* General Concepts
  1. **Types of Security Controls**
* **Categories**
  + Technical
  + Managerial
  + Operational
  + Physical
* **Control Types** 
  + Preventive
  + Deterrent
  + Detective
  + Corrective
  + Compensating
  + Directive

What is an Organization?

* It is an entity formed for specific purpose and composed of people who work together to achieve common goals.
* Government agencies, businesses, non-profit groups, educational institutions, etc.
* They are structured entities with defined roles, responsibilities and a hierarchical framework.

Organizational Structure and Hierarchy:

* Structure and hierarchy vary. However, there are common elements found in many structures.
* The **CEO** is the top executive responsible for overall management and decision-making.
* The **Executive Team** consists of two executives who manage specific functional areas within the organization: CFO, CISO, COO, etc.
* **Middle Management** includes managers who oversee specific departments within the organization.
* **Employees/Staff**: The Operational level where employees perform their specific roles and contribute to daily tasks.

Organizational Security:

* The measures implemented in an organization to protect its assets from various threats.
* The goal is to establish a system the protects organizational resources.
* Organizational security is important to protect information, reputation, and more.

Security Controls and Functions:

* To achieve protection, there are security controls. Security controls are measures taken to protect systems. They can be **technical**, **physical** or **administrative**.
* These controls are essential for managing and mitigating risks associated with cyberattacks.
* These controls can have specific functions (prevent an attack, discourage an attacker, correct after an attack, etc.)

Categories of Security Controls:

* **Technical controls** use technology to enforce security.

Examples: Firewalls, Anti- virus software, Encryption, Multi-factor authentication.

* **Managerial controls** involve policies, procedures, education to manage security practices in an organization.

Ex: Security policies, audits.

* **Operational controls** focus on people to implement the secure operation of systems (unlike technology).

Ex: Awareness programs, Change management.

* **Physical controls** involve the use of tangible measures to protect physical assets and control access to physical spaces. Ex: Biometric scanners, keycard systems, fire suppression systems.

Control Functions:

* **Preventive controls** stop security incidents before they occur. As the name implies, they "prevent" attacks.

Examples: firewalls, encryption, authentication technologies.

* **Detective controls** are used to identify attackers.

Examples: alarm systems, intrusion detection systems (IDS), CCTV.

* **Deterrent controls** are used to discourage attackers by increasing the perceived difficulty.

Examples: warning signs, security policies.

* **Corrective controls** are used to restore systems and reduce the impact of Attacks.

Examples: generators, patching, updates, backups.

* **Compensating controls** are alternative measures implemented to meet a requirement when the primary control is not feasible.

Examples: Primary control is automated patching and compensate with manual reviews.

* **Directive controls** direct the actions of individuals.

Examples: Security policies, Training and awareness, Standard Operating Procedures.

* 1. **Fundamental Concepts**
* **Confidentiality, Integrity, and Availability (CIA)**
* **Non-repudiation**
* **Authentication, Authorization, and Accounting (AAA)** 
  + Authenticating people
  + Authenticating systems
  + Authorization models
* **Gap analysis**
* **Zero Trust** 
  + Control Plane
    - Adaptive identity
    - Threat scope reduction
    - Policy-driven access control
    - Policy Administrator
    - Policy Engine
  + Data Plane
    - Implicit trust zones
    - Subject/System
    - Policy Enforcement Point
* **Physical security** 
  + Bollards
  + Access control vestibule
  + Fencing
  + Video surveillance
  + Security guard
  + Access badge
  + Lighting
  + Sensors
    - Infrared
    - Pressure
    - Microwave
    - Ultrasonic
* **Deception and disruption technology**
  + Honeypot
  + Honeynet
  + Honeyfile
  + Honeytoken

CyberSecurity Principles:

Cybersecurity is made of 3 fundamental principles called the **CIA** Triad.

* **Confidentiality**: ensures that data is kept private from unauthorized access.
* **Integrity**: maintains the trustworthiness of data.
* **Availability**: users should be able to access data whenever they need to.

Confidentiality:

* It is a fundamental principle in cybersecurity that focuses on protecting sensitive information from unauthorized access.
* With confidentiality, we want to prevent **unauthorized disclosure** of information.
* **Encryption** is one of the techniques used to provide confidentiality by converting data into an unreadable format.

Integrity:

* It is a principle in cybersecurity that focuses on ensuring the accuracy and reliability of data.
* The goal is to prevent unauthorized modification of data to maintain its trustworthiness.
* **Hashing** is one of the techniques used to provide integrity.
* **Example**: A sender wants to ensure that the content of an email message remains SULTING unchanged during transmission.

Availability:

* Availability refers to the accessibility of data when needed. The goal of availability is for timely access to resources.
* Ensuring availability is essential to prevent disruptions, downtime, or more attacks.
* There are multiple ways to achieve availability such as having backups, ONSULTING distributing network traffic, etc.

Non-Repudiation:

* Non-repudiation is a concept that ensures that a party cannot deny the origin of a message.
* It provides evidence that the sender of data cannot deny their involvement in the process.
* Non-repudiation is critical for maintaining trust in digital transactions. It helps ensure accountability and provide a means to resolve disputes.

IAM :- Identity & Access Management:

* IAM is a set technologies that organizations use to control access to their apps, data, and more.
* IAM ensures that only authorized entities can access the resources they need.
* IAM is essential for maintaining the security and CURITY integrity of an organization's resources. It helps prevent unauthorized access.

Authentication, Authorization & Accounting: (AAA)

* **AAA:** Several protocols provide authentication, authorization, and accounting services.
* **Identity:** Who is a user or system in the organization and what their attributes are, such as their name, email address, and role.
* **Authentication**: Verifying the identity of users and systems by requiring them to provide credentials, such as passwords.
* **Authorization**: Determining what users and systems are allowed to do by assigning them permissions to resources.
* **Accounting**: Track who accessed what resources and when, which can Be used to investigate security incidents.
* **Accountability:** Auditing logs and audit trails record events including the identity of the subject that performed an action.

Authentication People:

* Verifying the identity of individuals who attempt to access a system.
* Methods:
  + **Something you know** - Passwords, PIN numbers.
  + **Something you have** - Smart card, physical tokens.
  + **Something you are** - Biometrics, Physical characteristics (fingerprints, facial recognition, etc.

Authentication System:

* Verifying the identity devices to ensure they are trusted before allowing access.
* Methods:
  + **Certificates** - Digital certificates assigned to systems for identification.
  + **Kerberos** - Uses "tickets" issued by a third-party to authenticate systems.
  + **NAC (Network Access Control)** - inspect computers and allow compliant devices in the network.

Authorization Models:

* Authorization is the process of granting or denying access to authenticated users based on their roles, attributes, or other criteria.
* It determines what actions a user is allowed to perform and which resources they can access.
* By using authorization, organizations can ensure that only authorized users have access to resources.

Access Control Models:

* The methods used to manage access to resources.
* They are essential for ensuring that only authorized individuals have the appropriate level of access to specific resources.
* There are several access control schemes commonly employed in IAM: RBAC, MAC, Rule-BAC, ABAC, DAC.
  + **Role-based Access Control (RBAC):** is based on your role in the organization.
    - The administrator determines what kind of access a user has.
    - Useful for users in a department with same job functions.
  + **Mandatory Access Control (MAC)**: uses labels to determine access.
    - It is based on clearance levels. Every object gets a label, users are labelled with rights on what they can access.
    - It is common in the military.
  + **Discretionary Access Control (DAC)**: the **owner** of data determines access.
    - Access can be modified by users. It is has weak security because it relies on the owner of the file
  + **Attribute-based Access Control (ABAC)** creates relationships for authorization. Many criteria are used to determine access.
    - It considers IP address, time, GPS location, etc. Policies typically use plain language.

Gap Analysis:

* Gap analysis is a process used to identify the differences between an organization's current cybersecurity posture and the desired state.
* Where are you? Where are you trying to be? What is the difference (the gap)?
* This involves examining existing security controls and policies to identify areas where improvements YBERSECURIT are needed to meet requirements.NG
* Gap analysis helps organizations identify weaknesses in their cybersecurity practices.
* **Scenario**: A healthcare organization wants to ensure HIPAA compliance to protect sensitive patient information and avoid fines.
* **Review the current state**, conduct an inventory of all IT assets handling patient data, review policies, perform audits.
* **Identify the desired state**, review HIPAA rules, set objectives (encryption of patient data, risk assessments, secure access controls, etc.)
* **Conduct the gap analysis**, Compare the current policies against HIPAA requirements, identify the "gaps" (e.g. lack of encryption, improper access). Prioritize the gaps (low, medium, high), and develop an action plan.
* **Execute the plan**, start with the high priority, and monitor progress.
* **Document and report**, document your actions and findings, for stakeholders.

Zero Trust:

* **Zero-Trust** is a security model based on the principle of "**never trust, always verify**".
* It requires verification for every person/device trying to access resources, regardless of their status.
* Zero Trust requires all users/devices to be authenticated, authorized, and continuously validated before being granted access.
* **The control plane** decides who or what can access resources. The **data plane** enforces these decisions and handles the movement of data within the network.

Control Plane:

* The control plane is responsible for making all security-related decisions.
* **Adaptive Identity Management**: The control plane dynamically adjusts access based on user identity and context. It uses factors like location, device, and behavior.
* **Threat Scope Reduction**: Minimizing the attack surface by limiting access to resources based on least privilege. This limits the impact of a security breach.
* **Policy-Driven Access: Access** decisions are based on predefined policies.
* **Policy Administrator and Engine**: Components of the control plane that create and enforce policies, making real-time access decisions based on risk assessments and context.

Data Plane:

* The data plane enforces the decisions made by the control plane.
* **Implicit Trust Zones**: The data plane enforces segmentation and controls traffic between different
* trust zones. Ensures that even within trust zones, access is verified.
* **Subject/System**: The entities and devices requesting access to resources. The data plane ensures
* that only verified subjects (users) and systems (devices) can access the network.
* **Policy Enforcement Point (PEP)**: The component that enforces access control decisions. PEPs are
* responsible for enforcing decisions.

HoneyPots:

* Honeypots are fake systems (servers, software, etc.) designed to attract cybercriminals.
* The goal is to understand the attackers' tactics and improve defense strategies.
* A honeynet is a network of honeypots.
* A honeyfile is a fake file placed within a network to attract cybercriminals.

Physical Security:

* It is a critical aspect of cybersecurity, encompassing measures to protect physical assets and infrastructure from unauthorized access.
* While cybersecurity often focuses on digital threats, physical security is equally important in ensuring the safety of an organization's resources.
* The combination of physical and digital security measures creates a solid defense against threats.

Elements of P Physical Security:

* **Bollards** are barriers to control and restrict vehicle entry points, minimizing the risk of vehicular attacks.
* **Fences** surround premises to deter unauthorized entry and provide a clear boundaries.
* **Security Guards** are trained personnel at entry points and sensitive areas to monitor activities, verify credentials, and respond to threats.
* **Badges** are issued to personnel to authenticate their identities within the premises.
* **Mantraps** (Access control vestibules) are doors that restrict entry to one person at a time.
* **CCTVs** monitor and record activities in and around the premises.
* **Proper Lighting** improve visibility and deter unauthorized activities during low-light conditions.
* **Sensors detect movement (motion sensors) or specific environmental conditions.**
  + **Infrared**: Detect infrared radiation, emitted as heat.
  + **Pressure**: Measure the force exerted by a fluid on a surface.
  + **Microwave**: measuring changes in microwave signal.
  + **Ultrasonic**: Use sound waves to detect objects.
* **Alarm** systems provide alerts in response to security breaches.
* Implement secure **power distribution** and backup systems to ensure continuous operation.
* **HVAC** (Heating, Ventilation, & Air Conditioning) systems to prevent tampering or disruptions.
* Implement **fire suppression systems** to protect against physical threats, such as fire incidents.
* **RFID** (Radio Frequency Identification) is a technology that uses microchips to identify and track tags attached to objects. These tags contain electronic information.
* **Industrial Control Systems and SCADA** systems are designed to control and automate industrial processes.
  1. **Change Management**
* **Business processes impacting security operation** 
  + Approval process
  + Ownership
  + Stakeholders
  + Impact analysis
  + Test results
  + Backout plan
  + Maintenance window
  + Standard operating procedure
* **Technical implications**
  + Allow lists/deny lists
  + Restricted activities
  + Downtime
  + Service restart
  + Application restart
  + Legacy applications
  + Dependencies
* **Documentation**
  + Updating diagrams
  + Updating policies/procedures
* **Version control**

Security Policies:

* Security policies provide a foundation for implementing security practices in an organization.
* They are documents that outline an organization's approach to security.
* They serve as a guide for decision-making.
* Acceptable Use Policies, Change Management, Access control policies, etc.

Change Management:

* Change management is a policy that organizations follow to control changes to their IT systems.
* The goal is to ensure that any modifications are done in a controlled manner, encouraging accountability.
* It requires a formal and approval process.
* e.g. someone trying to modify software code at Spotify.

Business processes impacting security operation:

* **Approval Process**: Obtaining the necessary authorization before implementing a change. Users request and a board approves.
* **Ownership**: Individuals/groups responsible for overseeing changes.
* **Stakeholders**: Entities that have an interest in the outcome of a change. Employees, managers, customers, suppliers, clients, etc.
* **Impact Analysis**: The potential consequences of a proposed change.
* **Backout Plan**: The steps to revert a change to its previous state in case of unforeseen issues or failures.
* **Maintenance Window**: Period during which changes are scheduled to occur without causing disruption to normal operations.
* **Standard Operating Procedure** (SOP): Step-by-Step instructions that define how processes should be performed.

Technical implications:

* **Allow Lists:** Specify which entities are permitted to access certain resources. Only entities on the allow list are granted access, while all others are denied by default.
* **Deny Lists** (Blacklists): Specify entities that are explicitly prohibited from accessing certain resources.
* **Downtime**: The period during which a system is unavailable to users.
* **Service/Application Restart**: Stopping and then restarting a service/ application to implement changes.
* **Legacy Systems**: Systems that have been in use for an extended period and no longer supported by vendors. AINING
* **Dependencies**: Relationships between different systems that rely on each other to function properly.

Documentation:

* **Updating Diagrams**: Modifying diagrams to reflect changes.

Version Control:

* Record changes to a file over time so that specific versions can be recalled later.
  + Allows tracking of modifications to documents or code.
  + Enables reverting to previous versions if a change causes issues.
  1. **Cryptography**
* **Public key infrastructure (PKI)**
  + Public key
  + Private key
  + Key escrow
* **Encryption**
  + Level
    - Full-disk
    - Partition
    - File
    - Volume
    - Database
    - Record
  + Transport/communication
  + Asymmetric
  + Symmetric
  + Key exchange
  + Algorithms
  + Key length
* **Tools**
  + Trusted Platform Module (TPM)
  + Hardware security module (HSM)
  + Key management system
  + Secure enclave
* **Obfuscation**
  + Steganography
  + Tokenization
  + Data masking
* **Hashing**
* **Salting**
* **Digital signatures**
* **Key stretching**
* **Blockchain**
* **Open public ledger**
* **Certificates**
  + Certificate authorities
  + Certificate revocation lists (CRLs)
  + Online Certificate Status Protocol (OCSP)
  + Self-signed
  + Third-party
  + Root of trust
  + Certificate signing request (CSR) generation
  + Wildcard

Cryptography:

* The practice of securing networks by transforming data into a form that cannot be understood.
* Cryptography has 2 important concepts encryption and hashing.

PKI: (Public Key infrastructure)

* A system that uses cryptographic keys to secure data.
* PKI is used for secure communication, secure websites, email encryption, and apps where security is essential.
* PKI enables secure communication by ensuring that entities can trust each other.
* Concepts covered: Encryption, Digital certificates, Public keys, Private keys, Digital signatures.

Encryption:

* Encryption is a method of transforming readable data (**plaintex**t) into an unreadable form (**ciphertex**t).
* Once plaintext is transformed into ciphertext, neither human nor machine can process it until it is decrypted.
* Encryption uses "**keys**" to encrypt the data.
* Decryption is the opposite, it takes encrypted data and makes it readable.
* There are 2 types of encryption:
  + **Symmetric Encryption**
  + **Asymmetric Encryption**

Encryption Concepts:

* **Symmetric encryption** is a type of encryption where one key is used for encryption and decryption.
* **Asymmetric encryption** is a type of encryption that uses a pair of **public and private keys**. One key is used for encryption, and the corresponding key is used for decryption. The two keys are mathematically related.
* **Keys** are random values used to perform encryption or decryption.
* **Public Keys** are types of keys that are **shared openly** and used for encryption/decryption.
* **Private Keys** are secret keys known **only to the key's owner**.
* A **key escrow** is to a system in which keys are stored securely by a 3rd party.

Types of Encryption:

* Symmetric Encryption
  + It uses one key to encrypt/decrypt.
  + The key always has to be private, it should never be known to anyone else.
  + Anything encrypted with the key can only be decrypted with the same key.
* Asymmetric Encryption
* It uses 2 keys to encrypt/decrypt.
* It uses 2 keys, **public & private** keys. Public keys are known to everyone. Private keys should never be known to anyone else.
* Anything encrypted with a public key can only be decrypted with the matching private key; and vice-versa.

Encryption:

* **Full-disk Encryption** (FDE): Encrypts all data on a disk, the OS, apps, and data.
* **Partition Encryption**: Encrypts a specific partition on a disk rather than the entire disk.
* **File Encryption**: Encrypts individual files.
* **Database Encryption**: Encrypts data within a database to protect sensitive information stored in database
* **Record Encryption**: Encrypts individual records within a database or file.

Encryption Concepts:

* **Algorithms**: Mathematical procedures used to encrypt and decrypt data. Examples are **AES** (secure), **DES** (not secure).
* **Key Exchange**: The process of exchanging keys between parties. Ensures that keys used are securely distributed, preventing interception by unauthorized parties. **Diffie-Hellman** (DH) key exchange is one of the processes used to exchange keys.
* **Key Length**: The size of the key used in an encryption, typically measured in bits. Longer keys provide stronger security. AES has a secure version of **256-bit** keys.
* **Key Stretching**: Techniques used to make keys more secure.

Block & Stream Ciphers:

**Block Ciphers**:

* Encrypt data in fix sized blocks.
* Used when the size of the data to be encrypted is **known**.
* Used on fixed size files.

**Stream Ciphers**:

* Encrypt data bit by bit (one bit at a time).
* Used when the **size of the data is unknown**.
* Useful in live streaming.

Encryption Tools:

* **TPM (Trusted Platform Module)**: A chip integrated into the computer that provides cryptography.
* **HSM (Hardware Security Module)**: Removable devices that provide cryptography.
* **Secure Enclave**: Dedicated area within a computer's CPU to provide cryptography.

Obfuscation:

Obfuscation is a technique used to make data harder to understand. There are three includes methods such as steganography, tokenization, and data masking.

* **Steganography** is the practice of hiding information within other data. It aims to conceal the existence of data.
  + Example: Hiding data within an image, within an audio file, white ink on a file, etc. to make it unnoticeable.
* **Tokenization** is the process of replacing sensitive data with other data that retain essential information.
  + Example: Replacing credit card. numbers with tokens during transactions.
* **Data Masking** involves modifying data to hide its original content while retaining its usability.
  + Example: Removing or blacking out sensitive parts credit card information on a receipt.

Hashing:

* Hashing is a process that transforms data into a fixed- size string of characters called a **hash**.
* It is an **irreversible** process. You cannot retrieve the original data with the hash.
* Any change in the original data will result in a **completely different** hash value.
* Hashes are used to store passwords. Instead of storing the actual passwords, systems store the hashes.
* Hashing provides integrity. How can we be certain that a message we receive or a file we download has not been modified?

Blockchain:

* It is a distributed ledger technology that records transactions across multiple computers.
* Once a transaction is recorded, it cannot be altered.
* There is no central authority; the ledger is maintained by a network of computers.
* It uses cryptographic techniques to secure data and ensure the integrity of transactions.
* Bitcoin, Ethereum, and other crypto currencies rely on blockchain technology.
* **Advantage**: All participants have access to the same data, reducing the need for trust.

Digital Signatures:

* A digital signature is a technique used to ensure the **authenticity and integrity** of messages.
* How?
* It provides **authenticity** by encrypting messages with the user's private key, so only the sender can be the only person who sent it.
* It provides **integrity** by hashing the message, so no one can modify that message before it gets to the
* This combination of hashing + private keys form a concept called **digital signatures**.

Digital Certificates:

* It is a digital file that proves the **authenticity** of a website/computer / etc.
* Think of it as someone's driver's license.
* Certificates contain information such as the name, the period of validity, the public key of the server.
* Certificates are issued by a trusted entity known as a **Certificate Authority (CA)**.
* Websites use certificates to establish secure connections. This is indicated by the <https://sign>.
* Certificates can be revoked, if the validity period ends or if the organization was involved in fraud.

Certificate Authority: (CA)

* It is a trusted entity whose primary function is to issue digital certificates.
* CAs play a critical role in establishing trust on the internet by providing the platform for secure communication.
* With CAs, two entities that have never communicated together can do so securely.

Certificates:

* **CERTIFICATE:** A digital document that binds a public key to an entity (usually a website)
* **CERTIFICATE REVOCATION LIST (CRL)**: List containing certificates that have been revoked
* **ROOT OF TRUST**: The root of trust is the ultimate source of trust in a PKI
* **CERTIFICATE AUTHORITY**: Entities responsible for issuing digital certificates
* **ONLINE CERTIFICATE STATUS PROTOCOL (OCSP)**: Similar to CRL, but revoked certificates are shown in real time
* **CERTIFICATE SIGNING REQUEST (CSR)**: A request sent to a CA to apply for a certificate
* **SELF-SIGNED CERTIFICATE**: The entity signs its own certificate instead of obtaining it from a CA
* **WILDCARD CERTIFICATE**: Certificates that secure a domain and all its subdomains.
  + For example, a wildcard certificate for **\*.google.com** would secure
    - **mail.google.com**,
    - **drive.google.com**,
    - **maps.google.com**, etc.