Domain 1:
Security and Risk Management

CONFIDENTIALITY
INTEGRITY
AVAILABILITY

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).

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.

The major categories of intellectual property protection include:

- **Trademarks** protect words and symbols.
- **Copyrights** protect creative works.
- **Patents** protect inventions.
- **Trade secrets** require maintaining secrecy but don't expire.

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.

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

Security controls may be **preventive, detective,** or **corrective**.

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

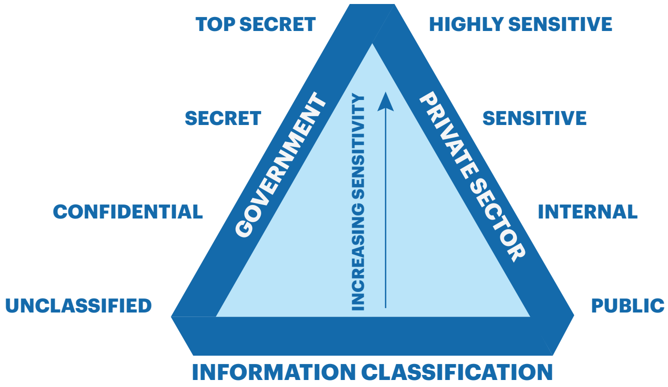
Domain 2: Asset Security

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.

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



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	Responsibilities
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

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

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

Domain 3:
Security Architecture and Engineering

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	$2\ n$ keys

Secure symmetric algorithms include 3DES, AES, IDEA, and Blowfish. DES is 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.

Digital certificates use the **X.509** standard and contain a copy of an entity's public key. They are digitally signed by a certificate authority (CA).

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**.

CPUs support two modes of operation: **user mode** for standard applications and **privileged mode** for processes that require direct access to core resources.

Model	Bell-LaPadula	Biba
Goal	Confidentiality	Integrity
Simple Property	No read up	No read down
***-Property**	No write down	No write up

Certification is the process of evaluating and assigning a security rating to a product. **Accreditation** is the approval of a specific configuration for a specific use.

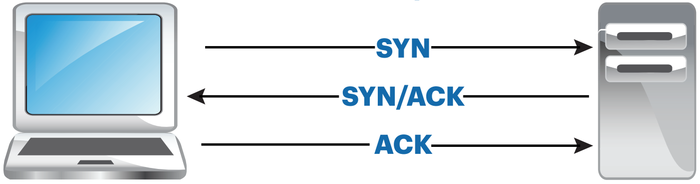
	Dedicated	System High	Compartmented	Multilevel
Users must be **cleared** for highest level of info processed by system.	Yes	Yes	Yes	No
Users must have **access approval** for all info processed.	Yes	Yes	No	No
Users must have **need to know** all info processed by system.	Yes	No	No	No

Two serious issues can occur when users are granted limited access to information in databases or other repositories. **Aggregation** attacks occur when a user is able to summarize individual records to detect trends that are confidential. **Inference** attacks occur when a user is able to use several innocuous facts in combination to determine, or infer, more sensitive information.

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

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

TCP Three-Way Handshake



Domain 4:
Communication and Network Security

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

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**.

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.

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.

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

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.

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 5:
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.

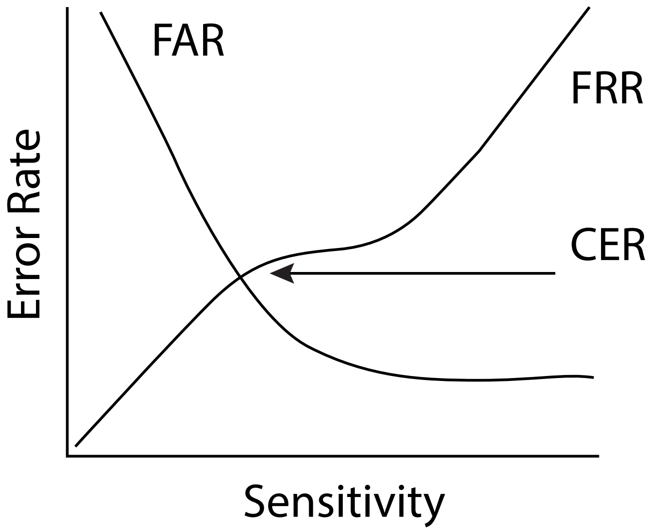
Multifactor authentication systems combine authentication technologies from two or more of the following categories:

- **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 5:
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.

Domain 6:
Security Assessment and Testing

Security tests verify that a control is functioning properly. **Security assessments** are comprehensive reviews of the security of a system, application, or other tested environment.

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.

Organizations that provide services to other organizations may conduct audits under SSAE 16. These engagements produce two different types of reports:

- **Type I reports** provide a description of the controls in place, as described by the audited organization, and the auditor's opinion whether the controls described are sufficient. The auditor does not test the controls.
- **Type II reports** results when the auditor actually tests the controls and provides an opinion on their effectiveness.

COBIT, ISO 27001, and **ISO 27002** are commonly used standards for cybersecurity audits.

Vulnerability assessments seek to identify known deficiencies in systems and applications.

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)

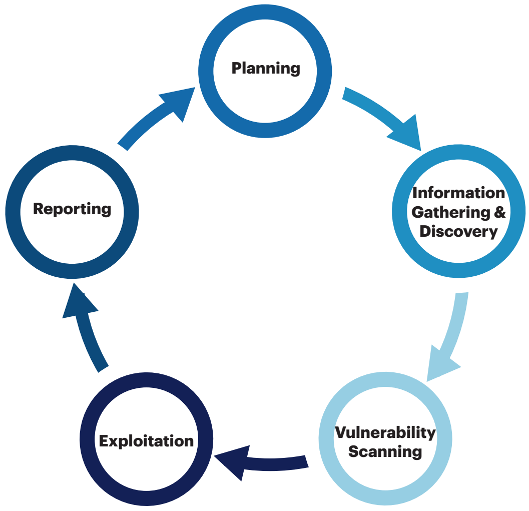
Network discovery scanning uses tools like nmap to check for active systems and open ports. Common scanning techniques include:

- **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.

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:



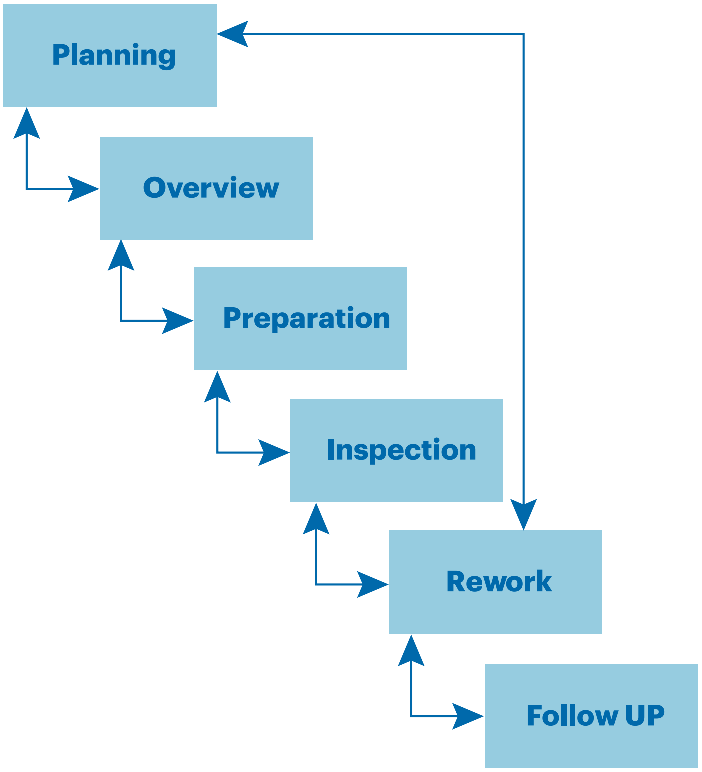
Domain 6:
Security Assessment and Testing

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.

Code review provides an important software assurance tool that allows peer review by fellow developers for security, performance, and reliability issues.

Fagan inspections are a formal code review process that follows a rigorous six-step process with formalized entry and exit parameters for each step:



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

Interface testing evaluates the connections between different system components.

Misuse case testing evaluates known avenues of attack in an application.

Test coverage analysis metrics evaluate the completeness of testing efforts using the formula:

$$\textit{test coverage} = \frac{\textit{(use cases tested)}}{\textit{(all use cases)}}$$

Common criteria for test coverage analysis include:

- **Branch coverage** (if statements tested under all conditions)
- **Condition coverage** (logical tests evaluated under all inputs)
- **Function coverage** (each function tested).
- **Loop coverage** (every loop executed multiple times, once, and not at all)
- **Statement coverage** (every line of code executed)

Domain 7:
Security Operations

Security professionals are often called upon to participate in a variety of investigations:

- **Criminal investigations** look into the violation of a criminal law and use the beyond a reasonable doubt standard of proof.
- **Civil investigations** examine potential violations of civil law and use the preponderance of the evidence standard.
- **Regulatory investigations** examine the violation of a private or public regulatory standard.
- **Administrative investigations** are internal to an organization, supporting administrative activities.

Investigations may use several different types of evidence:

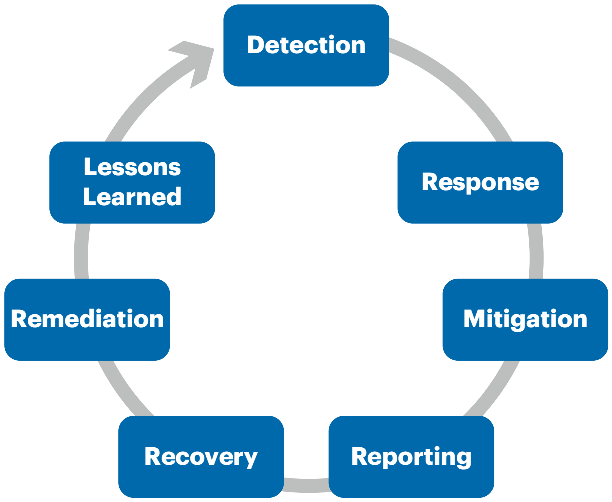
- **Real evidence** consists of tangible objects that may be brought into court.
- **Documentary evidence** consists of records and other written items and must be authenticated by testimony.
- **Testimonial evidence** is evidence given by a witness, either verbally or in writing.

The **best evidence rule** states that, when using a document as evidence, the original document must be used unless there are exceptional circumstances. The **parol evidence rule** states that a written agreement is assumed to be the complete agreement.

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.

The disaster recovery process begins when operations are disrupted at the primary site and shifted to an alternate capability. The process only concludes when normal operations are restored.

Cybersecurity incident response efforts follow this process:



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

Domain 7:
Security Operations

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
Warn Site	Yes	Yes	No
Hot Site	Yes	Yes	Yes

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.

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

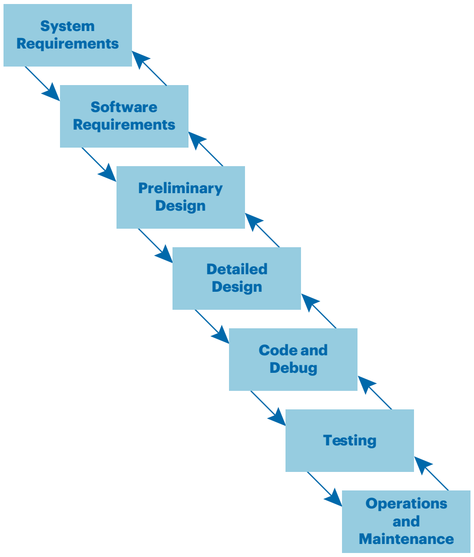
Fires require the combination of **heat, oxygen,** and **fuel**. They may be fought with fire extinguishers:

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

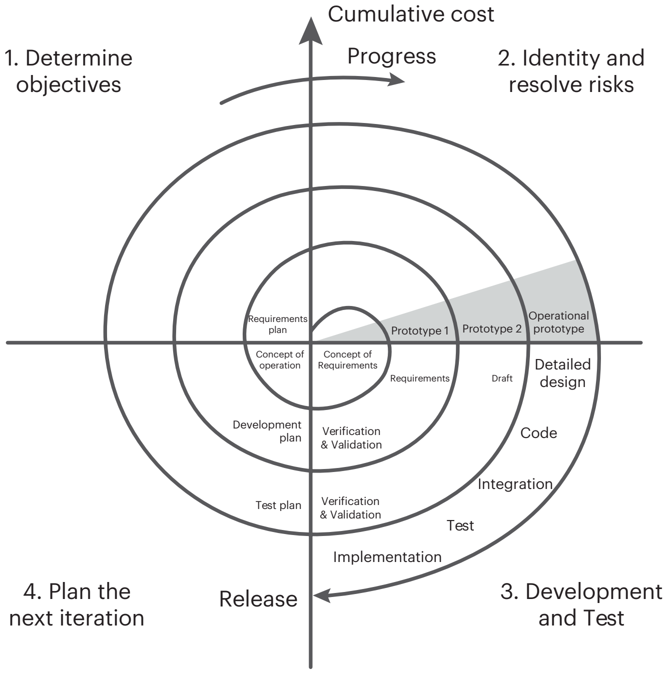
Organizations may use **wet pipe** fire suppression systems that always contain water, **dry pipe** systems that only fill with water when activated, or **preaction** systems that fill the pipes at the first sign of fire detection.

Domain 8:
Software Development Security

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

Software testing follows two primary approaches. In **static testing**, testers analyze the source code without executing it. **Dynamic testing** executes the source code against test datasets.

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.