Chapter 1 - Access Control

A. Control access by applying the following concepts/method-ology/techniques:
   A.1 Policies
   A.2 Types of controls (preventive, detective, corrective, etc.)
   A.3 Techniques (e.g., nondiscretionary, discretionary, and mandatory)
   A.4 Identification and authentication
   A.5 Decentralized/distributed access control techniques
   A.6 Authorization mechanisms

D. Identity and access provisioning lifecycle (e.g., provisioning, review, revocation)

The Access Control domain in the Common Body of Knowledge (CBK) for the CISSP certification exam deals with topics and issues related to granting and revoking the right to access data or perform an action on a system. Generally, an access control is any hardware, software, or organizational administrative policy or procedure that performs the following tasks:

■ Identifies users or other subjects attempting to access resources.

■ Determines whether the access is authorized.

■ Grants or restricts access.

■ Monitors and records access attempts.

Chapter 2 - Access Control Attacks and Monitoring

This chapter builds on key information on logging and monitoring, access control attacks, and assessing the effectiveness of access controls. Be sure to read and study the materials from
each of these chapters to ensure complete coverage of the essential material for the CISSP certification exam.

Objectives:

A. Control access by applying the following concepts/methodology/techniques:
   A.7 Logging and monitoring

B. Understand access control attacks
   B.1 Threat modeling
   B.2 Asset valuation
   B.3 Vulnerability analysis
   B.4 Access aggregation

C. Assess effectiveness of access controls
   C.1 User entitlement
   C.2 Access review & audit

Chapter 3 - Secure Network Architecture and Securing Network Components

This chapter discusses the OSI model as a guiding principle in networking, cabling, wireless connectivity, TCP/IP and related protocols, networking devices, and firewalls. The Telecommunications and Network Security domain for the CISSP certification exam deals with topics related to network components (i.e., network devices and protocols); specifically, how they function and how they are relevant to security.

Objectives:

Telecommunications and Network Security

A. Understand secure network architecture and design (e.g., IP and non-IP protocols, segmentation):
   A.1 OSI and TCP/IP models
   A.2 IP networking
A.3 Implications of multi-layer protocols

B. Securing network components:
   B.1 Hardware (e.g., modems, switches, routers, wireless access points)
   B.2 Transmission media (e.g., wired, wireless, fiber)
   B.3 Network access control devices (e.g., firewalls, proxies)
   B.4 Endpoint security

Chapter 4 - Secure Communications and Network Attacks

This chapter covers the many forms of communications security, vulnerabilities, and countermeasures. The Telecommunications and Network Security domain for the CISSP certification exam deals with topics of communications security and vulnerability countermeasures.

Objectives:

Telecommunications and Network Security

C. Establish secure communication channels (e.g., VPN, TLS/SSL, VLAN):
   C.1 Voice (e.g., POTS, PBX, VoIP)
   C.2 Multimedia collaboration (e.g., remote meeting technology, instant messaging)
   C.3 Remote access (e.g., screen scraper, virtual application/desktop, telecommuting)
   C.4 Data communications

D. Understand network attacks (e.g., DDoS, spoofing)

Chapter 5 - Security Governance Concepts, Principles, and Policies

The Information Security Governance and Risk Management domain of the Common Body of Knowledge (CBK) for the CISSP certification exam deals with the common and foundational elements of security solutions. These include elements essential to the design, implementation, and administration of security mechanisms.
Objectives:

Information Security Governance and Risk Management

A. Understand and align security function to goals, mission, and objectives of the organization.

B. Understand and apply security governance
   B.1 Organizational processes (e.g., acquisitions, divestitures, governance committees)
   B.2 Security roles and responsibilities
   B.3 Legislative and regulatory compliance
   B.4 Privacy requirements compliance
   B.5 Control frameworks
   B.6 Due care
   B.7 Due diligence

C. Understand and apply concepts of confidentiality, integrity, and availability.

D. Develop and implement security policy
   D.1 Security policies
   D.2 Standards/baselines
   D.3 Procedures
   D.4 Guidelines
   D.5 Documentation

E. Manage the information life cycle (e.g., classification, categorization, and ownership)

Chapter 6 - Risk and Personnel Management

The Information Security Governance and Risk Management domain of the Common Body of Knowledge (CBK) for the CISSP certification exam deals with hiring practices, formalizing security structure, risk management, awareness training, and management planning. This chapter explores the human side of security, from establishing secure hiring practices and job descriptions to developing an employee infrastructure. Additionally, we look at how employee
training, management, and termination practices are considered an integral part of creating a secure environment. Finally, we examine how to assess and manage security risks.

Objectives:

Information Security Governance and Risk Management

F. Manage third-party governance (e.g., on-site assessment, document exchange and review, process/policy review)

G. Understand and apply risk management concepts
   G.1 Identify threats and vulnerabilities
   G.2 Risk assessment/analysis (qualitative, quantitative, hybrid)
   G.3 Risk assignment/acceptance
   G.4 Countermeasure selection
   G.5 Tangible and intangible asset valuation

H. Manage personnel security
   H.1 Employment candidate screening (e.g., reference checks, education verification)
   H.2 Employment agreements and policies
   H.3 Employee termination processes
   H.4 Vendor, consultant, and contractor controls

I. Develop and manage security education, training, and awareness.

J. Manage the security function
   J.1 Budget
   J.2 Metrics
   J.3 Resources
   J.4 Develop and implement information security strategies
   J.5 Assess the completeness and effectiveness of the security program
Chapter 7 - Software Development Security

In this chapter, we examine some of the common threats that applications pose to both traditional and distributed computing environments. Next, we explore how to protect data. Finally, we take a look at some of the systems development controls that can help ensure the accuracy, reliability, and integrity of internal application development processes.

Objectives:

A. Understand and apply security in the software development life cycle
   A.1 Development life cycle
   A.2 Maturity models
   A.3 Operation and maintenance
   A.4 Change management

B. Understand the environment and security controls
   B.1 Security of the software environment
   B.2 Security issues of programming languages
   B.4 Configuration management

C. Assess the effectiveness of software security

D. Security Architecture and Design

E. Understand software and system vulnerabilities and threats
   E.3 Database security (e.g., inference, aggregation, data mining, warehousing)

Chapter 8 - Malicious Code and Application Attacks

This chapter takes an in-depth look at some of the specific threats faced on a daily basis by administrators in the field. We’ll begin this chapter by looking at the risks posed by malicious code objects—viruses, worms, logic bombs, and Trojan horses. We’ll then take a look at some of the other security exploits used by someone attempting to gain unauthorized access to a system or to prevent legitimate users from gaining such access.

Objectives:
Chapter 9 - Cryptography and Symmetric Key Algorithms

This chapter looks at the history of cryptography, the basics of cryptographic communications, and the fundamental principles of private key cryptosystems. The next chapter continues the discussion of cryptography by examining public key cryptosystems and the various techniques attackers use to defeat cryptography.

Objectives:

Cryptography

A. Understand the application and use of cryptography

   A.1 Data at rest (e.g., hard drive)

   A.2 Data in transit (e.g., on the wire)

B. Understand the cryptographic life cycle (e.g., cryptographic limitations, algorithm/protocol governance)

C. Understand encryption concepts

   C.1 Foundational concepts

   C.2 Symmetric cryptography

   C.3 Asymmetric cryptography
Chapter 10 - PKI and Cryptographic Applications

This chapter explores the world of asymmetric (or public key) cryptography and the public key infrastructure (PKI) that supports worldwide secure communication between parties that don’t necessarily know each other prior to the communication. We’ll also explore several practical applications of cryptography: securing electronic mail, web communications, electronic commerce, and networking. The chapter concludes with an examination of a variety of attacks malicious individuals might use to compromise weak cryptosystems.

Objectives:

Cryptography

C. Understand encryption concepts

C.3 Asymmetric cryptography

C.4 Hybrid cryptography

C.5 Message digests

C.6 Hashing

D. Understand key management processes

D.1 Creation/distribution

D.2 Storage/destruction

D.3 Recovery

D.4 Key escrow

F. Understand non-repudiation
D.3 Recovery

D.4 Key escrow

E. Understand digital signatures

F. Understand non-repudiation

G. Understand methods of cryptanalytic attacks
   G.2 Social engineering for key discovery
   G.3 Brute force (e.g., rainbow tables, specialized/scalable architecture)
   G.4 Cipher-text only
   G.5 Known plaintext
   G.6 Frequency analysis
   G.7 Chosen cipher-text
   G.8 Implementation attacks

H. Use cryptography to maintain network security

I. Use cryptography to maintain application security

J. Understand Public Key Infrastructure (PKI)

K. Understand certificate related issues

L. Understand information hiding alternatives (e.g., steganography, watermarking)

Chapter 11 - Principles of Security Models, Design, and Capabilities

In this chapter, we discuss security models, including state machine, Bell-LaPadula, Biba, Clark-Wilson, Take-Grant, and Brewer and Nash. This chapter also describes Common Criteria and other methods governments and corporations use to evaluate information systems from a security perspective, with particular emphasis on US Department of Defense and international
security evaluation criteria. Finally, we discuss commonly encountered design flaws and other issues that can make information systems susceptible to attack.

Objectives:

Security Architecture and Design

A. Understand the fundamental concepts of security models (e.g., Confidentiality, Integrity, and Multi-Level Models)

B. Understand the components of information systems security evaluation models
   B.1 Product evaluation models (e.g., common criteria)
   B.2 Industry and international security implementation guidelines (e.g., PCI-DSS, ISO)

C. Understand security capabilities of information systems (e.g., memory protection, virtualization, trusted platform module)

Chapter 12 - Security Architecture Vulnerabilities, Threats, and Countermeasures

This chapter covers those underlying security concerns by conducting a brief survey of a field known as computer architecture: the physical design of computers from various components. We’ll examine each of the major physical components of a computing system—hardware and firmware—from a security perspective. Obviously, the detailed analysis of a system’s hardware components is not always a luxury available to you because of resource and time constraints. However, all security professionals should have at least a basic understanding of these concepts in case they encounter a security incident that reaches down to the system design level. The Security Architecture and Design domain addresses a wide range of concerns and issues, including secure design elements, security architecture, vulnerabilities, threats, and associated countermeasures.

Objectives:

Security Architecture and Design

D. Understand the vulnerabilities of security architectures
   D.1 System (e.g., covert channels, state attacks, emanations)
   D.2 Technology and process integration (e.g., single point of failure, service oriented architecture)
E. Understand software and system vulnerabilities and threats

E.1 Web-based (e.g., XML, SAML, OWASP)
E.2 Client-based (e.g., applets)
E.3 Server-based (e.g., data flow control)
E.5 Distributed systems (e.g., cloud computing, grid computing, peer to peer)

F. Understand countermeasure principles (e.g., defense in depth)

Chapter 13 - Security Operations

The Security Operations domain is focused on identifying and protecting critical information within an organization. There are several core security operations concepts that any organization needs to implement to provide basic security protection and these concepts are covered in the first section of this chapter. Resource protection ensures that media and other assets that are valuable to an organization are protected throughout the lifetime of the resource. Patch and vulnerability management controls ensure that systems are kept up-to-date and protected against known vulnerabilities. Configuration management helps ensure that systems are configured similarly, and change management protects against outages from unauthorized changes. Security audits of these controls provide assurances that the controls are in place and providing the desired protections.

Objectives:

A. Understand security operations concepts
   A.1 Need-to-know/least privilege
   A.2 Separation of duties and responsibilities
   A.3 Monitor special privileges (e.g., operators, administrators)
   A.4 Job rotation
   A.5 Marking, handling, storing, and destroying of sensitive information
   A.6 Record retention

B. Employ resource protection
B.1 Media management

B.2 Asset management (e.g., equipment life cycle, software licensing)

E. Implement and support patch and vulnerability management

F. Understand change and configuration management (e.g., versioning, baselining)

**Chapter 14 - Incident Management**

Incident management is an ongoing process and can help reduce future attacks by applying lessons learned to improve an organization’s security posture. Security incidents are often the result of an attack, and there are preventive measures an organization can take to protect against and detect attacks. Many of these measures are discussed in this chapter.

Objectives:

Security Operations

A. Manage Incident Response
   
   A.1 Detection
   
   A.2 Response
   
   A.3 Reporting
   
   A.4 Recovery
   
   A.5 Remediation and review (e.g., root cause analysis)

D. Implement preventative measures against attacks (e.g. malicious code, zero-day exploit, denial of service)

G. Understand system resilience and fault tolerance requirements

**Chapter 15 - Business Continuity Planning**

In this chapter, we'll explore the concepts behind business continuity planning. Resilient organizations have plans and procedures in place to help mitigate the effects a disaster has on
their continuing operations and to speed the return to normal operations. Recognizing the importance of planning for business continuity and disaster recovery, the organization (ISC)² designated these two processes as one of the 10 domains of the Common Body of Knowledge for the CISSP program.

Objectives:

Business Continuity and Disaster Recovery Planning

A. Understand business continuity requirements
   A.1 Develop and document project scope and plan

B. Conduct business impact analysis
   B.1 Identify and prioritize critical business functions
   B.2 Determine maximum tolerable downtime and other criteria
   B.3 Assess exposure to outages (e.g., local, regional, global)
   B.4 Define recovery objectives

E. Exercise, assess and maintain the plan (e.g., version control, distribution)

Chapter 16 - Disaster Recovery Planning

Disaster recovery planning (DRP) steps in where BCP leaves off. When a disaster strikes and a business continuity plan fails to prevent interruption of business activities, the disaster recovery plan kicks in and guides the actions of emergency-response personnel until the end goal is reached, which is to see the business restored to full operating capacity in its primary operations facilities.

Objectives:

Business Continuity and Disaster Recovery Planning

C. Develop recovery strategy
   C.1 Implement a backup storage strategy (e.g., offsite storage, electronic vaulting, tape rotation)
   C.2 Recovery site strategies
D. Understand disaster recovery process
   D.1 Response
   D.2 Personnel
   D.3 Communications
   D.4 Assessment
   D.5 Restoration
   D.6 Provide training

E. Exercise, assess and maintain the plan (e.g., version control, distribution)

Chapter 17 - Laws, Regulations, and Compliance

In this chapter, we’ll cover the various types of laws that deal with computer security issues. We'll examine the legal issues surrounding computer crime, privacy, intellectual property, and a number of other related topics. We'll also cover basic investigative techniques, including the pros and cons of calling in assistance from law enforcement.

Objectives:

Legal, Regulations, Investigations, and Compliance

A. Understand legal issues that pertain to information security internationally
   A.1 Licensing and intellectual property (e.g., copyright, trademark)
   A.2 Import/export
   A.3 Trans-border data flow
   A.4 Privacy

E. Understand compliance requirements and procedures
   E.1 Regulatory environment
   E.2 Audits
   E.3 Reporting
F. Ensure security in contractual agreements and procurement processes (e.g., cloud computing, outsourcing, vendor governance)

Chapter 18 - Incidents and Ethics

This chapter/domain deals with topics and issues related to computer crime laws and regulations, investigative techniques used to determine whether a computer crime has been committed and to collect evidence when appropriate, and ethics issues and code of conduct for the information security practitioner.

Objectives:

Legal, Regulations, Investigations, and Compliance

A. Understand legal issues that pertain to information security internationally

B. Understand professional ethics
   B.1 (ISC)² code of professional ethics
   B.2 Support organization’s code of ethics

C. Understand and support investigations
   C.1 Policies, roles and responsibilities (e.g. rules of engagement, authorization, scope)
   C.2 Incident handling and response
   C.3 Evidence collection and handling (e.g., chain of custody, interviewing)
   C.4 Reporting and documenting

D. Understand forensic procedures
   D.1 Media analysis
   D.2 Network analysis
   D.3 Software analysis
   D.4 Hardware/embedded device analysis
Chapter 19 - Physical Security Requirements

The purpose of physical security is to protect against physical threats. The following physical threats are among the most common: fire and smoke, water (rising/falling), earth movement (earthquakes, landslides, volcanoes), storms (wind, lightning, rain, snow, sleet, ice), sabotage/vandalism, explosion/destruction, building collapse, toxic materials, utility loss (power, heating, cooling, air, water), equipment failure, theft, and personnel loss (strikes, illness, access, transport). This chapter explores each of these issues and discusses safeguards and countermeasures to protect against them. In many cases, you’ll need a disaster recovery plan or a business continuity plan should a serious physical threat (such as an explosion, sabotage, or natural disaster) occur.

Objectives:

Physical (Environmental) Security

A. Understand site and facility design considerations

B. Support the implementation and operation of perimeter security (e.g., physical access control and monitoring, audit trails/access logs)

C. Support the implementation and operation of internal security (e.g., escort requirements/visitor control, keys and locks)

D. Support the implementation and operation of facilities security (e.g., technology convergence)

D.1 Communications and server rooms

D.2 Restricted and work area security

D.3 Data center security

D.4 Utilities and Heating, Ventilation, and Air Conditioning (HVAC) considerations

D.5 Water issues (e.g., leakage, flooding)

D.6 Fire prevention, detection, and suppression

E. Support the protection and securing of equipment

F. Understand personnel privacy and safety (e.g., duress, travel, monitoring)