Domain 1:
General Security Concepts

The main goals of information security are:

- **Confidentiality** prevents unauthorized disclosure.
- **Integrity** prevents unauthorized alteration.
- **Availability** ensures authorized access.
- **Non-repudiation** means that someone who performed some action, such as sending a message, cannot later deny having taken that action.
- **Digital signatures** are commonly used to achieve non-repudiation.

Security controls are divided into four categories, based upon how they function:

Category	Description
Managerial	Procedural mechanisms that focus on the mechanics of the risk management process
Operational	Processes that we put in place to manage technology in a secure manner
Technical	Uses technological means to meet a security objective
Physical	Uses physical constraints to meet a security objective

We can also classify security controls into six different types, based upon what they are designed to achieve:

Type	Description
Preventive	Stops an adversary from violating security policies.
Deterrent	Discourages an adversary from even attempting an attack.
Detective	Identifies potential violations of security policies.
Corrective	Restores the original state after a security incident.
Compensating	Fills the gap when it is not possible to implement a required control.
Directive	Informs employees and others what they should do to achieve security objectives.

The **defense-in-depth** principle requires the use of overlapping controls to meet the same control objective, protecting against the failure of an individual control.

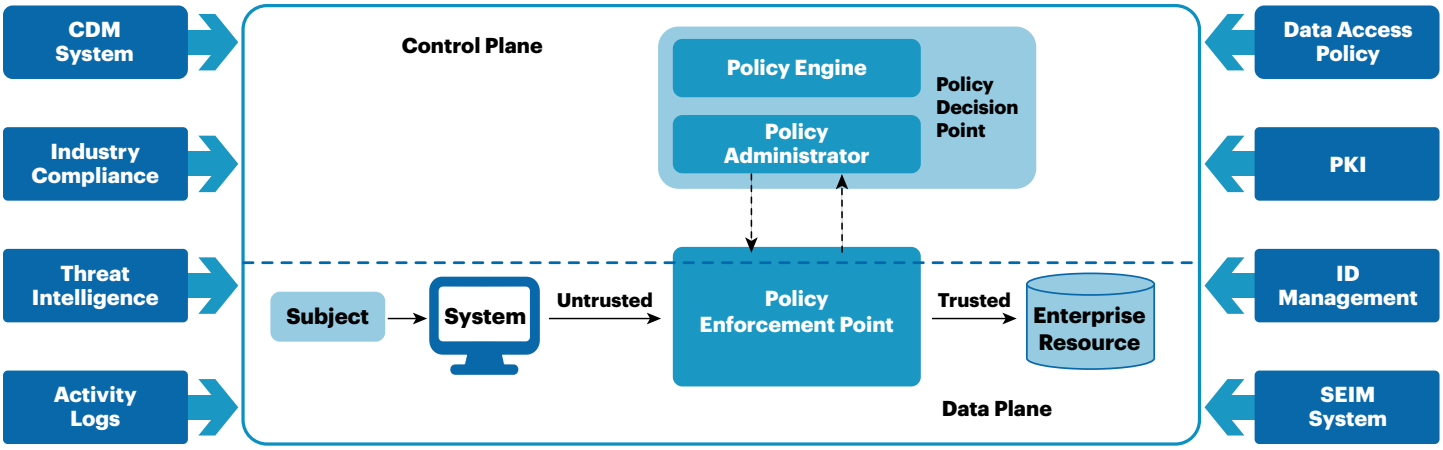
During a **gap analysis**, you review control objectives and examine the controls designed to achieve those objectives. If there are any cases where the controls do not meet the control objective, that is an example of a gap.

Sensor Type	Description
Infrared	Detects the presence of people using heat radiation
Pressure	Detects shifting weight on a pressure plate
Microwave	Detects people and objects present in an area
Ultrasonic	Detects inaudible sound waves

Zero Trust network access never grants trust implicitly, such as based upon an IP address, but continuously reevaluates trust. The **Control Plane** makes decisions about access and the **Data Plane** is where those decisions are enforced.

Domain 1:
General Security Concepts

Core Zero Trust Logical Components



Fencing may be used to prevent or deter anyone from entering an area. **Bollards** may be used to prevent vehicles from entering an area while permitting pedestrian access. They should be used in conjunction with proper **lighting** and **security guards**.

Deception Technology	Description
Honeypot	System that serves as a decoy to attract attackers
Honeynet	Unused network designed to capture probing traffic
Honeyfile	File that serves as a decoy to attract attackers
Honeytoken	Information that looks legitimate but is designed to identify attackers when accessed

Encryption protects sensitive information from unauthorized disclosure by making it unreadable to anyone without the appropriate decryption key.

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

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

In **asymmetric encryption**, users each have their own public/private key pair. 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, Twofish, and Blowfish. DES and RC4 are not secure. Secure asymmetric algorithms include RSA, El Gamal, and elliptic curve (ECC).

Domain 1: General Security Concepts

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.

The **hardware root of trust** is established through the use of the **trusted platform module (TPM)** and provides assurance that hardware has not been tampered with. The boot process for a system is managed by the **Unified Extensible Firmware Interface (UEFI)** which replaces the older BIOS approach. High security applications may require the use of a **trusted foundry** for chips that establishes a high degree of assurance that the chip was securely built.

Data minimization techniques lower risk by decreasing the amount of sensitive information maintained by the organization. When data can't be eliminated, **data obfuscation** techniques may render it less sensitive.

Data obfuscation techniques include:

- **Hashing** uses a hash function to transform a value in our dataset to a corresponding hash value.
- **Tokenization** replaces sensitive values with a unique identifier using a lookup table.
- **Data masking** partially redacts sensitive information by replacing some or all of sensitive fields with blank characters.
- **Steganography** embeds information in an image, video, audio, or other binary file to escape detection.

Key stretching is used to create encryption keys from passwords in a strong manner. PBKDF2 uses thousands of iterations of salting and hashing to generate encryption keys that are resilient against attack.

Blockchain creates a data store that nobody can tamper with by using a distributed and immutable **open public ledger**.

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.

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.

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.

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.

Domain 2:
Threats, Vulnerabilities, and Mitigations

You should be familiar with the most common categories of cybersecurity threat actor:

- **Nation-state** actors hack into foreign governments or corporations. The motive can be political or economic.
- **Unskilled attackers** are generally low-skilled attackers seeking a quick thrill.
- **Hacktivists** use hacking techniques to accomplish some activist goal motivated by the greater good.
- **Insider threats** occur when an employee or other individual with authorized access uses that access to attack the organization.
- **Organized crime** groups use cyberattacks for financial gain.
- **Shadow IT** takes place where individuals and groups seek out their own technology solutions. It poses a risk to the organization because it puts sensitive information in the hands of vendors outside of the organization's control.

Zero-day attacks exploit vulnerabilities that are yet not known to other attackers or cybersecurity teams.

Attackers may be internal to the organization or external threats. They have varying levels of sophistication and funding and may be motivated by:

- Data exfiltration
- Espionage
- Service disruption
- Blackmail
- Financial gain
- Philosophical/political beliefs
- Ethical intent
- Revenge
- Disruption/chaos
- War

As adversaries plan their attacks, they take advantage of different threat vectors:

- Message-based (Email, SMS, IM)
- Image-based
- File-based
- Voice call
- Removable devices
- Vulnerable software
- Unsupported systems/applications
- Unsecure networks
- Open service ports
- Default credentials
- Supply chain vulnerabilities
- Human vectors

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	Masquerades as desirable software to trick users into installing it.
Remote Access Trojan	Trojan horse that allows an attacker to gain remote access to a system.
Spyware	Monitors user activity, such as keystrokes and web visits. Keyloggers are an example of spyware.
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.
Botnet	Network of compromised systems that an attacker controls through the use of a command and control mechanism. Commonly used in denial of service attacks.
Bloatware	Unwanted software installed at the same time as a legitimate application install.

Domain 2:
Threats, Vulnerabilities, and Mitigations

Social engineering attacks manipulate individuals to gain unauthorized access or information.

Social engineering attacks exploit seven main mechanisms: **authority, intimidation, consensus, scarcity, familiarity, trust,** and **urgency.** 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.
Vishing	Solicits information via voice telephone calls.
Smishing	Solicits information via SMS text message.
Pretexting	Uses a fake scenario to manipulate someone into divulging confidential information.
Brand Impersonation	Mimics the identity of a trusted entity or brand to deceive individuals.
Typosquatting	Registers misspellings of common domain names to attract traffic.
Business Email Compromise (BEC)	Impersonates a company executive or other high-level employee in an attempt to deceive someone within the company. Commonly involves requests to transfer funds, fraudulent invoices, or impersonating attorneys.
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 visit.
Impersonation	Attacks where the attacker is able to appear to a remote user/system as another individual.

Misinformation is the dissemination of false information without malicious intent, while **disinformation** involves malicious intent.

On-path 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.

Password attacks seek to defeat the security of password-based authentication. Common password attacks include:

- **Brute force attacks** attempt to simply guess passwords repeatedly.
- **Dictionary attacks** guess passwords using a dictionary of words and phrases.
- **Password spraying attacks** are similar to dictionary attacks, using lists of common passwords.
- **Credential stuffing attacks** take lists of usernames and passwords from a compromised site and attempt to use them to login at another site.
- **Rainbow table attacks** precompute the hashes of common passwords and use them against a stolen password file. Rainbow table attacks may be defeated by using salted passwords.
- **Pass the hash attacks** reuse hashed credentials from one machine to login to another machine.

Birthday attacks seek to find **collisions** in hash functions, where the hash function generates the same value for two different inputs.

The OWASP Top Ten Web application security risks are:

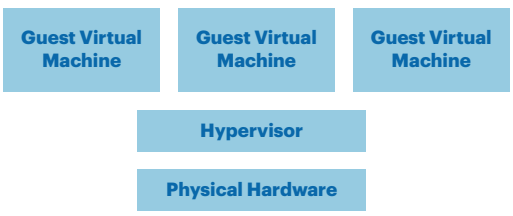
1. Broken access control
2. Cryptographic failures
3. Injection
4. Insecure design
5. Security misconfiguration
6. Vulnerable and outdated components
7. Identification and authentication failures
8. Software and data integrity failures
9. Security logging and monitoring failures
10. Server-side request forgery (SSRF)

Domain 2:
Threats, Vulnerabilities, and Mitigations

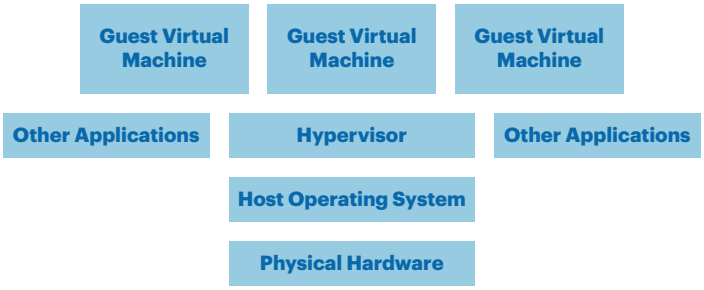
Attack Type	Description
SQL injection	Manipulates web applications to send unauthorized commands to the back-end database
Overflow	Places more data than expected in a memory buffer in an attempt to execute unauthorized code
Remote code execution	Allows an attacker to execute code of their choosing without accessing the system directly
Directory traversal	Embeds periods and slashes in URLs in an attempt to navigate the web server's file system
Privilege escalation	Exploits that allow an attacker to take a normal user account and manipulate it to gain administrative access. Often performed using a rootkit.
Session hijacking	Attacks where the adversary steals a cookie or other session credential to take over a user's existing authenticated session.
Cross-site scripting (XSS)	Attacks where the adversary tricks the user's browser into executing embedded scripts that are either stored on a web server (persistent XSS) or use input that is repeated as output (reflected XSS).
Race condition	Attacks that depend upon the timing of two operations.
TOC/TOU	Race condition that occurs when a program checks access permissions too far ahead of a resource request.

Virtual machines allow us to run multiple operating system instances on a single physical server. In a virtualized environment, the **hypervisor** is responsible for enforcing isolation.

Type 1 Hypervisor



Type 2 Hypervisor



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 2:
Threats, Vulnerabilities, and Mitigations

Indicators of compromise (IoC) are items of unusual activity that may suggest a security incident and require further investigation. Examples of IoC include:

- Unexpected account lockout
- Concurrent session usage
- Blocked content
- Impossible travel time
- Excessive resource consumption
- Resource inaccessibility
- Out-of-cycle logging
- Missing logs

When configuring security for a wireless network, you should use recent versions of **Wi-Fi Protected Access (WPA2** or **WPA3)**. The original version of WPA, which used the **Temporal Key Integrity Protocol (TKIP)** is no longer secure. WPA2 uses **CCMP** to provide security, while WPA3 uses **Simultaneous Authentication of Equals (SAE)**.

Network segmentation places different types of systems on different network segments, minimizing the likelihood of cross-infection. This may be done with physically separate networks or with virtual networks **(VLANs)**. Extremely sensitive network segments may be separated by an **air gap**, meaning they are not connected to any other network. **Virtual private clouds (VPCs)** are used to create virtual network segmentation in cloud environments.

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.

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.

Endpoint monitoring provides important operational information to cybersecurity analysts because endpoint behavior is often the first indicator of a compromise.

Endpoint detection and response (EDR) systems provide this insight, while **user and entity behavior analytics (UEBA)** solutions allow deeper behavioral inspection.

Domain 3: Security Architecture

Tool	Description
Intrusion Detection System	Monitors a host or network for signs of intrusion and reports to administrators.
Intrusion Prevention System	Monitors a host or network for signs of intrusion and attempts to block malicious traffic automatically.
Security Information & Event Management System	Aggregates and correlates security information received from other systems.
Firewall	Restricts network traffic to authorized connections.
Application Allow List	Limits applications to those on an approved list.
Application Deny List	Blocks applications on an unapproved list.
Sandboxing	Provides a safe space to run potentially malicious code.
DNS Sinkhole	Uses false DNS replies to block access to known malicious sites
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	Screens inbound messages for malicious content.
Cloud Access Security Broker (CASB)	Service that intercepts requests headed for cloud services to confirm their compliance with organizational security policies
Hardware Security Module (HSM)	Stores and manages encryption keys

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 Access Control** systems screen devices before allowing them to connect to the network. This screening may include both user authentication and device health checking.

Know the secure alternatives to commonly used protocols:

Insecure Protocol	Secure Alternative(s)
Telnet	SSH
HTTP	HTTPS
LDAP	LDAPS
FTP	FTPS or SFTP
DNS	DNSSEC
SNMPv1/2	SNMPv3

Power Issue	Brief Duration	Prolonged Duration
Loss of power	Fault	Power loss/power failure
Low voltage	Sag	Under-voltage event
High voltage	Spike	Surge
Disturbance	Transient	Noise

Access control vestibules use a set of double doors that open one at a time to restrict physical access to a facility.

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.

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.

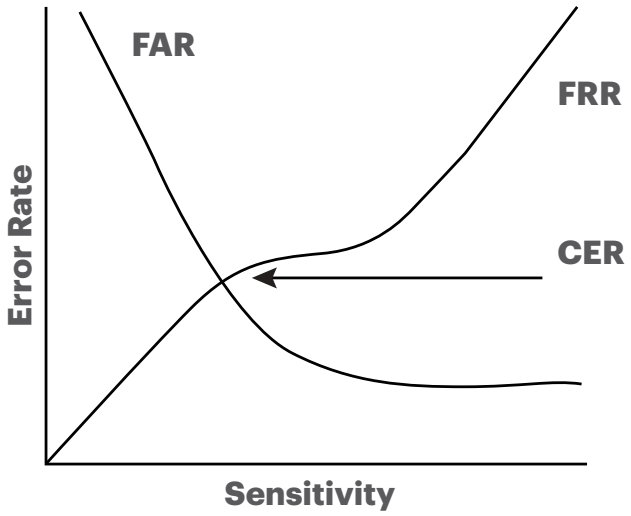
In access control systems, we seek to limit the access that **subjects** (e.g. users, applications, processes) have to **objects** (e.g. information resources, systems).

Domain 3:
Security Architecture

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

- **Something you know** factors rely upon secret information, such as a password.
- **Something you have** factors rely upon physical possession of an object, such as a smartphone.
- **Something you are** factors rely upon biometric characteristics of a person, such as a face scan or fingerprint.
- **Somewhere you are** factors rely upon a user's physical location.

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 below:



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	HVAC/Power	Configured Servers	Real-time Data
Cold Site	Yes	No	No
Warm Site	Yes	Yes	No
Hot Site	Yes	Yes	Yes

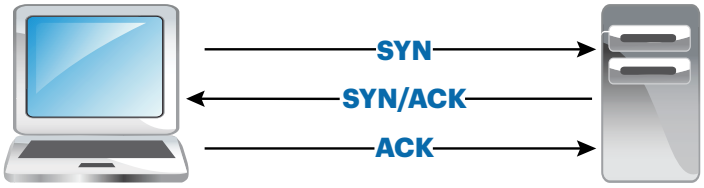
Disaster recovery plans require testing. There are four major test types:

DR Test Type	Description
Tabletop exercises	Plan participants review the plan and their specific role as a group or individually.
Simulation	DR team participates in a scenario-based exercise that uses the DR plan without implementing technical recovery controls.
Parallel processing	DR team activates alternate processing capabilities without taking down the primary site.
Fail over	DR team switches the primary site to a secondary site to simulate a disaster.

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

Domain 3:
Security Architecture

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.

Load balancers distribute connection requests among many identical servers.

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	Routes 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

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.

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.

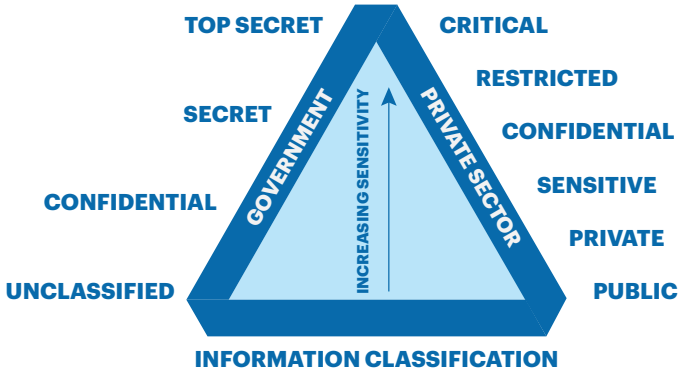
IPSec uses **Authentication Headers (AH)** to provide authentication, integrity and non-repudiation, and **Encapsulating Security Payload (ESP)** to provide confidentiality, authentication and integrity.

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

Common classes of sensitive information include:

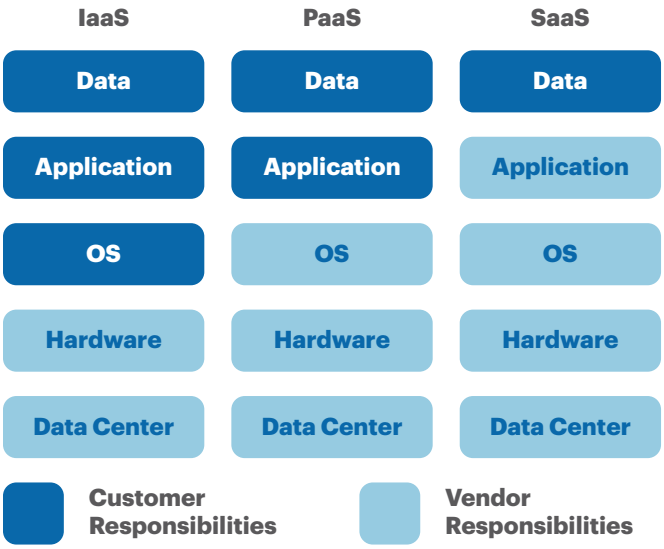
- **Personally identifiable information (PII)** uniquely identifies individuals and is regulated by many national, state and local laws. The most well known of these are the European Union's **General Data Protection Regulation (GDPR)** and the **California Consumer Privacy Act (CCPA).**
- **Protected health information (PHI)** includes individual health records and is regulated by the **Health Insurance Portability and Accountability Act (HIPAA).**
- **Payment card information (PCI)** includes credit and debit card data and is regulated by the **Payment Card Industry Data Security Standard (PCI DSS).**
- **Proprietary information** includes trade secrets maintained by an organization.

Domain 3:
Security Architecture



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

Security in the cloud follows the **shared responsibility model** where vendors and customers have different responsibilities depending upon the category of cloud service.



Data retention standards describe how long the organization should preserve records. Data that is no longer needed should be securely destroyed. The principle of **data sovereignty** says that data is subject to the legal requirements of any jurisdiction where it is collected, stored, processed, or transmitted. 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.

Domain 4:
Security Operations

Threat intelligence allows an organization to learn about changes in the threat landscape, including attacker identities, tools, and techniques. Common threat intelligence sources include:

- Open source intelligence (OSINT)
- Proprietary threat intelligence from security vendors
- Vulnerability databases
- Information sharing and analysis centers (ISACs)
- Dark web sites
- Indicators of compromise

Threat hunting exercises presume that attackers have already compromised an organization and then seek out evidence of that compromise.

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
636	LDAPS
1433/1434	SQL Server
1521	Oracle
1720	H.323
1723	PPTP
3389	RDP
9100	HP JetDirect Printing

Structured Threat Information eXpression (STIX) is used to provide a standardized format for exchanging threat information, while the **Trusted Automated eXchange of Intelligence Information (TAXII)** defines a protocol for the transmission of this information between components of a security automation environment.

Enterprises may deploy mobile devices in a variety of models:

- **Corporate-owned (CO)** provides devices for business use only.
- **Corporate-owned, personally enabled (COPE)** allows users to mix business and personal use.
- **Choose your own device (CYOD)** allows users to pick a device of their choice for business and personal use.
- **Bring your own device (BYOD)** allows users to access corporate data on their personally-owned devices.

Companies should use **mobile device management (MDM)** tools to enforce a variety of mobile security controls, including:

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

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 4: Security Operations

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**.

Validation of remediation includes **verifying** the remediation, **rescanning** the affected system(s), and periodic **auditing**.

Common parameters that you may tune when configuring vulnerability scans include:

- Using **credentialed scans** to log onto target systems and improve scan accuracy.
- Using a combination of **server-based** scans that run over the network and **agent-based** scans that run on the local system.
- Using different scan perspectives to determine the **external** view that an outside attacker would see and the **internal** view available to an insider or an attacker that has already gained a foothold on the network.

Active scanning techniques engage with the target system to probe it for known vulnerabilities while **passive scanning** techniques are stealthier. Passive scans do not engage with the target system but attempt to identify vulnerabilities by observing network traffic and other system characteristics.

The **Security Content Automation Protocol (SCAP)** provides a standard framework for vulnerability assessment. It includes the following components:

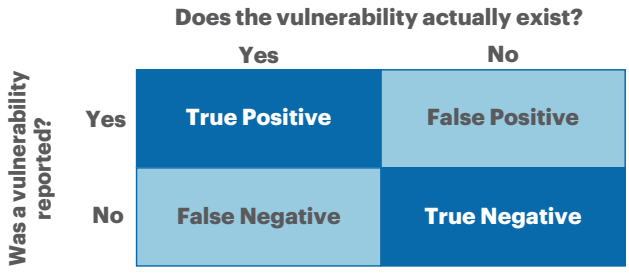
- Common Vulnerabilities and Exposures (CVE)
- Common Vulnerability Scoring System (CVSS)
- Common Configuration Enumeration (CCE)
- Common Platform Enumeration (CPE)
- Extensible Configuration Checklist Description Format (XCCDF)
- Open Vulnerability and Assessment Language (OVAL)

The **Common Vulnerability Scoring System (CVSS)** rates the severity of security vulnerabilities based upon eight criteria:

1. Attack Vector (AV)
2. Attack Complexity (AC)
3. Privileges Required (PR)
4. User Interaction (UI)
5. Scope (S)
6. Confidentiality (C)
7. Integrity (I)
8. Availability (A)

The CVSS base score combines all eight of these factors into a single score from 0.0 to 10.0, with the following severity descriptions:

CVSS Score	Rating
0.0	None
0.1-3.9	Low
4.0-6.9	Medium
7.0-8.9	High
9.0-10.0	Critical

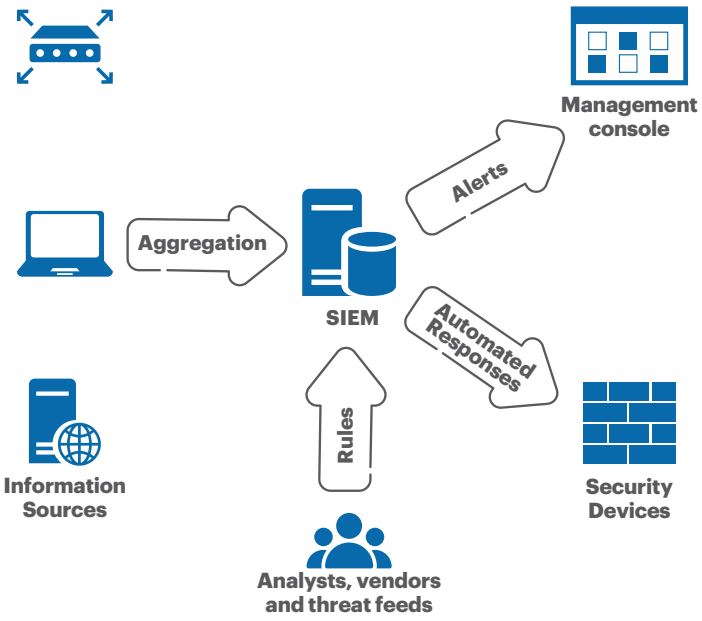


Bug bounty programs offer public rewards to security researchers who submit reports of new vulnerabilities to a firm.

Domain 4:
Security Operations

Security information and event management (SIEM) systems aggregate and correlate security log information received from many different sources.

Security orchestration, automation, and response (SOAR) systems use runbooks to trigger automated responses after security incidents occur.



Common use cases for automation and orchestration include:

- User and resource provisioning
- Creation of guard rails
- Security group management
- Ticket creation and escalation
- Enabling/disabling services and access
- Continuous integration and testing
- Integrations and APIs

The benefits of automation and orchestration include:

- Efficiency/time saving
- Enforcing baselines
- Standard infrastructure configurations
- Scaling in a secure manner
- Employee retention
- Reaction time
- Workforce multiplier

Administrators should also be aware of some other considerations related to automation and orchestration:

- Complexity
- Cost
- Creation of a single point of failure
- Technical debt
- Ongoing supportability

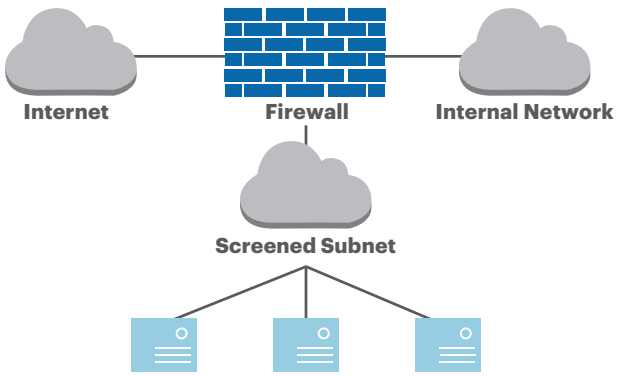
Security professionals working with specialized systems, such as **Supervisory Control and Data Acquisition (SCADA)** and **Industrial Control Systems (ICS)** should isolate those systems from other networks to the greatest extent possible.

Specialized technologies support the **Internet of Things (IoT)** and its embedded devices. These include **real-time operating systems (RTOS)** that are designed to serve as streamlined, efficient operating systems for use on IoT devices as well as **system on a chip (SoC)** technology that includes an operating system in firmware stored directly on a device.

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 **screened subnet** that houses publicly accessible servers. These networks are often created using a triple-homed firewall.

Domain 4:
Security Operations



Firewall Type	Description
Layer 4	Works at the transport layer, moderating connections between networks
Layer 7	Works at the application layer, inspecting network traffic with a great deal of context
Web Application Firewall (WAF)	Special type of layer 7 firewall focused specifically on web applications
Next-Generation Firewall (NGFW)	Firewall that incorporates information about users, applications, and other context into decision-making
Unified Threat Management (UTM)	Combines several security functions, including firewall capabilities into a single device. Typically used in a small/medium business environment.

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

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.

Attribute-based access control (ABAC) makes access decisions based upon attributes of a user's identity, such as department membership or job title.

Rule-based access control makes decisions based upon pre-defined rules. Firewalls are a common example of devices that enforce a rule-based policy.

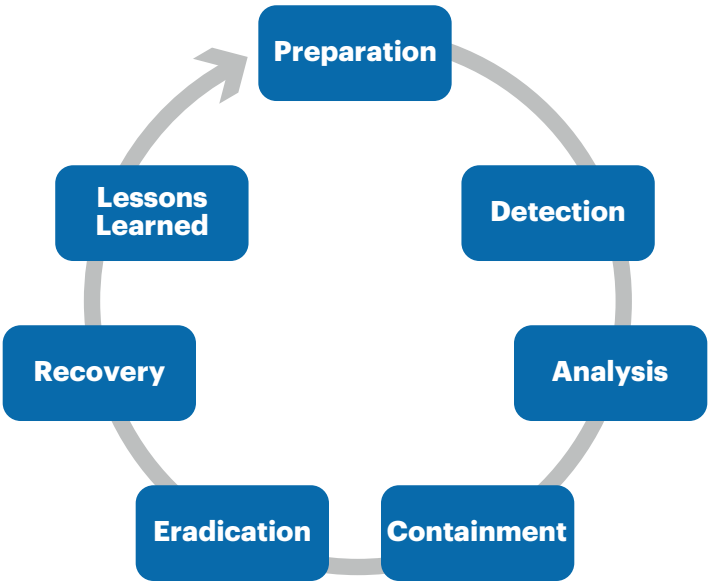
Transport Layer Security (TLS) is the replacement for Secure Sockets Layer (SSL) and uses public key cryptography to exchange a shared secret key used to secure web traffic and other network communications.

Email headers provide information about the path traveled by email messages across the network, although they are susceptible to forgery. **DomainKeys Identified Mail (DKIM)** allows organizations to sign both the body of the message and elements of the header to prove their authenticity. **Sender Policy Framework (SPF)** allows organizations to publish a list of authorized mail servers for their domains.

Domain 4:
Security Operations

Domain-based Message Authentication, Reporting, and Conformance (DMARC) uses SPF and DKIM to determine whether messages are authentic.

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



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.

As you prepare for an incident response effort, you should develop an **incident communication plan** that uses a secure means of communication to **limit communication** to trusted parties and prevent the inadvertent release of information.

Generally, you are not required to disclose security incidents to law enforcement unless you choose to do so or are subject to **legal or regulatory requirements**.

Your **incident response team** should include representatives from all relevant internal teams:

- Cybersecurity
- Other technology experts
- Legal
- Human resources
- Public relations
- Senior leadership

You should also have your team prepared to **coordinate** with external groups that are not represented directly on the team, including law enforcement and regulatory bodies.

Incident response plans should base the severity of an incident on the criticality of data involved, paying particular attention to:

- Personally identifiable information (PII)
- Protected health information (PHI)
- Personal financial information
- Sensitive personal information (SPI)
- Intellectual property and other corporate high-value assets

The **preparation phase** of incident response should include **training**, **testing**, and **documentation** of procedures.

Domain 4:
Security Operations

The **detection and analysis phases** of incident response determine that an incident is underway and determine the severity level and appropriate response. The objective of the **containment phase** is to limit the damage caused by the incident through the isolation of affected systems and assets. This is closely linked to **eradication and recovery** efforts that seek to restore normal operations.

During the **post-incident activities phase**, the organization conducts a **lessons learned** process, updates change management records, determines what evidence should be retained, writes an incident report, and makes any necessary updates to the incident response plan.

Many different data sources can support security investigations. These include:

- Firewall logs
- Application logs
- Endpoint logs
- OS-specific security logs
- IPS/IDS logs
- Network logs
- Metadata
- Vulnerability scans
- Automated reports
- Dashboards
- Packet captures

Log review provides cybersecurity analysts with insight into the behavior of users, systems, and network devices. Logs may be sent to a centralized log repository using the **syslog** protocol.

Network device logs often arrive using the **Simple Network Management Protocol (SNMP)** and may be accessed using vendor-specific commands. On Cisco devices, the show logging command provides access to router logs. Cisco devices report log events using a standard system of **log levels** that are numbered in decreasing order of severity:

Level	Level Keyword
0	Emergencies
1	Alerts
2	Critical
3	Errors
4	Warnings
5	Notifications
6	Informational
7	Debugging

Analysts can collect network traffic using the graphical **Wireshark** packet capture tool or the command-line **tcpdump** packet capture tool. They may send captured packets back out on the network using the **tcpreplay** tool.

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.

Domain 5:
Security Program Management and Oversight

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 Policy	Description
Acceptable Use Policy (AUP)	Defines how individuals may use corporate computing resources and information.
Information Security Policy	Creates the framework for the information security program and establishes authority for security activities.
Business Continuity/Disaster Recovery Policy	Defines the organization's approach to business continuity and disaster recovery planning and activities.
Incident Response Policy	Creates requirements for handling security and privacy incidents within the organization.
SDLC Policy	Defines the organization's software development lifecycle (SDLC) approach.
Change Management Policy	Establishes the organization's change and configuration management program.

Common standards define technical requirements for:
- Passwords
- Access controls
- Physical security
- Encryption

Organizations create step-by-step procedures for many routine activities, including:
- Change management
- Onboarding and offboarding
- Incident response playbooks

Data Role	Responsibilities
Data Owner	Senior-level executive who establishes rules and determines appropriate controls for information.
Data Steward	Person who is delegated authority for data by the data owner and acts on the data owner's behalf.
Data Controller	Organization or person within an organization who determines the purpose and means of data processing. Special significance under GDPR.
Data Custodians	Individuals who are responsible for managing data and data security controls for an organization. This role is commonly found within IT teams.
Data Processor	An organization that handles information on behalf of another organization, typically a business-to-business relationship.
Data Users	Individuals who interact with information during the normal course of business.
Data Subjects	Individuals who may be individually identified by name or another identifier within the records maintained by an organization.

Security audits use testing and assessment techniques but are performed by independent auditors. There are three types of security audits:
- **Internal audits** are performed by an organization's internal audit staff, normally led by a Chief Audit Executive who reports directly to the CEO.
- **External audits** are performed by an outside auditing firm.
- **Third-party audits** are conducted by, or on behalf of, another organization, such as a regulator.

Domain 5:
Security Program Management and Oversight

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

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

Audits of cloud service providers and other managed service providers should take place using the **System and Organization Controls (SOC)** standard, published in the Statement on Standards for Attestation Engagements #18 (SSAE 18).

There are three categories of SOC audits:
- **SOC 1** audits provide customers with the level of assurance they need when conducting their own financial audits.
- **SOC 2** audits evaluate the service provider's confidentiality, integrity, and availability controls. They contain sensitive information.
- **SOC 3** audits also evaluate confidentiality, integrity, and availability but are meant for public disclosure.

And there are two types of SOC 1 and SOC 2 audits:
- **Type I audits** describe the controls that the service provider has in place and offer an opinion on their suitability, but not their effectiveness.
- **Type II audits** describe the controls that the service provider has in place, offer an opinion on their suitability, and also provide the results of auditors' effectiveness tests.

SOC 1 and 2 audits can have type I or II reports. SOC 3 audits do not have different type reports.

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.

When accepting a risk, the organization may choose to grant an **exception** to or **exemption** from security policies and standards.

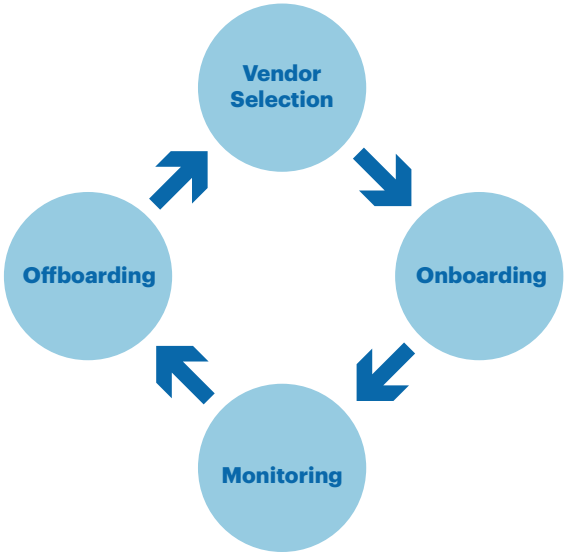
Risks should be documented in a **risk register** which includes details on the **key risk indicators (KRIs), risk owners,** and **risk thresholds**.

Organizations may have different levels of **risk appetite**:
- **Expansionary** risk appetites accept significant risks in the hope of significant rewards.
- **Conservative** risk appetites accept very little risk to preserve the status quo.
- **Neutral** risk appetites take a balanced approach to risk.

BIA Metric	Meaning
Recovery Time Objective (RTO)	The maximum amount of time the organization is willing to accept a system outage.
Recovery Point Objective (RPO)	The maximum amount of time from which the organization is willing to accept data loss.
Mean Time to Repair (MTTR)	The average time required to restore a system, application, or device to operation after a failure.
Mean Time Between Failures (MTBF)	The average time between failures of a system, application, or device.

Domain 5:
Security Program Management and Oversight

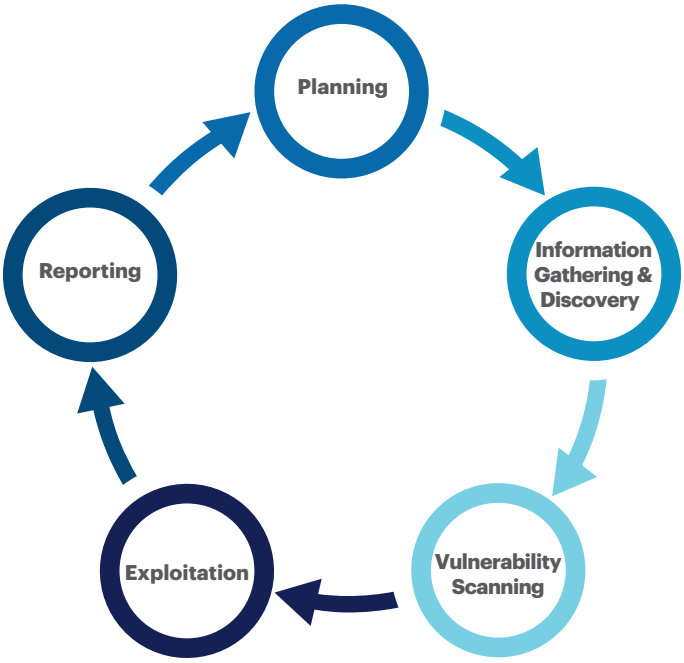
When working with **vendors**, ensure that the vendor's security policies and controls execute at least the same degree of care that you would take internally. The vendor management lifecycle follows vendors from selection through termination:



Customers should document their vendor relationships using a variety of agreements:

- **Service Level Agreements (SLA)** document the requirements for service performance in a written contract.
- **Memorandums of Understanding (MOU)** and **Memorandums of Agreement (MOA)** are used to document relationships in a less formal manner.
- **Business Partners Agreements (BPA)** document the parameters of a business partnership.
- **Master Service Agreements (MSA)** are used to create umbrella relationships with specific engagements documented in **Statements of Work (SOW)** and **Work Orders (WO)** that refer to the MSA.
- **Non-disclosure Agreements (NDA)** document the confidentiality requirements of a business relationship.

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



There are three different types of penetration test:

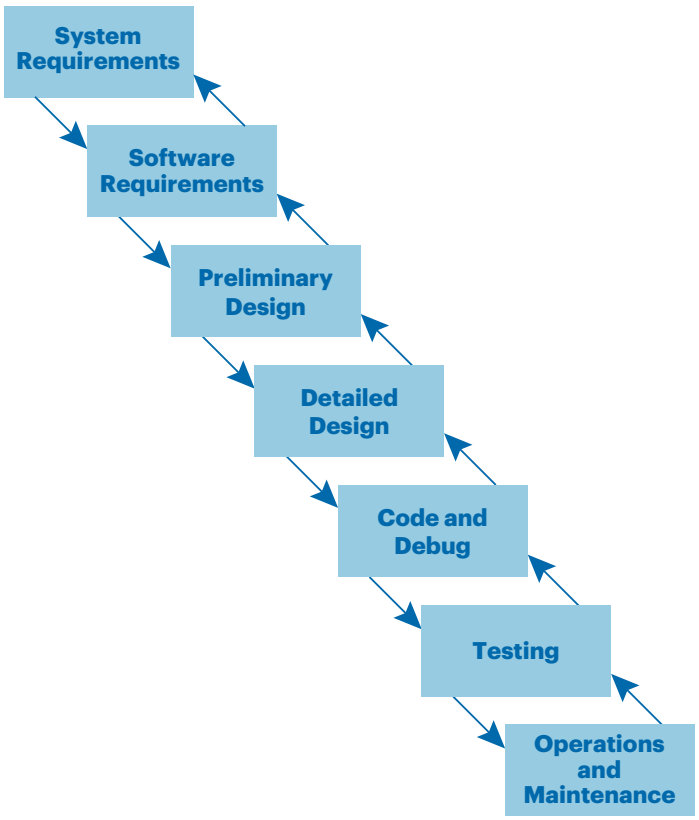
- During **known environment** penetration tests, testers have full access to information about the target systems.
- During **unknown environment** penetration tests, testers conduct their work without any knowledge of the target environment.
- **Partially known environment** penetration tests reside in the middle, providing testers with some knowledge about the environment.

Domain 5:
Security Program Management and Oversight

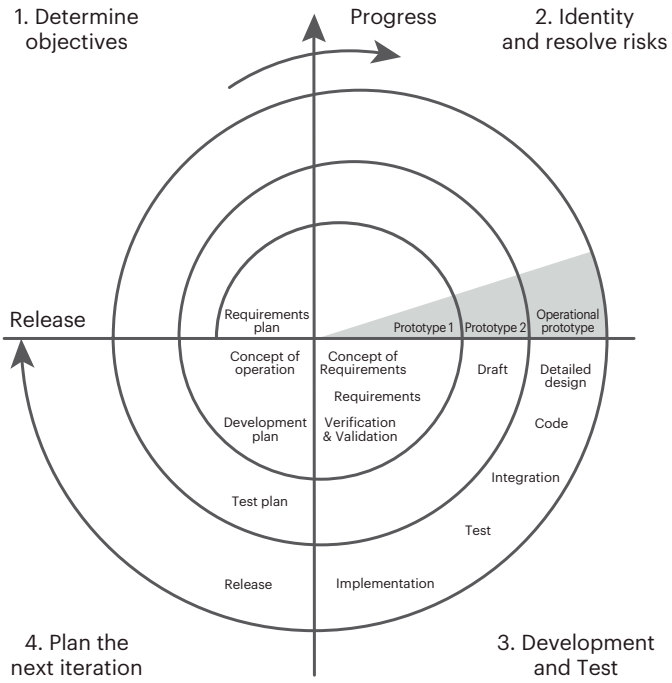
When developing new systems, organizations move them through a four-stage process using different environments:

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.

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** uses 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

Static analysis evaluates software code without executing it, while **dynamic analysis** executes the code during the test. **Fuzz testing** supplies invalid input to applications in an attempt to trigger an error state.

Domain 5:
Security Program Management and Oversight

Organizations are subject to a wide variety of legal and regulatory compliance obligations from:

- **Criminal laws** that may involve prison or fines.
- **Civil laws** that regulate non-criminal disputes.
- **Administrative laws** set by government agencies.
- **Regulations** from industry bodies.

Legal holds should be sent as soon as an organization reasonably anticipates litigation. **Collection** should occur when directed by the legal team. **Production** turns records over to the opposing side. All of these activities are part of the **e-Discovery** process.

Consequences of failure to comply with laws and regulations include:

- Fines/sanctions
- Reputational damage
- Loss of licenses
- Contractual impacts

Organizations should design their privacy programs to follow the **Generally Accepted Privacy Principles (GAPP)**. These principles include:

1. Management
2. Notice
3. Choice and Consent
4. Collection
5. Use, Retention, and Disposal
6. Access
7. Disclosure to Third Parties
8. Security for Privacy
9. Quality
10. Monitoring and Enforcement

Organizations should create **security awareness and training** programs that inform users of their security responsibilities. Topics covered should include:

- Policy/handbooks
- Situational awareness
- Insider threat
- Password management
- Removable media and cables
- Social engineering
- Phishing
- Operational security
- Hybrid/remote work environments
- Anomalous behavior recognition