
- Types of Viruses by Behavior
  - Polymorphic Virus
    - Alters itself as it spreads to evade detection
  - Encrypted Virus

- Uses encryption to hide from anti-malware; requires decryption for scanning
  - Multipartite Virus
    - Uses multiple infection methods to increase spread speed
  - Stealth Virus
    - Modifies system processes to hide its presence; erases activity evidence
- Key Takeaways for Exam
  - Understand the definition and purpose of malware and malcode
  - Familiarize with types of malware and their functions
  - Recognize various virus types by infection method and behavior
- **Anti-Malware**
  - Purpose of Anti-Malware
    - Software designed to scan, detect, isolate, and remove types of malware
    - Protects systems by analyzing files for malware during download or execution
  - Types of Malware Detection
    - Signature-Based Detection
      - Compares files against known malware signatures from a vendor-provided database
      - Requires regular updates to be effective against recent threats
      - Also known as knowledge-based detection or pattern matching detection
    - Heuristic-Based Detection

- Analyzes malware behavior, useful for zero-day malware
- Static Heuristic Analysis
  - Scans malware without executing it
- Dynamic Heuristic Analysis
  - Executes malware in a sandbox to observe behavior
    - E.g., propagation
- Anti-Malware Functions
  - Quarantine
    - Isolates suspicious files in a sandbox for further analysis
  - Disinfect
    - Attempts to remove malware from infected files (not always possible)
  - Delete
    - Removes malicious files if disinfection is not possible
- Types of Malware Scanning
  - On-Access Scanning
    - Scans files automatically upon download or execution
  - On-Demand Scanning
    - Scans files manually when requested by the user
- Defense Mechanisms Against Malware
  - Layered Security (Defense in Depth)
    - Multi-layered defenses including
      - Firewalls (Next-Gen Firewalls, Unified Threat Management)
      - Intrusion Detection and Prevention Systems (IDS/IPS)
      - Endpoint Detection and Response (EDR)

- Regular Updates
  - Ensures that anti-malware software and signature files are current
- Access Controls
  - Implement whitelist (permit by exception) and blacklist (deny by exception) policies
- Security Awareness Training
  - Educate users on safe browsing and email practices
  - Teach recognition of phishing and social engineering attempts
  - Promote cautious behavior around file downloads and external links
- Key Takeaways for Exam
  - Understand the function and importance of anti-malware software
  - Know the difference between signature-based and heuristic detection
  - Recognize the importance of security awareness training in malware prevention
- **Artificial Intelligence Tools**
  - Artificial Intelligence (AI) Levels
    - Narrow AI (Weak AI)
      - Focuses on a single task, no transfer of learning across tasks
    - Example
      - Virtual assistants like Siri, Alexa; chatbots, automated processes
    - Artificial General Intelligence (AGI)
      - Mimics human intelligence, handles complex tasks
      - Seeks to equate computer and human intelligence for problem-solving



- Artificial Superintelligence (ASI)
  - Future goal where AI surpasses human intelligence levels
- Applications of AI in Cybersecurity
  - Expert Systems
    - Mimics human behavior for decision-making; can function in narrow and general AI
  - Natural Language Processing (NLP)
    - Allows AI to process and understand human language, such as commands to virtual assistants
  - Machine Learning (ML)
    - Subset of AI focused on data pattern recognition and automation
- Machine Learning (ML) Types
  - Supervised Learning
    - Uses labeled data to train algorithms, relies on human-provided data for pattern detection
    - Applied in recommendation engines, threat pattern recognition
    - Risk
      - Can develop biases from labeled data
  - Unsupervised Learning
    - Analyzes unlabeled data, uses clustering to find hidden patterns
    - Used for anomaly detection, advanced threat detection
  - Semi-Supervised Learning
    - Combines labeled and unlabeled data, balances specificity and data exploration

- Useful in cybersecurity for targeted threat analysis and broad data mining
- Reinforcement Learning
  - Uses positive/negative feedback loops to refine decision-making
- Example
  - Autonomous driving in Tesla cars
- Artificial Neural Networks (ANNs)
  - Function
    - Simulates human decision-making by analyzing multiple data inputs and providing simplified outputs
  - Applications
    - Email spam detection, behavior-based threat detection, business intelligence
  - Structure
    - Input layer → Hidden layers (data processing) → Output layer (decisions or predictions)
- AI Risks
  - Misconfiguration
    - Poor implementation or data labeling can lead to faulty outputs
  - Inconsistent Outputs
    - Frequent data updates result in varying AI decisions
  - Resource Intensive
    - Requires time, financial investment, and infrastructure
  - Lack of Ethics/Sensitivity

# ISC2 CISSP

## (Study Guide)

- AI lacks awareness of privacy or ethical implications, requiring human oversight
- Key Takeaways for Exam
  - Understand the purpose and types of AI, focusing on Narrow AI for practical applications
  - Familiarize with machine learning types
    - Supervised, unsupervised, semi-supervised, and reinforcement learning
  - Recognize the limitations and risks of AI, including potential biases, inconsistent outputs, and the importance of human oversight

## Logging and Monitoring

Objective 7.2: Conduct logging and monitoring activities

- **Logging and Monitoring Introduction**

- Logging and Monitoring
  - Logging
    - Logs capture a detailed record of events and activities in the system
    - Events to monitor include user activity, system access, errors, and application behavior
    - Logs are foundational for identifying signs of potential security incidents
  - Security Information and Event Management (SIEM)
    - SIEM platforms aggregate and analyze log data across infrastructure
    - SIEM solutions identify suspicious patterns and generate alerts in real-time
    - SIEM helps manage large volumes of log data efficiently, enabling faster response
  - Threat Intelligence
    - Threat intelligence involves gathering information about current vulnerabilities and attack techniques
    - Threat intelligence helps anticipate attacker actions and integrate data into monitoring strategies
    - Incorporating threat intelligence enables a proactive approach to prevent attacks

- MITRE ATT&CK Framework
  - MITRE ATT&CK is a structured framework that catalogs real-world attack techniques
  - Correlating log data with the ATT&CK framework provides visibility into attacker methods
  - This helps understand an attacker's goals and take preventative action at the right stage
- Cyber Kill Chain
  - The Cyber Kill Chain outlines the stages of an attack from reconnaissance to exfiltration
  - Each stage provides an opportunity to detect signs of an attack and mitigate it
  - Logs can reveal clues that correspond to each stage of the kill chain
- Security Orchestration, Automation, and Response (SOAR)
  - SOAR optimizes logging and monitoring activities by automating incident response tasks
  - Automating routine tasks helps security teams focus on higher-priority threats
  - SOAR enhances efficiency and response time in dealing with security incidents
- User Behavior Analytics (UBA)
  - UBA identifies anomalies by comparing current user behavior against established baselines
  - UBA is effective for detecting insider threats and advanced persistent threats (APTs)

- UBA enhances security by detecting threats that signature-based tools may miss
- **Logging and Monitoring**
  - Logging Basics
    - Logs are system-generated records of events, essentially a digital journal tracking activities across various system components
    - Purpose
      - Used for investigating events, auditing compliance, troubleshooting issues, and ensuring system health
  - Types of Events to Log
    - User Authentication
      - Log successful and failed login attempts
      - Track session start and end times
    - Access Control
      - Record attempts (successful and failed) to access sensitive objects, files, or directories
    - Account Management
      - Log creation, modification, and deletion of user accounts.
    - Privilege Use
      - Track usage of privileged commands
        - E.g., sudo, root access
    - Application Initiation
      - Log start and stop of critical applications or services.
  - Logging Systems
    - Centralized Logging

- Collects logs from various sources to a single server or security information and event management (SIEM) system
- Facilitates real-time analysis and backup
- Decentralized Logging
  - Each device or server maintains its own log files
- Best Practice
  - Combine centralized and decentralized logging for optimal protection and analysis
- Essential Components of Log Entries
  - Who
    - User or account associated with the action
  - What
    - Description of the action taken
  - When
    - Date and time (requires a reliable time source like NTP)
  - Where
    - Hostname, IP address of the source
  - Result
    - Outcome (e.g., success, failure) of the action
- Monitoring Techniques
  - Audit Trails
    - Aggregate and correlate logs from multiple systems
    - Enable traceability and chronological analysis of events
  - Ingress Monitoring (North-South)
    - Monitors inbound traffic from external networks

- Helps detect potential threats or intrusions early
- Egress Monitoring (Southbound)
  - Tracks outbound traffic
  - Protects against unauthorized data exfiltration.
- Log Management Tools
  - SIEM (Security Information and Event Management)
    - Centrally collects and analyzes logs in real-time
  - IDS/IPS (Intrusion Detection/Prevention Systems)
    - Monitors for rule or policy violations
  - DLP (Data Loss Prevention)
    - Prevents unauthorized data transfer and exfiltration
- Protecting Log Files
  - Access Control
    - Limit access to sensitive log files
  - Encryption
    - Encrypt log files in storage and during transmission
  - Retention Requirements
    - Some industries require logs to be retained for several years
      - E.g., 1–5 years
  - Clipping Levels
    - Set thresholds to capture only significant events
      - E.g., after 3 failed login attempts
  - Transmission Security
    - Use secure protocols to transfer logs between decentralized and centralized systems



- Standards and Compliance
  - ISO 27001
    - Information security management, including controls for log management
  - NIST SP 800-53
    - Provides controls for information system logging
  - NIST SP 800-92
    - Guide to Computer Security Log Management, covering detailed logging best practices
- Key Points for the Exam
  - Understand logging's role in security operations
  - Know centralized vs. decentralized logging methods
  - Be familiar with monitoring techniques (ingress and egress)
  - Learn about log security practices and relevant standards
- **Security Information and Event Management (SIEM)**
  - Overview of SIEM
    - SIEM is a system for real-time analysis of security events and log data from multiple sources across an IT infrastructure
    - Primary Functions
      - SIEM tools collect, aggregate, analyze, and report on log data to detect advanced threats and security events
  - Components of SIEM
    - Security Information Management (SIM)

# ISC2 CISSP

## (Study Guide)

- Collects and aggregates logs and messages from hosts to a central repository
- Security Event Management (SEM)
  - Correlates, analyzes, and monitors these logs for potential security events
- Combined
  - Together, they form the SIEM, which is a unified tool capable of collection, aggregation, and correlation for threat detection and response
- Key Features of SIEM Systems
  - Data Collection
    - Logs from firewalls, servers, applications, and network devices
    - Centralized for a single analysis point
  - Aggregation and Correlation
    - Aggregates data to correlate events across multiple sources
    - Establishes audit trails by matching events from various logs, aiding in compliance and forensic analysis
  - Real-Time Monitoring and Alerts
    - Provides real-time alerts for security incidents and anomalies
    - Customizable alerts based on user-defined triggers or industry requirements
  - Dashboard and Reporting
    - Graphical user interface displaying relevant, filtered data
    - Configurable to display logins, visitor origins, operating system details, etc.

- Automatically generates reports for management and compliance
- Retention and Archive
  - Stores logs to meet industry compliance requirements (1–5 years, depending on regulations)
  - Protects logs in storage to maintain integrity and authenticity.
- Data Analysis
  - Uses machine learning and AI to filter and prioritize relevant data
  - Ideal for handling large volumes of log data, especially with legacy logs and historical data
- SIEM Deployment Options
  - Agent-Based
    - Specialized software (agent) is installed on each host
    - Agents send logs to the SIEM, allowing for deeper data collection
  - Agentless
    - Receives logs directly from systems without additional software
    - More commonly used in recent deployments due to reduced overhead
- SIEM Interface Example
  - Dashboard
    - Customizable with charts, logs, and filters
    - Real-time data on logins, access attempts, system health, and more
    - Visualized geographic locations of visitors, OS types, and activity patterns

- SIEM Benefits in Security Operations
  - Threat Detection
    - Centralizes log data for quick identification of threats and anomalous activities
  - Enhanced Response Time
    - Real-time alerts allow for prompt investigation and response
  - Regulatory Compliance
    - Supports retention, reporting, and traceability, meeting industry standards
  - Incident Forensics
    - Provides detailed logs to analyze security incidents retrospectively
- Points to Remember for the Exam
  - Know the difference between SIM, SEM, and SIEM
  - Understand SIEM's purpose in log aggregation, real-time monitoring, and threat detection
  - Recognize deployment options (agent-based vs. agentless)
  - Familiarize with core SIEM functions
    - Data collection, correlation, alerting, reporting, and data retention
- **Threat Intelligence**
  - Overview of Threat Intelligence
    - Analyzed information used to make threat-based decisions
    - Purpose
      - Supports security operations by providing insights on potential threats, enabling informed and proactive defense measures

- Core Components of Threat Intelligence
  - Threat Information vs. Threat Intelligence
    - Threat Information
      - Raw data about potential threats
        - E.g., logs, indicators
  - Threat Intelligence
    - Analyzed data that aids in decision-making by understanding the context of threats
  - Situational Awareness
    - Uses threat intelligence to understand the security posture and identify vulnerabilities
    - Allows organizations to proactively adapt to emerging threats based on past attack patterns
  - Tactics, Techniques, and Procedures (TTPs)
    - TTPs are proven strategies used by attackers
    - Knowing TTPs allows quicker adaptation to and defense against new threats
- Key Elements in Threat Intelligence
  - Threat Feeds
    - Sources of information that provide real-time updates on known threats
    - Can include suspicious IP addresses, malicious domains, active attack protocols, and more
    - Typically formatted in XML or similar data structures

- Threat Hunting
  - Proactive search for threats that are not detected by existing alerts
  - Goes beyond known indicators to identify new or hidden threats
  - Uses insights from threat intelligence to guide investigations across the system
- Threat Intelligence Tools and Platforms
  - Threat Feeds Tools
    - Examples
      - Yeti, AlienVault
    - Function
      - Ingests threat feed data and translates it into actionable information
      - Provides insight on malware, malicious domains, and current crimeware trends
  - Threat Hunting Tools
    - Uses threat intelligence to aid analysts in identifying and mitigating potential threats within the network
    - Can be part of SIEM or stand-alone tools for detailed analysis
- Benefits of Threat Intelligence
  - Enhanced Defense
    - Improves security posture by using verified threat data
  - Proactive Threat Hunting
    - Moves security operations from reactive to proactive
  - Informed Decision-Making

- Enables security teams to make quick, data-driven decisions based on threat intelligence
- Key Concepts for the Exam
  - Purpose of Threat Intelligence
    - Enables security operations to make informed, threat-based decisions
  - Threat Feeds
    - Know their role in providing real-time data about current threats
  - Threat Hunting
    - Understand that it is a proactive process using threat intelligence to identify undetected threats
- **MITRE ATT&CK Framework**
  - Overview of the MITRE ATT&CK Framework
    - An open knowledge base detailing tactics, techniques, and procedures (TTPs) used in real-world attacks
    - Purpose
      - Helps organizations develop threat models and enhance security strategies by understanding and anticipating attacker behaviors
  - Key Components
    - Tactics, Techniques, and Procedures (TTPs)
      - Tactics
        - High-level attack goals (e.g., gaining initial access)
    - Techniques
      - Specific methods to achieve a tactic

- Procedures
  - How techniques are implemented in attacks
- Categories
  - Reconnaissance
    - Gathering information through passive means, open source intelligence (OSINT), phishing, etc.
  - Resource Development
    - Identifying attack vectors and assets for potential exploitation
  - Initial Access
    - The point where an attacker first gains entry to the system
  - Execution
    - Running malicious code or scripts
  - Persistence
    - Maintaining access to the system by manipulating accounts or processes
  - Privilege Escalation
    - Gaining higher access privileges to critical system functions
  - Defense Evasion
    - Avoiding detection by intrusion detection systems (IDS) or endpoint security tools
  - Credential Access
    - Acquiring credentials for further access
  - Discovery
    - Locating more resources or systems to exploit



- Lateral Movement
  - Moving across the network (east-west traffic) between resources
- Collection
  - Gathering target data
- Command and Control
  - Taking control of compromised systems
- Exfiltration
  - Transferring stolen data out of the organization
- Impact
  - Affecting system operations or compromising confidentiality, integrity, or availability (CIA)
- Applications in Threat Modeling
  - Reconnaissance
    - Identify publicly available information on systems, users, or network structure
    - Conduct OSINT to understand potential weaknesses in external-facing systems
  - Resource Development
    - Identify possible attack vectors
      - E.g., SQL injection on a database or web application
  - Initial Access & Execution
    - Identify potential entry points for malware
      - E.g., email, web applications

- Ensure proper controls to detect and block execution of unauthorized code
- Persistence & Privilege Escalation
  - Regularly review accounts with elevated privileges
  - Ensure privilege management and monitoring to limit escalation
- Defense Evasion & Credential Access
  - Deploy and monitor intrusion detection/prevention systems (IDS/IPS)
  - Use secure password policies and frequent credential audits
- Lateral Movement & Discovery
  - Ensure segmentation between critical systems to prevent lateral spread
  - Monitor traffic between systems to detect unauthorized movement
- Exfiltration & Impact
  - Monitor egress traffic for potential data exfiltration
  - Protect data integrity through strong encryption and regular access control audits
- Key Concepts for the Exam
  - Purpose
    - Understand that the MITRE ATT&CK Framework provides structured insight into attacker behaviors to improve threat modeling
  - Utility
    - Recognize that it supports proactive threat modeling and defense by cataloging past TTPs used in attacks
  - Categories

- Familiarize with each of the major categories and their role in the attack lifecycle for informed threat modeling
- **Cyber Kill Chain**
  - Overview of the Cyber Kill Chain
    - A framework developed by Lockheed Martin to identify and prevent cyber intrusion activity
    - Purpose
      - To understand and detect Advanced Persistent Threats (APTs) by breaking the attack process at any stage in the "kill chain"
    - Goal
      - Stopping attackers by identifying where they are in the chain, breaking their progress, and preventing them from reaching their objective
  - Characteristics of Advanced Persistent Threats (APTs)
    - Advanced
      - Sophisticated attackers with high-level skills and knowledge
    - Persistent
      - Repeatedly target a specific organization over a period
    - Threat
      - Potential for harm to organizational assets or personnel
    - Tactics
      - Attackers use multiple vectors, including cyber, physical, and social engineering, to reach their objectives

- Cyber Kill Chain Stages
  - Reconnaissance
    - Objective
      - Gather information about the target passively, often through Open Source Intelligence (OSINT)
    - Focus
      - Identify useful data such as email addresses, employee names, network information, and organizational structure
    - Prevention
      - Minimize exposure of sensitive information, use threat intelligence to monitor for early signs of reconnaissance
  - Weaponization
    - Objective
      - Create an exploit tailored to vulnerabilities in the target environment
    - Focus
      - Design malicious code or tools based on the gathered information
    - Prevention
      - Use threat modeling to identify and patch potential vulnerabilities before exploitation
  - Delivery
    - Objective
      - Deliver the crafted exploit to the target system
    - Common Methods

# ISC2 CISSP

## (Study Guide)

- Phishing emails, malicious websites, or infected USB drives
- Prevention
  - Employ email filtering, web content filtering, and end-user training to identify and block suspicious activities
- Exploitation
  - Objective
    - Activate the exploit to take advantage of vulnerabilities
  - Focus
    - Execute malicious code, often aiming to gain access or control
  - Prevention
    - Employ endpoint protection, application control, and vulnerability management to limit exploitation
- Installation
  - Objective
    - Install malware or backdoors on the compromised system to maintain a foothold
  - Common Tools
    - Remote access tools, rootkits, and other malware
  - Prevention
    - Use endpoint detection and response (EDR) and ensure proper permissions and control measures
- Command and Control (C2)
  - Objective

# ISC2 CISSP

## (Study Guide)

- Establish and maintain a secure communication channel between the attacker and compromised systems
- Focus
  - Allow attackers to remotely control infected systems
- Prevention
  - Network monitoring, intrusion detection systems, and blocking known C2 IP addresses or domains
- Actions on Objectives
  - Objective
    - Execute the primary goal of the attack, such as data exfiltration, destruction, or disruption
  - Examples
    - Stealing data, sabotaging systems, or deploying ransomware
  - Prevention
    - Regularly review access controls, monitor for anomalies, and employ data loss prevention (DLP) tools
- Application of Threat Intelligence and Proactive Defense
  - Threat Intelligence
    - Use threat feeds, hunting, and monitoring to identify potential threats before they progress through the kill chain
  - Proactive Monitoring
    - Determine attackers' location in the kill chain to anticipate and disrupt their next move

- Incident Response
  - Incorporate the kill chain model into the incident response to address potential points of compromise
- Key Takeaways for the Exam
  - APTs
    - Know that the cyber kill chain targets APTs, sophisticated, persistent threats using various attack vectors
  - Stages of the Kill Chain
    - Familiarize with each stage, its objective, and how it fits into the overall attack strategy
  - Defensive Strategy
    - Understand the value of proactively identifying and breaking the kill chain to prevent attackers from reaching their goals
- **Security Orchestration, Automation and Response (SOAR)**
  - Overview of SOAR
    - SOAR stands for Security Orchestration, Automation, and Response, a technology that enables automated incident response across various tools and systems
    - Purpose
      - To reduce manual workload, minimize human error, and allow faster incident responses by automating responses to common security incidents
    - Benefits
      - Reduced workload for analysts and engineers

- Quicker response times
- Enhanced accuracy in responses, leveraging artificial intelligence (AI) and machine learning (ML)
- Components of SOAR
  - Data Collection
    - Source
      - Collects security data across the organization's infrastructure, covering users, devices, applications, and network elements
    - On-Prem & Off-Prem
      - Integrates data from on-premise and off-premise (cloud or off-site) environments
    - Tool
      - Typically uses a Security Information and Event Manager (SIEM) to centralize and analyze collected data
  - Detection
    - Objective
      - Minimize false positives and focus on genuine threats
  - Methods
    - Threat Intelligence
      - Uses known indicators of compromise and threat feeds
    - Analytics & Correlation
      - Groups and interprets alerts to identify true incidents requiring action
  - Automated Response



- Execution
  - Executes playbook steps to respond to incidents and prevent escalation
- Analysis
  - Analyzes scope and identifies root cause of security threats through automated investigation
- Key Terms in SOAR
  - Playbook
    - A set of predefined actions to investigate and respond to incidents automatically
  - Purpose
    - Standardizes the response process, creating a repeatable approach to specific threats
      - E.g., phishing, malware detection
- Runbook
  - A script that calls one or more playbooks and manages their execution
  - Role
    - Functions as a master sequence or “cookbook,” executing necessary playbooks in response to a detected event
  - Example
    - A phishing alert might trigger a runbook that calls a playbook for email analysis, IP reputation checks, and user notification
- Example Workflow Using SOAR
  - Trigger Detection
    - An email phishing attempt is detected through SIEM data

- Runbook Execution
  - The runbook initiates the phishing playbook
- Playbook Actions
  - Analyzes the email sender's reputation
  - Inspects email content for malicious links
  - Flags the user account if suspicious
- Response Outcome
  - Incident handled without manual intervention
- Key Takeaways for the Exam
  - SOAR Purpose
    - Understand that SOAR is a tool for automated, efficient incident response
  - Playbook & Runbook Functions
    - Playbook
      - Contains the response steps
    - Runbook
      - Executes one or more playbooks as part of an automated response
    - Vendor Variability
      - Terminology (playbook, runbook, workbook) may vary depending on the vendor, so focus on understanding the core functions rather than specific terms

- **Behavior Analytics**

- Overview of Behavior Analytics

- Behavior Analytics involves monitoring and analyzing user and device activities to detect potential security threats

- Purpose

- Used to detect anomalous behavior that could indicate security incidents, such as unauthorized access or data exfiltration

- Common Terms

- User Behavior Analytics (UBA)
        - Focuses on individual user behavior
      - User and Entity Behavior Analytics (UEBA)
        - Includes both user and device behavior in analysis

- Network Behavior Analytics

- Analyzes network traffic for anomalies

- Behavior Analytics Process

- Baseline Behavior

- Establish a profile of typical user and system behavior, such as login patterns, application usage, and data access frequency
      - Example
        - Monitoring workstations for regular activity

- E.g., logging in, accessing applications, making API calls

- Anomaly Detection

- Identifies deviations from established norms to flag potentially suspicious activities

- Example
  - A workstation running a vulnerability scan (normally conducted by a specific vulnerability server)
- Threat Detection
  - Detects privileged account abuse, privilege escalation, data exfiltration, and stealthy or unseen attacks
  - Enables detection of abnormal behavior potentially missed by other systems like IDS, IPS, or DLP
- Key Tools for Behavior Analytics
  - SIEM Systems
    - Security Information and Event Managers (SIEM) aggregate logs from various sources and assist in detecting anomalous behavior
  - Examples
    - Elastic Stack, AlienVault, RSA
  - Behavior Analytics Platforms
    - Splunk
      - Provides advanced threat detection through machine learning, supporting multiple log types (identity, DNS, network, application)
  - Key Capabilities
    - Machine learning for identifying unknown threats
    - Anomaly detection for early threat identification
    - Aggregation of anomalies into unified threat profiles, aiding in threat investigation

- Benefits of Behavior Analytics
  - Enhanced Threat Detection
    - Detects stealth and unknown attacks that may bypass traditional security measures
  - Advanced Threat Hunting
    - Provides deep insights into system and user activities across the network, aiding in proactive threat discovery
  - Improved Response Times
    - Automates identification of abnormal patterns, accelerating the response to potential threats
- Key Exam Points
  - Purpose of Behavior Analytics
    - Focus on understanding how behavior analysis helps detect threats based on deviations from normal activity
  - Vendor Neutrality
    - Know the concept and benefits, not specific vendor tools (Splunk, Elastic Stack, RSA, etc.)
- Behavior Analytics supports real-time detection and proactive threat hunting by analyzing activity across multiple systems and comparing it against historical data to reveal anomalies indicative of potential threats

## Configuration Management

### Objectives:

- 7.3 - Perform configuration management (CM)
    - E.g., provisioning, baselining, automation
  - 7.5 - Apply resource protection
  - 7.8 - Implement and support patch and vulnerability management
  - 7.9 - Understand and participate in change management processes
  - 8.1 - Understand and integrate security in the Software Development Life Cycle (SDLC)
  - 8.2 - Identify and apply security controls in software development ecosystems
- 
- **Configuration Management Introduction**
    - Configuration Management Overview
      - Ensures systems and software are securely configured, maintained, and updated
      - Prevents misconfigurations that could lead to security vulnerabilities
      - Involves provisioning new systems securely, maintaining system integrity, and automating management processes
    - System Patch Management
      - Patch management is a critical part of CM
        - Involves identifying vulnerabilities, testing patches in controlled environments, and deploying them to production

# ISC2 CISSP

## (Study Guide)

- Ensures systems and applications are updated with the latest security fixes
- Essential for maintaining a secure environment and mitigating vulnerabilities
- Change Control
  - Structured management of updates, new software, or configuration changes
  - Ensures security is maintained during changes
  - Change management process includes requesting, reviewing, approving, and implementing changes
  - Change control prevents misconfigurations and security incidents
  - Contributing to the Change Advisory Board (CAB) or review process is a key responsibility
- Software Configuration Management
  - Applies CM principles to the software development process
  - Configuration management is integrated into each phase of the SDLC
  - Ensures security controls are applied consistently throughout software development
  - Secures the build process of systems and applications from design to deployment
- Media Management
  - Involves the protection and control of both physical and digital media
  - Includes securing hard drives, backup tapes, and cloud storage
  - Ensures proper disposal of sensitive media and tracks media assets to prevent unauthorized access

- A part of resource protection, which is crucial for safeguarding sensitive information
- **Configuration Management**
  - Purpose of Configuration Management
    - Ensures system components maintain a known configuration state
    - Prevents unauthorized changes to system components
  - Configuration Management Terms
    - Configuration
      - Specifications or settings of an asset
        - E.g., server, workstation, firewall
    - Configuration Item (CI)
      - Asset requiring configuration control
    - Configuration Management Plan (CM Plan)
      - Document outlining the processes and procedures to manage configurations
  - Configuration Management Plan Components
    - Defines purpose, scope, roles, responsibilities, processes, and procedures
    - Outlines how CIs are managed and controlled
    - Identifies configuration items that need control (not all assets are CIs)
  - NIST Special Publication 800-128 (Four Main Phases of Configuration Management)
    - Planning Phase
      - Identify configuration items (CIs) to determine the configuration management plan's scope



# ISC2 CISSP

## (Study Guide)

- Create a CM policy with processes and procedures for CIs
- Establish Change Control Board (CCB) or Change Advisory Board (CAB) for reviewing and approving configuration item changes
- Implementation Phase
  - Define secure baseline configuration for each CI
    - E.g., configurations for web servers, network devices
  - Use baseline configurations as references for consistent deployment
  - Assign unique versioning to baseline configurations to track updates and ensure accurate recovery if needed
- Provisioning and Automation
  - Ability to create, manage, or destroy configuration items
  - Provisioning
    - Adding configurations; Deprovisioning
      - Removing configurations
    - Automate provisioning with tools like Chef, Puppet, or Ansible for efficient baseline deployment in DevOps or DevSecOps
- Controlling Configurations
  - Conduct security impact assessments for proposed and recent changes
  - Update CM plan and baseline documentation to reflect changes in configuration baselines
  - Introduce impact analysis to assess changes' security impacts
- Monitoring Phase
  - Analyze compliance with approved baseline configurations
  - Use tools such as integrity monitoring (e.g., AID, Tripwire) or discovery and vulnerability scans to monitor compliance

- Identify unauthorized changes and refine CM processes over time for improved security
- Key Configuration Management Terms for Exam
  - Configuration Item (CI)
    - Baseline
      - Established settings or version of a CI for reference
  - Provisioning
    - Adding configurations
  - Deprovisioning
    - Removing configurations
- Essential Understanding for Exam
  - Purpose of configuration management and its role in preventing unauthorized changes
  - Terms and concepts in configuration management such as CIs, baselines, and provisioning
- **System Patch Management**
  - Patch Management Purpose
    - Fixes functionality problems in software or firmware
    - Addresses vulnerabilities, performance issues, or adds features
    - Ensures patches do not negatively impact operations
  - Patch Management and Vulnerability Management
    - Work together as patches often fix vulnerabilities
    - Patch management is a process for identifying and installing patches consistently

- Patch management policy should define
  - Patch identification and acquisition
  - Installation process
  - Responsible parties
- Key Patch Management Characteristics
  - Consistent
  - Timely
  - Prioritized
  - Tested
- Challenges in Patch Management
  - Installation timing and frequency
  - Testing before deployment
  - Integrating patch management with configuration or change management
  - Handling systems that cannot accept patches
- Handling Unpatchable Systems
  - Reconfigure the system
  - Remove the system
  - Apply compensating controls
    - E.g., whitelisting, encryption
- Patch Management Approaches
  - Agent-Based Patching
    - Agents installed on hosts communicate with a centralized patch server
    - Hosts pull patches from the server and install them

- Agentless Patching
  - Scans network traffic to detect patch needs
  - Limited to protocol vulnerabilities; may miss application-specific issues
- Passive Network Monitoring
  - Monitors network traffic to identify patching needs
  - Identifies protocol vulnerabilities but not specific application patches
- Decentralized Patching
  - Each host manages its patches independently
  - Lacks central control and baseline consistency
- Comparison of Patch Management Methods (NIST SP 800-43)
  - Agent-Based
    - Requires administrative privileges
    - Supports remote hosts
    - Most effective for patch management control
  - Agentless
    - Requires administrative privileges
    - Minimal bandwidth but limited visibility into deep configurations
  - Passive Network Monitoring
    - No administrative privileges required
    - Good for unmanaged hosts and appliances but limited to protocol vulnerabilities
- General Patch Management Steps
  - Evaluation

- Identify applicable patches and verify against trusted sources
- Testing
  - Test patches in a non-production environment to assess for negative impacts
- Approval
  - Obtain authorization from Change Control Board (CCB) or stakeholders
- Deployment
  - Install patches in production promptly to reduce security risks
- Verification
  - Confirm patch installation effectiveness
  - Perform security assessments and compliance audits if needed
- Essential Knowledge for Exam
  - Purpose and challenges of patch management
  - Patch management architecture (agent-based, agentless, network monitoring)
  - General steps of patch management process
- **Change Control**
  - Overview of Change Control
    - Also known as change management; terms are interchangeable
    - Process for requesting, approving, and implementing changes to secure baseline configurations
  - Purpose of Change Control
    - Ensures system components maintain an authorized configuration state

- Prevents unauthorized or insecure modifications
- Applies to all configuration items (CIs) such as computers, servers, applications, firewalls, etc.
- Change Control Process Steps
  - Request the Change
    - Document proposed change to a configuration item
    - Must include a formal request for tracking and approval purposes
  - Review the Change
    - Conducted by the Change Control Board (CCB)
    - Assesses configuration control requirements and evaluates impact on security and operations
  - Build and Test
    - Conducted in a development environment
    - Evaluates any potential security or functional impacts
    - Involves security engineers to assess risks and confirm controls
  - Approval or Rejection
    - CCB approves, modifies, or rejects change based on testing results
  - Implementation
    - Approved changes moved to production (Ops or Prod) environments
    - Release Control phase ensures smooth release without operational impact
  - Verification
    - Ensures change was implemented as intended

- Updates CI baseline and configuration management (CM) documentation
- Closeout
  - Updates documentation and baseline version to reflect changes
  - Marks the official completion of the change request
- Roles in Change Control
  - Requester
    - Initiates change request
    - Could be from management, customer, or team member
  - Change Control Board (CCB)
    - Reviews and approves or rejects changes
    - Ensures separation of duties by involving multiple stakeholders
  - Engineers/Administrators
    - Conduct build, testing, and implementation of the change
    - Collaborate with security team for security checks
- Release Control
  - Final approval and release of changes to the production environment
  - Involves Security Impact Analysis to assess any risks or vulnerabilities introduced
- Security Impact Analysis
  - Identifies potential security risks, vulnerabilities, or impacts from proposed changes
  - Includes regression testing to ensure no adverse effects on existing controls

- Assesses how changes affect security controls and overall security posture
- Proactive safeguards and reactive countermeasures are planned to mitigate risks
- Key Terms
  - Change Request (CR)
    - Formal proposal to modify a configuration item
  - Configuration Item (CI)
    - Asset under configuration control
  - Change Control Board (CCB)
    - Group responsible for approving or rejecting changes
  - Release Control
    - Final approval process before deployment to production
- **Software Configuration Management**
  - Overview of Software Configuration Management
    - Ensures software maintains a known, consistent configuration
    - Crucial for large environments, enterprise-level systems, and complex setups
    - Involves managing system and software assets, known as configuration items (CIs), through configuration control
  - Key Terms in Software CM
    - Configuration Items (CIs)
      - System or software assets requiring configuration management
      - Example



- Operating systems, network operating systems, hypervisors, etc.
- Baselines
  - Pre-configured CIs that set a consistent standard
  - Used to ensure consistent configurations across similar systems
- Version
  - Unique identifier for a baseline configuration
  - Example
    - Baseline changes from version 1.1.2 to 1.1.3 or 2.0 upon updates
- Change Sets
  - Collective changes applied to a baseline as part of a change request
- Branches
  - Configurations under development alongside a baseline
  - Created by checking out a baseline configuration for modification; checked back in as the updated baseline after approval
- Software CM and DevOps/DevSecOps
  - Used to manage Infrastructure as Code (IaC) and Security as Code (SaC)
  - Baselines and versions allow consistent, secure configurations across deployments
- Change Management Process in Software CM
  - Process for making authorized modifications to the baseline configuration
  - Phases
    - Request Control

# ISC2 CISSP

## (Study Guide)

- Formal process to propose and document changes
  - Procedures outline how change requests are made and managed
- Change Control
  - Procedures to evaluate and approve the change
  - Includes identifying changes, assessing impact, and managing branches and change sets
- Release Control
  - Procedures for deploying the change into production (Ops or Prod)
  - Ensures controlled rollout with minimal disruption
- Detailed Change Control Process Steps
  - Request the Change
    - Submit formal change request with documentation
  - Review by Change Control Board (CCB)
    - Evaluate proposed changes and their impacts
  - Build and Test
    - Develop and test changes in a controlled environment to identify impacts
  - Approval or Rejection by CCB
    - Approve or reject based on testing results and impact analysis
  - Implementation
    - Roll out the approved change to production without impacting operations
  - Verification

# ISC2 CISSP

## (Study Guide)

- Confirm change was successful and free of adverse impacts
  - Close Out and Document
    - Finalize change, update baseline, and document new configuration
  - Importance of Traceability and Accountability
    - Ensures governance, auditability, and accountability at each step
    - Multiple personnel involved in each phase to maintain control and oversight
    - Ability to quickly reference documentation or revert to previous baselines if issues arise
- **Media Management**
  - Media
    - Refers to any medium capable of storing data
    - Examples include hard drives, solid-state drives, backup tapes, CDs, DVDs, mobile devices, thumb drives, and more
  - Primary Focus in Media Management
    - Protection of the confidentiality, integrity, and availability (CIA) of data stored on media
    - Ensures that media is tracked and managed effectively to prevent unauthorized access and maintain data availability
  - Media Lifecycle and Mean Time to Failure
    - All media has a finite life cycle and a mean time to failure (MTTF), impacting data availability

- Important to replace media as it ages to prevent loss of availability and slowdowns
- Importance of Marking and Labeling Assets
  - Physical Marking
    - Label media with a physical indicator (e.g., sticker) showing the data sensitivity or classification (e.g., secret, confidential)
  - Example
    - If a hard drive is labeled "secret," it signals that specific precautions are necessary for its handling and disposal
  - Digital Labeling
    - Assign labels in metadata or use digital markings to categorize data sensitivity or classification digitally
    - Ensures proper handling of both physical and digital media throughout its lifecycle
- Handling and Security of Removable Media
  - Apply physical security measures, such as labeling, encryption, and proper storage in secure locations
    - E.g., safes or vaults
  - For media transported outside the facility, ensure proper security controls are implemented during transit
- Sanitization and Data Remnants
  - Properly sanitize media to remove all data remnants before reusing or disposing of it
  - Prevents sensitive data from being accessible to unauthorized users, especially if the media will be used at a lower classification level

- Continuous Monitoring of Media
  - Track the mean time to failure and monitor assets to replace aging or failing media before they impact availability
  - Necessary for RAID systems and other configurations where media failure can result in a single point of failure, affecting data availability and system functionality

## Incident Management

### Objectives:

- 1.5 - Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, industry standards)
- 7.1 - Understand and comply with investigations
- 7.6 - Conduct incident management
- **Incident Management Introduction**
  - Incident Management
    - Incident management plays a critical role in maintaining organizational resilience and ensuring compliance with regulatory and industry standards
    - How an organization manages incidents can influence the outcome between a swift recovery and catastrophic failure
    - Incident management covers the full lifecycle from identification, containment, eradication, recovery, and lessons learned
    - Proactive preparation is essential to minimize harm to the organization and its stakeholders during incident response
  - Security Investigations
    - Conducting an investigation after a security incident determines the cause, scope, and impact of the incident
    - Investigations include processes such as initial reporting, evidence collection, and collaboration with legal teams or law enforcement

- Best practices include maintaining a chain of custody and documenting findings effectively
- Different investigation types require understanding of legal thresholds and potential outcomes
- Evidence Collection and Handling
  - Evidence collection and handling are critical tasks during an investigation to avoid contamination
  - Chain of custody must be maintained to ensure the integrity of the evidence
  - Evidence needs to be preserved and prepared for potential legal proceedings
- Digital Forensics
  - Digital forensics involves extracting, analyzing, and interpreting data from digital devices
  - Plays a pivotal role in investigations of cyber incidents
  - Understanding digital forensics is crucial for information security and the CISSP exam
  - Key methods include data recovery, file analysis, and understanding metadata
- Digital Forensic Incident Response
  - Integrates digital forensics into the incident response process
  - Ensures that digital evidence is preserved during an active incident response
  - Works with law enforcement or internal legal teams to prepare cases for further legal action

- Focuses on maintaining the integrity of the evidence while responding to an incident

- **Incident Management**

- Purpose of Incident Management
  - Manages events violating security policy, whether intentional or inadvertent
  - Detects, responds to, and recovers from incidents based on their impact on systems
- Key Guides for Incident Management
  - NIST SP 800-61 Rev 2
    - Computer Security Incident Handling Guide
  - ISO/IEC 27035
    - Information Security Incident Management standard
- Incident Management Steps (CBK)
  - Detection
  - Response
  - Mitigation
  - Reporting
  - Recovery
  - Remediation
  - Lessons Learned
- Incident Management Steps (NIST Mapping)
  - Preparation



# ISC2 CISSP

## (Study Guide)

- Establishes incident response policy, defines incidents, and sets priorities
- Outlines key performance/risk indicators, reporting requirements, tools, and resources
- Forms Incident Response Team (IRT), roles, responsibilities, and contacts
- Deploys necessary tools
  - E.g., IDS, DLP software, firewall rules
- Detection and Analysis
  - Uses system logs, IDS/IPS, endpoint security, and personnel reports
  - Triage
    - Analyzes events to confirm if they're security incidents based on criticality and severity
    - Documents findings and correlates data (timestamps, IPs, port numbers)
  - Response
    - Actions vary based on incident severity
    - Activates the IRT as needed, identifies, collects, and handles evidence with documentation
  - Mitigation
    - Contains the incident to limit damage and impact
    - Identifies threat sources (e.g., IP, port) and blocks them to prevent further attacks
    - Prevents further spread or impact by isolating compromised systems or restricting access

# ISC2 CISSP

## (Study Guide)

- Reporting
  - Generates detailed reports on the incident, including findings, actions, and recovery status
  - Internal reports
    - Provide senior management with situational awareness
  - External reports
    - Meet regulatory requirements without disclosing confidential details
  - GDPR requires reporting personal data breaches within 72 hours
- Recovery
  - Restores systems temporarily to operational state to prevent business impacts
  - Activates BCP/DRP if recovery cannot meet the maximum tolerable downtime
  - May involve temporarily enabling critical system components, accounts, or connections
- Remediation
  - Restores systems to full operational status post-incident
  - Repairs system damage, addresses legal impacts, and assesses financial costs
- Lessons Learned
  - Analyzes incident handling, identifies gaps, and enhances response plans
  - Evaluates threat causes, preventive actions, and stakeholder improvements
  - Implements and monitors changes for effectiveness in incident response

- Bottom Line
  - Know each incident management step, its purpose, and what happens in each
- **Security Investigations**
  - Purpose of Investigations
    - Collects and analyzes facts related to an event to determine its occurrence or non-occurrence
    - Supports legal and organizational compliance by verifying event outcomes and identifying violations
  - Roles in Investigations
    - Primarily a support role for security professionals unless trained in forensics
    - Responsibilities may include evidence collection, protection, chain of custody maintenance, and possible court testimony
  - Burden of Proof
    - Criminal Proceedings
      - Prove beyond a reasonable doubt to a jury (12 reasonable peers) that the crime occurred
    - Civil Proceedings
      - Prove by the preponderance of evidence (more likely than not) that a civil offense took place
    - Plaintiff (criminal) or Claimant (civil)
      - Accuses or blames the Defendant (criminal) or Respondent (civil)

- Evidence Collection Techniques
  - Interviewing
    - Gathers information from personnel
      - E.g., administrators, engineers
  - Interrogation
    - A specific type of interview typically conducted by law enforcement; involves focused questions on a subject's involvement in a violation
  - Surveillance
    - Monitors the subject via logs, CCTV, or other means to gather additional evidence if initial information is insufficient
  - Digital Forensics
    - Identifies, collects, analyzes, and preserves electronic data to support the investigation
- Types of Investigations
  - Administrative Investigation
    - Examines internal policy violations
  - Regulatory Investigation
    - Ensures compliance with legal or regulatory requirements (also called compliance investigation)
  - Criminal Investigation
    - Examines potential violations of law
  - Civil Investigation
    - Addresses private, non-criminal matters such as contract violations or service agreements

- Modus Operandi (MO) Analysis
  - Motive
    - Identifies who committed the offense and their reason for doing so
  - Opportunity
    - Determines if the subject was present and capable at the time of the offense
  - Means
    - Assesses if the subject had the knowledge, tools, and techniques necessary to commit the offense
- Bottom Line
  - Understand burden of proof and the roles of the plaintiff, defendant, claimant, and respondent
  - Recognize types of investigations and their purposes
  - Be familiar with modus operandi and how it supports narrowing down suspects based on motive, opportunity, and means
- **Cyber Related Investigations**
  - Purpose of Cyber-Related Investigations
    - Systematic examination of security violations to determine if they are criminal, civil, administrative, or regulatory
    - Involves evidence collection, preservation, and determination of the violation's type
  - Key Investigation Parties
    - Plaintiff

- Initiates legal action based on an accusation
- Defendant
  - Disputes the accusation made by the plaintiff
- Burden of Proof Standards
  - Criminal Cases
    - Proof must be beyond a reasonable doubt (convincing a reasonable person of the defendant's guilt)
  - Civil Cases
    - Proof requires a preponderance of evidence (proving fault or liability over reasonable doubt)
- Investigation Process
  - Incident Response Initiates Investigation
    - Begins with determining what happened and collecting evidence
    - Determines whether the event is administrative, criminal, or another violation type
- Types of Cyber Investigations
  - Administrative
    - Internal investigation of policy violations
      - E.g., acceptable use policy
    - Criminal
      - Involves law enforcement for potential crimes
        - E.g., data theft, security breaches
      - Jurisdiction often falls under federal law
        - E.g., FBI for U.S. computer crimes
  - Civil

# ISC2 CISSP

## (Study Guide)

- Addresses private matters
  - E.g., business contract violations, SLA breaches
- Regulatory
  - Ensures compliance with industry regulations, can become civil or criminal matters
- Security Professional Responsibilities
  - Evidence Collection
    - Identify, collect, and protect evidence, maintaining chain of custody to prevent tampering
  - Plaintiff Role
    - Collect and preserve evidence to defend the organization's innocence
  - Defendant Role
    - Collect and preserve evidence to support the organization's claims against an alleged violator
      - E.g., insider threat
- Bottom Line for Cyber Investigations
  - Understand burden of proof (reasonable doubt for criminal, preponderance of evidence for civil)
  - Recognize types of investigations (administrative, criminal, civil, regulatory)
  - Know security responsibilities when acting as plaintiff or defendant

- **Evidence Collection and Handling**

- Purpose of Evidence in Incident Management
  - Establishes facts to prove or disprove an incident's occurrence
  - Must be relevant to the incident to be admissible in court
- Types of Evidence
  - Real Evidence
    - Tangible objects
      - E.g., fingerprints, video recordings
  - Documentary Evidence
    - Written records
      - E.g., logs, entry records
    - Must be authenticated as true and accurate
  - Testimonial Evidence
    - Verbal or written witness statements about what was seen or experienced
  - Demonstrative Evidence
    - Illustrates or corroborates testimony (also called corroborating evidence)
- Key Evidence Rules
  - Best Evidence Rule
    - Use original documents whenever possible
    - Copies are secondary evidence and often inadmissible due to authenticity concerns
  - Parol Evidence Rule



- Requires that any verbal agreements about evidence be documented in writing
- Types of Testimonial Evidence
  - Direct Evidence
    - Witness testimony of direct observation
  - Hearsay Evidence
    - Information relayed from another person who did not witness the event firsthand
  - Opinion Evidence
    - Statements from subject matter experts offering professional opinions on evidence
- Additional Evidence Types
  - Circumstantial Evidence
    - Facts that, when combined, suggest an incident occurred
  - Corroborative Evidence
    - Supports or verifies other evidence
      - E.g., video footage alongside access logs
- Chain of Custody
  - Ensures evidence is properly handled, marked, and tracked to maintain integrity
  - Documentation should include
    - What was transferred
      - E.g., logs, devices
    - To whom it was transferred
    - Date, time, and method of transfer

- Signatures from both parties for each handoff
  - Essential for proving that evidence remained untampered from collection to presentation in court
- Example of Evidence Handling
  - Real Evidence
    - Physical object
      - E.g., thumb drive
  - Documentary Evidence
    - Logs showing system access
  - Testimonial Evidence
    - Witness statements from employees and system administrators
  - Circumstantial Evidence
    - Presence of subject in restricted area (access logs and video footage)
  - Corroborative Evidence
    - Combined statements and logs to confirm incident details
- Bottom Line
  - Understand types of evidence and their purposes in investigations
  - Recognize the importance of the Best Evidence Rule and Chain of Custody in handling and preserving evidence
- **Digital Forensics**
  - Digital Forensics Overview
    - Collection and analysis of digital evidence from computers and electronic devices

# ISC2 CISSP

## (Study Guide)

- Similar to criminal forensics but focuses on digital investigations
- Also referred to as eDiscovery or electronic data discovery
- Purpose of Digital Forensics
  - Identify who, what, when, where, and how of electronic violations
  - Used in investigations, security assessments, and regulatory compliance
- eDiscovery Reference Model
  - Information Governance
    - Ensures organized information for eDiscovery tasks
    - Involves policies, processes, and compliance with regulations
  - Identification
    - Locate potential sources of evidence
  - Preserve
    - Protect information from alteration, deletion, or changes
    - Ensures data integrity
  - Collect
    - Gather necessary information for the forensic process
  - Process
    - Screen and process collected information for relevance
    - Analyze data to ensure it meets evidence guidelines
  - Review
    - Evaluate the information for relevance to the investigation
  - Analyze
    - Determine the significance and implications of the data
  - Produce

- Format information for consumption by investigators, security managers, or court
- Presentation
  - Use of information in a court of law or by investigative parties
- Forensic Standards
  - NIST Special Publications
    - SP 800-86
      - Integrating forensic techniques into incident response
    - SP 800-101
      - Mobile device forensics
  - ISO Standards
    - ISO 27043
      - Incident investigation principles and processes
    - ISO 27037
      - Guidelines for identification, collection, acquisition, and preservation of digital evidence
  - Other Organizations
    - International Organization on Computer Evidence (IOCE)
    - Scientific Working Group on Digital Evidence (SWGDE or SWEDGE)
- Forensic Process in Incident Response
  - Must be documented in the incident response plan
  - Involves the stages of collection, examination, analysis, and reporting
- Key Points
  - Understand the purpose and process of digital forensics
  - Familiarize yourself with the eDiscovery reference model steps

- Know the relevant forensic standards and their applications in incident response
- **Digital Forensic Incident Response**
  - Purpose of Digital Forensics
    - Collects and analyzes digital evidence to prove or disprove a security incident
    - Follows the NIST Special Publication 800-86 guidelines for forensic processes
  - Phases of the Digital Forensic Process
    - Collection
      - Identifies all data sources relevant for forensic analysis
      - Defines collection priorities and sources, including storage devices, remote storage, personnel statements
      - Requires written authorization from senior management or through incident response plans
      - Focuses on creating exact copies to avoid evidence tampering
      - Collects all possible evidence, including system logs, system files, hardware, applications, and media
    - Examination
      - Reviews and processes collected data to determine relevance
      - Identifies best evidence and real evidence for admissibility in court
      - Uses forensic tools like NCASE, Forensic Toolkit, Macquisition, and Sleuth Kit for data processing

- Analysis
  - Formulates an investigative conclusion based on examined evidence
  - Establishes an audit trail of events, devices, and persons involved
  - Ensures conclusions are supported by evidence beyond a reasonable doubt or preponderance of evidence
- Reporting
  - Documents forensic data to explain conclusions
  - Focuses on accuracy and authenticity in reporting to prove conclusions in court
  - Presents findings with admissible evidence and clear explanations
- Considerations for Forensic Investigations
  - Investigators should be competent and aware of potential data sources
  - Uses a consistent policy, process, and procedure for investigations
  - Individuals handling digital evidence are responsible for compliance with policies
  - Chain of custody is critical for evidence handling, logging, and transferring
- Key Points for Exam
  - Know each phase of the digital forensic process
  - Recognize the importance of chain of custody and admissible evidence
  - Understand the role of investigators and tools in forensic analysis

## Business Continuity and Disaster Recovery

### Objectives:

- 1.7 - Identify, analyze, assess, prioritize, and implement Business Continuity (BC) requirements
- 7.10 - Implement recovery strategies
- 7.11 - Implement disaster recovery (DR) processes
- 7.12 - Test disaster recovery plans (DRP)
- 7.13 - Participate in Business Continuity (BC) planning and exercises
- **Business Continuity and Disaster Recovery**
  - Business Continuity Planning (BCP)
    - BCP ensures that organizations can continue operating during and after a disruption
    - Involves identifying critical business functions and the resources needed to support them, especially during a crisis
    - Regular updates and participation in Business Continuity exercises are necessary to maintain relevance
  - Business Impact Analysis (BIA)
    - BIA identifies the most critical parts of the business and assesses how disruptions will impact them
    - Helps calculate potential financial, operational, and reputational costs of downtime
    - Defines recovery time objectives (RTOs) and recovery point objectives (RPOs)

- Disaster Recovery Planning (DRP)
  - DRP is focused on restoring IT infrastructure after a disaster
  - Key components include defining recovery objectives and establishing roles and responsibilities
  - Helps create a plan that minimizes downtime and data loss
- Disaster Recovery Strategies
  - Short-term and long-term recovery techniques are discussed
  - Focuses on establishing alternate processing sites and the methods to recover from different types of disasters
- Disaster Recovery Sites
  - Types of recovery sites
    - Hot sites, warm sites, and cold sites
  - Advantages and disadvantages of each site are discussed based on cost, recovery time, and critical business functions
- Data Backup Strategies
  - Different backup types
    - Full, incremental, and differential
  - Best practices for storing backups, ensuring data integrity, and minimizing data loss
- Disaster Recovery Processes
  - Specific steps organizations need to follow during and after a disaster
  - Focus on recovery coordination, communication protocols, and following established procedures for orderly restoration of services
- Disaster Recovery Testing
  - Essential to test DR plans to ensure they work as intended



- Types of tests
  - Tabletop exercises, simulation tests, and more
- **Business Continuity Planning**
  - Continuity Planning
    - Minimizes operational impacts of a disruption or disaster
    - Involves proactive preparation for major disruptions
    - Demonstrates due care and due diligence in BCP updates
    - Involves people, time, effort, processes, functions, and components
    - Also known as Continuity of Operations (COOP) or Contingency Planning
  - Goal of Continuity Planning
    - Prioritizes data from Business Impact Analysis (BIA)
    - Uses BIA results and strategy to protect critical assets
    - Focuses on responding to risks and ensuring people are the top priority
  - Resources in Continuity Planning
    - Defines supporting resources and assets for operations during disruptions
    - Includes personnel, alternate processing sites, and communications plans
    - Communicates with media, law enforcement, and internally as needed
  - Training and Education
    - Business continuity team members trained on tasks and roles
    - Organization personnel informed of BCP's creation or existence
    - New hires read and understand BCP as part of onboarding
    - Cross-training for continuity personnel in case of turnover or other issues
  - Approval Process
    - Project scope defined, BIA complete, continuity planning identified

- Senior Management Approval required for BCP implementation
- Senior Management support necessary for BCP effectiveness
- Implementation and Testing
  - Begins once senior management approves
  - Tests BCP elements during implementation to ensure effectiveness
  - BCP kept up to date with new configurations, updates, or risks
  - Tests include checking coverage gaps, performance indicators, and team effectiveness
- Evaluation and Exercises
  - Evaluate team members to ensure appropriate roles and responsibilities
  - Run exercises to test response and plan effectiveness
  - Exercises ensure readiness in real disruptions
- Key Points
  - People come first in continuity planning and disaster scenarios
  - Senior Management approval drives BCP success
- **Business Impact Analysis**
  - Business Impact Analysis (BIA)
    - Assesses impacts of disruptions or disasters on critical business functions
    - Identifies critical processes, assets, and resources for business continuity
    - Determines organization's resilience and required contingency planning
    - Also known as Business Impact Assessment (BIA)
  - Focus of BIA
    - Identifying Critical Business Functions (CBF) required for business operations and compliance

- Compliance is equally important for sectors like medical, financial, and government
- Examples of CBFs
  - Identification and authentication, web services, cloud services
- Purpose of BIA
  - Establishes business resiliency and contingency strategies
  - Determines support system criticality to the business or mission
  - Evaluates potential impacts of disruption or disaster
- Risk Assessment
  - Assesses probability and impact of threat events to assets
  - Qualitative Assessment
    - Uses ranking or categories for threat probability
  - Quantitative Assessment
    - Uses monetary values for potential asset losses
- Measures of Impact
  - Maximum Tolerable Downtime (MTD)
    - Maximum time critical asset/process can be down before impacting business
  - Recovery Time Objective (RTO)
    - Planned time to restore critical asset/process
  - Recovery Point Objective (RPO)
    - Point in time to recover and restore operations, determined by backup availability
- Example of Measures of Impact
  - Authentication Server Example

- MTD
  - 60 minutes (1 hour of downtime before business is impacted)
- RTO
  - 30 minutes (time to fully restore authentication server)
- RPO
  - Time of last backup used to restore, representing maximum data loss allowed
- Useful Reference
  - NIST SP 800-34
    - Contingency Planning Guide for Federal Information Systems
- Key BIA Steps
  - Identify critical business processes and stakeholders
  - Evaluate potential impacts (risks) and determine tolerance levels
  - Document MTD, RTO, and RPO for each critical process and asset
- Key Takeaways
  - Understand BIA's purpose
  - Identify critical business functions
  - Know the measures of impact
- **Disaster Recovery Planning**
  - Disaster
    - Event causing significant damage or destruction to property, facilities, or personnel
    - Two main types

- Natural disasters and man-made disasters
- Types of Disasters
  - Natural Disasters
    - Result of planetary occurrences, such as
      - Earthquakes
        - Tectonic plate movement causing ground tremors
      - Floods
        - Water overflows onto dry land due to storms, hurricanes, etc.
      - Hurricanes, tornadoes, and lightning storms
      - Wildfires and volcanic eruptions (less common but relevant in certain areas)
      - Man-Made Disasters - Result of human actions, such as
        - Fires
        - Terrorist attacks
        - Sabotage
        - Cyber attacks
  - Non-Disaster
    - Device malfunction or failure requiring recovery without significant damage
- Natural Disaster Considerations
  - Facility location determines disaster risk
  - Earthquake Zones
    - Example - high-risk areas in the U.S. West Coast

- Flood Zones
  - FEMA Flood Zone Designation defines flood risk
    - 100-Year Floodplain
      - 1% chance of flood occurring in a year
    - 500-Year Floodplain
      - 0.2% chance of flood occurring in a year
    - Flood Map Example
      - High flood risk in red areas; Central Texas typically low-risk
- Man-Made Disaster Considerations
  - Crime rates and local police reports help assess facility safety
  - Includes risks such as sabotage, terrorism, and utility attacks
    - E.g., power or water supply
- Business Continuity vs. Disaster Recovery
  - Business Continuity (BC)
    - Focus on operational processes and critical business functions
  - Disaster Recovery (DR)
    - Focus on maintaining IT assets that support business operations
    - Ensures application servers, web servers, database servers, and networks remain functional
- Key Takeaway
  - Know the impacts of natural and man-made disasters on your organization
  - Distinguish between business continuity (operations focus) and disaster recovery (technology focus)

- **Disaster Recovery Strategies**

- Disaster
  - Event causing severe damage, destruction, or loss of life
  - Impacts organizational facility, resources, or personnel
- Disaster Recovery vs. Business Continuity
  - Business Continuity
    - Focus on critical business functions
  - Disaster Recovery
    - Focus on assets supporting business functions
- Recovery Strategies
  - System Resilience
    - System's ability to recover from disruption, minimizes single points of failure
  - Fault Tolerance
    - System continues to operate during a failure
  - High Availability
    - System continues to operate without interruption over extended periods
  - Redundant Systems
    - Multiple systems, servers, applications ensure continuity
- Data Protection Methods
  - RAID (Redundant Array of Independent Disks)
    - RAID 0 (Striping)
      - Data divided across multiple disks, no fault tolerance

- RAID 1 (Mirroring)
  - Identical data on two disks, high resilience and security
- RAID 5 (Striping with Parity)
  - Requires three or more disks, data can be restored using parity information
- RAID 10 (Stripe of Mirrors)
  - Combines striping and mirroring, uses four or more disks
- Server Protection
  - Failover Cluster
    - Two or more servers/nodes connected to maintain availability during a failure
  - Load Balancing
    - Distributes network traffic among multiple servers to increase response times and system resilience
- Power Protection
  - UPS (Uninterruptible Power Supply)
    - Short-term battery backup, provides power briefly during an outage
  - Generators
    - Motor-driven machines for long-term power backup, require fuel supply and maintenance
  - Additional Options
    - Voltage Regulators
      - Maintain consistent voltage levels
    - Line Conditioners



- Improve electricity quality
  - Surge Protectors
    - Protect devices from power surges
- Network Communications
  - Quality of Service (QoS)
    - Prioritizes critical business function traffic on limited networks, shapes traffic by
      - Throughput/Bandwidth
        - Volume of data sent
      - Latency
        - Delay in network response
      - Jitter
        - Variance in latency
      - Error Management
        - Reduces transmission errors
- Device Failure and Security
  - Fail Secure
    - System defaults to no access during a failure (recommended for security)
  - Fail Open
    - System defaults to open access during a failure (not recommended, increases security risks)
  - Application to Devices
    - Ensure firewalls, switches, and load balancers fail secure to avoid exploitation

- Key Takeaways
  - Know RAID levels for storage resilience
  - Understand system resilience options (fault tolerance, high availability)
  - Be familiar with power and network protection methods (UPS, generators, QoS)
  - Recognize the importance of fail-secure configuration
- **Disaster Recovery Sites**
  - Recovery Site Purpose
    - Alternate location to temporarily resume business operations during disaster or disruption
    - Used for short-term recovery, typically lasting days
  - Site Selection Factors
    - Based on business impact analysis results
    - Considers maximum tolerable downtime, recovery time objectives, and budget
  - Types of Recovery Sites
    - Cold Site
      - No computing equipment, minimal infrastructure
      - Least expensive, minimal maintenance
      - Long recovery time, takes days or weeks to set up fully
    - Warm Site
      - Pre-configured computing equipment, basic infrastructure
      - Moderate cost

- Requires transportation of data from primary site, takes around 12 hours to activate
- Hot Site
  - Fully equipped with computing equipment, near real-time data
  - Includes all system components, networks, and data
  - Most expensive, ready within minutes to a few hours
- Additional Recovery Site Options
  - Mobile Site
    - Self-contained site in a mobile container or trailer
    - Typically configured as a warm site
  - Can be towed to a location as needed
  - Cloud Managed Recovery Site
    - Hosted in cloud platforms
      - E.g., AWS, Azure
    - Typically warm or hot in configuration
    - Requires well-defined Service Level Agreement (SLA) for service levels, performance, and cost
  - Shared Site
    - Site shared with one or more external organizations
    - Includes a Mutual Assistance Agreement (MAA) or Reciprocal Agreement defining responsibilities, services
    - Rare due to data sensitivity and legal concerns
  - Site Geographical Location
    - Sites should be geographically separated from the primary location to avoid concurrent disasters

- Example
  - An organization in Silicon Valley may choose a recovery site in Seattle or Denver for regional separation
- Key Points
  - Understand the characteristics of each site type (cold, warm, hot) and other options (mobile, cloud, shared)
  - Recognize the importance of geographical separation for recovery sites
- **Data Backup Strategies**
  - Data Backup Purpose
    - Duplicates data for retrieval in case of host failure, system recovery, or restoration
  - Key Concepts
    - Mirroring
      - Creates an identical data copy on two or more storage media
    - Archive Bit (Backup Bit)
      - Indicates if a file needs backup
      - 0 = File backed up
      - 1 = File changed since last backup
  - Backup Types
    - Full Backup
      - Complete copy of all system data
      - Sets all archive bits to 0 upon completion
      - Typically done during low system usage times

- E.g., Sunday
- Differential Backup
  - Backs up changes since the last full backup
  - Does not reset the archive bit
- Incremental Backup
  - Backs up changes since the last full or incremental backup
  - Only changes with the archive bit set to 1 are backed up
- Backup Strategy Example
  - Full Backup on Sunday
  - Incremental Backups on Monday, Tuesday, Thursday, Saturday
  - Differential Backup on Wednesday and Friday
  - New full backup cycle starts on the following Sunday
- 3-2-1 Backup Rule
  - 3 copies of data
  - 2 copies stored on different storage media (on-premise)
  - 1 copy stored off-premise
- Electronic Vaulting
  - Remote Journaling
    - Sends logs and metadata off-premise for audit and recovery
  - Remote Mirroring
    - Streams real-time data changes to off-premise location
- Backup Storage Media Options
  - Can include tapes, disks, external drives, etc.
- Snapshot Backups

- Virtual copies of files, directories, or volumes
- Common in virtualized environments using hypervisors
- Escrow Arrangements
  - Key Escrow
    - Third-party holds cryptographic keys and certificates for recovery
  - Software Escrow
    - Stores copies of software licenses, source code, and related documentation for operational continuity
- Backup Rotation Strategies
  - First In, First Out (FIFO)
  - Grandfather-Father-Son (GFS)
  - Tower of Hanoi
  - Important to ensure compliance with data retention regulations
- Key Points
  - Understand the types of backups (full, differential, incremental) and when each is used
  - Know the 3-2-1 backup rule and purpose of off-premise storage
  - Recognize the purpose of electronic vaulting, escrow arrangements, and rotation strategies
- **Disaster Recovery Processes**
  - Disaster Recovery Purpose
    - Ensures that critical business assets and processes remain operational
    - Applies to both on-premise and off-premise (cloud-based) assets
  - Focus of Disaster Recovery Plan (DRP)

- Steps for recovering the technology infrastructure supporting critical business functions
- Includes servers, workstations, websites, databases, etc.
- NIST SP 800-34
  - Primary reference for DRP guidelines
    - Contingency Planning Guide for Federal Information Systems
- Recovery Process Priorities
  - Top Priority
    - Safety and security of human life
  - Secondary
    - Technology and asset recovery following human safety
- DRP Documentation and Communication
  - Designate a scribe or spokesperson to document and communicate all recovery steps
  - Centralize communication through one point of contact for clear, consistent messaging
- Training and Awareness Process
  - Ensure team members understand DRP procedures, their roles, and responsibilities
  - Training includes first aid, fire suppression, crisis management, and collaboration with emergency services
- Response Process
  - Procedures define recovery steps based on disaster type (natural or man-made)

- Business Continuity Plan (BCP) activated if DRP cannot restore infrastructure within tolerance levels
- Personnel Processes
  - Personnel roles, responsibilities, and response times must be clear
  - Assign primary and backup personnel for each role in DRP to ensure coverage
- Communication Processes
  - Centralize communication to keep personnel informed of DRP activation, updates, and instructions
  - Communicate with external entities (emergency services, law enforcement, media) as needed
  - Include a contact list for personnel and external contacts in the DRP
- Assessment Processes
  - Assess the disaster's extent and impact on tolerance levels, business operations, contracts, and reputation
  - Determine if human life is at risk and prioritize impacts for recovery triage
- Restoration Process
  - Recovery
    - Bringing critical operations back to normal
  - Restoration
    - returning operations to their original state at the primary site
    - Focus on least critical functions first to ensure continuous operation of critical functions during restoration



- Key Points
  - Know the difference between Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)
  - Human life is the top priority in all DRP processes
  - Understand each recovery process's purpose, including documentation, communication, and personnel processes
- **Disaster Recovery Testing**
  - Disaster Recovery Overview
    - Ensures critical business assets and processes remain operational during disruptions or disasters
    - Business continuity focuses on critical business functions; disaster recovery focuses on technology assets
  - Key Document for Testing
    - NIST Special Publications 800-84
      - Guide to test, training, and exercise programs for IT plans and capabilities
  - Types of Disaster Recovery Tests
    - Tabletop Exercises
      - Read-through Test (Checklist Test)
      - First test in DRP testing
      - DR team reviews the DRP for roles, responsibilities, and processes
      - Team members update (redline) the plan based on expertise or corrections
    - Walkthrough Test (Structured Meeting)

# ISC2 CISSP

## (Study Guide)

- Personnel gather to rehearse DRP procedures, often called a tabletop exercise
- Scenarios discussed
  - Fires, floods, cyberattacks, etc.
- Helps to coordinate responses and discuss sequence of actions
- Simulation Test (Preparedness Test)
  - Physically simulates disaster scenarios under realistic conditions on-premise
  - Includes drills (e.g., fire alarms, evacuation) but does not involve relocation
  - Purpose
    - Evaluate readiness without affecting regular operations
- Parallel Test
  - Activates recovery site using DRP while primary site maintains regular operations
  - Provides live DRP practice without impacting primary site
  - Involves external services if needed, and tests service level agreements (SLAs)
- Full Interruption Test
  - Simulates disaster by migrating primary operations to the recovery site
  - Performed only after successful completion of other tests
  - Requires senior management authorization due to potential production impact

# ISC2 CISSP

## (Study Guide)

- Typically conducted during off-hours to minimize operational impact
- Post-Test Adjustments
  - Update the Business Continuity Plan (BCP) and DRP as needed
  - Apply changes through configuration management (CM) processes
  - Continuous monitoring triggers reviews of BCP/DRP for personnel changes, process changes, regulatory updates, and risk or threat changes
- Key Points
  - Know the purpose and scope of each disaster recovery test type
  - Understand that only the full interruption test should impact production

## Software Development Security

### Objectives:

- 8.1 - Understand and integrate security in the Software Development Life Cycle (SDLC)
- 8.2 - Identify and apply security controls in software development ecosystems
- **Software Development Security**
  - Software Development Lifecycle (SDLC)
    - SDLC involves planning, requirements gathering, development, testing, deployment, and maintenance
    - Security must be integrated from the start, rather than being added later
    - Security in each phase ensures protection against data breaches, compliance failures, and vulnerabilities
  - Software Development Methodologies
    - Approaches like Waterfall, Spiral, and Agile have different strengths and weaknesses regarding security integration
    - Waterfall
      - Sequential development, security can be planned upfront
    - Spiral
      - Iterative model, security is reviewed at each iteration
    - Agile
      - Emphasizes flexibility and speed, but security can become challenging due to frequent changes
  - Agile Development
    - Agile provides flexibility but poses unique security challenges

- Security teams must collaborate with developers to ensure security isn't compromised during rapid iteration and frequent updates
- DevOps and DevSecOps
  - DevOps integrates development and operations, with continuous development and deployment
  - DevSecOps incorporates security controls into the DevOps pipeline
  - Automated security testing and continuous monitoring are crucial in DevSecOps environments
- Software Maturity Models
  - Assess the effectiveness of an organization's software development process
  - Maturity models evaluate how well security is integrated into software development practices
- Software Operations and Maintenance (O&M)
  - O&M focuses on patching vulnerabilities, monitoring threats, and maintaining security standards over time
  - Ensures software remains secure throughout its operational life cycle
- Integrated Product Teams (IPTs)
  - Cross-functional teams including developers, security experts, and project managers
  - IPTs ensure security is integrated from multiple perspectives throughout the project
- Code Repositories (Code Repos)
  - Code repositories manage code versions, track changes, and enable collaboration

- Security measures for code repos include access control, audit logging, and threat monitoring
- **Software Development Lifecycle**
  - Software Development Lifecycle (SDLC)
    - Series of phases that move software from inception to reproduction
    - Aims to mature the software product throughout the lifecycle
  - Key Phases of SDLC
    - Initiation
      - Define and document the need for a new system or software product
      - Conduct a Privacy Impact Assessment (PIA)
      - Identify privacy, security, and data protection requirements
      - Determine whether to build or acquire the product
    - Development and Acquisition
      - Understand risks associated with developing or acquiring software
      - Determine security and privacy controls needed
      - Update security documentation as needed
      - Output includes a Risk Assessment Report and updated security architecture design
    - Implementation and Assessment
      - Obtain stakeholder approval for deployment
      - Securely deploy the new software to production
      - Conduct a security assessment or audit for compliance
      - Update documentation as necessary

- Operations and Maintenance (O&M)
  - The software/system provides functionality and is maintained
  - Apply configuration management and change control
  - Continuously monitor security controls for effectiveness
  - Document any changes or updates
- Disposal
  - Decommission the system/software
  - Sanitize or declassify data before removal from operations
  - Follow configuration management and change control procedures
  - Document the disposal process for audit purposes
- NIST Special Publications
  - Original document
    - NIST SP 800-64
  - Updated document
    - NIST SP 800-160
  - Both documents emphasize similar phases and processes.
- Important Considerations
  - Security and privacy must be integrated at every phase
  - Change control is critical during the O&M phase
  - Documentation is essential throughout the lifecycle for compliance and audit purposes
- Summary
  - Understand the purpose and significance of each phase in the SDLC
  - Familiarity with the relationship between the phases and their outputs

- Acknowledge the importance of continuous monitoring and documentation

- **Software Development Methodologies Part 1**

- Software Development Methodologies - Part 1
  - Software Development Methodologies Introduction
  - Different models and frameworks used to create software
  - Models provide structured processes to build software
- Waterfall Model
  - Sequential and repetitive development lifecycle
  - Created in 1970 by Winston Royce
  - Described in the paper "Managing the Development of Large Software Systems"
  - Steps include Requirements, Design, Implementation, and Operations and Maintenance
  - Consistent steps across variations include Requirements, Design, Implementation, Testing, Operations, and Maintenance
  - Example of steps by Winston Royce
    - System Requirements
    - Software Requirements
    - Analysis
    - Program Design
    - Coding
    - Testing



- Operations
  - Sequential model requiring completion of one step before moving to the next
  - Allows feedback loops between steps, such as Testing back to Implementation
  - Lacks a completion step like disposal or retirement, continuing as an iterative process
  - Drawbacks
    - Requires requirements definition upfront before moving to design
    - Limits flexibility and agility if new requirements arise during development
    - Suitable for high-risk or sensitive applications needing methodical planning
- Increment Build Model
  - Model focused on building software in smaller, manageable parts or increments
  - Emphasizes specific functions and tasks developed in increments that are compiled to complete the project
  - Resembles Agile but predates it
  - Steps include Analysis, Design, Coding, Testing, and Delivery for each increment
  - Enables system engineering during analysis and design phases
  - Allows for learning from previous increments to improve future increments
  - Helps in adapting to environmental impacts and dependencies

- Spiral Model
  - Model allows revisiting of development phases multiple times for each prototype
  - Steps include Planning, Risk Analysis, Engineering, and Evaluation
  - Risk analysis focuses on software development, not security
  - Prototypes are repeatedly cycled through phases for ongoing evaluation and improvement
  - Drawbacks
    - Challenging to integrate security with multiple prototypes in various stages
    - Can be cumbersome for ensuring security at each phase
- **Software Development Methodologies Part 2**
  - Cleanroom Reference Model (CRM)
    - Focuses on embedding development and testing within quality control to prevent software defects
    - Developed by Carnegie Mellon University or the Software Engineering Institute
    - Emphasizes strict engineering processes with a goal of defect prevention rather than removal
    - Consists of four principle functions
      - Software Management
      - Specification
      - Development
      - Certification

- Requires following 14 processes to produce 20 work products
  - E.g., guides, plans, cases) to prove the software is defect-free
- Model name derived from hardware engineering cleanrooms where strict procedures prevent defects
- Joint Application Development (JAD) Model
  - Encourages continuous interaction between user and developer to jointly develop applications
  - Aims to reduce delivery timeframes and costs, and improve quality by gathering direct user feedback
  - Also called JAD sessions, or J A D sessions
  - Steps
    - Define objectives (requirements, scope, stakeholders, expected outcomes)
    - Session preparation (gather information from stakeholders regarding requirements and minimum viable product)
    - Session conduct (address software issues to make it as error-free as possible)
    - Documentation (document results and publish for stakeholder review)
- Rapid Application Development (RAD) Model
  - Built in response to deficiencies in the waterfall model, focusing on working software over structured processes
  - Often combined with JAD and CASE tools to automate SDLC phases

- Useful for creating software prototypes, R&D, or rapidly developing a product
- Steps
  - Requirements (define scope, requirements, stakeholders, and expected outcomes)
  - User Design (gather stakeholder input on desired features)
  - Construction (develop, update, and test working software)
  - Cutover (deliver software to customer or operations, including conversions, testing, and changeover)
  - Designed to provide a faster, more condensed development process
- Choosing a Development Methodology (Review)
  - Waterfall Model
    - Best for methodical approach with known requirements, target environment, software design, and potential users; suitable for critical or sensitive applications
  - Spiral Model
    - Ideal for large, complex projects needing quick responses to changes and risk adjustments, focusing on project risks rather than security risks
  - Incremental Build Model
    - Faster approach similar to waterfall but with added flexibility for project scope and user feedback
  - Cleanroom Development Model

# ISC2 CISSP

## (Study Guide)

- Formal engineering approach with strict processes to prevent software defects, suitable for projects needing rigorous quality control
- JAD Model
  - Preferred for continuous user input, short development timeframes, and focus on user satisfaction
- RAD Model
  - Optimal for fast development, deployment, and feedback, particularly in R&D or proof-of-concept projects
  - Regardless of the model, well-defined requirements are essential for building a satisfactory product and integrating security
  - Consider prep time, cost, and effort required when selecting a methodology
- **Agile Development**
  - Agile Development Overview
    - A flexible, adaptive approach to software development
    - Emphasizes collaboration, problem-solving, and adaptability over strict processes
    - Agile mindset focuses on fluid and collaborative development
  - Agile Core Values
    - Individuals and Interactions over processes and tools
      - Focus on developers, customers, stakeholders, and their interactions rather than tools or specific models
    - Working Software over comprehensive documentation

# ISC2 CISSP

## (Study Guide)

- Prioritize building working software and documenting afterward
- Customer Collaboration over contract negotiation
  - Emphasis on customer satisfaction and product quality over strict contract terms
- Responding to Change over following a plan
  - Adapt to customer needs and changes within a structured process
- Agile Manifesto - 12 Principles
  - Customer Satisfaction as the highest priority
  - Welcome Requirement Changes even late in development
  - Deliver Frequently to show progress and allow iterative feedback
  - Business and Developer Teaming for effective collaboration
  - Build Projects Around People by assigning the right people to the right tasks
  - Face-to-Face Communication preferred over messages and emails
  - Working Software Defines Progress as the primary measure of progress
  - Sustainable Development with a consistent and maintainable pace
  - Technical Excellence and Good Design enhance agility
  - Simplicity to maximize work while keeping processes simple
  - Self-Organized Teams bring out the best architecture, requirements, and design
  - Regular Reflection and Adjustment to improve team effectiveness and schedule alignment
- Scrum Methodology in Agile
  - Scrum Roles
    - Product Owner

# ISC2 CISSP

## (Study Guide)

- Defines goals, objectives, and project scope
- Scrum Master
  - Manages Agile process, removes impediments, supports team
- Development Team
  - Self-managed, self-organized team creating product increments based on the Definition of Done (DoD)
- Sprint
  - Time-boxed iteration where work is planned, developed, and reviewed
- Sprint Planning
  - Defines tasks to complete within the sprint duration
- Backlog
  - Collection of tasks or tickets planned for the sprint
- Kanban Board
  - Board used for tracking tasks in progress
- Daily Scrum
  - Daily 5-15 minute meetings to review completed work, upcoming work, and any roadblocks
- Sprint Lifecycle and Process
  - Steps include Sprint Planning, Development/Acquisition, Implementation, Review, and Retrospective
  - Sprint Retrospective
    - Reflection on completed sprint for lessons learned and process improvement

- Other Agile Methodologies
  - Variants include
    - Crystal
    - Kanban
    - Lean
    - RUP (Rational Unified Process)
    - AUP (Agile Unified Process)
    - DSDM (Dynamic Systems Development Method)
    - Feature Driven Development, and Extreme Programming (XP)
  - Most common in field
    - Scrum, Kanban, SAFE, Lean, and XP
- Security in Agile
  - Define security controls upfront for integration into the Agile process
  - Integrate Configuration Management and include it in DevOps/DevSecOps
  - Perform Regular Security Assessments and Audits to ensure compliance throughout Agile development
- Agile Development Key Exam Points
  - Understand the four core values of Agile
  - Familiarize with the 12 principles of Agile Manifesto and their purpose
  - Recognize the importance of integrating security within Agile



- **DevOps and DevSecOps**

- DevOps Overview

- Combines development activities with operations for continuous software delivery
- Emphasizes merging personnel, processes, and technology to quickly develop and deliver software capabilities
- Aims for a minimum viable product that meets customer needs and is refined over time

- DevOps Workflow and Pipeline

- DevOps cycle

- Plan, Develop, Deliver, Operate, then return to Plan

- Pipeline

- Automated workflow integrating development, quality assurance, and security testing
- Continuous integration and delivery of code to end users
- Workflow challenges include separation of duties and segregation of roles

- Infrastructure as Code (IaC)

- Automates infrastructure provisioning with code (XML, Python) using tools like Chef, Ansible, Terraform
- Reduces deployment time, ensures consistency, and mitigates security risks
- Immutable architecture
  - Static, unchanging configurations trusted for compliance and security

- Security and Access Controls in DevOps
  - Enforce least privilege and separation of duties in role assignments
  - Avoid authorization creep by establishing clear role-based access controls
  - Ensure DevOps automation tools (e.g., Jenkins) have minimal necessary privileges
- DevSecOps Overview
  - Integrates security into DevOps to ensure compliance before deployment
  - Known as Security as Code
    - Embeds security checks (e.g., scans, configurations) within the pipeline
- DevSecOps Manifesto Principles
  - Lean In
    - Security listens and collaborates rather than just rejecting ideas
    - Data and Science over Fear, Uncertainty, and Doubt
    - Open Contribution and Collaboration over strict security requirements
    - Consumable Security Services with APIs over mandated controls and paperwork
    - Business-Driven Security Scores over token approvals
    - Red and Blue Team Testing over sole reliance on scans
    - 24/7 Proactive Security Monitoring over reactive incident response
    - Shared Threat Intelligence over isolated knowledge
    - Compliance Operations over mere checklists

- CI/CD Pipeline and Security Integration
  - Continuous Integration
    - Automates new code integration into existing codebase
  - Continuous Delivery
    - Automates code delivery to the end-user environment
  - Continuous Deployment
    - Final pipeline stage, automating release to users
  - Pipeline steps include
    - Build, Test, Deploy to Test Environment, Automated Checks, Deploy to Production, Continuous Monitoring
- Security in CI/CD Pipelines
  - Security involvement at each stage of the pipeline
    - E.g., change control, testing, compliance checks, monitoring
  - Example steps
    - Version control in change management
    - Compliance testing in deployment to test environments
    - Security regression testing upon deployment to production
    - Continuous monitoring during operations and maintenance
  - Benefits of CI/CD Pipelines
    - Faster, more consistent delivery and quality control
    - Immediate customer feedback on functionality
    - Rapid response to security vulnerabilities via infrastructure as code and security as code
- Key Exam Points
  - Purpose and benefits of DevOps and DevSecOps

- Importance of Infrastructure as Code and Security as Code
- Role and benefits of Continuous Integration and Continuous Delivery
- **Software Maturity Models**
  - Purpose of Maturity Models
    - Evaluates and improves the current software development processes
    - Focuses on process maturity rather than security controls
  - Capability Maturity Model (CMM) / SWCMM / SCMM
    - Developed by Software Engineering Institute (SEI) at Carnegie Mellon University in 1993 for the U.S. Department of Defense
    - Five maturity levels
      - Level 1 - Initial
        - Few defined processes; success relies on effort
      - Level 2 - Repeatable
        - Basic discipline and ability to repeat successes
      - Level 3 - Defined
        - Standardized and consistent processes across engineering activities
      - Level 4 - Managed
        - Processes are measurable and quantitatively understood
      - Level 5 - Optimizing
        - Continuous improvement of fully optimized processes
  - IDEAL Model
    - Model for Strategic Planning of Software Process Improvement (SPI) by SEI

# ISC2 CISSP

## (Study Guide)

- Stands for Initiating, Diagnosing, Establishing, Acting, Learning
- Phases
  - Initiating
    - Create infrastructure, define roles, assign resources
  - Diagnosing
    - Review objectives, vision, and lessons learned
  - Establishing
    - Define measurable goals and outcomes
  - Acting
    - Test and evaluate new/improved processes
  - Learning
    - Use lessons learned and metrics for future improvements
- Capability Maturity Model Integration (CMMI)
  - Focuses on business performance improvement through key capabilities
  - Helps organizations and consumers assess maturity and compare capabilities
  - Areas of focus include
    - Development
      - Product development and engineering
    - Services
      - Service management best practices
    - Supply Management
      - Product and service acquisition practices
    - Security
      - Security approach improvement

- Safety
  - Safety approach for organizations
- People Management
  - People Capability Maturity Model (PCMM)
- Five maturity levels
  - Level 1 - Initial
    - Unpredictable, reactive processes
  - Level 2 - Managed
    - Project-level management (planned, performed, measured, controlled)
  - Level 3 - Defined
    - Organization-wide standards guiding projects
  - Level 4 - Measured and Controlled
    - Data-driven, quantitatively controlled processes
  - Level 5 - Optimizing
    - Stable, flexible processes with continuous improvement
- Software Assurance Maturity Model (SAM)
  - Developed by OWASP to analyze and improve software security posture
  - Integrates security strategy within the Software Development Lifecycle (SDLC)
  - Focuses on lifecycle stages
    - Governance
      - Administrative controls
    - Design, Implementation, Verification, Operations

- Stages of planning, building, testing, deploying, and maintaining software
- **Maturity levels**
  - **Level 0 - None**
    - No security practices; immature security posture
  - **Level 1 - Initial**
    - Ad hoc security practices
  - **Level 2 - Managed**
    - Effective security practices with some process management
  - **Level 3 - Mastered**
    - Comprehensive and mature security practices
- **Exam Focus**
  - Understand the purpose of the SWCMM model and its maturity levels
  - Familiarize with the IDEAL model and phases
  - Know the purpose and maturity levels of CMMI
  - Understand the SAM model and its security-focused maturity levels
- **Software Operations And Maintenance**
  - Purpose of Operations and Maintenance (O&M)
    - Ensures that the software application securely provides its intended function in production
    - Focuses on maintaining confidentiality, integrity, and availability in the software once deployed
  - Software Patch Management in O&M

- Manages and installs patches to address flaws, bugs, and vulnerabilities
- Follows a consistent process for identifying, testing, and installing patches
- Importance of configuration management in patch management
- Patch Management Process
  - Evaluation
    - Identify patches and assess risk to the system
    - Evaluate relevance
      - E.g., non-relevant patches for unused software
    - Identify security or operational impact for critical patches
  - Testing
    - Deploy patch in a test environment to check for negative impacts
  - Approval
    - Obtain authorization from the change control board (CCB) for deployment
  - Rollout
    - Deploy patch to production hosts
  - Verification
    - Confirm installation success and that security and functionality are intact
- Regression and Regression Testing
  - Regression
    - Occurs when a patch or bug fix causes unintended changes or vulnerabilities
  - Regression Testing Types
    - Unit Test



- Verifies individual functionality
- Functional Test
  - Confirms operational requirements are met
- Integration Test
  - Ensures software interacts properly with other systems
- Security Test
  - Verifies software meets security requirements, often through vulnerability or security assessments
- Role of DevOps and CI/CD in O&M
  - Using CI/CD (Continuous Integration, Continuous Delivery) pipelines in patch management for consistency
  - Steps in CI/CD
    - Apply patch in test environment
    - Perform automated security tests (e.g., vulnerability scans, SCAP scans)
    - Approve for production deployment and validate the new version
- Continuous Monitoring in O&M
  - Continuous assessments to maintain security baseline and prevent unauthorized changes
  - Helps identify issues such as unauthorized patches or backdoors
- Key Exam Points for O&M
  - Understand the purpose and components of O&M
  - Know about regressions and regression testing types
  - Recognize the necessity of including O&M in the Configuration Management (CM) plan

- **Integrated Product Teams**

- Purpose of an Integrated Product Team (IPT)
  - Cross-functional team working to deliver a customer product
  - Comprised of multi-disciplined, cross-functional members from various fields
  - Focused on collaborative development of a software product
- Typical IPT Members
  - Development team, IT personnel, project managers, architects, security experts, engineers
  - Can include third-party auditors, quality assurance staff, senior management, and stakeholders
- Benefits of IPT
  - Reduces time and cost to deliver an operational product
  - Diverse skill sets improve operational and security risk management
  - Ensures continuous improvement and better quality of the product
- IPT Priorities
  - Customer Focus
    - Determines project outcomes, processes, and schedules
  - Proactive Risk Management
    - For the product, user, and security considerations
  - Seamless Tools
    - Use tools that do not interfere with development workflow
  - Concurrent Product and Process Development
    - Identifies improvement opportunities throughout the lifecycle

- Early and Continuous Planning
  - Spot risks and technical impacts early in the lifecycle
- Flexibility
  - Optimize team efforts with standardized, cost-effective approaches
- Empowerment
  - Grant team members authority and responsibility to improve the lifecycle
- Key Exam Points
  - Understand the role and benefits of an IPT
  - Familiarize with IPT priorities and the importance of empowering team members
- **Code Repositories**
  - Purpose of Code Repositories (Repos)
    - Centralized storage for software code
    - Supports collaborative software development by providing features such as
      - Web hosting, notifications, wiki pages, secure storage, code review, version control, and bug tracking
  - Git and Code Repositories
    - Git is the most commonly used version control language for code repositories
    - Developed by Linus Torvalds, released in 2005
    - Allows developers to interact with code files, supporting version control

- Popular code repos include GitHub, GitLab, SourceForge, Bitbucket, ProjectLocker, CodeCommit, and Azure Repos
- Basic Git Operations (Example)
  - Git Init
    - Initializes a new local repository
  - Git Clone
    - Checks out a repository to work with it
  - Git Push
    - Sends changes back to the repository
- Security Considerations for Code Repositories
  - Avoid storing sensitive data in publicly accessible repos
  - Most repos are public by default and should be set to private when confidentiality is required
  - Use access controls to permit only authorized access and modifications to the code base
  - Secure API connections to private repos using API keys, and securely store and protect these keys
  - Ensure API keys are not hard-coded or stored within the repository code, especially in public repos

## Application Security

### Objectives:

- 8.2 - Identify and apply security controls in software development ecosystems
- 8.3 - Assess the effectiveness of software security
- 8.4 - Assess security impact of acquired software
- 8.5 - Define and apply secure coding guidelines and standards
  
- **Application Security**
  - Programming Languages and Application Security
    - Every programming language introduces unique security considerations
    - Security issues may arise from memory management or injection vulnerabilities
    - Understanding different programming languages helps in selecting appropriate security controls
  - Application Security Testing
    - Static analysis
      - Examines code without executing it, identifying vulnerabilities early in the SDLC
    - Dynamic analysis
      - Tests the application in real-time to uncover vulnerabilities during execution
    - Both testing methodologies are crucial for early identification of security issues

- Software Assurance
  - Ensures software functions as intended while protecting against threats
  - Verifies that software meets security requirements through development practices and evaluations
- Acquired Software Security
  - Involves assessing third-party, open-source, and cloud software for security risks
  - Requires due diligence, such as conducting security reviews and vulnerability assessments, to ensure the software aligns with organizational standards
- Application Attacks
  - Common application attacks include injection attacks and cross-site scripting (XSS)
  - Secure coding guidelines and standards help defend against these attacks
  - Key focus on secure coding practices to mitigate risks from these types of attacks
- OWASP Top 10 Vulnerabilities
  - 2017 Top 10 includes vulnerabilities such as injection, broken authentication, and sensitive data exposure
  - Updated 2021 list includes new vulnerabilities like insecure design and server-side request forgery (SSRF)
  - Understanding OWASP vulnerabilities is critical for preventing application breaches
- Software API Security

- APIs pose risks like insufficient authentication and excessive data exposure
- API security involves applying strong authentication, encryption, and input validation controls
- Secure Coding Practices
  - Key practices include input validation, proper error handling, and defense against injection attacks
  - Secure coding ensures software is built with security integrated into the code from the start
  - Best practices mitigate risks outlined in the OWASP Top 10
- Software-Defined Security
  - Security approach for software-defined environments like cloud and virtual networks
  - Provides a flexible, scalable security solution that adapts to modern application ecosystems
- **Programming Languages**
  - Purpose of Programming Languages
    - Provides structured instructions sent to a computer for execution
    - Converts human-friendly code to binary or machine language, which computers understand
  - Types of Programming Languages
    - Low-Level Languages
      - Interfaces directly with hardware, especially the CPU
    - High-Level Languages
      - Uses interpreters or compilers to interact with hardware indirectly

- Compiled vs. Interpreted Languages
  - Compiled Languages
    - High-level languages converted to low-level machine code using a compiler
    - Examples
      - C, C++, C#, Rust, Visual Basic, Swift, Java
  - Interpreted Languages
    - Executed directly without compiling to machine instructions
    - Examples
      - PHP, Perl, JavaScript, Python, VBScript, Ruby
- Programming Language Generations
  - First Generation
    - Machine code, binary (0s and 1s)
  - Second Generation
    - Assembly language, uses English words that convert to machine code
  - Third Generation
    - High-level language converted to machine code via a compiler
      - E.g., Java, C++
  - Fourth Generation
    - Domain-specific, performing specialized functions
      - E.g., SQL
  - Fifth Generation
    - Problem-solving and AI-based languages that generate logic based on constraints



- Code Libraries
  - Contains reusable code, procedures, or programs for software development
  - Enhances efficiency, consistency, and security when properly managed
  - Examples include
    - DLL files, Java Runtime Environment (JRE), and libraries hosted in code repositories like GitHub or Bitbucket
- Runtime Environment
  - Combination of hardware and software resources necessary to execute an application
  - Includes servers, operating systems, compilers, interpreters, storage, and network connections
  - Requires proper security measures such as hardening, configuration management, and monitoring
- Software Development Kit (SDK)
  - A toolkit containing the tools to create, compile, test, and debug software applications
  - Platform-dependent, specific to environments like Windows, Unix/Linux, or mobile OS
  - May include third-party resources
  - Integrated Development Environment (IDE)
    - Provides a graphical user interface for SDKs, simplifying development
    - Examples
      - Visual Studio, NetBeans, Eclipse

- Includes debugging, version control, and tools for efficient development
- Key Exam Points
  - Understand the types and uses of programming languages and code libraries
  - Familiarize with the runtime environment and its security requirements
  - Know the purposes of SDKs and IDEs and their role in software development
- **Application Security Testing**
  - Purpose of Application Security Testing
    - Identifies bugs, flaws, and vulnerabilities that may pose security risks
    - Applies to in-house developed applications or acquired software
      - E.g., COTS products
  - Types of Application Security Testing
    - Static Application Security Testing (SAST)
      - Analyzes software code without running or executing it
      - Often applied to in-house developed software where source code is available
    - Dynamic Application Security Testing (DAST)
      - Analyzes software in an operational environment, often without access to source code
      - Commonly used for COTS, open-source software, and closed-source applications

- Testing Approaches
  - White Box Testing
    - Performed by internal testers with full knowledge of the source code; uses SAST
  - Black Box Testing
    - Performed by third-party testers with no knowledge of source code; uses DAST
- Additional Types of Software Tests
  - System Test
    - Verifies that software meets functional and security requirements
  - Unit Test
    - Tests specific application components or scripts
  - Integration Test
    - Ensures interoperability between different software components
  - Regression Test
    - Confirms that code updates do not introduce new security risks
  - Sanity Test
    - Informally checks feature feasibility and functionality
  - Smoke Test
    - Quickly assesses basic functionality of newly built software
  - Fuzz Testing
    - Dynamic testing that sends invalid inputs to detect bugs and flaws
- Types of Fuzz Testing
  - Mutational Fuzzing
    - Uses valid data as seed data, then mutates to create invalid inputs

- Sometimes referred to as "dumb fuzzing"
- Generation Fuzzing
  - Creates invalid data based on a predefined data model
  - Sometimes called "smart or intelligent fuzzing"
- Interactive Application Security Testing (IAST)
  - Analyzes real-time software functionality, communications, runtime behavior, traffic, and frameworks
  - Runtime Application Self Protection (RASP)
  - Tool that intercepts application data requests on the server and validates them
  - Analyzes communications (e.g., API calls) without accessing source code directly
- Key Exam Points
  - Understand SAST and DAST purposes and applications
  - Familiarize with Interactive Application Security Testing (IAST) and RASP
  - Recognize types of fuzz testing and when to apply white, black, and gray box tests
- **Software Assurance**
  - Purpose of Software Assurance
    - Provides confidence that software is secure and performs as designed
    - Assesses software security effectiveness
  - OWASP Application Security Verification Standard (ASVS)
    - Community-driven framework of security requirements and controls

- Helps organizations develop and maintain secure applications based on assurance levels
- Assurance levels are tailored to application data sensitivity and customer needs
- ASVS Assurance Levels
  - Level 1 - Low Security Assurance
    - Bare minimum requirements for all applications
    - Protects against low-effort threats and simple vulnerabilities
    - Suitable as a first step in a multi-phase security enhancement
  - Level 2 - Moderate Security Assurance
    - Sufficient to defend against most application security risks
    - Protects against skilled and motivated hackers
    - Includes controls for standard penetration testing and ethical hacking defenses
  - Level 3 - High Security Assurance
    - Necessary for applications critical to organizational operations
    - Protects against advanced threats, including Advanced Persistent Threats (APTs)
    - Highest level of security assurance with extensive controls
  - Determining Assurance Levels
    - Based on the Software Development Lifecycle (SDLC)
      - Risk Analysis
        - Identifies and evaluates risks; unmitigated or unaccepted risks limit assurance level
      - Change Control

# ISC2 CISSP

## (Study Guide)

- Ensures controlled, authorized code changes through a change control board
- Continuous Monitoring
  - Verifies ongoing control effectiveness and compliance
  - Includes static and dynamic application security tests
- Data Protection
  - Safeguards data in compliance with relevant regulations
    - E.g., GDPR, HIPAA, SOX
- Logging
  - Tracks transactions and code changes for accountability and traceability
- Key Exam Points
  - Understand the ASVS levels (1, 2, and 3) and associated security capabilities
  - Know the evaluation criteria (SDLC, risk analysis, change control, monitoring, data protection, logging)
- **Acquired Software Security**
  - Acquired Software
    - Software obtained through purchase or lease from a third-party vendor or provider
    - Includes commercial off-the-shelf (COTS), government off-the-shelf (GOTS), open-source software (OSS), and non-developmental items (NDIs)

- Types of Acquired Software
  - COTS
    - Commercial software purchased and managed by the organization
  - OSS/FOSS
    - Free software maintained by a community; typically hosted on platforms like GitHub
  - GOTS
    - Software acquired from the government, usually for use with a government license
  - NDIs
    - Third-party libraries or modules included with COTS, GOTS, or OSS products, raising supply chain risk considerations
- Cloud-Based Lease Software Models
  - Software as a Service (SaaS)
    - Cloud provider manages OS and supporting applications; user manages data and access controls
  - Platform as a Service (PaaS)
    - Cloud provider manages OS; user owns the application but may have limited control over security
- Security Considerations for Acquired Software
  - Implement a security-focused acquisition policy to minimize risks from acquired applications
  - Identify threats and vulnerabilities relevant to the application
  - Communicate security requirements (e.g., GDPR, SOX, HIPAA compliance) to vendors or providers

- Use trusted vendors and implement supply chain risk management for NDIs
- NIST Acquisition Controls (SpecialPub 800-160 and 800-64)
  - Preparation
    - Define security needs and include in acquisition requests
  - Selection
    - Conduct thorough vendor evaluation to ensure a trustworthy provider
  - Agreement Management
    - Develop SLAs or contracts addressing security requirements and compliance
  - Monitoring
    - Regularly assess provider's performance and adherence to the SLA
  - Acceptance
    - Confirm compliance with security needs before purchasing or licensing
- Best Practices for Acquired Software
  - Follow vendor-provided security guidelines and industry best practices for hardening applications
  - Conduct security testing, including vulnerability assessments and privacy impact assessments, prior to production deployment
  - Monitor acquired applications continuously for new threats and vulnerabilities



- Key Exam Points
  - Understand risks associated with COTS, GOTS, OSS, and cloud-based applications
  - Familiarize with the purpose of an acquisition policy and supply chain risk management
  - Recognize the steps in NIST's acquisition approach to ensure software security
- **Application Attacks**
  - Application Attacks
    - Targets flaws in inputs, session management, process operations, and other areas at the source level code
    - Typically conducted through the application's user interface
  - Injection Attacks
    - SQL Injection
      - Unauthorized SQL queries submitted to a database via a web application
    - LDAP Injection
      - Unauthorized queries to a directory server (e.g., LDAP or Active Directory) to access account information
    - XML Injection
      - Injection of unauthorized queries into XML-based applications
    - DLL Injection
      - Malicious code placed in DLL files, typically targeting Microsoft systems

- Mitigations for Injection Attacks
  - Enforce input validation and access controls
    - Constrain interfaces to limit user interaction with the database or directory
    - Harden servers by disabling unnecessary services and setting up proper access controls
- Hijacking Attacks
  - Session Hijacking
    - Takes over an active session using stolen session tokens, cookies, or credentials
    - Sometimes known as a replay attack, reusing valid credentials to gain unauthorized access
  - Domain Hijacking
    - Unauthorized changes to registered domain records (e.g., modifying DNS entries) to redirect traffic
  - Backdoor Attack
    - Allows unauthorized access by bypassing normal authentication, often left in code by developers for maintenance
- Rootkit Attacks
  - Rootkits
    - Malware providing tools to gain root or administrator access
    - Often embedded in applications, OS components, boot sectors, or firmware
    - Best detected by host-based intrusion detection systems (HIDS)

- Privilege Escalation
  - Horizontal Privilege Escalation
    - Lateral movement across systems without increasing privilege level
  - Vertical Privilege Escalation
    - Gains higher privileges, often from a general user to an administrator level
- Time of Check and Time of Use (TOCTOU) Attack
  - Targets race conditions by modifying resources between the time of check and time of use (TOC/TOU)
  - For example, intercepts a transaction after conditions are checked but before it is executed to alter the result
- Key Exam Points
  - Recognize various application attacks
    - Injection, hijacking, rootkits, privilege escalation, and TOCTOU
    - Understand how each attack exploits different aspects of application flaws and vulnerabilities
- **OWASP Top 10 Vulnerabilities - Part 1**
  - Overview of OWASP Top 10 Security Risks
    - Established by the OWASP Foundation (Open Web Application Security Project)
    - Focuses on the most critical risks to web applications, applicable to general software

- Includes rankings based on industry feedback and Common Weakness Enumeration (CWE)
- OWASP Top 10 Overview (2017)
  - Top 10 critical security risks impacting applications at the source code level
  - Likely exam focus on 2017 version, covering injection attacks, broken authentication, sensitive data exposure, XML external entities, and broken access control in this first part
- OWASP Top 5 Security Risks for 2017
  - Injection Attacks
    - Occurs when untrusted data is sent to a command interpreter, attempting to manipulate data
    - Common Types
      - SQL Injection (database queries), LDAP Injection (directory server access), XML Injection (XML-based application access)
    - Mitigation
      - Use whitelisted, approved stored procedures, input validation, and escape sequences
  - Broken Authentication
    - Caused by poorly managed user accounts, credentials, and session tokens
    - Consequences
      - Leads to account compromise and unauthorized access
    - Mitigation

- Implement proper identity and access management, strong session management, and update accounts regularly
- Sensitive Data Exposure
  - Involves unprotected sensitive data, including data at rest, in transit, and in use
  - Mitigation
    - Encrypt and control sensitive data and discard it when not needed
- XML External Entities (XXE)
  - Targets vulnerabilities in XML parsing that allow calls to external entities
  - Consequences
    - Risk of denial of service, forgery attacks, or unauthorized data exposure
  - Mitigation
    - Block external entities, disable Document Type Definitions (DTDs), install web application firewall, and keep XML parsers updated
- Broken Access Control
  - Improper access control leading to unauthorized access, privilege escalation, and data exposure
  - Mitigation
    - Use a deny-by-default model, enforce least privilege, and regularly review and update privileges

- **OWASP Top 10 Vulnerabilities - Part 2**

- Overview of OWASP Top 10 Security Risks
  - Target common security flaws at the source code level for web applications and software
  - Continued from Part 1 to address security misconfigurations through logging and monitoring
- OWASP Top 10 Security Risks (Continued)
  - Security Misconfiguration
    - Vulnerability due to unpatched software, default accounts, and lack of hardening, increasing the attack surface
    - Mitigation
      - Follow industry best practices, regularly patch, disable unnecessary services, minimize attack surface, and regularly test and assess software security
  - Cross-Site Scripting (XSS)
    - An unauthorized script injected into a web page and executed in the victim's browser; browser-side attack
    - Types
      - Stored XSS
        - Script stored on the target server, later executed by the victim
      - Reflected XSS
        - Malicious script reflected off a web server via the victim's HTTP request

# ISC2 CISSP

## (Study Guide)

- DOM-based XSS
  - Malicious script modifies the Document Object Model, impacting the browser's client-side code
- Mitigation
  - Use modern scripting languages with escape sequences, and implement a Content Security Policy (CSP) for HTML pages
- Insecure Deserialization
  - Process of reversing data serialization (format conversion) to reuse an object; a risk in communication formats, especially JSON, XML, and Python
  - Mitigation
    - Use digital certificates or mutual authentication, sandbox or isolate deserialization code, restrict connectivity to applications that perform serialization
- Components with Known Vulnerabilities
  - Risk caused by using software components with known vulnerabilities, which increase exploitation potential
  - Mitigation
    - Identify known vulnerabilities, apply patches, monitor the vulnerabilities, research them via sources like the National Vulnerability Database (NVD) and Common Vulnerabilities and Exposures (CVE), and consider moving to newer applications if critical

- Insufficient Logging and Monitoring
  - Lacking sufficient logging and monitoring, which prevents detecting vulnerabilities, threats, and attacks on applications
  - Mitigation
    - Log critical system changes, privilege level changes, and communications
- **OWASP Top 10 Vulnerabilities - Part 3**
  - Overview of the 2021 OWASP Top 10 Update
    - Focus on key changes introduced in 2021, highlighting new security risks A4, A5, A8, and A10
    - Emphasis on source code vulnerabilities and mitigations relevant for both web applications and general software
  - New OWASP Risks in 2021
    - A4 - Insecure Design
      - Risk from ineffective security or privacy controls built into the software design
      - Mitigation
        - Conduct regular risk analysis, implement secure system designs and threat modeling to assess potential risks and implement secure architectural decisions
    - A5 - Security Misconfiguration (Updated)
      - Common issues include unpatched software, default accounts, and lack of system hardening
      - Mitigation



- Follow industry best practices, disable unnecessary services, and regularly test security to ensure compliance and minimize attack surface
- A8 - Software and Data Integrity Failures
  - Risk caused by insufficient integrity protections in software, especially concerning automated updates and libraries
  - Mitigation
    - Limit or prevent automated updates, only use trusted sources for libraries and repositories, verify digital signatures and checksums for all updates
- A10 - Server-Side Request Forgery (SSRF)
  - Occurs when an application accesses remote resources without validating the URL, leading to potential unauthorized access to internal servers or services
  - Mitigation
    - Validate all client-provided inputs, use whitelisting for URLs and allowed ports, and deny non-whitelisted requests by default
- **Software API Security**
  - Overview of Application Programming Interfaces (APIs)
    - APIs enable direct connections between software applications and services to improve integration and user experience without needing intermediary layers like web pages
    - Common uses

- Single sign-on, payment gateways, social media integrations, and more
- Key commands used in API operations
  - GET (retrieve a resource)
    - POST (create a new resource)
    - PUT (edit/update a resource)
    - DELETE (remove a resource)
- Types of APIs
  - Public (Open) API
    - Allows anyone to connect using HTTP protocol, high exposure, poses security risks
  - Private (Internal) API
    - Used for internal applications and services, restricted access behind firewalls or in private cloud environments
  - Partner API
    - Accessible to selected entities, commonly used in controlled business applications like payment gateways
  - Composite API
    - Combines multiple requests into a single API call, often used in dashboards and data gathering applications
- Common Protocols for APIs
  - SOAP (Simple Object Access Protocol)
    - XML-based, an earlier protocol for API requests
  - REST (Representational State Transfer)
    - More flexible than SOAP, supports both XML and JSON

- Note
  - SOAP and REST are common on the CISSP exam; others (e.g., JSON-RPC, gRPC) are less likely to appear but are relevant in modern implementations
- API Security Measures
  - Require and protect API keys
    - Long, complex keys used for authentication and authorization, protected against unauthorized access
  - Data Type Security
    - Understanding the type of data shared through APIs (e.g., health information) to ensure compliance with regulatory policies
  - Testing APIs
    - APIs should be included in software application testing (e.g., unit tests, assessment tests) to ensure security measures like correct protocols, whitelisting, and port control
  - Access and Resource Control
    - Limit API permissions to only those necessary, preventing excessive resource requests and potential DoS or DDoS attacks
  - Input Validation
    - Reject invalid or unauthorized commands to prevent common attacks
      - E.g., injection attacks
    - Logging and Monitoring
      - Track API activities for potential threats and misuse

- **Secure Coding Practices**

- Overview of Secure Coding

- Purpose

- Secure coding reduces security risks in in-house or organization-developed software
      - Not applicable to acquired software, as secure coding must be built into the development process by the original developers

- Key resource

- OWASP Secure Coding Practices Quick Reference Guide

- General Coding Practices

- Use Approved Code Only

- Prevent use of unmanaged or unapproved code; implement change control to enforce this

- Restrict Unauthorized Code Creation and Modification

- Configuration management and change management processes help maintain code integrity

- Verify Code Integrity

- Use hash functions (checksums) to confirm the integrity of acquired code and libraries from trusted sources

- E.g., GitHub

- Employ Modern Cryptographic Ciphers

- Use secure, unbroken cryptographic ciphers to protect communication in APIs and other application functions

- Error Handling

- Ensure proper error handling to prevent injection attacks, buffer overflows, and DoS attacks
- Manage Computer Memory
  - Prevent memory leaks and denial of service conditions by carefully managing computer memory allocation and use
- Avoid Hard-Coded Credentials
  - Do not include hard-coded passwords, tokens, or other sensitive data in code; hard-coded credentials can lead to exposure if uploaded to public repositories
- Limit Privileged Escalation
  - Restrict applications from requiring elevated privileges unless absolutely necessary, as high-privilege applications are more vulnerable if compromised
- **Software-Defined Security**
  - Overview of Software Defined Security
    - Provides security functions as part of developed software
    - Originated from virtualizing security functions, replacing traditional hardware/software solutions like firewalls and IDS/IPS appliances
    - Encompasses concepts like Software Defined Networks (SDN), Infrastructure as Code, and Software Defined Data Centers
  - Key Concepts in Software Defined Security
    - Security as Code

# ISC2 CISSP

## (Study Guide)

- Integrates security processes into DevOps workflows, ensuring compliance throughout the DevOps and CI/CD (Continuous Integration and Continuous Delivery) processes
- Configuration as Code
  - Applies standardized, approved configurations to resources, enabling "gold images" (secure, hardened, and immutable configurations)
- Policy as Code
  - Merges Infrastructure as Code and Configuration as Code, creating immutable resources and enforcing strict policy compliance
- Implementing Security as Code
  - Use configuration management to authorize changes to code
  - Identify security controls compatible with code-based implementation, applying administrative controls where feasible
  - Add security gates/checks throughout the pipeline to verify that risk remains within acceptable tolerance
  - Regular testing of security as code functions as part of the SDLC or DevOps lifecycle ensures continued compliance and security

## Conclusion

- **Conclusion**
  - Congratulations on completing your CISSP certification course! Here's a summary of what you've accomplished and what lies ahead as you prepare for the exam
  - Course Recap
    - Extensive Coverage
      - Explored 32 sections encompassing a wide range of information security concepts and practices across all eight CISSP domains
    - In-depth Learning
      - Delved into key areas such as Security Management, Asset Security, Security Architecture, and more, ensuring a thorough preparation for the CISSP exam
  - Importance of Course Topics
    - Comprehensive Understanding
      - Each topic covered is crucial for not only passing the CISSP exam but also for practical applications in securing organizations
    - Strategic Teaching Order
      - The course content was structured not by following the CISSP exam outline strictly but to facilitate easier learning and retention of information

- Preparation for CISSP Exam
  - Real-World Application
    - The principles taught are not just theoretical but are daily applied by professionals to safeguard organizations in an ever-evolving threat landscape
  - Exam Readiness
    - Equipped with practical examples and a deep understanding of essential security principles, you are well-prepared to tackle the CISSP exam confidently
- Next Steps
  - Practice Exams
    - Utilize the included full-length practice exam to assess readiness. If scoring below 75%, revisit the necessary sections to reinforce knowledge
  - Official CISSP Practice Tests
    - Consider additional practice through official sources or other reputable materials to ensure a broad exposure to potential exam questions
- Exam Registration and Tips
  - Scheduling the Exam
    - Obtain your CISSP exam voucher via ISC2 or PearsonVue and plan your exam date at a convenient testing center
  - Exam Strategy



# ISC2 CISSP

## (Study Guide)

- Manage your time effectively during the exam, which will consist of 100-150 questions over three hours, ensuring to address each question thoughtfully
- Certification Benefits
  - Career Advancement
    - Achieving CISSP certification will open new career opportunities and enhance your credibility and marketability in the field of information security
  - Continual Learning
    - The journey of learning does not end with this course or the exam; continue to build on this foundation and stay updated with the latest security trends and best practices
- Community and Support
  - Engagement
    - Share your success and insights within the community, and participate in discussions to further enrich your understanding and network with peers
  - Ongoing Education
    - Look forward to more advanced courses and specialized learning paths that can further deepen your expertise in specific areas of information security
- You've shown remarkable dedication and effort throughout this course. As you move forward, remember that this journey is not just about passing an exam but about becoming a leader in cybersecurity. Good luck, and here's to your success on the CISSP exam and beyond!