

CramSession

The Original Study Guide



Over
4 Million
Downloaded

ISC2

CISSP

Certified Information Systems
Security Professional

Written by **Subject
Matter Experts**

Your **Trusted
Study Resource** for
Technical Certification

The **Most Popular
Study Guide** on the web

Table of Contents

CBK #1: Access Control Systems and Methodology	4
<i>Accounting phase</i>	<i>4</i>
CBK #2: Telecommunications and Network Security.....	6
Ports and Protocols.....	8
Cabling	8
Cabling	9
Network Access Techniques.....	9
CBK #3 Security Management Practices	12
Goals of Information Security.....	12
Important Information Security Concepts.....	12
Data Classification.....	13
<i>U.S. Government Classification Levels</i>	<i>13</i>
<i>Private Industry Classification Levels</i>	<i>13</i>
Security Management Hierarchy.....	13
Computer Incident Response Teams.....	14
Risk Management	14
<i>Risk Analysis (RA)</i>	<i>14</i>
<i>Risk Management Techniques</i>	<i>15</i>
Security Awareness Training	15
CBK #4: Applications and Systems Development.....	15
System Lifecycle	15
Application Environment	16
Databases	17
Expert Systems	17
Application and System Vulnerabilities and Threats.....	18
CBK #5: Cryptography	18
Simple Cryptosystems	19
<i>Substitution Ciphers.....</i>	<i>19</i>
<i>Transformation Ciphers</i>	<i>20</i>
<i>Vernam Ciphers.....</i>	<i>20</i>
<i>Running Key Ciphers.....</i>	<i>20</i>
Modern Cryptosystems	21
<i>Secret Key Cryptography.....</i>	<i>21</i>
<i>Public Key Cryptography</i>	<i>21</i>
Applied Cryptography.....	22
<i>Steganography.....</i>	<i>22</i>

<i>Digital Signatures</i>	22
<i>E-mail Encryption</i>	22
<i>Transaction Security</i>	22
Public Key Infrastructure	23
Cryptographic Attacks	23
CBK #6: Security Architecture and Models	24
Computer System Components	24
Processing.....	24
<i>Security Modes of Operation</i>	25
Access Control Models	25
Integrity Models	26
Rainbow Series	26
Trusted Computer System Evaluation Criteria.....	26
Common Criteria	28
Certification versus Accreditation.....	28
<i>DITSCAP</i>	28
Threats	29
CBK #7: Operational Security	29
General Principles of Operations Security	29
Workforce Security	29
Control Categories	30
<i>Operational Assurance</i>	30
<i>Lifecycle Assurance</i>	30
Change Control	31
Auditing	31
CBK #8: Business Continuity Planning and Disaster Recovery Planning	31
Business Continuity Planning.....	31
Disaster Recovery Planning.....	32
<i>Data Processing Continuity</i>	32
<i>Data Backups</i>	32
<i>Disaster Recovery Plan Testing</i>	33
CBK #9: Law, Investigation, and Ethics	34
Law	34
<i>Information Security Laws</i>	34
<i>Intellectual Property Laws</i>	35
Evidence.....	35
Investigation	36

Ethics..... 36

(ISC)² Code of Ethics..... 36

Internet Activities Board..... 36

CBK #10: Physical Security..... **37**

 Facility Security 37

Site Selection..... 37

Construction..... 37

Facility management..... 37

Emergency procedures..... 37

 Fire 37

 Fences..... 39

 Electrical Power..... 39

 Media Security..... 40

CBK #1: Access Control Systems and Methodology

Access control systems are designed to enforce the requirement that resources be available only to authorized individuals. The process of ensuring accountability for access to system resources includes four phases:

- ❖ Identification phase
- ❖ Authentication phase
- ❖ Authorization phase

Accounting phase

An access control system has three important concepts:

- ❖ **Subjects** of the access control system are those entities that may be assigned permissions.
- ❖ **Objects** are the types of resources that subjects may access.
- ❖ **Access permissions** are relationships between subjects and the objects they may access.

An **access control list (ACL)** contains **access control entries (ACEs)** that correspond to access permissions.

There are many different types of access controls:

- ❖ **Preventative controls** - Designed to prevent unwanted activity from occurring
- ❖ **Detective controls** - Provide a means of discovering unwanted activities that have occurred
- ❖ **Corrective controls** - Provide mechanisms for bringing a system back to its original state prior to the unwanted activity
- ❖ **Deterrent controls** - Used to discourage individuals from attempting to perform undesired activities
- ❖ **Compensatory controls** - Implemented to make up for deficiencies in other controls

Another way of categorizing access controls is by their mechanism of action. The three categories under this scheme are:

- ❖ **Administrative controls** - Consist of policies and procedures, disaster recovery plans, awareness training, security reviews and audits, background checks, review of vacation history, separation of duties, and job rotation
- ❖ **Logical/Technical controls** - Restrict access to systems and the protection of information. Encryption, smart cards, anti-virus software, audit trails, log files, ACLs, biometrics, and transmission protocols
- ❖ **Physical controls** - Protect access to the physical facilities housing information systems and include guards and building security, biometric access restrictions, protection of cables, file backups

There are several important principles to keep in mind when you are designing an access control system:

- ❖ **Principle of Least Privilege** - States that subjects of an access control system should have the minimum set of access permissions necessary to complete their assigned job functions
- ❖ **Principle of Separation of Duties and Responsibilities** - States that the ability to perform critical system functions should be divided among different individuals to minimize the risk of collusion
- ❖ **Need-to-Know** - States that users should only have access to information that they have a need to know to perform their assigned responsibilities.

There are four types of access control systems:

- ❖ Mandatory access control (MAC)
- ❖ Discretionary access control (DAC)
- ❖ Non-discretionary access control (NDAC)
- ❖ Lattice-based access control (LBAC)

Access control systems may also be classified by their location:

- ❖ Centralized access control systems
- ❖ Decentralized access control systems

There is a growing movement toward the use of **single sign-on (SSO)** technology to enable centralized authentication. Common SSO implementations include Kerberos, Secure European System for Applications in a Multivendor Environment (SESAME), and KryptoKnight.

There are many different types of authentication techniques, but they may all be divided into three broad factors:

- ❖ **Something you know.** The most common technique in this category is the use of a password or passphrase for authentication.
- ❖ **Something you have.** Examples are an access token, a physical key, or an identification card.
- ❖ **Something you are.** These techniques, known as **biometric authentication** techniques, include fingerprint scans, retinal scans, voiceprint identification, behavior patterns, and similar measures.

Access controls are vulnerable to a number of types of attack. These include:

- ❖ **Brute force** - In this type of attack, the attacker simply guesses passwords over and over again until eventually succeeding. Brute force attacks are especially effective against short passwords or cryptographic keys.
- ❖ **Dictionary** - In this type of attack, the attacker uses the password encryption algorithm to encrypt a dictionary of common words and then compares the encrypted words to the password file. When a match is found, the attacker has discovered a password. This type of attack makes it important to ensure that users don't have real-word passwords.
- ❖ **Spoofing** - These attacks occur when an individual or system poses as a third party. Spoofing attacks are especially effective against standard e-mail, which performs no sender authentication.
- ❖ **Denial of service (DoS)** - It is not necessary to break into a system to successfully attack it. Attackers can confuse the system into an inoperable state or flood it with so much traffic that it can't provide service to legitimate users. DoS can be just as effective as a successful penetration.
- ❖ **Man-in-the-middle** - A malicious individual might be able to convince two communicating parties that they are communicating with each other when they are both actually communicating with the intruder. The intruder passes all traffic through to the other end but may eavesdrop on the conversation or even alter the content of the communication.
- ❖ **Sniffer** - An individual who has access to a network may be able to install and run software like **tcpdump** or **ethereal** that allow a user to "sniff (or monitor) all traffic occurring on the same network segment.

Penetration tests are an effective way to assess the security of an access control system. In this type of attack, a "white hat hacker" poses as an outsider and attempts to gain access to the system without using legitimate administrative powers.

Intrusion detection systems (IDSs) are commonly used to detect malicious activity on a host or network. IDSs are divided based upon the **monitored environment** and the **detection methodology** that they implement.

The types of intrusion detection systems when classified by **monitored environment** include:

- ❖ **Host-based IDSs**
- ❖ **Network-based IDSs**

Intrusion prevention systems (IPSs) are a subset of IDSs that actually intervene when they detect an attack.

The types of intrusion detection systems when classified by **detection methodology** include:

- ❖ **Signature-based IDSs**
- ❖ **Anomaly-based IDSs**

CBK #2: Telecommunications and Network Security

Networked communications may be best thought of by using a number of different **models**. The **Open Systems Interconnection (OSI)** model from the International Standards Organization is the most commonly used model and consists of seven layers, as shown in Table 1.

Table 1 – Layers of the OSI Model

Layer Number	Layer Name	Description
7	<i>Application</i>	Security: Confidentiality, authentication, data integrity, non-repudiation Technology: Gateways Protocols: FTP, SNMP, SMTP, DNS, TFTP, NFS, S-HTTP
6	Presentation	Security: Confidentiality, authentication, encryption Technology: Gateways
5	Session	Security: None Technology: Gateways Protocols: RPC, SQL
4	Transport	Security: Confidentiality, authentication, integrity Technology: Gateways Protocols: TCP, UDP, SSL, SSH-2
3	Network	Security: Confidentiality, authentication, data integrity

		data integrity Technology: Virtual circuits, routers Protocols: IP, IPSec, ARP, RARP, ICMP
2	Data Link	Security: Confidentiality Technology: Bridges, switches Protocols: HDLC, PPTP, L2F, L2TP, Token Ring, Ethernet, PPP, and SLIP
1	Physical	Security: Confidentiality Technology: ISDN, repeaters, hubs Protocols: IEEE 802, IEEE 802.2, X.21, HSSI

Another common network model is the Department of Defense TCP/IP model, which has only four layers, as shown in Table 2.

Table 2 - Layers of the TCP/IP Model

Layer Number	Layer Name	Protocols
4	<i>Application</i>	--
3	Host-to-Host	TCP and UDP
2	Internet	IP, ARP, RARP, and ICMP
1	Network Access (Link)	--

Data encapsulation is process in which information from one packet is wrapped around or attached to the data of another packet. In the OSI model, each layer encapsulates the layer immediately above it.

The two common transport protocols are the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP). Table 3 compares and contrasts the two protocols.

Table 3 – TCP versus UDP

TCP	UDP
Acknowledged	Unacknowledged
Sequenced	Subsequence
Connection-oriented	Connectionless
Reliable	Unreliable
High overhead	Low overhead (faster)

TCP, UDP, and other Transport layer protocols rely upon the network protocol to provide data routing. The most common routing protocol, the Internet Protocol (IP) uses a hierarchical series of IP addresses to route traffic.

Ports and Protocols

Servers use [well-known ports](#) (in the range of 0 to 1023) to offer services to Internet hosts. Clients use **high-numbered ports** (in the range of 1024 to 65536) to initiate connections.

Common protocols and their associated well-known ports include:

- ❖ File Transfer Protocol (FTP) (ports 20 and 21)
- ❖ Secure Shell (SSH) (port 22)
- ❖ Telnet (port 23)
- ❖ Simple Mail Transfer Protocol (SMTP) (port 25)
- ❖ Domain Name Service (DNS) (port 53)
- ❖ Trivial File Transfer Protocol (TFTP) (port 69)
- ❖ Hypertext Transfer Protocol (HTTP) (port 80)
- ❖ Post Office Protocol v3 (POP3) (port 110)
- ❖ Simple Network Management Protocol (SNMP) (ports 161 and 162)
- ❖ Secure Hypertext Transfer Protocol (HTTPS) (port 443)

The **Address Resolution Protocol (ARP)** operates at the Data Link layer and resolves IP addresses into Media Access Control (MAC) addresses.

The **Reverse Address Resolution Protocol (RARP)** resolves MAC addresses into IP addresses.

Network address translation (NAT) is used to map private IP addresses to public IP address when data must cross between public and private networks. **Port address translation (PAT)** is similar, but all hosts share a small pool of public addresses.

Take Your Exam for Less!



Discount Exam Vouchers from PrepLogic

Why pay retail price for the exam when you can save up to **40%** with discount exam vouchers?

[Buy Your Voucher Now](#)

PrepLogic

Be Prepared. Be Confident. Get Certified.

Cabling

[Network cabling](#) comes in a variety of mediums:

- ❖ **Coaxial** cable uses an insulated copper conductor.
 - It is available in 50-ohm and 75-ohm resistances.
 - It is resistant to eavesdropping and electromagnetic interference.
 - It normally uses BNC connectors.
 - 10Base2 (Thinnet) coax can carry 10 Mbps up to 185 meters per network segment.
 - 10Base5 (Thicknet) coax can carry 10 Mbps up to 500 meters per network segment.
- ❖ **Twisted-pair** cabling uses pairs of conductors that are twisted around each other.
 - Unshielded twisted-pair (UTP) cable is inexpensive but susceptible to EMI.
 - Shielded twisted-pair (STP) cable is less susceptible to EMI but more expensive.
 - There are seven categories of twisted pair cable:
 - Cat 1 is not suitable for data communications.
 - Cat 2 is not suitable for networks but may be used to connect terminals to mainframes.
 - Cat 3 can carry 10 Mbps and is commonly used in 10BaseT Ethernets.
 - Cat 4 can carry 16 Mbps and is commonly used in Token Ring networks.
 - Cat 5 can carry 100 Mbps and is commonly used in 100BaseTX networks.
 - Cat 6 can carry 155 Mbps.
 - Cat 7 can carry 1 Gbps.
- ❖ **Fiber-optic** cabling is the most expensive type of conductor.
 - It uses light instead of electromagnetism so it is completely resistant to EMI.
 - It may be used for distances up to 2km.
 - It is difficult to install and manipulate.
 - It is the most resistant to eavesdropping.
- ❖ **Wireless networks** are becoming increasingly pervasive. They use radio frequencies to eliminate the need for conductors.

Network Access Techniques

Networks use a variety of access control techniques to determine who may "speak" on a network at any given time. Common techniques include:

- ❖ **Carrier Sense Multiple Access (CSMA)** - Is basically a free-for-all where systems check to see if a network is in use. If it's not, they simply start transmitting.
- ❖ **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)** - Networks require each host to ask for permission before transmitting. AppleTalk networks use CSMA/CA.
- ❖ **Carrier Sense Multiple Access with Collision Detection (CSMA/CD)** - Networks use a variant on CSMA where hosts transmit when they believe the network is clear but continue monitoring for other hosts. If they detect another host transmitting at the same time (a "collision") they stop transmitting and wait a random period of time to begin again. Ethernet uses CSMA/CD.

- ❖ **Token Ring** - Networks pass a logical token from host to host. A host may transmit only when it possesses the token.
- ❖ **Polling** - Networks use a master/slave hierarchy. The master system asks ("polls") each system on the network to see if it has traffic. When a system is polled, it may transmit any data in the queue.

There are several types of data networks in existence:

- ❖ **Local area networks (LANs)** cover a limited geographical area (typically a building or floor).
- ❖ **Metropolitan area networks (MANs)**, also known as campus networks, connect LANs within a defined geographical area, such as buildings within the same city.
- ❖ **Wide area networks (WANs)** connect a number of smaller networks
- ❖ The **Internet** is a global network connecting most sites worldwide
- ❖ **Intranets** are private networks limited to a particular organization
- ❖ **Extranets** are extensions of an Intranet to outside organizations

There are three methods of network communications in IPv4:

- ❖ **Broadcast** - Communications are from a single host directed to all hosts
- ❖ **Unicast** - Communications are between two individual hosts
- ❖ **Multicast** - Communications are from a single host to many separate hosts

LANs may be laid out using one of several topologies. The physical topology may differ from the logical topology. Common topologies include:

- ❖ In a **bus** topology, all hosts are connected to a single conductor. That conductor is a SPOF. Ethernet uses a logical bus topology.
- ❖ In a **ring** topology, each host is connected to two adjacent hosts, forming a ring. In this topology, any single host is a SPOF. Token Ring uses a logical ring topology.
- ❖ In a **star** topology, all hosts are connected to a central hub (or other networking device). The networking device is a SPOF. Ethernet and Token Ring can both use a physical star topology.
- ❖ In a **tree** topology, several busses or stars are connected together retaining the SPOFs of those methodologies. Ethernet can use a physical tree topology.
- ❖ In a **mesh** topology, there are several links between hosts. No host serves as a SPOF.

There are a number of common **network devices** found on LANs and WANs. These include:

- ❖ Repeaters amplify signals and operate at OSI Layer 1.
- ❖ Hubs are simply repeaters with multiple ports and operate at OSI Layer 1.
- ❖ Bridges connect similar networks and operate at OSI Layer 2.
- ❖ Switches block broadcasts and connect similar networks. They may be used to create virtual LANs (VLANs) to enhance security. Switches are also known as intelligent hubs. They operate at either OSI Layer 2 or OSI Layer 3.
- ❖ Routers also block broadcasts and connect similar networks. They operate at OSI Layer 3.

- ❖ Gateways connect dissimilar networks and operate at OSI Layer 7.

WANs may be implemented using a number of different technologies including:

- ❖ **Dedicated lines** include circuits such as T1, T3, E1, and E3 circuits, which are point-to-point links between networks.
- ❖ **Nondedicated lines** include DSL and ISDN circuits. They operate over the telephone network.
- ❖ **X.25 networks** use packet-switching with permanent virtual circuits (PVCs).
- ❖ **Frame Relay networks** also use PVCs but allow multiple PVCs on a single line.
- ❖ **ATM networks** use 53-byte cells and are able to allocate bandwidth on demand.

You can avoid SPOFs on a server basis by using either **mirrored servers** or **server clusters**.

Redundant Arrays of Inexpensive Disks (RAID) are often used to avoid SPOFs in servers resulting from hardware failures. There are many different levels of RAID that provide different levels of protection. The levels of RAID protection are:

- ❖ **RAID 0** - Disk striping consists of using several disks to store different pieces of data. It increases performance but **offers no added security**.
- ❖ **RAID 1** - Disk mirroring consists of maintaining two disks that are mirror images of each other. This is highly effective in terms of redundancy but also quite slow and wasteful in terms of disk space.
- ❖ **RAID 5** - Interleave parity uses a minimum of three physical disks and stripes data blocks and a parity block across the disks. It is configured such that the failure of any one disk won't result in the loss of data. The administrator simply needs to replace the disk and regenerate the RAID array.
- ❖ **RAID 10** - Uses two striped disk sets that are mirror images of each other.

Firewalls are network devices that sit between a protected network and an untrusted network and filter communications entering the protected network. There are four major types of firewalls:

- ❖ **Packet filtering (screening router)** - Examines source and destination address of IP packet. Can deny access to specific applications or services based on ACL. First generation firewall. Operates at network or transport layer
- ❖ **Application-level firewall (proxy server, application-layer gateway)** - Second generation. Reduces network performance. Circuit level firewall is a variation, creates virtual circuit between client and server
- ❖ **Stateful inspection firewall** - Third generation. Packets are captured by an inspection engine. Can be used to track connectionless protocols like UDP
- ❖ **Dynamic packet filtering firewalls** - Mostly used for UDP. Fourth generation
- ❖ **Firewall architectures:** Packet-filtering routers, Screened host systems, Dual-homed host firewalls, Screened subnet firewalls

Virtual private networks (VPNs) create secure communications links over inherently insecure networks, such as the Internet.

Common VPN protocols include:

- ❖ The **Point-to-Point Tunneling Protocol (PPTP)** is based upon the Point-to-Point Protocol (PPP) and allows the use of several authentication techniques, including: CHAP, MS-CHAP, PAP, EAP and SPAP
- ❖ **Layer Two Forwarding (L2F)** is a proprietary VPN protocol developed by Cisco that does not support encryption and is not commonly used.
- ❖ **Layer Two Tunneling Protocol (L2TP)** combines elements of PPTP and L2F. It typically uses IPsec for security.
- ❖ **IPsec** is the most common VPN protocol in use today. It operates in two different modes:
 - In **tunnel mode**, the entire data packet is encrypted and encased in an IPsec packet.
 - In **transport mode**, only the datagram is encrypted, not the header

CBK #3 Security Management Practices

Goals of Information Security

There are three main goals of any information security program that are encapsulated by the CIA Triad:

- ❖ **Confidentiality** - Ensures that private information remains protected from unauthorized disclosure. Confidentiality is often enforced through the use of access controls, encryption, classification policies and user training.
- ❖ **Integrity** - Ensures that data isn't modified in an unintended manner, either through accidental modification by authorized individuals or malicious modification by any individual (authorized or unauthorized). Integrity is often enforced through the use of cryptographic hashes and checksums.
- ❖ **Availability** - Ensures that data is always available for the use of authorized individuals. Availability is often enforced through the use of redundant systems, system backups, disaster recovery/business continuity plans and prevention of denial of service attacks.

Important Information Security Concepts

In addition to the CIA and DAD triads, you should be familiar with the following concepts of information security:

- ❖ **Identification** - The means by which users make an identity claim to the system.
- ❖ **Authentication** - The means by which the system validates the user's identity.
- ❖ **Authorization** - The system's ability to determine which activities may be permitted to an identified and authenticated user.
- ❖ **Accountability** - The system's ability to determine actions of users within the system and attribute those actions to individually identifiable users. This is supported by the use of audit trails and logs.
- ❖ **Non-repudiation** - The inability of the sender of a message to refute sending the message in the first place.
- ❖ **Privacy** - The user's level of confidence that their data is safe from unauthorized disclosure.

Data Classification

Data classification systems are often used to label data according to its sensitivity level. Classification levels are often used to specify the levels of control that must be in place for systems that store, process, or transmit sensitive information.

U.S. Government Classification Levels

The [classification system](#) used by the federal government has five main classification levels (listed in order of ascending sensitivity):

- ❖ Unclassified
- ❖ Sensitive but Unclassified (SBU) or For Official Use Only (FOUO)
- ❖ Confidential
- ❖ Secret
- ❖ Top Secret

Private Industry Classification Levels

Private industry uses a number of different classification systems. One common example appears below (again in order of ascending sensitivity):

- ❖ Public
- ❖ Internal
- ❖ Confidential
- ❖ Restricted
- ❖ Highly Restricted

Private industry classification systems may also have fewer levels. It's not uncommon to see a three-level classification system (public, confidential, restricted). The labels assigned to these systems often vary from company to company.

Security Management Hierarchy

Responsibility for security policies lies within the highest levels of the organization. Senior management should ensure policies are in place and support the policy development effort.

Most organizations have a security management hierarchy consisting of four levels of documents:

- ❖ **Security policies** - Consist of broad statements about the organization's commitment to information security and the goals of the program.



Who Do You Trust for Your Certification Training?

PrepLogic's dependable training products help thousands of professionals and students worldwide achieve their certification goals for A+, MCSE, Network+, CCNA, CEH, PMP, and more.

PrepLogic Comprehensive Training Tools:

- CBT • Practice Exams • Audio Training
- Mega Guides • Discount Exam Vouchers

For Free Product Demos,
[Click Here.](#)

PrepLogic
Be Prepared. Be Confident. Get Certified.

- ❖ **Security standards** - Provide specific technical requirements for security mechanisms.
- ❖ **Security guidelines** - Offer general guidance in areas of information security where formal policies and standards don't exist.
- ❖ **Security procedures** - Provide step-by-step instructions for performing specific security-related tasks.

Computer Incident Response Teams

An organization's Computer Incident Response Team (CIRT) is often a formal mechanism for responding to any incident that appears to be a violation of a security policy, standard, guideline or procedure that threatens the overall information security of the organization.

Risk Management

Prime objective of security controls is to reduce effects of threats and vulnerabilities to a level that is tolerable (i.e., mitigate risk). It is important to remember that the entire risk management process should be based upon prior determination of the value of particular data elements. It would be nonsensical to spend more on protecting a data element than that data element is worth in the first place.

Risk Analysis (RA)

A risk is a potential harm or loss to a system; the probability that a threat will materialize.

Key Terms

- ❖ **Asset** – A resource, process, product, system, etc.
- ❖ **Threat** – Any event that causes an undesirable impact on an organization.
- ❖ **Vulnerability** – Absence of a safeguard.
- ❖ **RM triple:** Asset, threat, and vulnerability.
- ❖ **Exploit** – A technical means to exploit a vulnerability.
- ❖ **Exposure Factor (EF)** – Percentage loss a realized threat would have on an asset. A hardware failure on a critical system may result in 100% loss.
- ❖ **Single Loss Expectancy (SLE)** – Loss from a single threat. $SLE = \text{Asset Value}(\$) \times EF$.
- ❖ **Annualized Rate of Occurrence (ARO)** – Estimated frequency in which a threat is expected to occur. The ARO range is from 0 (never) to a large number (e.g., minor threats, such as misspellings).
- ❖ **Annualized Loss Expectancy (ALE)** – The total of the SLE multiplied by the ARO. $ALE = SLE \times ARO$
- ❖ **Safeguard** – Control or countermeasure to reduce risk associated with a threat.

Elements of Risk Analysis

- ❖ **Quantitative RA** – Assigns objective dollar costs to assets
- ❖ **Qualitative RA** – Intangible values of data loss and other issues that are not pure hard costs (i.e. high, medium and low risk categories)

Risk Analysis Steps

1. **Identify asset.** Estimate potential losses to assets by determining their values.
2. **Identify threats.** Analyze potential threats to assets.
3. **Determine risk.** Qualitatively and/or quantitatively evaluate the degree of risk.

Risk Management Techniques

Once you have identified risks, you may choose one or more of the following four risk management techniques for each identified risk:

- ❖ **Mitigate the risk** – Put controls in place that reduce the risk to the organization.
- ❖ **Avoid the risk** – Change the organization's activities to completely avoid the risk.
- ❖ **Accept the risk** – Acknowledge the risk and take no action whatsoever.
- ❖ **Transfer the risk** – Place the burden of the risk on someone else.

Security Awareness Training

All organizations should provide some level of information security training to all employees. The type, depth, and scope of the training should vary based on the needs of the organization and the individual responsibilities of the trainee with respect to information security.

CBK #4: Applications and Systems Development

Security must be planned and managed throughout the development process for applications and systems. Security that is "bolted on" after the fact is ordinarily expensive and less effective than security integrated from the start of the design process.

System Lifecycle

Phases of the system lifecycle include:

- ❖ Project initiation
- ❖ Functional design
- ❖ System design and specification
- ❖ Software development
- ❖ Installation
- ❖ Maintenance
- ❖ Revision

Common Software Development LifeCycle (SDLC) models include:

- ❖ Waterfall model allows for iteration back to the previous phase of development
- ❖ Modified waterfall model incorporates verification and validation
- ❖ Spiral model uses iterations of the entire process gradually refining the finished product

All phases of the lifecycle should include testing for security vulnerabilities. Maintenance should take place in a controlled environment using a formal change control system. Configuration management should be used to ensure consistency in production environments.

The Software Engineering Institute's (SEI's) Capability Maturity Model ([CMM](#)) consists of five levels of ascending maturity:

- ❖ Level 1: Initiating
- ❖ Level 2: Repeatable
- ❖ Level 3: Defined
- ❖ Level 4: Managed
- ❖ Level 5: Optimized

The IDEAL model (based on CMM) also has five phases:

- ❖ Level 1: Initiating
- ❖ Level 2: Diagnosing
- ❖ Level 3: Establishing
- ❖ Level 4: Acting
- ❖ Level 5: Learning

Formal engineering techniques are sometimes applied to software development in Computer Aided Software Engineering (CASE).

Application Environment

Programming languages are generally considered to belong to a specific generation of languages. The accepted generations are:

- ❖ **First Generation Language (1GL)** – Otherwise known as machine language, 1GLs use the native binary format recognized by the computer.
- ❖ **Second Generation Language (2GL)** – Otherwise known as assembly language, 2GLs consist of basic instructions that are specific to the hardware used but still may be interpreted by humans.
- ❖ **Third Generation Language (3GL)** – Otherwise known as high-level languages, 3GLs are compiled or interpreted from a human-friendly format to machine language. 3GLs include Java, C, Basic, FORTRAN and other common programming languages
- ❖ **Fourth Generation Language (4GL)** – 4GLs are designed to resemble natural language as much as possible. Structured Query Language (SQL) is a common example.

- ❖ **Fifth Generation Language (5GL)** – 5GLs use visual tools to create code in a 3GL or 4GL. Microsoft's Visual Studio is a good example.

Programs may be written in two types of high-level languages:

- ❖ **Interpreted programs** - Remain in the original programming language..
- ❖ **Compiled programs** - Are converted into machine language all at once by the programmer using a compiler.

Object-oriented languages use individual objects that interact with each other to create programmed systems. Components of an object-oriented environment include: Attributes, Methods, Class and Instance.

Databases

Modern databases follow the **relational database management system (RDBMS) model**. This model is based on the concept of tables of data with rows representing individual records and columns representing attributes.

- ❖ Rows, records, and tuples are synonymous in RDBMSs.
- ❖ A table's **cardinality** is equal to the number of rows in the table.
- ❖ Attributes and columns are synonymous in RDBMSs.
- ❖ A table's **degree** is equal to the number of columns in the table.
- ❖ Most relational databases use SQL for user interaction with the database and its data.

RDBMS systems rely upon **keys** to maintain record consistency.

- ❖ A **candidate key** is any combination of attributes that uniquely identifies the rows in a table. A given table may have many candidate keys.
- ❖ Each table has one **primary key** that is the candidate key selected by the database administrator to uniquely identify the rows of the table. The uniqueness of the primary key is enforced by the database system's management engine.
- ❖ **Foreign keys** are used to reference other tables in the same database.
- ❖ Databases should be **normalized** to ensure that attributes in a table are dependent only upon the primary key.

Database integrity mechanisms are essential to ensure the reliability and consistency of the data:

- ❖ **Concurrency controls** - Ensure that two processes don't modify the data at the same time.
- ❖ **Referential integrity controls** - Ensure that foreign key values actually correspond to an entry in the referenced table.
- ❖ **Transactions** - Ensure that groups of related statements either succeed or fail as a group. All transactions must meet the following standard criteria: Atomic, Consistent, Isolated, and Durable.

Based on their names, these criteria are known as the ACID criteria.

Expert Systems

Expert systems attempt to use a series of rules to mimic the behavior of a human expert in decision-making. These systems often use **fuzzy logic** to determine the likelihood that a certain condition exists.

Neural networks are a common type of artificial intelligence system used to predict future events based on a large history of past events.

Application and System Vulnerabilities and Threats

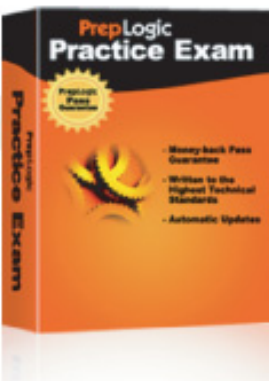
- ❖ **Viruses** are malicious code objects that spread from system to system based on some user intervention.
- ❖ **Worms** are similar to viruses and use many of the same infection vectors but spread from system to system without user intervention.
- ❖ **Trojan horses** disguise themselves as legitimate programs to trick the user into executing them but then perform malicious activity in the background.
- ❖ **Logic bombs** wait for a certain event to occur and then deliver their payload. Logic bombs are often tied to a particular date, time, holiday, or system event (such as accessing a particular Web site).
- ❖ **Denial of Service (DoS) attacks** attempt to prevent legitimate use of the system by disabling it in some way. DoS attacks typically either flood the target system with so much activity that it is unable to respond to legitimate requests or use specific exploits to disable the target system.

Many types of malicious code may be blocked through the use of antivirus software at both the network/enterprise and host level. Typically, antivirus software uses signature detection to identify known viruses. The signature definition files must be updated on a frequent basis.

- ❖ **Honeypots** are systems specifically designed to attract attackers in an attempt to study their activity and/or deflect them from attacking high-value targets. **Honeynets** are networks of honeypots, commonly made up of varied operating systems and patch levels.
- ❖ **Darknets** are monitored IP subnets that should have no legitimate activity. (There are no authorized hosts in the darknet address range.) Therefore, any activity with a destination address in the darknet may be presumed malicious.

CBK #5: Cryptography

- ❖ **Cryptology** - The science that involves the use of codes and ciphers to obscure the meaning of a message. It consists of two subdisciplines: cryptography and cryptanalysis.
- ❖ **Cryptography** - The science of protecting data so that it may be stored and transmitted between parties while preserving confidentiality and/or integrity.
- ❖ **Cryptanalysis** - The science of breaking cryptographic algorithms to obtain the secret message without authorization.
- ❖ **Cryptosystems** - Sets of techniques that implement cryptography. The key elements of a cryptosystem are:



Are You Ready to Take the Exam?

Comprehensive Exam Preparation:

- Progress tracking
- Detailed answers and explanations
- Packed with quality practice questions
- Customizable learning features

[Try a Demo Now](#)

A+, MCSE, CCNA, CEH,
CISSP, PMP, and more.

PrepLogic
Be Prepared. Be Confident. Get Certified

- **Algorithm** - The mathematical function used to encrypt and decrypt messages.
- **Key** - The binary sequence used to provide secrecy to the algorithm. Different algorithms use public/private keypairs or secret keys.
- **Plaintext** - The original message in an unencrypted, readable form.
- **Ciphertext** - The encrypted version of the message, unreadable without use of the correct algorithm and key.
- **Encryption** - The practice of transforming plaintext into ciphertext with an algorithm and key.
- **Decryption** - The practice of transforming ciphertext into plaintext with an algorithm and key
- ❖ **Codes** - Symbols or words to represent other words or phrases.
- ❖ **Ciphers** - Mathematical functions to transform bits or characters into other bits or characters. Ciphers are used to ensure confidentiality and/or integrity between trusted parties.
 - **Block ciphers** - Work on plaintext and ciphertext in chunks of a discrete size.
 - **Stream ciphers** - Work on plaintext and ciphertext in a bitwise or characterwise fashion.
- ❖ **Nonces** - Random numbers used to introduce unpredictability into a cryptosystem.

Simple Cryptosystems

Before discussing modern cryptosystems, it is necessary to have a brief understanding of basic cryptosystems.

Substitution Ciphers

Substitution ciphers simply replace one character with another. The simplest form of substitution cipher is the "Captain Crunch decoder ring," on which each letter of the alphabet simply maps to another letter.

The **Caesar cipher** is a historical substitution cipher that is generated by shifting each character three places to the right. ("A" becomes "D", "B" becomes "E", etc.) The full Caesar cipher is shown as follows:

Plaintext	ABCDEFGHIJKLMN OPQRSTUVWXYZ
Ciphertext	DEFGHIJKLMN OPQRSTUVWXYZABC

Basic substitution ciphers provide practically no confidentiality as they are simple to defeat using **frequency analysis**. For example, the most commonly used letters in the English language are E, T, A, O and N. Therefore, if you look at the ciphertext and determine the five most commonly used letters, they most probably map to E, T, A, O and N. The rest of the cryptosystem may be deduced in a similar fashion.

Polyalphabetic substitution ciphers overcome this limitation by using multiple alphabets on a rotating basis but they are subject to more advanced cryptanalytic techniques.

Transformation Ciphers

Transformation ciphers move the letters of a message around in a manner that obscures their meaning. For example, you could perform a **columnar transposition** by taking the message "I wish to ensure the confidentiality and integrity of this message" and writing it in six columns as follows:

I	W	I	S	H	T
O	E	N	S	U	R
E	T	H	E	C	O
N	F	I	D	E	N
T	I	A	L	I	T
Y	A	N	D	I	N
T	E	G	R	I	T
Y	O	F	T	H	I
S	M	E	S	S	A
G	E				

To create the ciphertext, you simply read down the columns instead of across the rows to get:

IOENTYTYSGWETFIAEOMEINHIANGFESSEDLDRTSHUCEIIHSTRONTNTIA

Numerous variations exist that use different numbers of columns and different transformation techniques.

Vernam Ciphers

Vernam ciphers are the only truly unbreakable ciphers. They make use of a "one-time pad" that uses a new key for each message, preventing most cryptanalytic techniques. The length of the key is equal to the length of the message.

The problem with Vernam ciphers is key distribution. You must be able to secretly exchange keys that are just as long as the message. Presumably, if you have the ability to secretly exchange the keys, you could simply use that same capability to exchange the secret message instead!

However, Vernam ciphers are useful when you have the ability to exchange the keys securely now but may not have that capability in the future. For example, a spy could physically obtain the one-time pads in bulk while at headquarters and then use them to exchange messages in the field.

Running Key Ciphers

Running key ciphers use an extremely long key, usually drawn from a source such as a book. (They are also known as "book ciphers".) The two parties use the same key source and perform modulo arithmetic on the message with the key to perform encryption and decryption.

Modern Cryptosystems

Modern cryptosystems are divided into two classes. Secret key (or symmetric) cryptosystems use a single key for a communication while public key (or asymmetric) cryptosystems use pairs of keys for each communicating party.

Secret Key Cryptography

In a secret key cryptosystem, the two parties communicate with each other using the same secret key to encrypt and decrypt messages.

Data Encryption Standard (DES)

DES was once the federal government's only approved symmetric cryptosystem for the exchange of classified information among government entities.

- ❖ DES was created in 1972 and uses a 56-bit key, which was considered extremely secure at the time.
- ❖ DES operates on 64-bit blocks of data.
- ❖ Four modes of encryption are available: Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB) and Output Feedback (OFB)
- ❖ CBC and CFB modes have the inherent problem that errors propagate. An error in the transmission of one block affects the ability to decrypt subsequent blocks.

DES is now considered too weak to provide confidentiality, because it is possible to perform a brute-force attack against its relatively short key.

An alternative to DES is Triple DES (3DES), which encrypts the same message three times using two or three different keys. This increases the effective length of the key to 168 bits.

Advanced Encryption Standard

The **Rijndael block cipher** was selected in a competition to succeed DES as the Advanced Encryption Standard (AES). Its use is mandated by a Federal Information Processing Standard ([FIPS-197](#)). AES uses a variable length key of 128, 192, or 256 bits and operates on 128-bit blocks of data.

Public Key Cryptography

In a public key (asymmetric) cryptosystem, each user has a pair of keys: one public and one private.

- ❖ The public key is freely shared with all users of the cryptosystem whereas the private key is maintained as a personal secret.
- ❖ A message encrypted with one key in the pair may only be decrypted with the other key from the same pair.
- ❖ When user X wants to send an encrypted message to user Y, he encrypts it with user Y's public key. It may then only be decrypted by user Y's private key. Therefore, user Y (the only one with knowledge of Y's private key) is the only user that can decrypt the message. User X cannot decrypt the message that he himself encrypted.
- ❖ Key exchange is not an issue in public key cryptography. The only thing a user needs to communicate with another user is knowledge of the other user's public key, something which may be freely exchanged.
- ❖ Public key cryptography is much slower than private key cryptography. Therefore, public key cryptosystems are commonly used to create an initial session between two users, who then exchange a symmetric session key that they use for the remainder of the session.

- ❖ Keys used in public key cryptography must be longer than keys used for private key cryptography to achieve the same level of security.

RSA Algorithm

The RSA algorithm (developed by Rivest, Shamir, and Adelman) is one of the most common public key cryptosystems. It is based on the difficulty of factoring a number that is the product of two very large prime numbers. It provides confidentiality, integrity, and nonrepudiation.

Diffie-Hellman Key Exchange

Diffie-Hellman key exchange is based on the algorithm developed by Whitfield Diffie and Martin Hellman. It allows two users who do not know each other to securely exchange a secret key for symmetric communication.

Applied Cryptography

Cryptosystems are used in a number of ways in our modern computing environment.

Steganography

Steganography is the use of image manipulation techniques to hide information in images. Steganography has obtained a bad name due to its prolific use among purveyors of child pornography.

Digital Signatures

Digital signatures use asymmetric algorithms to certify the integrity of a message while in transit and ensure nonrepudiation.

The security of the digital signature process depends upon the strength of the hash function used:

- ❖ Message Digest 5 (MD5) hashes a message of arbitrary length to a 128-bit digest.
- ❖ Secure Hash Algorithm (SHA) is an implementation of the Secure Hash Standard (SHS).
 - SHA-1 produces a 160-bit digest.
 - SHA-256 uses the same algorithm to produce a 256-bit digest.
 - SHA-512 uses the same algorithm to produce a 512-bit digest.

E-mail Encryption

E-mail encryption is commonly used to provide confidentiality, integrity, and non-repudiation for messages. Encryption functionality is now built into most commercial e-mail software.

E-mail encryption standards include: S/MIME, MOSS, PEM and PGP

Transaction Security

A number of standards have been proposed for secure financial transactions over the Internet:

- ❖ **Secure Sockets Layer (SSL)** - A standard proposed by Netscape and commonly used today to secure communications over the Web and other Internet protocols. It supports RSA, IDEA, DES, 3DES, and MD5.
- ❖ **Secure Electronic Transactions (SET)** - A standard proposed by credit card issuers in 1997 but never became widely adopted. It used DES and RSA algorithms.

- ❖ **Transport Layer Security (TLS)** – A follow-on protocol to SSL used to secure application layer protocols including SMTP, IMAP, POP3, and HTTP. It uses public key cryptography to initiate a session and then exchange a symmetric key.

Public Key Infrastructure

The Public Key Infrastructure ([PKI](#)) solves the problem of distributing authenticated public keys among users of an asymmetric cryptosystem. PKI is based on the use of **X.509v3 certificates**, and works as follows:

1. A user submits his public key to a **certification authority (CA)** along with proof of identity.
2. The CA issues an X.509 certificate that contains: Serial number, Version number, Cryptosystem information, User's identity, Validity dates and Signature of the certificate authority.
3. The CA sends the certificate to the user who may then distribute it to anyone needing the user's public key.
4. Recipients of the certificate may verify it by confirming the digital signature contained within the certificate using the CA's public key.

As the CA is the one actually signing the user's key, the PKI model works only if all users of the system trust the CA's determination of a user's identity.

Cryptographic Attacks

There are a number of attacks possible against cryptographic systems:

- ❖ **Brute-force** - Guess the key by exhaustively checking all possibilities. Brute-force attacks are more effective against shorter-length keys, because there are fewer possibilities.
- ❖ **Vulnerability exploits** - Look for weaknesses in the cryptographic algorithm itself or a particular software/hardware implementation of a cryptographic algorithm.
- ❖ **Statistical** - Use mathematical analysis of a message to break the cryptosystem. One example is the frequency analysis discussed as an attack against substitution ciphers.
- ❖ **Known plaintext** - Begin with the attacker having knowledge of a plaintext message and the corresponding ciphertext.
- ❖ **Chosen plaintext** - Occur when the attacker is able to determine the ciphertext that corresponds to a plaintext message of his or her choosing.
- ❖ **Chosen ciphertext** - Occur when the attacker is able to determine the plaintext message that corresponds to a ciphertext of his or her choosing.
- ❖ **Birthday** - Occur when the attacker is able to find two plaintext messages that generate the same ciphertext.
- ❖ **Meet-in-the-middle** - Occur when an attacker has the plaintext and ciphertext and is able to use both simultaneously to determine the secret key.
- ❖ **Man-in-the-middle** - Occur when the attacker is able to trick both communicating parties into thinking they are communicating with each other when they are both really communicating with the attacker who relays messages between the two.
- ❖ **Replay** - Occur when an attacker is able to obtain the ciphertext and later use it to impersonate the transmitter by simply using the same ciphertext, even though she may not even know the corresponding plaintext.

CBK #6: Security Architecture and Models

Computer System Components

The major components of a computer are the central processing unit (CPU), memory, and input/output devices.

Memory management requires the use of protection techniques to prevent processes from accessing memory space not allocated to them.

Memory is more than just random access memory (RAM). In the general sense, there are a number of types of memory:

- ❖ **Real storage** - Consists of temporary storage available to the computer, usually in the form of RAM.
- ❖ **Secondary storage** - Includes nonvolatile memory sources, such as CD-ROMs, hard disks, and universal serial bus (USB) memory sticks.
- ❖ **Virtual memory** - Uses secondary storage to imitate primary storage.
- ❖ **Sequential memory** - Must be accessed in order from beginning to end. Tapes are the most common example.
- ❖ **RAM** - May be static or dynamic. Dynamic RAM must be refreshed or it loses its charge.
- ❖ **Read-only memory (ROM)** - Retains its state even when the computer is powered off. There are two special cases of ROM: EPROM and EEPROM

The CPU has four distinct operating states: Ready State, Supervisory State, Problem State and Wait State.

Processing

A **process** is an executing program with its own memory space. Each process can consist of multiple **threads**, or streams of execution.

High-performance systems can handle multiple processes in different manners:

- ❖ **Multithreading systems** - Process multiple threads simultaneously
- ❖ **Multitasking systems** - Process multiple processes simultaneously
- ❖ **Multiprocessing systems** - Use more than one processor simultaneously

The operating system uses a ring protection model to define security models. The rings are:

- ❖ **Ring 0** - Kernel
- ❖ **Ring 1** - Remaining OS components



The PrepLogic Mega Guide

PrepLogic took the CramSession Study Guide and made it better!

- Over 100 pages
- More in-depth content
- Expanded resources
- Includes review practice questions

Get \$10 Off
Get it Now

Coupon Code: **MEGA10**

A+, MCSE, CCNA, CEH,
CISSP, PMP, and more.

PrepLogic
Be Prepared. Be Confident. Get Certified.

Get this **Study Guide and many more** for **FREE** at

CramSession
www.cramsession.com

- ❖ **Ring 2** - Input/output software
- ❖ **Ring 3** - User-level applications

Processes running in a particular ring can access resources only in the same ring or a higher ring. For example, the kernel can access any resources, but other OS components cannot access the kernel.

Security Modes of Operation

- ❖ **Dedicated Security mode** - Each subject must have clearance for all information on the system and a valid "need to know" for all information.
- ❖ **System High Security mode** - Each subject must have clearance for all information on the system and a valid need to know some of the information. All users may not have a need to know.
- ❖ **Compartmented Security mode** - Each subject must have clearance for most restricted information on the system and valid need to know.
- ❖ **Multilevel mode** - Some subjects do not have clearance for all information. Each subject has a need to know for all information to which they will have access.

The **Trusted Computing Base (TCB)** is the combination of protection mechanisms within a system.

- ❖ The **security perimeter** is a boundary separating the TCB from the remainder of the system. The TCB must be tamperproof and non-compromisable.
- ❖ **Security Kernel** consists of hardware, software, and firmware elements of the TCB that implement the reference monitor concept.
- ❖ The **reference monitor** is a system component that enforces access controls on an object. The reference monitor concept is an abstract machine that mediates all access of subject to objects. Must be verified correct.

Layering and **data hiding** are used to protect resources assigned to one protection domain from processes in another protection domain.

Access Control Models

There are four access control models:

- ❖ The **state machine model** allows the operating system to transition only between a series of well-defined states.
- ❖ The **access matrix model** uses a combination of Read, Write, and Execute permissions assigned to various users. Each row in the matrix represents a user and each column represents a resource. The columns are also called **access control lists (ACLs)** and the rows are called **access control entries (ACEs)**.
- ❖ The **take-grant model** uses directed graphs to illustrate the security permissions that one object can take from another object and those that an object can grant to another object.
- ❖ The **Bell-LaPadua model** is a lattice-based model designed to strictly enforce the military's Mandatory Access Control (MAC) model.
 - Information can never flow from a high level to a lower level (that is, a user with Secret access permissions can never access Top Secret data). This is the "no read up" or "Simple Security" rule.
 - This model requires ensuring that users can never write information to a lower clearance level (that is, a user accessing Top Secret data can never write that data to a Secret file). This is the "no write down" or "-Property" rule.

Integrity Models

There are two integrity models to consider:

- ❖ The **Biba model** is a lattice-based model that is similar to the Bell-LaPadua model. It has two rules:
 - Users can never write information to a higher security level (that is, a user with Secret access permissions can never write to a Top Secret file). This is the "no write up" rule or "Simple Integrity Axiom."
 - Information can never flow from a low level to a higher level (that is, a user with Top Secret access permissions cannot read information at a Secret level). This is the "no read down" rule or "*-Integrity Axiom."
- ❖ The **Clark-Wilson model** enforces separation of duties to maintain data integrity.

Rainbow Series

In 1985, the National Computer Security Center published a series of books identified by the color of their covers. Major works in this series include:

- ❖ The **Orange Book** includes the DoD Trusted Computer System Evaluation Criteria (TCSEC).
- ❖ The **Red Book** is the Trusted Network Interpretation of the TCSEC.
- ❖ The **Purple Book** is the DoD Trusted Database Management System.
- ❖ The **Green Book** is the DoD Password Management Guideline.
- ❖ The **Amber Book** is the Guide to Understanding Configuration Management in Trusted Systems.

Trusted Computer System Evaluation Criteria

The criteria for evaluating systems, as specified in the TCSEC are:

- ❖ **Security policy** - The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.
- ❖ **Identification** – The ability to uniquely identify each user of a trusted system.
- ❖ **Labels** – Elements assigned to each security object describing the sensitivity of that object.
- ❖ **Documentation** – Written evidence of a trusted system's compliance with TCSEC criteria.
- ❖ **Accountability** – The ability to audit user actions at an individually identifiable level.
- ❖ **Lifecycle Assurance** – The use of formal methods to validate the system design and implementation process.
- ❖ **Continuous Protection** – Elements of the trusted computing system must be continuously protected against tampering and/or unauthorized changes

The designations that may be awarded under TCSEC are defined in the Orange Book as:

- ❖ Minimal Protection (D) includes those systems that have been evaluated but fail to meet the requirements for a higher evaluation class.
- ❖ Discretionary Protection (C1) includes systems that nominally satisfy the criteria for discretionary access controls. Specific requirements for C1 certification include:

- Discretionary Access Control Security Policy
 - Identification and Authentication
 - Operational Assurance of System Architecture and System Integrity
 - Lifecycle Assurance of Security Testing
 - Documentation including a Security Features Users' Guide, Trusted Facility Manual, Test Documentation, and Design Documentation
- ❖ Controlled Access Protection (C2) includes systems that have more finely grained discretionary access controls. C2 systems must meet all of the criteria for C1 systems and the following additional requirements:
- Object Reuse Security Policy
 - Audit
- ❖ Labeled Security Protection (B1) systems introduce labeling requirements. B1 systems must meet all of the criteria for C2 systems and the following additional requirements:
- Label Integrity Policy
 - Policy on Exportation of Labeled Information to Single-Level Devices, Multilevel Devices, and Human-Readable Output
 - Mandatory Access Control Policy
 - Lifecycle Assurance of Design Specification and Verification
- ❖ Structured Protection (B2) systems are cited in the Orange Book as relatively resistant to penetration. B2 systems must meet all of the requirements for B1 systems with the following additions:
- Additions to Labeling Policy that Address Subject Sensitivity Labels and Device Labels
 - Trusted Path for Identification and Authentication
 - Additions to Operational Assurance of Covert Channel Analysis and Trusted Facility Management
 - Addition of Configuration Management to Lifecycle Assurance
- ❖ Security Domains (B3) systems are cited in the Orange Book as highly resistant to penetration. B3 systems must meet all of the requirements for B2 systems and must also implement:
- Trusted Recovery Operational Assurance
 - Use of a Trusted Computing Base (TCB) small enough that it can be subjected to rigorous testing
- ❖ Verified Design (A1) systems do not add any additional architectural features or policy requirements. Rather, they must be developed using formal design specification and verification techniques that follow a five-step model:
1. Develop a formal model of the security policy including a mathematical proof.
 2. Develop a formal top-level specification (FTLS) of the design including abstract definitions of TCB functions.
 3. Use a combination of formal and informal techniques to verify that the FTLS of the TCB is consistent with the model.
 4. Show that the implementation of the TCB is consistent with the FTLS through informal techniques.
 5. Perform a formal analysis designed to identify any covert channels in the system.

Common Criteria

In the late twentieth century, several governments banded together to revise their information security models and develop the Common Criteria for Information Technology Security Evaluation (CC). They are described by ISO/IEC 15408. The Common Criteria model was designed to replace the following models:

- ❖ The U.S. Trusted Computer System Evaluation Criteria (TCSEC)
- ❖ The European Information Technology Security Evaluation Criteria (ITSEC)
- ❖ The Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)

The Common Criteria use a combination of **protection profiles** which specify security requirements for a product and **security targets**, which are the design claims made by vendors to provide a structured system for the evaluation of information technology products.

Products evaluated under the Common Criteria are assigned an Evaluation Assurance Level (EAL) from the following hierarchy:

- ❖ EAL1: Functionally Tested
- ❖ EAL2: Structurally Tested
- ❖ EAL3: Methodically Tested and Checked
- ❖ EAL4: Methodically Designed, Tested and Reviewed
- ❖ EAL5: Semiformally Designed and Tested
- ❖ EAL6: Semiformally Verified Design and Tested
- ❖ EAL7: Formally Verified Design and Tested

Certification versus Accreditation

Certification and accreditation are distinct processes defined by security professionals. The U.S. Department of Defense offers the following definitions to guide the process:

- ❖ **Certification** is a comprehensive evaluation of the technical and non-technical security features of an IT system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meets a set of specified security requirements.
- ❖ **Accreditation** is a formal declaration by the Designated Accrediting Authority (DAA) that an IT system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

DITSCAP

The Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) is the DoD's formal model for implementing certification and accreditation. DITSCAP is defined by Department of Defense Instruction (DODI) 5200.40.

DITSCAP is a four-phase process:

- ❖ **Phase 1: Definition** requires agreement of concerned parties on system and security requirements. The end product is the System Security Authorization Agreement.
- ❖ **Phase 2: Verification** ensures that the system complies with the SSAA.

- ❖ **Phase 3: Validation** has the goal of obtaining system accreditation.
- ❖ **Phase 4: Post Accreditation** includes tasks designed to maintain an acceptable level of risk.

Threats

There are a number of security threats that must be addressed within the scope of this domain.

- ❖ **Covert Channels** are unintended communications paths that allow the surreptitious transfer of information outside of normal security controls and mechanisms.
 - **Timing Channels** relay information by modulating consumption of system resources.
 - **Storage Channels** relay information between processes by writing data to a storage system.
- ❖ **Salami Attacks** siphon off small bits of data to gain through aggregation.
- ❖ **Time of Check to Time of Use (TOC/TOU) Attacks** exploit differences between the time a process verifies the access permissions of a security object and the time the permissions are used.
- ❖ **Buffer Overflow Attacks** attempt to execute malicious code through the exploitation of buffers that are manipulated without proper bounds checking procedures.

CBK #7: Operational Security

General Principles of Operations Security

- ❖ The goal of operations security is to implement security controls that protect information resources from harm and misuse while being as transparent as possible to legitimate users.
- ❖ Security of controls should never solely depend upon their secrecy.
- ❖ Controls should exist in a layered fashion. The security community refers to this as "defense in depth."

Workforce Security

- ❖ Control of security mechanisms should be divided among several people whenever possible. The more people involved in a process, the lower the risk of collusion.
- ❖ Rotation of duties, a practice commonly used in the financial world, should be used in information security settings whenever possible. This involves rotating individuals into different work assignments on a temporary basis.



Who Do You Trust for Your Certification Training?

PrepLogic's dependable training products help thousands of professionals and students worldwide achieve their certification goals for A+, MCSE, Network+, CCNA, CEH, PMP, and more.

PrepLogic Comprehensive Training Tools:
CBT • Practice Exams • Audio Training • Mega Guides • Discount Exam Vouchers

For Free Product Demos, [Click Here.](#)

PrepLogic
Be Prepared. Be Confident. Get Certified.

Get this **Study Guide** and many more for **FREE** at

CramSession
www.cramsession.com

- ❖ Individuals should be required to take at least one full week of vacation each year. At least one full week should be taken consecutively to cause an extended absence from the office. In addition to providing a well-deserved recovery period, this extended absence tends to allow problems to rise to the surface.

Control Categories

Controls are normally divided into three categories:

- ❖ **Preventive controls** aim to stop an attack from succeeding.
- ❖ **Detective controls** aim to identify malicious activity on the network.
- ❖ **Corrective controls** aim to restore a resource to its pre-attack state.

Other common control types include: Deterrent controls, Application controls, Input controls, Processing controls, Output controls, Change controls and Test controls.

The Orange Book includes controls categorized into two types of assurance mechanisms: operational assurance and lifecycle assurance.

Operational Assurance

Operational Assurance focuses on the features and system architecture used to ensure that the security policy is uncircumventably enforced during system operation.

- ❖ System Architecture
- ❖ System Integrity
- ❖ Covert Channel Analysis
- ❖ Trusted Facility Management
- ❖ Trusted Recovery ensures security is not breached when system crashes or has other failures. The Common Criteria outlines four types of recovery: Manual Recovery, Automated Recovery, Automated Recovery without Undue Loss, Function Recovery

Lifecycle Assurance

Lifecycle Assurance refers to steps taken by an organization to ensure that the system is designed, developed, and maintained using formalized and rigorous controls and standards.

- ❖ Security Testing
- ❖ Design Specification and Verification
- ❖ Configuration Management

Change Control

Configuration change management covers the entire lifecycle of system/software. Under the Orange Book criteria, it is required only for B2, B3, and A1 levels of certification.

The change control process has five steps:

1. Applying to introduce a change
2. Cataloging the change
3. Scheduling the change
4. Implementing the change
5. Reporting the change to appropriate parties

Auditing

The goal of any audit is to ensure compliance with the security policy. Some audits are against organizational policies whereas others are for compliance with specific legal, regulatory, or accounting standards.

The audit function should always be independent of undue influence.

Audit trails should be configured on critical/sensitive systems that record, as a minimum:

- ❖ Date and time of each event
- ❖ Identity of the user who caused the event
- ❖ Details of the event-related activity
- ❖ Source of the event (IP, physical location, etc.)

CBK #8: Business Continuity Planning and Disaster Recovery Planning

Business Continuity Planning

The [business continuity planning process](#) has four phases:

- ❖ **Phase 1: Scope and Plan Initiation:**
 - Criticality Prioritization in which each business function is ranked in order of importance to the business
 - Maximum Tolerable Downtime (MTD) estimation in which the business determines the longest period of time it can operate without a critical business function.
 - Determination of resources required to carry out each critical business function
- ❖ **Phase 2: Business Impact Assessment (BIA):**
 - Acquiring materials necessary for the assessment including organizational charts, business process workflows, business associate agreements, etc.
 - Vulnerability Assessment (VA) determines the exposure of the business to various risks and vulnerabilities

- Analysis of information acquired during the previous two steps
- Recommending actions to the business continuity team and documenting the results
- ❖ **Phase 3: Business Continuity Plan Development** - Involves putting the plan down on paper. BCP analysts take the recommendations developed during phase 2 and the information obtained during phase 1 and develop a comprehensive, written business continuity plan.
- ❖ **Phase 4: Plan Approval and Implementation** - Where the plan meets reality. The BCP team should obtain final approval from senior management and promulgate the plan among all affected employees.

Disaster Recovery Planning

In any disaster situation, the organization's primary focus should be on the **safety of people**.

The goal of [disaster recovery](#) is to restore the business as quickly as possible. Disaster recovery is not complete until the business is up and running again in the primary facility at full capacity.

Data Processing Continuity

Organizations have several options when it comes to data processing continuity planning:

- ❖ Mutual assistance agreements - This is a contractual arrangement between two organizations with similar computing needs that each will support the other in the event of a disaster.
- ❖ Alternate data processing facilities provide critical capabilities in time of disaster
 - Hot sites are ready-to-run, dedicated sites that have equipment, software, and real-time data in place.
 - Warm sites provide all of the equipment and environmental controls necessary to restore operations but do not have applications installed or data restored.
 - Cold sites are buildings with proper infrastructure to support computing operations (i.e., power, environmental controls, etc.) but without any computer equipment, data, or software in place.
 - Hot sites, warm sites, and cold sites may be either owned and operated by the organization that they serve or by a subscription service that keeps the facilities available for its clients.
 - Many large organizations arrange for data centers in remote cities.
 - Other alternatives include mobile data recovery sites and prefabricated relocateable buildings.

Data Backups

Data backup is a critical part of any disaster recovery/business continuity plan. Security professionals must ensure that proper backup procedures are in place and effectively carried out.

Backup Types

There are three primary types of backups:

- ❖ **Full backups** – Create a duplicate copy of all files on the primary media and store them on the backup media.
- ❖ **Differential backups** – Create a duplicate copy of all files that have been modified since the last full backup.
- ❖ **Incremental backups** – Create a duplicate copy of all files that have been modified since the last full or incremental backup (whichever was more recent).

The major difference between differential and incremental backups are their treatment of the archive bit:

- ❖ Incremental backups clear the archive bit.
- ❖ Differential backups do not clear the archive bit.

The media used for restoring data after a loss depends upon the last type of backup that was performed:

- ❖ If the last backup was a full backup, only the full backup must be restored from tape.
- ❖ If the last backup was a differential backup, you must restore the last full backup and the most recent incremental backup.
- ❖ If the last backup was an incremental backup, you must restore the last full backup and all intervening incremental backups.

There are tradeoffs in time to backup and time to restore:

- ❖ Using incremental backups in combination with periodic full backups requires less time to create the backups but requires more time to restore in the event of a disaster.
- ❖ Using differential backups in combination with periodic full backups requires more time to create the backups but requires less time to restore in the event of a disaster.

Backup Media

Most enterprise backup systems rely on the use of magnetic tapes for storing backup data.

Media Rotation

Common backup media [rotation schemes](#) include:

- ❖ The **grandfather-father-son** model requires 12 media sets to fully implement. It uses three different media sets.
- ❖ The **Tower of Hanoi** model requires four media sets.

Disaster Recovery Plan Testing

Testing is used to find weaknesses in the disaster recovery plan. If a plan is not tested, you must assume that it is not going to work. The five types of DRP testing include:

- ❖ **Checklist** – Copies of plan are distributed to members of the disaster recovery team and management for a thorough review
- ❖ **Structured walk-through** – Business unit management meets to review plan
- ❖ **Simulation** – Support personnel meet in a practice execution session but don't actually execute the plan
- ❖ **Parallel** – DRP is fully executed with critical systems run at an alternate site. Normal business operations continue at the primary processing facility
- ❖ **Full-Interruption** – Normal production shutdown, with real disaster recovery processes at the alternate recovery sites

CBK #9: Law, Investigation, and Ethics

Law

There are three ways federal laws may be enacted in the United States:

- ❖ Statutory law is enacted by Congress and embodied in the United States Code.
- ❖ Administrative law is enacted by agencies of the executive branch and embodied in the Code of Federal Regulations.
- ❖ Case law is recognized by the judicial branch and documented in the legal precedents of the courts.

The law is further divided into three categories of law:

- ❖ Criminal law provides for punishment by imprisonment and fines for crimes against society.
- ❖ Civil law provides for financial damages for crimes against an individual or organization.
- ❖ Administrative law provides sanctions for violations of administrative requirements promulgated by regulatory bodies.

Another category of law, common law, is based upon principles handed down through the generations and recognized by the courts, but not codified in a legislative fashion.

Information Security Laws

In recent years, a large number of [laws](#) affecting the information security profession have been enacted:

- ❖ The **Electronic Communications Privacy Act of 1986** restricts eavesdropping on electronic communications.
- ❖ The **Privacy Act of 1974** places restrictions on the types of information that federal agencies may collect from individuals and the ways they may use that information.
- ❖ The **Health Insurance Portability and Accountability Act (HIPAA)** consists of two components: The Security Rule and the Privacy Rule.
- ❖ The **Sarbanes-Oxley (SOX) Act** requires that publicly traded organizations have security procedures in place to ensure that critical business records are protected and maintained for specified periods of time. It places personal accountability for compliance and accurate reporting in the hands of corporate officers.
- ❖ The **Gramm-Leach-Bliley Act (GLBA)** requires financial institutions to take reasonable and appropriate measures to protect personal financial information.
- ❖ The **Computer Fraud and Abuse Act of 1986 (as amended in 1996)** covers crimes against "federal interest" computing systems.
- ❖ The **National Information Infrastructure Protection Act** requires government entities to implement measures to ensure the confidentiality, integrity, and availability of government data.
- ❖ The **Family Education Rights and Privacy Act (FERPA)** grants students and their families specific rights with regard to the dissemination of student data and requires educational institutions to implement safeguards to ensure privacy is maintained.

Intellectual Property Laws

Intellectual property may be protected by one or more of the following legal mechanisms:

- ❖ **Copyrights** - Used to protect original works of authorship and last for 70 years after the death of the author.
- ❖ **Patents** - Used to protect novel inventions and generally last for 17 years from the time of invention.
- ❖ **Trademarks** - Used to protect words, symbols, or other markings that identify the source of a product or service
- ❖ **Trade secrets** - Confidential business secrets kept within a business and not released to outsiders. Trade secrets are only protected by law if the owner takes reasonable precautions to ensure that they do not fall into the public domain.

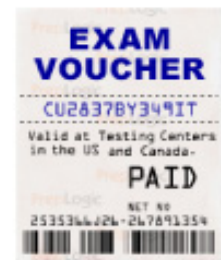
Evidence

There are two types of evidence, depending upon the circumstances of its intended use:

- ❖ In connection with an audit:
 - Physical examination
 - Confirmation (response from third party)
 - Documentation
 - Observation
 - Inquiry
 - Mechanical accuracy
 - Analytical procedures (using comparisons and ratios)
- ❖ Relevant to legal proceedings:
 - Best evidence
 - Secondary
 - Direct
 - Circumstantial
 - Conclusive
 - Corroborative
 - Opinion
 - Hearsay

To be admissible in court, evidence must meet three standards:

Take Your Exam for Less!



Discount Exam Vouchers from PrepLogic

Why pay retail price for the exam when you can save up to 40% with discount exam vouchers?

[Buy Your Voucher Now](#)

PrepLogic

Be Prepared. Be Confident. Get Certified.

- ❖ It must be **relevant**, meaning that it must provide information related to the commission of the crime.
- ❖ It must be **reliable**, meaning that it has not been tampered with from the time of collection.
 - Reliability is established through the use of a documented **chain of custody**.
- ❖ It must be **legal**, meaning that it must have been [gathered](#) within the parameters of the law and the subject's rights under the Constitution and other relevant laws.

Investigation

Investigations should be spearheaded by a **computer incident response team (CIRT)**.

An early decision must be made regarding the planned outcome of the investigation. If you wish to leave the option of criminal prosecution open, you must ensure that the CIRT follows digital forensic procedures designed to produce evidence that will be admissible in court.

You must also decide whether law enforcement will be involved in the investigation.

Ethics

(ISC)² Code of Ethics

All Certified Information Systems Security Professionals (CISSPs) are required to abide by the Code of Ethics promulgated by [\(ISC\)2](#). The Code of Ethics has two preamble elements:

- ❖ Safety of the commonwealth, duty to our principals, and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
- ❖ Therefore, strict adherence to this Code is a condition of certification.

From this, there are four required canons of ethics:

- ❖ Protect society, the commonwealth, and the infrastructure.
- ❖ Act honorably, honestly, justly, responsibly, and legally.
- ❖ Provide diligent and competent service to principals.
- ❖ Advance and protect the profession.

Internet Activities Board

The Internet Activities Board Code of Ethics is defined in RFC 1087. It declares that it is unethical and unacceptable to engage in any activity which purposely:

- ❖ Seeks to gain unauthorized access to the resources of the Internet
- ❖ Disrupts the intended use of the Internet
- ❖ Wastes resources (people, capacity, computer) through such actions
- ❖ Destroys the integrity of computer-based information, and/or
- ❖ Compromises the privacy of users

CBK #10: Physical Security

Facility Security

Facilities must be designed with security in mind from the start. Processes that require security involvement include: Site selection, Construction, Facility management and Emergency procedures.

Site Selection

- ❖ Consider the location of the site relative to natural disaster hazards.
- ❖ Consider the location of the site with respect to the vulnerability to other security incidents. Is it being built in a high-crime area? Is it next to a facility that works with flammable and/or toxic substances that may be accidentally released?

Construction

- ❖ Are the building materials rated to withstand disasters that are likely to occur?
- ❖ Weigh the cost of compensating controls against the likelihood that a risk will occur and the cost to recover from such an incident. m.
- ❖ Does the facility construction plan allow for the establishment of a secure data center?

Facility management

- ❖ Physical security of the facility should be managed through a four-layered approach:
 - Penetration should first be deterred. Deterrent controls include guard dogs and posted signs warning of the consequences of trespassing.
 - The next layer of protection should deny physical access to the facility. The most common control used to deny access is a locked door.
 - The third layer of protection should allow for the detection of unauthorized access to the facility. Detective controls include alarm systems and security cameras
 - The final layer of protection should provide a delay for security officers to respond to a detected incident. Delay controls may include *man traps*, which use a series of time delayed doors that take a predetermined period of time to open.

Emergency procedures

- ❖ Employees should know their roles and responsibilities in the event of an emergency.
- ❖ Formal procedures should exist for declaring and responding to an emergency.
- ❖ Emergency procedures should tie into the organization's business continuity plan and disaster recovery plan.

Fire






Creation of a fire requires three elements: Oxygen, Heat and Fuel

Denial of any one of these elements is enough to prevent and/or extinguish a fire:

- ❖ Carbon dioxide may be used to remove oxygen
- ❖ Water may be used to reduce heat
- ❖ Soda acid may be used to remove fuel

There are five classes of fire extinguisher, each of which is suitable for a different type of fire, as described in Table 5.

Table 5 – Fire Extinguisher Classes

Class	Description	Suppression Medium	Symbol
A	Ordinary combustibles	Water or soda acid	
B	Flammable liquids	CO2, soda acid, Halon	
C	Electrical	CO2 or Halon	
D	Combustible metals	Copper, sodium chloride	
K	Combustible cooking	Commercial kitchen extinguishers	

Unless you have special training, you should not attempt to fight a Class D fire under any circumstances.

Different fire detection systems have triggers based on the detection of:

- ❖ Heat
- ❖ Flame
- ❖ Smoke

In sensitive environments, you should include detective controls that work on each of these three elements.

Water-based fire extinguishers come in four forms:

- ❖ Wet pipe systems are always full of water and discharge water immediately upon trigger.
- ❖ Dry pipe systems do not contain water and are useful in areas where bursting pipes are a risk. When the trigger occurs, they fill with water.
- ❖ Deluge systems literally soak an entire area when one of the sensors is triggered.
- ❖ Preaction systems are a combination of wet pipe and dry pipe systems.

Gas-based fire extinguishers:

- ❖ The most common gas-based extinguishers use carbon dioxide to remove oxygen from a fire.
- ❖ Data centers commonly used Halon systems in the past to prevent damage to sensitive electronic equipment. However, Halon systems are shown to damage the environment and jeopardize human life.
- ❖ The current "gas of choice" for fire suppression systems is FM-200.

Fire damage is caused by (in order of damage likelihood and magnitude):

- ❖ Smoke
- ❖ Heat
- ❖ Water
- ❖ Contamination

Fences

Table 6 lists three different categories of fences based on the height of the fence.

Table 6- Fence Heights

Fence Height	Objective
3' to 4' (1 meter)	Deters casual trespasser
6' to 7' (2 meters)	Too hard to climb easily
8' with 3 strands of barbed wire (2.4 meters)	Deters intruders

Electrical Power

The greatest risk posed by electrical power is electric noise generated by electromagnetic interference (EMI). EMI is generated by the interaction among the three wires in a standard electric line (hot, neutral, and ground).

Radio frequency interference (RFI) is generated by devices that consume electricity as a byproduct of that consumption.

Electrical noise may be prevented through the use of:

- ❖ Shielding of cables and devices

- ❖ Proper electrical grounding procedures
- ❖ Power conditioning devices

Threats to electronic systems created by electricity and electric power systems include:

- ❖ **Blackouts** – Loss of power to a system
- ❖ **Faults** – Short periods of power loss
- ❖ **Brownouts** – Extended period of low voltage
- ❖ **Sags** – Short periods of low voltage
- ❖ **Surges** – Extended period of high voltage
- ❖ **Spikes** – Short periods of high voltage
- ❖ **Static electricity** - More likely in the event of low humidity and can cause significant damage to electronic components


Media Security

Your media security plan must address:

- ❖ Media storage
- ❖ Labeling of media containing sensitive data
- ❖ Inventory procedures
- ❖ Accountability logs
- ❖ Physical access controls
- ❖ Environmental conditions of media storage

There are two additional areas that must be addressed due to specific media security threats:

- ❖ **Media reuse** - Reusing data storage media after initial use.
- ❖ **Data remanence** - Residual information remaining on media after erasure, which may be restored. Orange Book requires magnetic media be formatted seven times before discard or reuse.



The PrepLogic Mega Guide

PrepLogic took the CramSession Study Guide and made it better!

- Over 100 pages
- Expanded resources
- More in-depth content
- Includes review practice questions

Get \$10 Off
Get it Now
Coupon Code: **MEGA10**

A+, MCSE, CCNA, CEH, CISSP, PMP, and more.

PrepLogic
Be Prepared. Be Confident. Get Certified.

Get this **Study Guide and many more** for **FREE** at

CramSession
www.cramsession.com

There are three common problems with media erasure:

- ❖ Deleting does not actually remove data; it merely erases the entry from the file allocation table.
- ❖ Damaged sectors may not be overwritten by a disk format that does not involve degaussing.
- ❖ Improper use or equipment failure of degausser.

There are three possible techniques that you may use to handle the disposition of media after initial use:

- ❖ **Clearing** - Overwriting data on media for reuse within same secured environment (i.e., not used in a lesser security environment)
- ❖ **Purging** - Degaussing or overwriting media to be removed from monitored environment, such as resale, use in unsecured environment, or donation
- ❖ **Destruction** - Completely destroying media; good practice to purge media before submitting for destruction