SY0-701 Objectives
An Unofficial Reference Guide
https://networklogician.com

1.1 Compare and contrast various types of security controls

Categories:

1. **Technical Controls:**
    - Technical controls involve the use of technology to manage and control access to systems and data. Examples include firewalls, encryption, authentication mechanisms and intrusion detection systems.
    - Designed to protect against unauthorized access, detect and respond to security incidents and secure the technical aspects of information systems.
2. **Managerial Controls:**
    - Managerial controls focus on policies, procedures and the management of resources to ensure that security objectives are met. Examples include security policies, risk assessments and security awareness training.
    - To establish a framework for security governance, allocate resources effectively and guide the overall management of security within an organization.
3. **Operational Controls:**
    - Operational controls deal with the day-to-day processes and activities that support security policies and procedures. Examples include access controls, backups and incident response procedures.
    - To implement and enforce security policies, manage ongoing security operations and ensure the effective execution of security measures.
4. **Physical Controls:**
    - Physical controls are measures that protect physical assets, facilities and resources. Examples include biometric access controls, surveillance cameras and locks.
    - To safeguard the physical environment and prevent unauthorized access or damage to physical assets.

Control Types:

1. **Preventive Controls:**
    - Preventive controls are measures designed to stop security incidents before they occur. Examples include firewalls, access controls and encryption. This will reduce the likelihood of security breaches.
2. **Deterrent Controls:**
    - Deterrent controls aim to discourage potential attackers or intruders. Examples include warning signs, security patrols and visible security measures.
3. **Detective Controls:**
    - Detective controls are implemented to identify and detect security incidents or violations after they have occurred. Examples include intrusion detection systems, log analysis and security monitoring.
4. **Corrective Controls:**
    - Corrective controls are measures taken to mitigate the impact of a security incident or restore systems to a secure state. Examples include incident response procedures, system patches and data recovery processes.
5. **Compensating Controls:**
    - Compensating controls are alternative measures put in place to offset the failure or absence of primary controls. For example, implementing additional security measures if a primary control is not feasible. This can help to provide an alternative means of achieving security objectives when the primary control is not fully effective or feasible.
6. **Directive Controls:**
    - Directive controls are policies or measures that guide or instruct individuals on proper security behavior. Examples include security policies, guidelines and training programs. This will help to educate and guide individuals on security-related actions and responsibilities.

1.2 Summarize fundamental security concepts

1. **Confidentiality, Integrity and Availability (CIA):**
    - *Confidentiality:* Ensuring that information is accessible only to those who have the proper authorization.
    - *Integrity:* Guaranteeing the accuracy and reliability of information by preventing unauthorized alterations.

- *Availability:* Ensuring that systems and data are consistently accessible and usable by authorized individuals.

2. **Non-repudiation:**
    - The ability to prove the origin or delivery of a message or transaction, preventing individuals from denying their involvement.
3. **Authentication, Authorization and Accounting (AAA):**
    - *Authenticating People:* Verifying the identity of individuals accessing systems or data.
    - *Authenticating Systems:* Confirming the identity of computer systems or devices.
    - *Authorization Models:* Granting or denying access rights based on authenticated identities.
4. **Gap Analysis:**
    - An assessment of the difference between current practices and desired objectives to identify areas that need improvement.
5. **Zero Trust:**
    - *Control Plane:*
        - *Adaptive Identity:* Dynamically adjusting access based on user behavior and risk factors.
        - *Threat Scope Reduction:* Minimizing the potential attack surface by restricting access.
        - *Policy-Driven Access Control:* Implementing access policies based on continuous evaluation.
        - *Policy Administrator:* Managing and enforcing access policies centrally.
        - *Policy Engine:* The system that evaluates and enforces access policies.
    - *Data Plane:*
        - *Implicit Trust Zones:* Restricting trust assumptions and verifying access continuously.
        - *Subject/System:* Users or systems requiring access.
        - *Policy Enforcement Point:* The location where access policies are implemented and enforced.
6. **Physical Security:**
    - *Bollards:* Physical barriers to control or direct vehicle traffic.
    - *Access Control Vestibule:* An enclosed space with controlled access to enhance security.
    - *Fencing:* Physical barriers to prevent unauthorized entry.
    - *Video Surveillance:* Using cameras to monitor and record activities for security purposes.
    - *Security Guard:* Personnel responsible for monitoring and enforcing security measures.
    - *Access Badge:* A physical or digital credential granting access to specific areas.
    - *Lighting:* Illumination to enhance visibility and deter unauthorized activities.
    - *Sensors:*
        - *Infrared:* Sensors detecting heat signatures for intrusion detection.
        - *Pressure:* Devices sensing changes in pressure, often used for floor-based security.
        - *Microwave:* Sensors using microwave technology for motion detection.
        - *Ultrasonic:* Sensors detecting sound waves for surveillance and intrusion detection.
7. **Deception and Disruption Technology:**
    - *Honeypot:* A decoy system designed to attract and analyze malicious activity.
    - *Honeynet:* A network of honeypots used to detect and study cyber threats.
    - *Honeyfile:* A bait file used to detect unauthorized access or actions.
    - *Honeytoken:* A piece of information or token that, when accessed, indicates a security breach.

1.3 Explain the importance of change management processes and the impact to security

Business Processes Impacting Security Operation:

- *Approval Process:* Ensures changes are authorized by relevant stakeholders, preventing unauthorized modifications that might compromise security.
- *Ownership:* Designates responsibility, ensuring that changes are overseen by accountable individuals who consider security implications.
- *Stakeholders:* Involves relevant parties, including security experts, to provide insights and ensure changes align with security requirements.
- *Impact Analysis:* Evaluates potential consequences of changes on security, helping in preemptively addressing vulnerabilities or risks.

- *Test Results:* Verifies that changes won't negatively impact security measures and that security controls remain intact.
- *Backout Plan:* Defines a method to revert changes if security issues arise post-implementation, minimizing potential damage.
- *Maintenance Window:* Specifies a designated time for implementing changes, reducing the chance of disruptions to security operations.
- *Standard Operating Procedure:* Ensures changes adhere to established security procedures, maintaining consistent security practices.

Technical Implications:

- *Allow Lists/Deny Lists:* Ensures that only authorized entities have access, limiting security breaches caused by unauthorized users.
- *Restricted Activities:* Identifies and controls actions that could jeopardize security, preventing unintended breaches or unauthorized actions.
- *Downtime:* Minimizes the time systems are offline, reducing the window of opportunity for potential attacks.
- *Service Restart:* Ensures security configurations remain effective after restarting services, maintaining a secure state.
- *Application Restart:* Revalidates application security settings post-restart, safeguarding against security misconfigurations.
- *Legacy Applications:* Manages security risks associated with older applications that might lack modern safeguards.
- *Dependencies:* Considers how changes in one system might impact security in interconnected systems, avoiding unforeseen vulnerabilities.

Documentation:

- *Updating Diagrams:* Reflects changes in system architecture, helping stakeholders understand current security arrangements.
- *Updating Policies/Procedures:* Ensures security-related documents accurately reflect changes, maintaining compliance and best practices.

Version Control: Tracks changes to code, configurations and documentation, assisting in identifying unauthorized alterations and ensuring proper oversight.

1.4 Explain the importance of using appropriate cryptographic solutions

Public Key Infrastructure (PKI):

- *Public Key:* A cryptographic key used for encryption and verification of digital signatures.
- P*rivate Key:* A secret key paired with a public key for decryption and creating digital signatures.
- *Key Escrow:* A mechanism to securely store and manage private keys for recovery purposes.

Encryption:

- *Full-Disk Encryption:* Encrypts an entire storage device to protect data at rest.
    - *Partition:* Encrypts specific partitions on a storage device.
    - *File:* Encrypts individual files.
    - *Volume:* Encrypts logical volumes.
    - *Database:* Encrypts database contents.
    - *Record:* Encrypts individual database records.
- *Transport/Communication Encryption:* Protects data during transmission over networks.
- *Asymmetric Encryption:* Uses different keys for encryption and decryption (ex. RSA).
- *Symmetric Encryption:* Uses the same key for both encryption and decryption (ex. AES).
- *Key Exchange:* Securely exchanging encryption keys.
- *Algorithms:* Mathematical techniques for encryption/decryption.
- *Key Length:* Length of cryptographic keys, influencing security strength.

Tools:

- *Trusted Platform Module (TPM):* Hardware chip for secure key storage and encryption.
- *Hardware Security Module (HSM):* Hardware device for secure key management and cryptographic operations.
- *Key Management System:* Software/hardware for managing cryptographic keys.

- *Secure Enclave:* Isolated area for secure computations.

Obfuscation:
- *Steganography:* Concealing data within other data.
- *Tokenization:* Replaces sensitive data with tokens.
- *Data Masking:* Substitutes sensitive data with fictional data.

Hashing & Salting:
- *Hashing:* Creating fixed-size hashes from variable-sized data.
- *Salting:* Adding random data to passwords before hashing for added security.

Digital Signatures: Verifies the authenticity and integrity of digital documents.

Key Stretching: Increases password security by making brute-force attacks harder.

Blockchain: ***def***
- *Open Public Ledger:* Distributed, tamper-evident data structure.
- *Certificates:* Digital documents binding public keys to identities.
    - *Certificate Authorities:* Issue and verify certificates.
    - *Certificate Revocation Lists (CRLs):* Lists of invalidated certificates.
    - *Online Certificate Status Protocol (OCSP):* Checks certificate validity.
    - *Self-Signed:* Certificate signed by the entity it certifies.
    - *Third-Party:* Certificate issued by a trusted third party.
    - *Root of Trust:* Trusted entity used to verify certificates.
    - *Certificate Signing Request (CSR) Generation:* Request for a certificate.
    - *Wildcard:* Certificate that matches multiple subdomains.

2.1 Compare and contrast common threat actors and motivations

Threat Actors:
- *Nation-State:* Government-sponsored entities aiming for political, economic, or military advantages through cyber activities.
- *Unskilled Attacker:* Individuals lacking technical expertise, often using simple methods to exploit vulnerabilities.
- *Hacktivist:* Activists using hacking for ideological, political, or social causes to spread their message.
- *Insider Threat:* Individuals within an organization with access to sensitive information, exploiting their position.
- *Organized Crime:* Criminal groups pursuing financial gain through cybercrime activities.
- *Shadow IT:* Unauthorized technology and software used within an organization, often introducing security risks.

Attributes of Actors:
- *Internal/External:* Whether the threat actor is affiliated with the targeted organization (internal) or operates from outside (external).
- *Resources/Funding:* The level of financial and technological resources available to the threat actor.
- *Level of Sophistication/Capability:* The technical expertise and tools possessed by the threat actor to execute cyber attacks.

Motivations:
- *Data Exfiltration:* Stealing sensitive data for espionage or resale on the black market.
- *Espionage:* Gaining unauthorized access to gather information for political, economic, or competitive advantage.
- *Service Disruption:* Intentionally disrupting services to cause inconvenience or damage to an organization.
- *Blackmail:* Threatening to disclose sensitive information unless demands are met.
- *Financial Gain:* Engaging in cybercrime for monetary profit.
- *Philosophical/Political Beliefs:* Pursuing cyber activities to advance certain ideologies or political agendas.
- *Ethical:* Hacking for a cause aligned with personal or collective ethical values.
- *Revenge:* Targeting an entity due to perceived grievances.
- *Disruption/Chaos:* Seeking to create disorder and confusion without a clear financial motive.
- *War:* Carrying out cyber attacks as part of a larger conflict or cyber warfare strategy.

2.2 Explain common threat vectors and attack surfaces

Message-based:

- *Email:* Attackers can use phishing emails to trick users into clicking malicious links or downloading attachments that contain malware.
- *SMS:* Attackers can send malicious text messages (smishing) containing links to phishing sites or asking users to respond with sensitive information.
- *Instant Messaging (IM):* Similar to email, attackers can send malicious links or attachments through instant messaging platforms to spread malware or steal information.

Image-based:
Attackers can embed malicious code or malware in image files, taking advantage of vulnerabilities in image processing software to compromise a system when the image is opened or processed.

File-based:
Malicious files, such as infected documents or executable files, can be shared through various means, exploiting vulnerabilities in software to gain unauthorized access or execute malicious code on the victim's system.

Voice call:
Attackers can use social engineering techniques in voice calls (vishing) to manipulate victims into revealing sensitive information or taking actions that compromise security.

Removable device:
Malware can spread through infected removable devices like USB drives when connected to a computer, exploiting autorun features or tricking users into opening malicious files.

Vulnerable software:
Attackers target security vulnerabilities in software, either through client-based attacks (exploiting vulnerabilities in locally installed software) or agentless attacks (targeting vulnerabilities in remote systems).

Unsupported systems and applications:
Outdated systems and software that are no longer supported receive no security updates, making them vulnerable to known exploits.

Unsecure networks:

- *Wireless:* Attackers can exploit weak encryption, intercept data, or launch man-in-the-middle attacks on unsecured Wi-Fi networks.
- *Wired:* Physical access to wired networks can enable attackers to intercept data or gain unauthorized network access.
- *Bluetooth:* Attackers can target Bluetooth-enabled devices to gain access, steal data, or spread malware.

Open service ports:
Attackers can exploit services running on open ports to gain unauthorized access, spread malware, or perform other malicious activities.

Default credentials:
Many systems and devices are shipped with default usernames and passwords, which attackers can easily exploit if users don't change these credentials.

Supply chain:
Attackers can compromise software or hardware at any stage of the supply chain, including managed service providers (MSPs), vendors and suppliers, to introduce malicious components.

Human vectors/social engineering:

- *Phishing:* Attackers send deceptive emails to trick users into revealing sensitive information or taking malicious actions.
- *Vishing:* Attackers use phone calls to impersonate trusted entities and manipulate victims into sharing sensitive information.
- *Smishing:* Similar to phishing, attackers use SMS to trick users into sharing information or clicking on malicious links.
- *Misinformation/Disinformation:* Spreading false information to manipulate user behavior or decision-making.
- *Impersonation:* Pretending to be someone trusted to deceive users into sharing sensitive information.
- *Business Email Compromise:* Attackers impersonate company executives to trick employees into transferring funds or sensitive information.
- *Pretexting:* Creating a fabricated scenario to manipulate individuals into disclosing information or performing actions.
- *Watering Hole:* Attackers compromise websites frequently visited by target users to distribute malware.
- *Brand Impersonation:* Creating fake online entities to impersonate well-known brands for malicious purposes.
- *Typosquatting:* Registering domain names similar to legitimate ones to trick users into visiting malicious websites.

2.3 Explain various types of vulnerabilities

Application:

- *Memory Injection:* Injecting malicious code into a program's memory space to manipulate its behavior and potentially execute unauthorized actions.
- *Buffer Overflow:* When a program writes more data into a buffer (temporary data storage) than it can hold, leading to overwriting adjacent memory areas and potentially executing malicious code.
- *Race Conditions:* These occur when multiple processes or threads access shared resources concurrently, leading to unpredictable behavior. Time-of-check (TOC) race conditions involve changes between security checks and operations, while time-of-use (TOU) race conditions happen between resource allocation and their use.
- *Malicious Update:* Attackers compromise software updates to deliver malware or malicious changes to systems.

Operating System (OS)-based:

Vulnerabilities that target weaknesses in the operating system, allowing attackers to gain unauthorized access, execute code, or disrupt services.

Web-based:

- S*tructured Query Language Injection (SQLi):* Attackers insert malicious SQL code into web application inputs, manipulating databases and potentially gaining unauthorized access to data.
- *Cross-site Scripting (XSS):* Attackers inject malicious scripts into web applications, which are then executed by users' browsers, potentially leading to data theft or unauthorized actions.

Hardware:

- *Firmware:* Exploiting vulnerabilities in device firmware, which is low-level software controlling hardware components.
- *End-of-life:* Using security vulnerabilities in hardware that manufacturers no longer support with updates.
- *Legacy:* Exploiting vulnerabilities in outdated hardware systems.

Virtualization:

- *Virtual Machine (VM) Escape:* Exploiting vulnerabilities in virtualization software to break out of a virtual machine and compromise the host system.
- *Resource Reuse:* Exploiting vulnerabilities that occur when resources allocated to a virtual machine are not properly cleaned up, leading to unauthorized access or data leakage.

Cloud-specific:

Vulnerabilities unique to cloud environments, often involving misconfigurations, shared resources and compromised credentials.

Supply Chain:

- *Service Provider:* Compromising services offered by external providers to infiltrate systems.
- *Hardware Provider:* Exploiting vulnerabilities in hardware components supplied by external parties to compromise the overall system.
- *Software Provider:* Targeting vulnerabilities in third-party software integrated into a system.

Cryptographic:
Exploiting weaknesses in encryption, decryption, or cryptographic key management to gain unauthorized access to data.

Misconfiguration:
Security vulnerabilities arising from incorrect or insecure configuration of systems, software, or services.

Mobile Device:
- *Side Loading:* Installing apps from unofficial sources, which can contain malware or unauthorized software.
- *Jailbreaking:* Removing software restrictions on mobile devices, potentially exposing them to malicious software.

Zero-day:
Exploiting vulnerabilities in software or hardware that are unknown to the vendor and do not yet have available patches or fixes.

2.4 Given a scenario, analyze indicators of malicious activity

Malware Attacks:
- *Ransomware:* Malicious software that encrypts the victim's files or system and demands a ransom for decryption.
- *Trojan:* A type of malware disguised as legitimate software, often used to create a backdoor for unauthorized access.
- *Worm:* A self-replicating malware that spreads across a network without user intervention.
- *Spyware:* Malware that secretly gathers information about a user's activities, often without their knowledge.
- *Bloatware:* Software that's pre-installed on a device and consumes resources unnecessarily or has malicious functions.
- *Virus:* Malware that attaches itself to legitimate programs and spreads when those programs are executed.
- *Keylogger:* Malware that records keystrokes to capture sensitive information like passwords.
- *Logic Bomb:* Code that lies dormant until triggered by a specific condition, often causing malicious actions.
- *Rootkit:* Malware that provides unauthorized access to a system while hiding its presence.

Physical Attacks:
- *Brute Force:* Repeatedly attempting all possible combinations to guess a password or encryption key.
- *RFID Cloning:* Copying data from a radio frequency identification (RFID) card for unauthorized access.
- *Environmental:* Physically tampering with hardware, such as cutting cables or disabling devices.

Network Attacks:

- *Distributed Denial-of-Service (DDoS):* Overwhelming a target system with a flood of traffic to disrupt its services.
    - *Amplified:* Using amplification techniques to increase the volume of traffic sent in a DDoS attack.
    - *Reflected:* Exploiting network devices to bounce and amplify attack traffic to the target.
- *DNS Attacks:* Manipulating or overwhelming the Domain Name System to redirect or disrupt traffic.
- *Wireless:* Exploiting vulnerabilities in wireless networks to gain unauthorized access.
- *On-Path:* Intercepting and altering data transmitted between two parties.
- *Credential Replay:* Reusing intercepted credentials to gain unauthorized access.
- *Malicious Code:* Inserting code with harmful intent into legitimate programs or systems.

Application Attacks:

- *Injection:* Inserting malicious code (ex. SQL, OS) into an application to exploit vulnerabilities.
- *Buffer Overflow:* Overloading a program's buffer to execute malicious code.
- *Replay:* Capturing and retransmitting valid data to impersonate a legitimate user.
- *Privilege Escalation:* Exploiting vulnerabilities to gain higher levels of access than intended.
- *Forgery:* Creating unauthorized or fake transactions, requests, or identities.

- *Directory Traversal:* Exploiting weaknesses to gain unauthorized access to directories and files.

Cryptographic Attacks:

- *Downgrade:* Forcing a system to use weaker cryptographic protocols or algorithms.
- *Collision:* Finding two different inputs that produce the same hash value.
- *Birthday:* Exploiting the probability of two different inputs having the same hash value.

Password Attacks:

- *Spraying:* Using common passwords across many accounts to increase the chances of success.
- *Brute Force:* Repeatedly trying all possible password combinations to gain unauthorized access.

Indicators:

- *Account Lockout:* Repeated failed attempts to access an account lead to locking it.
- *Concurrent Session Usage:* Abnormal multiple active sessions for a single user.
- *Blocked Content:* Preventing access to certain content or resources due to security concerns.
- *Impossible Travel:* Detected attempts to log in from geographically distant locations in a short time.
- *Resource Consumption:* Unusually high utilization of system resources, often a sign of malicious activity.
- *Resource Inaccessibility:* Inability to access critical resources due to unauthorized actions.
- *Out-of-Cycle Logging:* Irregular logging patterns that may indicate tampering or intrusion.
- *Published/Documented:* Security information exposed in public sources, which can aid attackers.
- *Missing Logs:* Absence of expected logs, potentially indicating an attempt to cover tracks.

2.5 Explain the purpose of mitigation techniques used to secure the enterprise

1. **Segmentation:** Dividing a network into smaller segments to limit the lateral movement of threats. This reduces the potential impact of a breach and helps contain incidents.
2. **Access Control:** Regulating who can access what resources in a system. It includes:
    - *Access Control List (ACL):* A list that specifies what actions users or groups are allowed or denied on specific resources.
    - *Permissions:* Rights granted to users or groups for accessing files, directories, or system resources.
3. **Application Allow List:** A security measure that permits only approved applications to run on a system, preventing unauthorized or malicious software from executing.
4. **Isolation:** Isolating critical systems or sensitive data from less secure areas to minimize the potential attack surface and limit the impact of breaches.
5. **Patching:** Applying updates and fixes to software and systems to address known vulnerabilities and ensure they are up to date against emerging threats.
6. **Encryption:** Converting data into a secure format to prevent unauthorized access. It ensures that even if data is intercepted, it remains unreadable without the proper decryption key.
7. **Monitoring***:* Continuously observing system activity to detect and respond to suspicious or malicious behavior in real-time, enhancing overall security posture.
8. **Least Privilege:** Assigning the minimum necessary access rights to users, processes, or systems to reduce the potential impact of breaches or misuse of privileges.
9. **Configuration Enforcement:** Ensuring that systems and software are configured according to security best practices to prevent misconfigurations that could be exploited by attackers.
10. **Decommissioning:** Properly retiring or removing systems, applications, or data that are no longer needed to reduce the attack surface and potential risks.
11. **Hardening Techniques:** Strengthening system security through various measures:
    - *Encryption:* Protecting data at rest and in transit.
    - *Endpoint Protection:* Installing security software on endpoints devices to prevent, detect and respond to threats.
    - *Host-Based Firewall:* A firewall that operates at the host level, controlling incoming and outgoing network traffic.

- *Host-Based Intrusion Prevention System (HIPS):* Monitoring and preventing unauthorized activities on a single host.
- *Disabling Ports/Protocols:* Closing unused network ports and protocols to limit potential entry points for attackers.
- *Default Password Changes:* Changing default passwords on devices and systems to prevent unauthorized access.
- *Removal of Unnecessary Software:* Eliminating unnecessary software to reduce attack surface and potential vulnerabilities.

3.1 Compare and contrast security implications of different architecture models

Architecture and infrastructure concepts:

1. *Cloud Architecture:*
   - *Responsibility Matrix:* In cloud environments, there's a shared responsibility model where the cloud provider and customer share security responsibilities.
   - *Hybrid Considerations:* Combining on-premises and cloud resources introduces complexities in data flow and security enforcement.
   - *Third-Party Vendors:* Cloud services often involve third-party vendors, requiring trust and due diligence to ensure their security measures align with your needs.
2. *Infrastructure as Code (IaC):*
   - IaC allows automated provisioning of infrastructure using scripted code, reducing human error and ensuring consistent security configurations.
3. *Serverless:*
   - Serverless platforms manage underlying infrastructure, reducing attack surface but requiring trust in the platform's security controls. The cloud provider handles the server and you use the service.
4. *Microservices:*
   - Microservices promote modularity but increase the complexity of security management due to inter-service communication. These normally involve using an Application Programming Interface (API).
5. *Network Infrastructure:*
   - *Physical Isolation (Air-gapped):* Provides strong security by disconnecting from the network but introduces additional operational challenges since data transfers require physical action.
   - *Logical Segmentation:* Isolating networks logically reduces lateral movement of threats.
   - *Software-Defined Networking (SDN):* Offers dynamic network management but requires strong security controls to prevent unauthorized changes.
6. *On-Premises:*
   - Direct control over physical infrastructure but requires managing all aspects of security.
7. *Centralized vs. Decentralized:*
   - Centralized architectures offer streamlined security management, while decentralized architectures distribute control, requiring careful synchronization.
8. *Containerization:*
   - Isolates applications and enhances security but proper configuration and management are essential to avoid vulnerabilities as seen in Mobile Device Management (MDM) solutions.
9. *Virtualization:*
   - Abstracting hardware to run multiple OS’s on the same physical device. This is an efficient resource utilization but can introduce vulnerabilities if not properly segmented and managed.
10. *IoT:*
    - Internet of Things designed to enhance connectivity and automation but this also expands the overall attack surface due to diverse devices, often with limited security controls.
11. *Industrial Control Systems (ICS) / Supervisory Control and Data Acquisition (SCADA):*
    - Critical infrastructure components with specific security challenges due to their role in controlling physical processes.
12. *Real-Time Operating System (RTOS):*

- Used in time-sensitive systems, security concerns may arise due to limited resources and specialized nature. Examples include VxWorks, Zephyr and FreeRTOS.

13. *Embedded Systems:*
    - Often constrained in resources, security measures need to be balanced with performance and functionality. These can sometimes pose additional risk due to lack of routine security updates.
14. *High Availability:*
    - Ensures continuous operation but requires careful redundancy planning to avoid single points of failure.

Considerations:

- *Availability, Resilience, Scalability:* These are common goals across architectures, with different methods to achieve them.
- *Cost:* Various architectures have different cost implications, impacting the level of security investment.
- *Responsiveness, Ease of Deployment:* Trade-offs exist between rapid deployment and thorough security checks.
- *Risk Transference:* Using third-party services transfers some security responsibilities.
- *Ease of Recovery:* Architecture affects how quickly systems can be restored after incidents.
- *Patch Availability, Inability to Patch:* Timely patching is crucial; some architectures may limit patching options.
- *Power, Compute:* Different architectures demand varying power and compute resources, affecting security configurations.

3.2 Given a scenario, apply security principles to secure enterprise infrastructure

Infrastructure Considerations:

- *Device Placement:* Deciding where to position security devices within the network to maximize their effectiveness.
- *Security Zones:* Dividing the network into zones with varying levels of trust to control access and protect sensitive data.
- *Attack Surface:* Reducing the potential points of entry for attackers into the network.
- *Connectivity:* Managing how different devices and components connect to the network.
- *Failure Modes:* Preparing for and addressing potential system failures.
    - *Fail-Open:* Devices or systems that continue to operate when they fail, potentially exposing security vulnerabilities.
    - *Fail-Closed:* Devices or systems that shut down or restrict access when they fail to prevent security breaches.
- *Device Attribute:* Determining whether devices are active or passive, inline or tap/monitor for security monitoring and enforcement.
- *Network Appliances:* Various network devices used for security purposes, including:
    - *Jump Server:* A secure gateway for accessing internal resources.
    - *Proxy Server:* An intermediary server that acts as a buffer between a user's device and the internet to enhance security and privacy.
    - *Intrusion Prevention System (IPS)/Intrusion Detection System (IDS):* Tools for monitoring network traffic and identifying potential security threats.
    - *Load Balancer:* Distributes incoming network traffic across multiple servers for improved performance and availability.
    - *Sensors:* Devices that collect data about the network and its activity for security monitoring.
- *Port Security:*
    - *802.1X:* A standard for port-based network access control, requiring authentication before granting network access.
    - *Extensible Authentication Protocol (EAP):* A framework for various authentication methods used within 802.1X.
- *Firewall Types:*
    - *Web Application Firewall (WAF):* Designed to protect web applications from various attacks.
    - *Unified Threat Management (UTM):* Combines multiple security features like firewall, antivirus and intrusion detection in a single appliance.

    - *Next-Generation Firewall (NGFW):* Offers advanced capabilities beyond traditional firewalls, such as application layer filtering and threat intelligence.
    - *Layer 4/Layer 7:* Refers to the level of the OSI model at which the firewall operates (transport layer or application layer).

Secure Communication/Access:

- *Virtual Private Network (VPN):* Securely extends a private network over a public network, enabling remote access and secure communication.
- *Remote Access:* Secure methods for connecting to a network from remote locations.
- *Tunneling:*
    - *Transport Layer Security (TLS):* A protocol for secure data transmission over a network, often used for securing web traffic.
    - *Internet Protocol Security (IPSec):* A suite of protocols for securing IP communication by authenticating and encrypting data.
- *Software-Defined Wide Area Network (SD-WAN):* A technology that simplifies and enhances the management and security of wide area networks.
- *Secure Access Service Edge (SASE):* A cloud-based security architecture that combines network security and wide-area networking into a single, integrated service.

3.3 Compare and contrast concepts and strategies to protect data

Data Types:

- *Regulated:* Data subject to legal regulations and compliance requirements, such as personal data under GDPR.
- *Trade Secret:* Proprietary information that provides a competitive advantage.
- *Intellectual Property:* Creative or innovative work protected by copyright or patents.
- *Legal Information:* Documents related to legal matters, contracts, or litigation.
- *Financial Information:* Data related to financial transactions and assets.
- *Human- and Non-Human-Readable:* Data that can be understood by humans (*text*) and data that is only machine-readable (*binary*).

Data Classifications:

- *Sensitive:* Data that, if exposed, could have a significant impact on the organization or individuals, often subject to strict access controls.
- *Confidential:* Data that should be kept private but may not have the same level of sensitivity as "sensitive" data.
- *Public:* Information that is intentionally made available to the public and doesn't require protection.
- *Restricted:* Data with limited access based on specific criteria.
- *Private:* Information intended for a specific audience but not as highly sensitive as "sensitive" data.
- *Critical:* Data that is essential to an organization's operations or survival.

General Data Considerations:

- *Data States:*
    - *Data at Rest:* Data that is stored on physical or digital media.
    - *Data in Transit:* Data actively moving between devices or networks.
    - *Data in Use:* Data being processed or accessed by applications or users.
- *Data Sovereignty:* The legal jurisdiction or country where data is stored and subject to that region's laws.
- *Geolocation:* Determining the physical location of data, which may be important for compliance or security reasons.

Methods to Secure Data:

- *Geographic Restrictions:* Controlling access to data based on the physical location of users or devices.
- *Encryption:* Transforming data into a secure format that can only be decrypted by authorized parties.
- *Hashing:* Creating a fixed-size hash value from data, often used for data integrity checks.
- *Masking:* Hiding or obfuscating specific portions of data to protect sensitive information.
- *Tokenization:* Replacing sensitive data with tokens or placeholders while maintaining referential integrity.
- *Obfuscation:* Making data intentionally unclear or ambiguous to protect its meaning.
- *Segmentation:* Isolating data or networks to prevent unauthorized access or lateral movement of attackers.
- *Permission Restrictions:* Implementing access controls and permissions to limit who can access, modify, or delete data.

3.4 Explain the importance of resilience and recovery in security architecture

1. **High Availability:** High availability refers to the ability of a system to remain operational and accessible even in the face of hardware or software failures. It minimizes downtime and ensures that services are consistently available.
2. **Load Balancing vs. Clustering:** Load balancing distributes network traffic across multiple servers to ensure efficient resource utilization and minimize the risk of server overloads. Clustering involves grouping multiple servers together to work as a single unit, providing redundancy and fault tolerance.
3. **Site Considerations:**
    - *Hot Site:* A fully equipped data center ready for immediate use.
    - *Cold Site:* A backup facility with infrastructure but no active equipment.
    - *Warm Site:* A partially equipped backup facility with some hardware and infrastructure in place but not fully operational.
    - *Geographic Dispersion:* Spreading critical assets and data centers across different geographical locations to reduce the risk of a single point of failure.
4. **Platform Diversity:** Using different hardware and software platforms to decrease the likelihood of widespread failures due to vulnerabilities affecting a specific technology.
5. **Multi-Cloud Systems:** Deploying applications and data across multiple cloud service providers to avoid service disruptions caused by issues with a single provider.
6. **Continuity of Operations:** Ensuring that essential business functions can continue in the event of a disruption, disaster or cyberattack.
7. **Capacity Planning:**
    - *People:* Ensuring that there are enough trained personnel to manage and respond to security incidents.
    - *Technology:* Assessing and scaling the IT infrastructure to meet current and future demands.
    - *Infrastructure:* Ensuring that physical infrastructure, like data centers, can handle increased loads and provide redundancy.
8. **Testing:**
    - *Tabletop Exercises:* Simulated scenarios where stakeholders discuss how they would respond to specific security incidents.
    - *Failover:* Testing the process of switching to backup systems when the primary system fails.
    - *Simulation:* Creating realistic scenarios to evaluate the performance of security and recovery processes.
    - *Parallel Processing:* Testing multiple systems in parallel to ensure they can take over seamlessly in case of failure.
9. **Backups:**
    - *Onsite/Offsite:* Storing copies of data and systems either on the same premises or at remote locations.
    - *Frequency:* How often backups are taken to minimize data loss.
    - *Encryption:* Securing backups with encryption to protect sensitive data.
    - *Snapshots:* Point-in-time copies of data for fast recovery.
    - *Recovery:* The process of restoring data and systems from backups.
    - *Replication:* Creating real-time copies of data to ensure availability.
    - *Journaling:* Recording changes to data for efficient recovery.
10. **Power:**
    - *Generators:* Backup power sources to maintain operations during power outages.

- *Uninterruptible Power Supply (UPS):* Provides short-term power to prevent disruptions during brief power interruptions.

4.1 Given a scenario, apply common security techniques to computing resources

1. **Secure Baselines:**
    - *Establish:* Define and document a set of secure configuration standards for each type of resource.
    - *Deploy:* Apply these secure configurations during the initial setup of devices and systems.
    - *Maintain:* Regularly update and review the configurations to ensure ongoing security compliance.
2. **Hardening Targets:**
    - *Mobile Devices:* Disable unnecessary services, enable device encryption and implement remote wipe capabilities.
    - *Workstations:* Disable unused ports, apply security patches and enforce strong password policies.
    - *Switches/Routers:* Secure management interfaces, disable unused ports and implement access control lists (ACLs).
    - *Cloud Infrastructure:* Configure security groups, enable multi-factor authentication (MFA) and regularly audit resource permissions.
    - *Servers:* Remove unnecessary software, apply the principle of least privilege and enable intrusion detection systems (IDS).
    - *ICS/SCADA:* Isolate from the corporate network, update firmware and implement role-based access control.
    - *Embedded Systems/RTOS:* Disable unnecessary services, limit network exposure and apply signed firmware updates.
    - *IoT Devices:* Change default passwords, encrypt communication and segment IoT networks.
3. **Wireless Devices:**
    - *Installation Considerations:*
        - *Site Surveys:* Conduct surveys to determine optimal placement of wireless access points.
        - *Heat Maps:* Use heat maps to visualize signal coverage and identify dead zones.
4. **Mobile Solutions:**
    - *Mobile Device Management (MDM):* Use MDM solutions to enforce security policies, remote device wipe and application management.
    - *Deployment Models:*
        - *BYOD (Bring Your Own Device):* Implement policies to secure personal devices used for work.
        - *COPE (Corporate-Owned, Personally Enabled):* Provide company-owned devices with user customization options.
        - *CYOD (Choose Your Own Device):* Allow employees to select from a list of approved devices.
    - *Connection Methods:*
        - *Cellular:* Encrypt data in transit and use VPNs for secure communication.
        - *Wi-Fi:* Implement WPA3 security and strong encryption.
        - *Bluetooth:* Disable unnecessary services and use secure pairing.
5. **Wireless Security Settings:**
    - *WPA3 (Wi-Fi Protected Access 3):* Use the latest Wi-Fi security standard with strong encryption.
    - *AAA/RADIUS (Remote Authentication Dial-In User Service)*: Implement central authentication and authorization for network access.
    - *Cryptographic Protocols:* Use up-to-date cryptographic protocols for secure communication.
    - Authentication Protocols: Implement strong authentication methods, such as multi-factor authentication (MFA).
6. **Application Security:**
    - Input Validation: Validate user inputs to prevent injection attacks.
    - Secure Cookies: Use secure and HTTP-only flags for cookies.
    - Static Code Analysis: Analyze code for vulnerabilities before deployment.
    - Code Signing: Sign code to verify its authenticity and integrity.
7. **Sandboxing:** Isolate untrusted applications or processes in controlled environments to limit potential damage.

8. **Monitoring:** Implement continuous monitoring of all resources to detect and respond to security incidents in real-time. Use intrusion detection systems (IDS) and security information and event management (SIEM) solutions.

4.2 Explain the security implications of proper hardware, software and data asset management

1. **Acquisition/Procurement Process:**
    - *Security Implication:* During the acquisition or procurement process, it's essential to assess the security features and risks associated with the hardware and software being acquired. This includes evaluating vendor security practices, patch management and ensuring that the products meet security compliance standards.
    - *Benefits:* Proper evaluation helps in avoiding the purchase of vulnerable or insecure products, reducing the risk of introducing security vulnerabilities into the organization.
2. **Assignment/Accounting:**
    - *Ownership:*
        - *Security Implication:* Properly assigning ownership of hardware and software assets ensures accountability and responsibility. Unauthorized ownership changes can lead to security breaches.
        - *Benefits:* Clear ownership helps in tracking who is responsible for maintaining and securing assets, making it easier to identify and address security incidents.
    - *Classification:*
        - *Security Implication:* Classifying assets based on their sensitivity and criticality is essential. Failure to do so can result in inadequate security measures for high-value assets or excessive protection for less critical ones.
        - *Benefits:* Proper classification allows for appropriate security controls and resource allocation based on asset importance.
3. **Monitoring/Asset Tracking:**
    - *Inventory:*
        - *Security Implication:* Maintaining an accurate inventory of hardware and software assets is critical for security. Missing or undocumented assets can become vulnerable points.
        - *Benefits:* A comprehensive inventory helps identify and secure all assets, reducing the risk of unauthorized access or data breaches.
    - *Enumeration:*
        - *Security Implication:* Regularly enumerating assets involves identifying their configuration and status. Unpatched or misconfigured assets can be exploited by attackers.
        - *Benefits:* Enumeration helps in identifying security vulnerabilities and ensuring timely updates and patches to maintain a secure environment.
4. **Disposal/Decommissioning:**
    - *Sanitization:*
        - *Security Implication:* Inadequate data sanitization before disposal can result in sensitive information being leaked or recovered by malicious actors.
        - *Benefits:* Proper sanitization ensures that data cannot be easily retrieved from retired assets, maintaining data confidentiality.
    - *Destruction:*
        - *Security Implication:* Physical destruction of assets is essential to prevent their reuse or data recovery. Failure to destroy assets securely can lead to data breaches.
        - *Benefits:* Secure destruction ensures that assets and data are permanently removed from the organization's environment.
    - *Certification:*
        - *Security Implication:* Certification processes confirm that assets have been securely decommissioned or destroyed. Skipping this step can lead to uncertainty about the state of security for disposed assets.
        - *Benefits:* Certification provides a documented record of proper disposal, reducing legal and compliance risks.
    - *Data Retention:*

- *Security Implication:* Retaining data for longer than necessary can increase the risk of data breaches and legal compliance violations.
- *Benefits:* Proper data retention policies help in reducing the exposure of sensitive information and ensure compliance with data protection regulations.

4.3 Explain various activities associated with vulnerability management

Identification Methods:

- *Vulnerability Scan:*
  - Regularly scanning systems and networks using automated tools to identify known vulnerabilities.
- *Application Security:*
  - *Static Analysis:* Analyzing the source code of applications to identify vulnerabilities before they are deployed.
  - *Dynamic Analysis:* Testing running applications to find vulnerabilities in their behavior.
  - *Package Monitoring:* Monitoring software packages and dependencies for known vulnerabilities.
- *Threat Feed:*
  - *Open-source Intelligence (OSINT):* Gathering information from publicly available sources to identify potential threats and vulnerabilities.
  - *Proprietary/Third-Party:* Utilizing commercial or third-party threat feeds for information on emerging vulnerabilities.
  - *Information-sharing Organization:* Collaborating with industry groups or organizations to share and receive threat intelligence.
  - *Dark Web:* Monitoring underground forums and sources to detect discussions of potential threats and vulnerabilities.
- *Penetration Testing:*
  - Simulating cyberattacks to identify vulnerabilities that may not be detectable through automated scans or analysis.
- *Responsible Disclosure Program:*
  - *Bug Bounty Program:* Encouraging external security researchers to report vulnerabilities in exchange for rewards.
- *System/Process Audit:*
  - Reviewing systems, processes and configurations to identify vulnerabilities through manual inspection and assessment.

Analysis:

- *Confirmation:*
  - *False Positive:* Verifying whether reported vulnerabilities are indeed valid and not false alarms.
  - *False Negative:* Ensuring that no vulnerabilities were missed during the identification phase.
- *Prioritization:*
  - Assessing the severity and potential impact of vulnerabilities to prioritize remediation efforts.
- *Common Vulnerability Scoring System (CVSS):*
  - Assigning a score to vulnerabilities based on their characteristics, helping in prioritization.
- *Common Vulnerability Enumeration (CVE):*
  - Using standardized identifiers to track and reference vulnerabilities.
- *Vulnerability Classification:*
  - Categorizing vulnerabilities by type (ex. buffer overflow, SQL injection) for better understanding.
- *Exposure Factor:*
  - Calculating the potential impact of a vulnerability on the organization.
- *Environmental Variables:*
  - Considering specific factors within the organization that may affect the risk posed by a vulnerability.
- *Industry/Organizational Impact:*
  - Evaluating how a vulnerability may impact the specific industry or organization.

- *Risk Tolerance:*
    - Determining the organization's willingness to accept certain levels of risk associated with vulnerabilities.

Vulnerability Response and Remediation:

- *Patching:*
    - Applying security patches or updates to remediate vulnerabilities.
- *Insurance:*
    - Evaluating the need for cybersecurity insurance as a risk mitigation strategy.
- *Segmentation:*
    - Isolating vulnerable systems from critical assets to minimize risk.
- *Compensating Controls:*
    - Implementing alternative security measures when immediate patching is not feasible.
- *Exceptions and Exemptions:*
    - Managing cases where vulnerabilities cannot be immediately addressed due to operational or business reasons.

Validation of Remediation:

- *Rescanning:*
    - Conducting follow-up vulnerability scans to ensure that remediation efforts were successful.
- *Audit:*
    - Performing detailed examinations or audits to verify that vulnerabilities have been adequately addressed.
- *Verification:*
    - Confirming that remediation actions were implemented correctly and effectively.

Reporting:

- Providing clear and concise reports to relevant stakeholders, including management, IT teams and auditors, to communicate the status of vulnerabilities, their remediation and ongoing risks.

4.4 Explain security alerting and monitoring concepts and tools

Monitoring Computing Resources:

- *Systems:* Monitoring the health and security of individual computer systems, servers and endpoints to detect abnormal behavior or potential threats.
- *Applications:* Monitoring the performance and security of software applications to identify any anomalies or suspicious activities that may indicate a security breach.
- *Infrastructure:* Monitoring the underlying network infrastructure, including routers, switches and firewalls, to ensure they are functioning correctly and to detect any unauthorized access or suspicious network traffic.

Activities:

- *Log Aggregation:* Collecting and centralizing log data from various sources, such as servers, applications and network devices, for analysis and correlation.
- *Alerting:* Generating notifications or alerts when predefined security events or anomalies are detected, allowing for rapid response to potential threats.
- *Scanning:* Performing regular vulnerability scans to identify weaknesses in systems, applications, or networks that could be exploited by attackers.
- *Reporting:* Creating detailed reports and summaries of security events, incidents and performance metrics for analysis and compliance purposes.
- *Archiving:* Storing historical data and logs for future analysis, forensics, or compliance requirements.
- *Alert Response and Remediation/Validation:*

- *Quarantine:* Isolating or blocking systems or users that are exhibiting suspicious behavior to prevent further damage.
- *Alert Tuning:* Fine-tuning alerting systems to reduce false positives and ensure that alerts are relevant and actionable.

Tools:

- *Security Content Automation Protocol (SCAP):* A set of standards and specifications that enable automated vulnerability management, including vulnerability assessment, measurement and reporting.
- *Benchmarks:* Industry-recognized standards and best practices for configuring and securing systems and applications.
- *Agents/Agentless:* Monitoring agents are software components installed on systems to collect and transmit data to monitoring tools, while agentless monitoring relies on existing system capabilities and protocols to gather information.
- *Security Information and Event Management (SIEM):* A comprehensive tool that collects, correlates and analyzes security events and logs from various sources to identify and respond to security incidents.
- *Antivirus:* Software designed to detect, prevent and remove malware and other threats from computer systems and networks.
- *Data Loss Prevention (DLP):* Tools and technologies that monitor and protect sensitive data from unauthorized access, sharing, or leakage.
- *Simple Network Management Protocol (SNMP) Traps:* SNMP traps are asynchronous notifications sent by network devices to alert management systems about specific events or issues.
- *NetFlow:* A network protocol that provides data on network traffic and helps in network monitoring, traffic analysis and security incident detection.
- *Vulnerability Scanners:* Automated tools that scan systems and networks for known vulnerabilities and weaknesses, providing reports and recommendations for remediation.

4.5 Given a scenario, modify enterprise capabilities to enhance security

1. **Firewall:**
    - *Rules:* Review and update firewall rules regularly to ensure they are specific, necessary and based on the principle of least privilege.
    - *Access Lists:* Implement strict access control lists (ACLs) to restrict access to sensitive resources.
    - *Ports/Protocols:* Restrict open ports and protocols to those required for business operations.
    - *Screened Subnets:* Implement screened subnets to segment the network and control traffic flow between different zones.
2. **IDS/IPS (Intrusion Detection System/Intrusion Prevention System):**
    - *Trends:* Continuously monitor and analyze the latest threat trends and adapt IDS/IPS rules accordingly.
    - *Signatures:* Regularly update and fine-tune intrusion detection signatures to detect and block emerging threats effectively.
3. **Web Filter:**
    - *Agent-Based:* Deploy agent-based web filtering solutions on endpoints to enforce web security policies locally.
    - *Centralized Proxy:* Use a centralized proxy server to filter web traffic, enabling centralized policy enforcement.
    - *URL Scanning:* Implement URL scanning to block access to malicious or inappropriate websites.
    - *Content Categorization:* Categorize web content to enforce policies based on content type.
    - *Block Rules:* Create and enforce specific rules to block known threats and unwanted content.
    - *Reputation:* Utilize reputation-based filtering to identify and block access to known malicious domains and IPs.
4. **Operating System Security:**
    - *Group Policy:* Enforce security policies on Windows systems using Group Policy to control access and configurations.

- *SELinux:* Implement SELinux or similar mandatory access control mechanisms on Linux systems to restrict unauthorized access.

5. **Implementation of Secure Protocols:**
   - *Protocol Selection:* Choose secure protocols such as TLS/SSL for communication.
   - *Port Selection:* Use non-standard ports for services where feasible to reduce exposure to automated attacks.
   - *Transport Method:* Prioritize encrypted transport methods for data in transit, like VPNs or secure tunnels.
6. **DNS Filtering:**
   - Implement DNS filtering to block access to known malicious domains and prevent DNS-based attacks.
7. **Email Security:**
   - *DMARC, DKIM, SPF:* Implement and enforce DMARC, DKIM and SPF to prevent email spoofing and phishing attacks.
   - *Gateway:* Use an email security gateway to scan and filter incoming and outgoing emails for threats and malicious content.
8. **File Integrity Monitoring:**
   - Implement file integrity monitoring to detect unauthorized changes to critical system files and configurations.
9. **DLP (Data Loss Prevention):**
   - Deploy DLP solutions to monitor and prevent the unauthorized transfer of sensitive data.
10. **Network Access Control (NAC):**
    - Use NAC solutions to ensure that only authorized devices and users can access the network.
11. **Endpoint Detection and Response (EDR)/Extended Detection and Response (XDR):**
    - Implement EDR/XDR solutions for real-time monitoring, detection and response to advanced threats on endpoints.
12. **User Behavior Analytics:**
    - Utilize user behavior analytics to identify abnormal behavior patterns and potential insider threats.

4.6 Given a scenario, implement and maintain identity and access management

1. **Provisioning/De-Provisioning User Accounts**:
   - *Provisioning:* The process of creating user accounts with the necessary access rights and privileges when new employees join the organization.
   - *De-Provisioning:* The process of revoking or disabling user accounts and access when employees leave the organization or no longer require access.
2. **Permission Assignments and Implications**:
   - Assigning specific permissions to users or groups based on their roles and responsibilities.
   - Understanding the implications of these permissions to ensure users have the necessary access without unnecessary privileges.
3. **Identity Proofing**:
   - The process of verifying the identity of users before granting them access. This can involve document verification, biometrics, or other identity verification methods.
4. **Federation**:
   - Federation allows users to access resources across multiple domains or organizations using a single set of credentials.
   - It enables single sign-on (SSO) across different systems and services.
5. **Single Sign-On (SSO)**:
   - *LDAP (Lightweight Directory Access Protocol):* A protocol used for managing and accessing directory information. It is often used for user authentication and authorization.
   - *OAuth (Open Authorization):* An open standard for access delegation, commonly used for granting third-party applications limited access to a user's resources.
   - *SAML (Security Assertions Markup Language):* An XML-based standard for exchanging authentication and authorization data between parties, often used for SSO.
6. **Interoperability**:

- Ensuring that IAM systems can work seamlessly with various applications, platforms and identity providers.

7. **Attestation**:
    - A process to verify and confirm that user access permissions are accurate and up to date. It involves periodic reviews and approvals of user access rights.
8. **Access Controls**:
    - *Mandatory Access Control:* Enforces security policies based on system-wide rules, typically used in highly classified environments.
    - *Discretionary Access Control:* Allows users to define access permissions on their resources.
    - *Role-Based Access Control:* Assigns permissions to roles and users are assigned to roles based on their job functions.
    - *Rule-Based Access Control:* Access decisions are determined by specific rules or conditions.
    - *Attribute-Based Access Control:* Access decisions are based on attributes like user roles, time of day and other factors.
    - *Time-of-Day Restrictions:* Limiting access based on specific time windows.
    - *Least Privilege:* Users are granted only the minimum access necessary to perform their job tasks.
9. **Multifactor Authentication (MFA)**:
    - *Implementation:* Enhancing security by requiring users to provide multiple forms of authentication.
    - *Factors:* Types of authentication factors include something you know (password), something you have (smart card), something you are (biometrics) and somewhere you are (geolocation).
10. **Password Concepts**:
    - *Password Best Practices:* Enforcing password policies regarding length, complexity, reuse, expiration and age.
    - *Password Managers:* Tools that securely store and manage passwords.
    - *Passwordless:* Authentication methods that do not rely on traditional passwords.
11. **Privileged Access Management Tools**:
    - *Just-in-Time Permissions:* Granting temporary, time-limited access to privileged accounts only when needed.
    - *Password Vaulting:* Securely storing and managing privileged account credentials.
    - *Ephemeral Credential:* Temporary, short-lived credentials used for privileged access to reduce exposure to risk.

4.7 Explain the importance of automation and orchestration related to secure operations

Importance of Automation and Orchestration:

- *Efficiency and Time Saving:* Automation reduces manual, repetitive tasks, allowing security teams to focus on more strategic and complex issues. It speeds up processes such as user provisioning, resource provisioning and ticket creation.
- *Enforcing Baselines:* Automation ensures that security and compliance baselines are consistently applied across the organization. This helps maintain a standardized and secure infrastructure configuration.
- *Standard Infrastructure Configurations:* Automation helps maintain uniformity in infrastructure configurations, reducing the attack surface by eliminating inconsistencies or misconfigurations.
- *Scaling Securely:* Automation enables organizations to scale their operations while maintaining security. This is crucial in today's dynamic and cloud-centric environments.
- *Employee Retention:* Reducing the burden of repetitive tasks through automation can improve employee satisfaction and retention within security teams.
- *Reaction Time:* Automation enables rapid responses to security incidents by automating alerting, incident triage and remediation tasks, minimizing the time it takes to contain threats.
- *Workforce Multiplier:* By automating routine tasks, security teams can achieve more with existing resources, effectively acting as a "force multiplier."

Use Cases of Automation and Scripting:

- *User Provisioning:* Automatically create, modify, or revoke user accounts and access permissions based on predefined criteria and policies.
- *Resource Provisioning:* Automatically provision and deprovision resources like servers, databases, or cloud instances while adhering to security policies.
- *Guard Rails:* Implement automated guardrails to enforce security policies, such as configuring firewalls, intrusion detection systems and access controls.
- *Security Groups:* Manage security groups and access controls for users and resources.
- *Ticket Creation:* Automatically generate incident tickets or alerts for security events and vulnerabilities.
- *Escalation:* Implement automated escalation procedures for incidents that require higher-level attention or expertise.
- *Enabling/Disabling Services and Access:* Automate the activation or deactivation of services and access rights as needed.
- *Continuous Integration and Testing:* Integrate security testing into the continuous integration/continuous delivery (CI/CD) pipeline to identify and address vulnerabilities early in the development process.
- *Integrations and APIs:* Automate the integration of security tools and systems through APIs for better visibility and control.

Benefits of Automation and Orchestration:

- *Efficiency/Time Saving:* Reduces manual effort and accelerates tasks.
- *Enforcing Baselines:* Ensures consistent security configurations.
- *Standard Infrastructure Configurations:* Maintains a secure and consistent infrastructure.
- *Scaling Securely:* Facilitates secure growth.
- *Employee Retention:* Improves job satisfaction.
- *Reaction Time:* Speeds up incident response.
- *Workforce Multiplier:* Maximizes the value of security teams.

Other Considerations:

- *Complexity:* Automation can introduce complexity, especially when managing intricate workflows or integrating multiple systems.
- *Cost:* While automation can save time, there may be upfront costs associated with tooling and development.
- *Single Point of Failure:* Overreliance on automation can become a single point of failure; therefore, redundancy and failover mechanisms are important.
- *Technical Debt:* Poorly designed or maintained automation scripts can accumulate technical debt over time, leading to future challenges.
- *Ongoing Supportability:* Automation and orchestration require ongoing maintenance and updates to remain effective and secure.

4.8 Explain appropriate incident response activities

Process:

- *Preparation*: Establish an incident response plan, define roles and responsibilities and ensure all necessary tools and resources are in place.
- *Detection:* Continuously monitor the network and systems for signs of suspicious or malicious activity using intrusion detection systems, security information and event management (SIEM) tools and other security controls.
- *Analysis:* Investigate and analyze the incident to understand its scope, impact and the nature of the threat. Determine if it's a false positive or a real incident.
- *Containment:* Isolate and contain the incident to prevent further damage or unauthorized access. This may involve disconnecting compromised systems from the network or blocking malicious traffic.
- *Eradication:* Identify and eliminate the root cause of the incident to ensure that the threat is completely removed from the environment.

- *Recovery:* Restore affected systems and services to normal operation while ensuring that they are secure and free from vulnerabilities.
- *Lessons Learned:* Conduct a post-incident review to assess the effectiveness of the response and identify areas for improvement. Document lessons learned and update incident response procedures accordingly.

Training:

- *Training:* Regularly train incident response team members and relevant staff on incident response procedures, including their roles and responsibilities.

Testing:

- *Tabletop Exercise:* Conduct simulated incident scenarios in a controlled environment to evaluate the effectiveness of the incident response plan and team's ability to execute it.
- *Simulation:* Simulate real-world incident scenarios to test the organization's response capabilities, including technical and human aspects.

Root Cause Analysis:

- *Root Cause Analysis:* Investigate the underlying causes of the incident to prevent similar incidents from occurring in the future. Identify weaknesses in security controls or processes that need improvement.

Threat Hunting:

- *Threat Hunting:* Proactively search for signs of hidden or persistent threats within the environment, even if no specific incident has been detected. This involves exploring logs, network traffic and endpoint data to uncover anomalies and potential threats.

Digital Forensics:

- *Legal Hold:* Ensure that potential evidence is preserved and not altered, deleted, or tampered with to support legal or regulatory requirements.
- *Chain of Custody:* Maintain a documented record of who has handled evidence and its whereabouts throughout the investigation.
- *Acquisition:* Collect digital evidence from relevant sources, such as servers, workstations, or network devices, using forensically sound methods.
- *Reporting:* Document findings and actions taken during the investigation, including the evidence collected, analysis performed and remediation steps.
- *Preservation:* Ensure the integrity and confidentiality of digital evidence throughout the investigation process.
- *E-Discovery:* If the incident may lead to legal action, collaborate with legal teams to ensure that digital evidence is prepared and presented according to legal requirements.

4.9 Given a scenario, use data sources to support an investigation

Log Data:

- *Firewall Logs:* Review firewall logs to identify any unusual or unauthorized traffic patterns or connections to the critical server. Look for any outbound connections or traffic originating from suspicious IP addresses.
- *Application Logs:* Analyze application logs specific to the server in question. Check for any anomalies, such as unexpected user access, login failures, or unusual application behavior.
- *Endpoint Logs:* Examine logs from the endpoint where the critical server is hosted. Look for any signs of suspicious activities, unauthorized access attempts, or changes to system configurations.
- *OS-specific Security Logs:* Access and inspect the security logs of the server's operating system. These logs may contain information about login attempts, privilege escalation, or security-related events.

- *IPS/IDS Logs:* Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) logs can provide alerts and details about potentially malicious network traffic or intrusion attempts.
- *Network Logs:* General network logs, including those from switches, routers and other network devices, can reveal patterns of communication and connections to the server.
- *Metadata:* Metadata from logs can include timestamps, source and destination IP addresses, port numbers and user identifiers. This information helps in building a timeline of events and tracing the source of the unauthorized access.

Data Sources:

- *Vulnerability Scans:* Conduct vulnerability scans on the critical server to identify any weaknesses or vulnerabilities that may have been exploited by the attacker.
- *Automated Reports:* Gather automated reports from security tools and systems, which may include alerts or indicators of compromise (IOCs) related to the incident.
- *Dashboards:* Utilize security dashboards to visualize and analyze real-time security data, such as alerts, traffic patterns and system health.
- *Packet Captures:* Capture network packets associated with the critical server to examine in detail the traffic and communication between the server and other systems. This can help identify any malicious payloads or unusual network behavior.

5.1 Summarize elements of effective security governance

1. **Guidelines:** Guidelines are advisory documents that provide recommendations and best practices for specific security areas. They offer general advice on how to achieve security objectives but may not be mandatory.
2. **Policies:** Policies are high-level documents that outline an organization's overarching approach to security. They provide the foundation for security governance and often include the following types:
    - *Acceptable Use Policy (AUP):* Defines the acceptable use of an organization's IT resources, including computers, networks and data.
    - *Information Security Policies:* Broad policies that cover various aspects of information security.
    - *Business Continuity:* Outlines strategies for maintaining business operations during disruptions.
    - *Disaster Recovery:* Focuses on plans and procedures for recovering from disasters and data loss.
    - *Incident Response:* Specifies how an organization should respond to and manage security incidents.
    - *Software Development Lifecycle (SDLC):* Describes security considerations at each stage of software development.
    - *Change Management:* Addresses how changes to systems and processes are managed to ensure security.
3. **Standards:** Standards are detailed specifications that provide specific requirements and expectations for security practices. Some common security standards include:
    - *Password Standards:* Guidelines for creating and managing passwords.
    - *Access Control Standards:* Specifications for controlling user access to systems and data.
    - *Physical Security Standards:* Requirements for securing physical facilities and assets.
    - *Encryption Standards:* Guidelines for encrypting sensitive data.
4. **Procedures:** Procedures are step-by-step instructions that detail how specific security tasks and processes should be carried out. Examples include:
    - *Change Management Procedures:* Define how changes to systems are requested, approved and implemented.
    - *Onboarding/Offboarding Procedures:* Outline steps for adding or removing employees' access to systems and data.
    - *Playbooks:* Detailed response plans for specific security incidents.
5. **External Considerations:** External considerations encompass external factors that influence security governance, including:
    - *Regulatory:* Compliance with government regulations.

- *Legal:* Adherence to laws related to data protection and privacy.
- *Industry:* Industry-specific security standards and practices.
- *Local/Regional/National/Global:* Considerations based on the geographic scope of operations.

6. **Monitoring and Revision:** Regularly monitoring security measures and policies to identify weaknesses and areas for improvement. Policies and procedures should be updated as needed to address evolving threats and compliance requirements.
7. **Types of Governance Structures:** Different governance structures for security management, including:
    - *Boards:* High-level decision-making bodies responsible for setting security strategy.
    - *Committees:* Groups responsible for specific security functions, such as an Information Security Committee.
    - *Government Entities:* Government agencies that may regulate and oversee security in certain industries.
    - *Centralized/Decentralized:* Describes how security responsibilities are distributed within an organization.
8. **Roles and Responsibilities for Systems and Data:** Clarifies the roles individuals or groups play in managing and protecting systems and data:
    - *Owners:* Individuals or departments responsible for specific systems or data.
    - *Controllers:* Those who determine how data is processed and for what purpose.
    - *Processors:* Entities that handle data on behalf of data controllers.
    - *Custodians/Stewards:* Responsible for the physical or technical protection of data.

5.2 Explain elements of the risk management process

1. **Risk Identification:** This is the process of identifying potential risks that could affect an organization's objectives, assets, or projects. Risks can come from various sources, including internal and external factors.
2. **Risk Assessment:** Risk assessment involves evaluating the identified risks to determine their potential impact and likelihood. There are different approaches to risk assessment:
    - *Ad Hoc:* Informal assessments conducted as needed.
    - *Recurring:* Regularly scheduled assessments, such as quarterly or annually.
    - *One-Time:* Assessments performed for specific projects or situations.
    - *Continuous:* Ongoing monitoring and assessment of risks.
3. **Risk Analysis:** Risk analysis involves a deeper examination of risks to understand their characteristics and potential consequences. It can be done qualitatively or quantitatively:
    - *Qualitative:* Involves assessing risks using non-numerical methods, often categorizing risks as low, medium, or high based on impact and likelihood.
    - *Quantitative:* Involves assigning numerical values to risks to calculate metrics like Single Loss Expectancy (SLE), Annualized Loss Expectancy (ALE), Annualized Rate of Occurrence (ARO) and more:
        - *Single Loss Expectancy (SLE):* The expected monetary loss from a single occurrence of a risk event.
        - *Annualized Loss Expectancy (ALE):* The expected monetary loss from a risk over a year.
        - *Annualized Rate of Occurrence (ARO):* The estimated frequency of a risk event occurring in a year.
        - *Probability:* The likelihood of a risk event occurring.
        - *Exposure Factor:* The percentage of loss if a risk event occurs.
        - *Impact:* The potential consequences or magnitude of harm from a risk event.
4. **Risk Register:** A risk register is a structured document that records information about identified risks, including their descriptions, potential impacts, likelihood, risk owners and risk mitigation strategies.
    - *Key Risk Indicators:* Metrics or data points that provide early warning signs of potential risks.
    - *Risk Owners:* Individuals or groups responsible for monitoring and managing specific risks.
    - *Risk Threshold:* The predefined level at which a risk is considered acceptable or unacceptable.
5. **Risk Tolerance:** The level of risk that an organization is willing to accept before taking action to mitigate it. It reflects the organization's overall attitude toward risk.
6. **Risk Appetite:** The organization's willingness to take on risk to achieve its strategic objectives. It can be categorized as:

- *Expansionary:* A higher willingness to take on risk to pursue growth opportunities.
- *Conservative:* A cautious approach, avoiding excessive risk.
- *Neutral:* A balanced approach between expansionary and conservative.

7. **Risk Management Strategies:** Strategies to deal with identified risks, which can include:
   - *Transfer:* Shifting the risk to another party, typically through insurance or outsourcing.
   - *Accept:* Acknowledging and monitoring the risk. Acceptance strategies may include exemption (certain risks are exempt from mitigation) or exception (specific situations where the risk is accepted).
   - *Avoid:* Taking actions to eliminate or reduce the likelihood of a risk.
   - *Mitigate:* Implementing measures to reduce the impact or likelihood of a risk.
8. **Risk Reporting:** The process of communicating risk information to relevant stakeholders, including executives, board members and other decision-makers. Effective reporting helps inform risk management decisions.
9. **Business Impact Analysis:** A process that assesses the potential impact of a disruption to an organization's operations. Key metrics in business impact analysis include:
   - *Recovery Time Objective (RTO):* The maximum allowable downtime for a system or process.
   - *Recovery Point Objective (RPO):* The maximum allowable data loss in the event of a disruption.
   - *Mean Time to Repair (MTTR):* The average time it takes to restore a system or process.
   - *Mean Time Between Failures (MTBF):* The average time between failures for a system or component.

5.3 Explain the processes associated with third-party risk assessment and management

1. **Vendor Assessment:**

   - *Penetration Testing:* A security assessment method where a third-party organization tries to exploit vulnerabilities in a vendor's systems to identify potential security weaknesses.
   - *Right-to-Audit Clause:* A contractual provision that grants the organization the right to audit the vendor's processes and systems to ensure compliance with security and contractual requirements.
   - *Evidence of Internal Audits:* Documentation or proof that the vendor conducts internal audits to assess its own security practices and compliance.
   - *Independent Assessments:* Evaluations performed by third-party organizations or auditors to verify the vendor's security controls and compliance.
   - *Supply Chain Analysis:* An examination of the entire supply chain to identify and assess potential risks associated with vendors, suppliers and subcontractors.

2. **Vendor Selection:**
   - *Due Diligence:* The process of thoroughly researching and investigating potential vendors to assess their capabilities, financial stability, reputation and security posture.
   - *Conflict of Interest:* Identifying and managing any potential conflicts of interest that could compromise the vendor's ability to provide services impartially.

3. **Agreement Types:**
   - *Service-Level Agreement (SLA):* A contract that defines the specific services a vendor will provide, along with performance expectations, metrics and penalties for non-compliance.
   - *Memorandum of Agreement (MOA):* A less formal agreement outlining specific terms and conditions of cooperation between parties.
   - *Memorandum of Understanding (MOU):* Similar to an MOA but often used for broader, non-binding agreements.
   - *Master Service Agreement (MSA):* A comprehensive agreement that outlines the general terms and conditions that apply to multiple transactions or projects between parties.
   - *Work Order (WO)/Statement of Work (SOW):* Documents specifying the scope, deliverables, timelines and costs for specific projects or tasks.

- *Non-Disclosure Agreement (NDA):* A legal agreement that protects sensitive information shared between parties.
- *Business Partners Agreement (BPA):* A contract that formalizes the business relationship between two parties, often used for long-term partnerships.

4. **Vendor Monitoring:** Continuously assessing and tracking the vendor's performance, security practices and compliance with contractual obligations throughout the duration of the business relationship.

5. **Questionnaires:** Surveys or questionnaires that vendors are asked to complete to provide information about their security practices, controls and compliance with relevant standards and regulations.

6. **Rules of Engagement:** A set of guidelines and procedures that outline the scope, objectives and boundaries of a security assessment or engagement when assessing a vendor's security controls and practices.

5.4 Summarize elements of effective security compliance

1. **Compliance Reporting:**
   - *Internal Reporting:* Regular assessments and reporting within the organization to ensure adherence to cybersecurity standards.
   - *External Reporting:* Submission of compliance reports to relevant regulatory bodies and external authorities to demonstrate cybersecurity measures.
2. **Consequences of Non-Compliance:**
   - *Fines:* Financial penalties for failing to meet cybersecurity compliance standards.
   - *Sanctions:* Imposed restrictions or penalties for non-compliance.
   - *Reputational Damage:* Harm to the organization's reputation due to cybersecurity breaches or failures.
   - *Loss of License:* Revocation of licenses or permits related to cybersecurity operations.
   - *Contractual Impacts:* Negative effects on business relationships and contracts due to non-compliance with cybersecurity requirements.
3. **Compliance Monitoring:**
   - *Due Diligence/Care:* Ongoing efforts to ensure that cybersecurity measures are in place and effective.
   - *Attestation and Acknowledgment:* Formal acknowledgment of compliance status from relevant stakeholders.
   - *Internal and External Monitoring:* Continuous assessment of cybersecurity measures both within the organization and through external audits.
   - *Automation:* Utilization of automated tools and technologies to enhance the efficiency and accuracy of compliance monitoring processes.
4. **Privacy:**
   - *Legal Implications:* Awareness of and adherence to local, national and global privacy laws and regulations.
   - *Data Subject:* Recognition and protection of the rights and privacy of individuals whose data is being handled.
   - *Controller vs. Processor:* Clear understanding of roles and responsibilities regarding data handling.
   - *Ownership:* Clearly defined ownership of cybersecurity and privacy responsibilities within the organization.
   - *Data Inventory and Retention:* Maintaining a comprehensive inventory of data and implementing secure retention practices.
   - *Right to Be Forgotten:* Acknowledgment and implementation of the right for individuals to have their data erased or forgotten as part of privacy measures.

5.5 Explain types and purposes of audits and assessments

1. **Attestation:**
    - Attesting to the accuracy and reliability of information or processes related to cybersecurity.
    - *Example:* A third-party attesting that an organization's cybersecurity controls meet specific standards or regulations.
2. **Internal Audits and Assessments:**
    - *Compliance Audits:* Evaluating adherence to internal policies and external regulations.
    - *Audit Committee Assessments:* Assessing the effectiveness of cybersecurity measures and reporting to the organization's audit committee.
    - *Self-Assessments:* Organizations internally evaluating their own cybersecurity controls and practices.
3. **External Audits and Assessments:**
    - *Regulatory Audits:* Ensuring compliance with external regulations and industry standards.
    - *Examinations:* Thorough review and evaluation of cybersecurity controls, often by external regulatory bodies.
    - *Assessment:* Comprehensive evaluation of cybersecurity practices, often conducted by external experts.
    - *Independent Third-Party Audit:* Evaluation of cybersecurity controls by an external entity independent of the organization.
4. **Penetration Testing:**
    - *Physical Penetration Testing:* Assessing the security of physical infrastructure and access controls.
    - *Offensive Penetration Testing:* Simulating cyber attacks to identify vulnerabilities in systems and applications.
    - *Defensive Penetration Testing:* Evaluating the effectiveness of defense mechanisms and response capabilities.
    - *Integrated Penetration Testing:* Combining various testing methods to provide a holistic view of cybersecurity.
    - *Known Environment Testing:* Testing in an environment where information about the systems is known.
    - *Partially Known Environment Testing:* Testing in an environment with limited information about the systems.
    - *Unknown Environment Testing:* Testing in an environment where little to no information about the systems is provided.
    - *Reconnaissance:*
        - *Passive Reconnaissance:* Collecting information without directly interacting with systems.
        - *Active Reconnaissance:* Actively probing systems to gather information for potential vulnerabilities.

5.6 Given a scenario, implement security awareness practices

1. **Phishing:**
    - *Campaigns:*
        - *Development:* Create simulated phishing campaigns to mimic real-world scenarios.
        - *Execution:* Distribute these simulated phishing emails to employees.
        - *Reporting and Monitoring (Initial):* Track employee responses and identify those who fall for the simulated phishing attempts.
    - *Recognizing a Phishing Attempt:*
        - *User Guidance and Training (Policy/Handbooks):* Develop and distribute clear policies and handbooks outlining common phishing indicators (ex. suspicious email addresses, unexpected links).
        - *User Guidance and Training (Situational Awareness):* Conduct training sessions to enhance employees' situational awareness, teaching them to be cautious about unexpected emails.
        - *User Guidance and Training (Social Engineering):* Provide guidance on recognizing social engineering tactics commonly used in phishing attacks.

        - *Reporting and Monitoring (Recurring):* Encourage employees to report any suspicious emails they encounter.
        - *User Guidance and Training (Reporting):* Train employees on the reporting process for suspected phishing attempts.
        - *Reporting and Monitoring (Recurring):* Regularly reinforce the importance of reporting and monitor trends in reported incidents.
    - *Responding to Reported Suspicious Messages:*
        - *User Guidance and Training (Operational Security):* Train employees on the appropriate steps to take when they receive a suspicious email, emphasizing not clicking on links or downloading attachments.
        - *User Guidance and Training (Hybrid/Remote Work Environments):* Address specific considerations for recognizing phishing attempts in hybrid or remote work settings.
2. **Anomalous Behavior Recognition:**
    - *Risky, Unexpected, Unintentional:*
        - *User Guidance and Training (Insider Threat):* Educate employees on identifying risky behavior that may indicate an insider threat.
3. **User Guidance and Training:**
    - *Policy/Handbooks:*
        - *Development:* Create comprehensive policies and handbooks covering various aspects of security awareness.
    - *Situational Awareness:*
        - *User Guidance and Training:* Conduct regular training sessions to enhance employees' overall situational awareness regarding security threats.
    - *Insider Threat:*
        - *User Guidance and Training:* Provide specific training on recognizing and reporting insider threat indicators.
    - *Password Management, Removable Media and Cables:*
        - *User Guidance and Training:* Conduct training sessions on secure password practices, the risks associated with removable media and the importance of secure cable management.
    - *Social Engineering:*
        - *User Guidance and Training:* Educate employees on various social engineering techniques and how to avoid falling victim to them.
    - *Operational Security:*
        - *User Guidance and Training:* Emphasize the importance of operational security measures, such as not sharing sensitive information unnecessarily.
    - *Hybrid/Remote Work Environments:*
        - *User Guidance and Training:* Tailor security awareness training to address the unique challenges and considerations in hybrid or remote work environments.
4. **Reporting and Monitoring:**
    - *Initial:*
        - *Reporting and Monitoring:* Establish a system for employees to report any security concerns or incidents promptly.
    - *Recurring:*
        - *Reporting and Monitoring:* Regularly communicate the importance of ongoing vigilance and reporting.
5. **Development:**
    - *User Guidance and Training:* Continuously update and evolve security awareness programs to address emerging threats.
6. **Execution:**
    - *User Guidance and Training:* Regularly conduct simulated exercises, such as phishing campaigns, to test and reinforce security awareness.