Domain 1:
Threats, Attacks, and Vulnerabilities

Malware comes in many different forms. You should be able to review a scenario and identify the type of malware involved. Major malware types include:

Malware Type	Description
Virus	Spreads between systems based upon some user action.
Worm	Spreads between systems by exploiting vulnerabilities; no user action required.
Trojan Horse	Masquerades as desirable software to trick user into installing it.
Remote Access Trojan	Trojan horse that allows an attacker to gain remote access to a system.
Adware	Displays advertisements on the user's system to generate ad revenue.
Spyware	Monitors user activity, such as keystrokes and web visits.
Ransomware	Encrypts user files and demands a ransom before releasing the key.
Logic Bomb	Waits until certain conditions are met before triggering a malicious action.
Rootkit	Elevates privileges of a normal user to gain administrative rights.
Backdoor	Provides an unauthorized mechanism for accessing a system.

Social engineering attacks exploit seven main mechanisms: **authority**, **intimidation**, **consensus**, **scarcity**, **familiarity**, **trust**, and **urgency**.

Social engineering attacks manipulate individuals to gain unauthorized access or information. Variants of social engineering attacks include:

Attack Type	Description
Phishing	Solicits information via email.
Spear Phishing	Solicits information via highly targeted email designed for one person.
Whaling	Targets high value individuals, such as senior executives.
Tailgating	Accesses a building by having someone hold the door open.
Dumpster Diving	Discovers sensitive information discarded in the trash.
Shoulder Surfing	Monitors user activity by watching them as they enter/read information.
Watering hole	Places malware on a site where users are known to congregate.

Attackers vary widely in their sophistication, resources, and intent. **Script kiddies** are generally low-skilled attackers seeking a quick thrill. **Advanced Persistent Threats (APTs)** are extremely sophisticated attackers often sponsored by government agencies.

Network discovery scanning uses tools like nmap to check for active systems and open ports. Common scanning techniques include:

- **TCP SYN** scans send a single packet with the SYN flag set.
- **TCP Connect** scans attempt to complete the three way handshake.
- **TCP ACK** scans seek to impersonate an established connection.
- **Xmas** scans set the FIN, PSH, and URG flags.

Domain 1:
Threats, Attacks, and Vulnerabilities

Network vulnerability scanning first discovers active services on the network and then probes those services for known vulnerabilities. **Web application vulnerability scans** use tools that specialize in probing for web application weaknesses.

The vulnerability management workflow includes three basic steps: **detection, remediation,** and **validation**.

Penetration testing goes beyond vulnerability scanning and attempts to exploit vulnerabilities. It includes five steps:

There are three different types of penetration tests:

- During **white box** penetration tests, testers have full access to information about the target systems.
- During **black box** penetration tests, testers conduct their work without any knowledge of the target environment.
- **Gray box** tests reside in the middle, providing testers with partial knowledge about the environment.

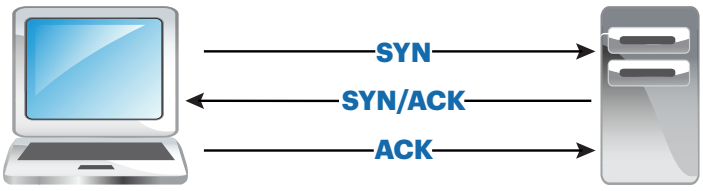
Domain 2: Technologies and Tools

OSI Model

Layer	Description
Application	Serves as the point of integration for user applications with the network
Presentation	Transforms user-friendly data into machine-friendly data; encryption
Session	Establishes, maintains, and terminates sessions
Transport	Manages connection integrity; TCP, UDP, SSL, TLS
Network	Routing packets over the network; IP, ICMP, BGP, IPsec, NAT
Data Link	Formats packets for transmission; Ethernet, ARP, MAC addresses
Physical	Encodes data into bits for transmission over wire, fiber, or radio

TCP is a connection-oriented protocol, while **UDP** is a connectionless protocol that does not guarantee delivery.

TCP Three-Way Handshake



DNS converts between IP addresses and domain names. **ARP** converts between MAC addresses and IP addresses. **NAT** converts between public and private IP addresses.

Wireless networks should be secured using **WPA** or **WPA2** encryption, not **WEP**.

Load balancers distribute connection requests among many identical servers.

Network switches generally work at layer 2 and connect directly to endpoints or other switches. Switches may also create **virtual LANs (VLANs)** to further segment internal networks at layer 2.

Port(s)	Service
20, 21	FTP
22	SSH
23	Telnet
25	SMTP
53	DNS
80	HTTP
110	POP3
123	NTP
135, 137-139, 445	Windows File Sharing
143	IMAP
161/162	SNMP
443	HTTPS
1433/1434	SQL Server
1521	Oracle
1720	H.323
1723	PPTP
3389	RDP
9100	HP JetDirect Printing

Routers generally work at layer 3 and connect networks to each other. **Firewalls** are the primary network security control used to separate networks of differing security levels. **TLS** should be used to secure network communications. **SSL** is no longer secure.

Most **Virtual Private Networks (VPN)** use either TLS or IPsec. IPsec uses **Authentication Headers (AH)** to provide authentication, integrity and nonrepudiation and **Encapsulating Security Payload (ESP)** to provide confidentiality.

Domain 2: Technologies and Tools

Split tunnel VPNs only send traffic destined for the corporate network through the VPN while **full tunnel VPNs** send all traffic through the VPN.

Network Admission Control (NAC) systems screen devices before allowing them to connect to the network. This screening may include both user authentication and device health checking.

Tool	Description
Intrusion Detection System	Monitor a host or network for signs of intrusion and report to administrators.
Intrusion Prevention System	Monitor a host or network for signs of intrusion and attempt to block malicious traffic automatically.
Security Information & Event Management System	Aggregate and correlate security information received from other systems.
Firewall	Restricts network traffic to authorized connections.
Application Whitelisting	Limits applications to those on an approved list.
Application Blacklisting	Blocks applications on an unapproved list.
Sandbox	Provides a safe space to run potentially malicious code.
Honeypot	System that serves as a decoy to attract attackers.
Honeynet	Unused network designed to capture probing traffic
VPN Concentrator	Provides a central aggregation point for VPN connections.
Proxy Server	Makes requests to other servers on behalf of an end user, providing anonymization and performance enhancement.
Data Loss Prevention	Blocks the exfiltration of sensitive information from an organization.
Mail Gateway	Screen inbound messages for malicious content.

Security professionals use a variety of **command-line tools to** assist in their work. You should be familiar with the following tools when taking the exam:

Tool	Purpose
ping	Verifies connectivity to a remote networked system.
netstat	Lists open network connections and listening ports on a system.
tracert	Determines the network path between two systems.
nslookup	Performs DNS queries.
dig	dig Performs DNS queries. (Newer alternative to nslookup)
arp	Performs MAC address queries.
ipconfig	Queries network configuration information on a Windows system.
ifconfig	Queries network configuration information on a Linux/Mac system.
nmap	Scans for open network ports on a remote system.
netcat	Reads and writes traffic to/from network connections.

Enterprises may deploy mobile devices in a variety of models. In a strict corporate-owned model, devices are for business use only. Users mix personal and business use in a **bring your own device (BYOD) or corporate owned, personally enabled (COPE)** model. Companies should use **mobile device management (MDM)** tools to enforce a variety of mobile security controls, including:

- Restricting applications
- Remote wiping of lost/stolen devices
- Geolocation and geofencing services
- Screen locking and password/PIN requirements
- Full device encryption

Know the secure alternatives to commonly used protocols:

Insecure Protocol	Secure Alternative(s)
Telnet	SSH
HTTP	HTTPS
LDAP	LDAPS
FTP	FTPS or SFTP

Domain 3:
Architecture and Design

The three main goals of information security are:
- **Confidentiality** prevents unauthorized disclosure
- **Integrity** prevents unauthorized alteration
- **Availability** ensures authorized access

Security activities must be aligned with **business strategy, mission, goals, and objectives**. This requires **strategic, tactical,** and **operational** planning.

Security **frameworks** provide templates for security activities. These include COBIT, NIST CSF, and ISO 27001/2.

Due care is taking reasonable steps to protect the interest of the organization. **Due diligence** ensures those steps are carried out.

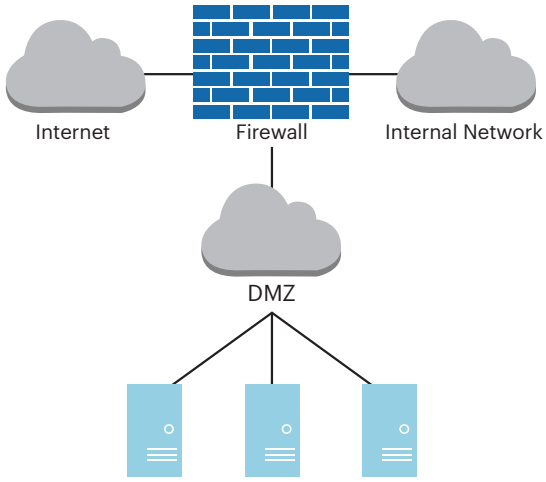
Security governance is carried out through
- **Policies** which state high-level objectives (mandatory compliance).
- **Standards** which state detailed technical requirements (mandatory compliance).
- **Procedures** which provide step-by-step processes (mandatory compliance).
- **Guidelines** which offer advice and best practices (optional compliance).

Security baselines, such as **NIST SP 800-53**, provide a standardized set of controls that an organization may use as a benchmark.

Typically, organization don't adopt a baseline standard wholesale, but instead tailor a baseline to meet their specific security requirements.

The principle of **defense-in-depth** says that organizations should use a variety of overlapping security controls to prevent against the failure of a single control. When designing overlapping controls, strive for diversity of vendors and control types.

The most common firewall deployment topology uses three zones: a trusted intranet, an untrusted Internet, and a **demilitarized zone (DMZ)** that houses publicly accessible servers. These networks are often created using a triple-homed firewall.

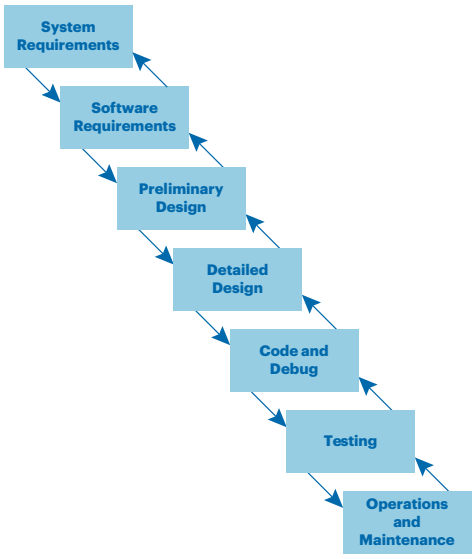


When managing security of a system, keep in mind the following operating system security principles:
- Disable unnecessary services and applications
- Close unneeded network ports
- Disable default accounts and passwords
- Apply all security patches

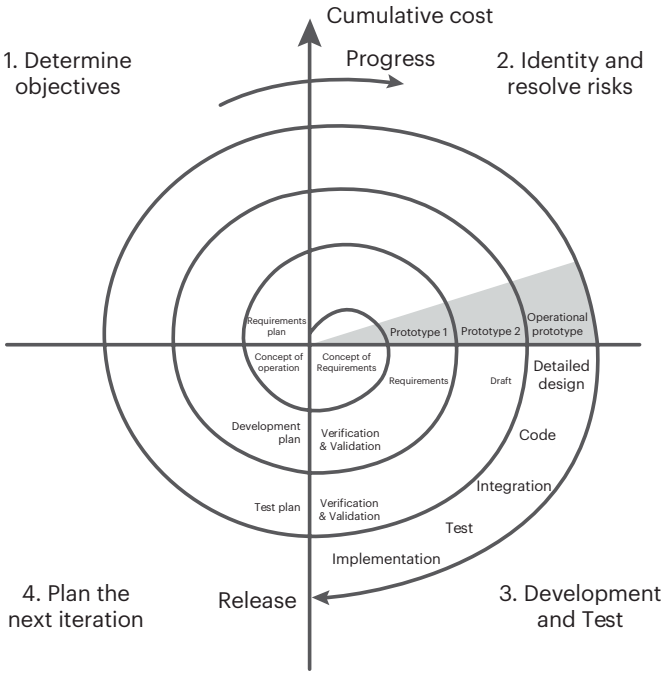
When developing new systems, organizations move them through a four-stage process using different environments:
1. **Development** environments are where developers create and modify the system.
2. **Test** environments are where the system is tested. If flaws are discovered, it is returned to development.
3. **Staging** environments are where approved code is placed, awaiting release to production.
4. **Production** environments contain systems that are currently serving customer needs.

Domain 3:
Architecture and Design

The **waterfall model** of software development is fairly rigid, allowing the process to return only to the previous step:



The **spiral model** uses a more iterative approach:



While the **agile approach** eschews this rigidity for a series of incremental deliverables created using a process that values:

- **Individuals and interactions** instead of processes and tools
- **Working software** instead of comprehensive documentation
- **Customer collaboration** instead of contract negotiation
- **Responding to change** instead of following a plan

In **virtualized environments** many guest systems run on a single piece of hardware. The **hypervisor** is responsible for separating resources used by different guests. **Type 1 hypervisors** run directly on the "bare metal" hardware while **type 2 hypervisors** run on a host operating system. **Application virtualization** virtualizes individual software apps instead of entire operating systems.

When deploying services in the cloud, organizations may choose from three major cloud strategies:

- **Software-as-a-Service (SaaS)** deploys entire applications to the cloud. The customer is only responsible for supplying data and manipulating the application.
- **Infrastructure-as-a-Service (IaaS)** sells basic building blocks, such as servers and storage. The customer manages the operating system and configures and installs software.
- **Platform-as-a-Service (PaaS)** provides the customer with a managed environment to run their own software without concern for the underlying hardware.

Cloud services may be built and/or purchased in several forms:

- **Public cloud** providers sell services to many different customers and many customers may share the same physical hardware.
- **Private cloud** environments dedicate hardware to a single user.
- **Hybrid cloud** environments combine elements of public and private cloud in a single organization.
- **Community cloud** environments use a model similar to the public cloud but with access restricted to a specific set of customers.

Domain 3:
Architecture and Design

When managing the physical environment, you should be familiar with common power issues:

Power Issue	Brief Duration	Prolonged Duration
Loss of power	Fault	Blackout
Low voltage	Sag	Brownout
High voltage	Spike	Surge
Disturbance	Transient	Noise

Fires require the combination of **heat, oxygen,** and **fuel**. They may be fought with fire extinguishers:

- Class A: common combustible fires
- Class B: liquid fires
- Class C: electrical fires
- Class D: metal fires

Organizations may use **wet pipe** fire suppression systems that always contain water, **dry pipe** systems that only fill with water when activated, or **preaction** systems that fill the pipes at the first sign of fire detection.

Mantraps use a set of double doors to restrict physical access to a facility.

Hot and cold aisle approaches manage cooling by aligning data centers so that the front of one row of servers faces the front of the adjacent row (cold aisle) and the backs of servers also face each other (hot aisle).

Software testers can have varying degrees of knowledge about the software they are testing. In a **white box test**, they have full knowledge of the software. In a **black box test**, they have no knowledge, while **grey box tests** reside in the middle, providing testers with partial knowledge.

The top ten security vulnerabilities in web applications, according to OWASP are:

1. Injection attacks
2. Broken authentication
3. Sensitive data exposure
4. XML external entities
5. Broken access control
6. Security misconfiguration
7. Cross-site scripting
8. Insecure deserialization
9. Using components with known vulnerabilities.
10. Insufficient logging and monitoring

In addition to maintaining current and patched platforms, one of the most effective application security techniques is **input validation** which ensures that user input matches the expected pattern before using it in code.

Domain 4:
Identity and Access Management

The core activities of identity and access management are:

- **Identification** where a user makes a claim of identity.
- **Authentication** where the user proves the claim of identity.
- **Authorization** where the system confirms that the user is permitted to perform the requested action.

In access control systems, we seek to limit the access that **subjects** (e.g. users, applications, processes) have to **objects** (e.g. information resources, systems)

Access controls work in three different fashions:

- **Technical (or logical) controls** use hardware and software mechanisms, such as firewalls and intrusion prevention systems, to limit access.
- **Physical controls**, such as locks and keys, limit physical access to controlled spaces.
- **Administrative controls**, such as account reviews, provide management of personnel and business practices.

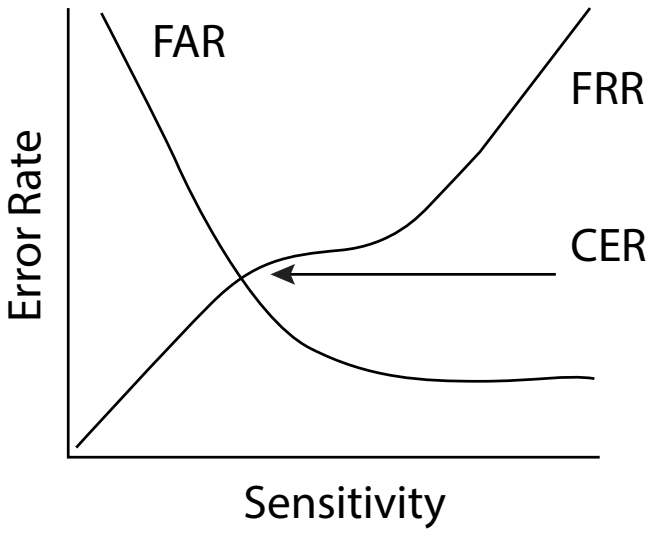
Multifactor authentication systems combine authentication technologies from two or more of the following categories:

- **Something you know** (Type 1 factors) rely upon secret information, such as a password.
- **Something you have** (Type 2 factors) rely upon physical possession of an object, such as a smartphone.
- **Something you are** (Type 3 factors) rely upon biometric characteristics of a person, such as a face scan or fingerprint.

Authentication technologies may experience two types of errors. **False positive** errors occur when a system accepts an invalid user as correct. It is measured using the false acceptance rate (FAR). **False negative** errors occur when a system rejects a valid user, measured using the false rejection rate (FRR). We evaluate the effectiveness of an authentication technology using the **crossover error rate (CER)**, as shown in the diagram to the right:

Organizations often use centralized access control systems to streamline authentication and authorization and to provide users with a single sign on (SSO) experience. These solutions often leverage **Kerberos** which uses a multi step logon process:

1. User authenticates to a client on his or her device.
2. Client sends the authentication credentials to the Key Distribution Center (KDC).
3. KDC verifies the credentials and creates a ticket granting ticket (TGT) and sends it to the user.
4. Client makes a service access request to the KDC using the TGT.
5. KDC verifies the TGT, creates a service ticket (ST) for the user to use with the service, and sends the ST to the user.
6. User sends the ST to the service.
7. Service verifies the ST with the KDC and grants access.



Domain 4:
Identity and Access Management

RADIUS is an authentication protocol commonly used for backend services. **TACACS+** serves a similar purpose and is the only protocol from the TACACS family that is still commonly used.

The **implicit deny** principle says that any action that is not explicitly authorized for a subject should be denied.

Access control lists (ACLs) form the basis of many access management systems and provide a listing of subjects and their permissions on objects and groups of objects.

Discretionary access control (DAC) systems allow the owners of objects to modify the permissions that other users have on those objects. **Mandatory access control (MAC)** systems enforce predefined policies that users may not modify.

Role-based access control assigns permissions to individual users based upon their assigned role(s) in the organization. For example, backup administrators might have one set of permissions while sales representatives have an entirely different set.

Brute force attacks against password systems try to guess all possible passwords. **Dictionary attacks** refine this approach by testing combinations and permutations of dictionary words. **Rainbow table attacks** precompute hash values for use in comparison. **Salting** passwords with a random value prior to hashing them reduces the effectiveness of rainbow table attacks.

Man-in-the-middle attacks intercept a client's initial request for a connection to a server and proxy that connection to the real service. The client is unaware that they are communicating through a proxy and the attacker can eavesdrop on the communication and inject commands.

The **least privilege** principle says that users should be provided with the minimum set of privileges necessary to complete their job function. **Separation of duties** ensures that a single user does not have the ability to perform two actions that, when combined, allow an undesirable result. **Two-person control** requires the approval of two different individuals to take a sensitive action.

Domain 5:
RIsk Management

Risks are the combination of a **threat** and a corresponding **vulnerability**.

Quantitative risk assessment uses the following formulas:

SingleLossExpectancy **=**
*AssetValue * ExposureFactor*
AnnualizedLossExpectancy **=**
*AnnualizedRateofOccurence * SLE*

Responses to a risk include:

- **Avoid** risk by changing business practices
- **Mitigate** risk by implementing controls
- **Accept** risk and continue operations
- **Transfer** risk through insurance or contract

There are eight major categories of security controls. Note that a single control may fit into more than one category.

Category	Description
Deterrent	Discourages an adversary from attempting a violation of security.
Preventive	Stops an adversary from violating security.
Detective	Identifies potential violations of security.
Corrective	Restores the original state after a violation of security.
Compensating	Fills the gap left when it is not possible to implement a required control.
Technical	Uses technological means to meet a security objective.
Administrative	Uses policy, process, or procedure to meet a security objective.
Physical	Uses physical constraints to meet a security objective.

Personnel security principles include:

- **Need to know** requires a legitimate business need to access information.
- **Least privilege** grants individuals the minimum necessary permissions to perform their jobs.
- **Separation of duties** blocks someone from having two sensitive privileges in combination.
- **Two-person control** requires two people to perform a sensitive activity.
- **Mandatory vacations** and **job rotation** seek to prevent fraudulent activity by uncovering malfeasance.

Business continuity planning conducts a **business impact assessment** and then implements controls designed to keep the business running during adverse circumstances.

Backups provide an important disaster recovery control. Remember that there are three major categories of backup:

Backup Type	Description
Full Backup	Copies all files on a system.
Differential Backup	Copies all files on a system that have changed since the most recent full backup.
Incremental Backup	Copies all files on a system that have changed since the most recent full or incremental backup.

Disaster recovery sites fit into three major categories:

Site Type	Support Systems	Configured Servers	Real-time Data
Cold Site	Yes	No	No
Warm Site	Yes	Yes	No
Hot Site	Yes	Yes	Yes

Domain 5:
RIsk Management

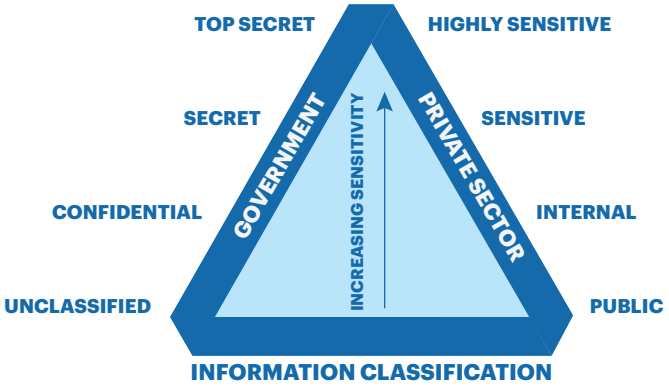
Disaster recovery plans require testing. There are five major test types:

DR Test Type	Description
Read-through/ tabletop	Plan participants review the plan and their specific role, either as a group or individually.
Walkthrough	The DR team gathers to walk through the steps in the DR plan and verify that it is current and matches expectations.
Simulation	DR team participates in a scenario-based exercise that uses the DR plan without implementing technical recovery controls.
Parallel	DR team activates alternate processing capabilities without taking down the primary site.
Full interruption	DR team takes down the primary site to simulate a disaster.

Information should be **classified** based upon its sensitivity to the organization.

Common classes of sensitive information include:

- **Personally identifiable information (PII)** which uniquely identifies individuals.
- **Protected health information (PHI)** which includes individual health records.
- **Proprietary information** which contains trade secrets.



Information should be labeled with its classification and security controls should be defined and appropriate for each classification level.

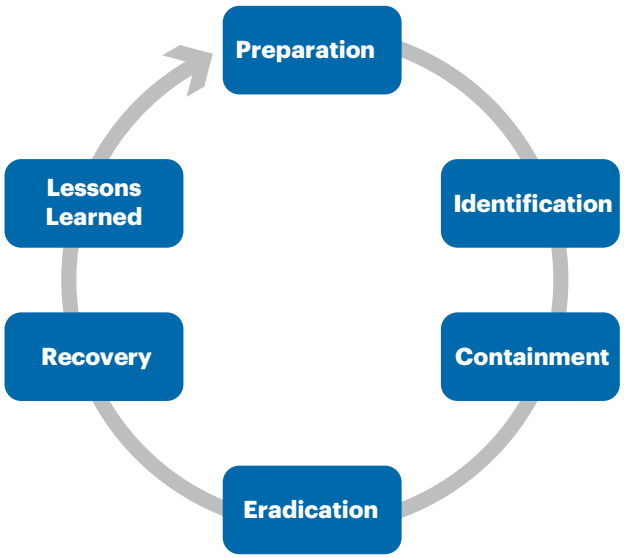
Collect only data that is necessary for legitimate business purposes. This is known as **data minimization**.

Data should be retained no longer than necessary. Use **sanitization** technology to ensure that no traces of data remain on media (data remnance) before discarding it.

- **Erasing** performs a delete operation on a file but the data remains on disk.
- **Clearing** overwrites the data with random values to ensure that it is sanitized.

Data Role	Description
Data Owner	Senior-level executive who establishes rules and determines controls
System Owner	Individual responsible for overseeing secure operation of systems
Data Processor	Individual with access to personal or sensitive information

When responding to a security incident, organizations should follow a six-step incident response process, shown in the figure below:



Domain 6:
Cryptography and PKI

Forensic investigators must take steps to ensure that they do not accidentally tamper with evidence and that they preserve the **chain of custody** documenting evidence handling from collection until use in court.

When performing forensic analysis, be certain to observe the **order of volatility** and capture information that is not likely to exist for a long period of time first.

Forensic analysts should perform their work using an image of original evidence whenever possible. MInimize the handling of the original evidence.

Common use cases for encryption include:
- Providing confidentiality for sensitive information
- Confirming the integrity of stored or transmitted information
- Authenticating users

The two basic cryptographic operations are **substitution** which modifies characters and **transposition**, which moves them around.

Symmetric encryption uses the same shared secret key for encryption and decryption.

In **asymmetric encryption**, users each have their own public/private keypair. Keys are used as follows:

	Confidentiality	Digital Signature
Sender Encrypts with...	Recipient's public key	Sender's private key
Recipient Decrypts with...	Recipient's private key	Sender's public key

Anything encrypted with one key from a pair may only be decrypted with the other key from that same pair.

Symmetric Cryptography Requires	Asymmetric Cryptography Requires
$\frac{n(n-1)}{2}$ keys	$2n$ keys

Secure symmetric algorithms include 3DES, AES, IDEA, Twofish, and Blowfish. DES and RC4 are not secure. Secure asymmetric algorithms include RSA, El Gamal, and elliptic curve (ECC).

The **Diffie-Hellman** algorithm may be used for secure exchange of symmetric keys.

Hashes are **one-way functions** that produce a unique value for every input and cannot be reversed.

Common hashing algorithms include SHA, HMAC, and RIPEMD. The MD5 hashing algorithm is still widely used but has significant security vulnerabilities.
Transport Layer Security (TLS) is the replacement for Secure Sockets Layer (SSL) and uses public key cryptography to exchange a shared secret key used to secure web traffic and other network communications.

The **Trusted Computing Base (TCB)** is the secure core of a system that has a **secure perimeter** with access enforced by a **reference monitor**.

Data State	Description
Data at Rest	Data stored on a system or media device
Data in Motion	Data in transit over a network
Data in Use	Data being actively processed in memory

When configuring security for a wireless network, always use the **WiFi Protected Access (WPA or WPA2)** protocols. Both versions of this protocol are secure. The **Wired Equivalent Privacy (WEP)** protocol is insecure. WPA uses the **Temporal Key Integrity Protocol (TKIP)** to rapidly change encryption keys while WPA2 uses the **CCM Mode Protocol (CCMP)** to provide security.

Digital certificates are a secure means to provide an unknown third party with a trusted copy of the public key belonging to an individual, organization, or device. Digital certificates are issued by a trusted **Certificate Authority (CA)**. When creating a digital certificate, the CA takes a copy of the subject's public key along with other certificate information and then digitally signs the certificate using the CA's private key. When a user or application wishes to verify the digital certificate, they do so by validating the digital signature using the CA's public key. If the signature is authentic and the CA is trusted, the public key may then be trusted.

Domain 6:
Cryptography and PKI

Certificate authorities may revoke a digital certificate by placing it on the **Certificate Revocation List (CRL)**. However, this approach is slow and is replaced by the **Online Certificate Status Protocol (OCSP)** which provides real-time certificate verification.

Digital certificates issued by CAs come in three varieties. They differ in the amount of verification performed by the CA before issuing the certificate.

Certificate Type	Validation Performed
Domain validation (DV)	CA verifies that the certificate subject controls the domain name. Weakest form of validation.
Organization validation (OV)	CA verifies the name of the business purchasing the certificate in addition to domain ownership.
Extended validation (EV)	CA performs additional checks to verify the physical presence of the organization at a registered address.

Organizations not wishing to purchase a digital certificate from a CA may create their own **self-signed certificates**. These certificates are fine for internal use but will not be trusted by external users.