- **Security controls Types:**
  - Technical: includes the many technologies used to protect assets, such as encryption, authentication, etc.
  - Operational: relate to maintain day-to-day security environment.
  - Managerial: centered on how the Technical and Operational controls reduce risk, includes policies, standards, and procedures.
- Information Privacy: the protection of unauthorized access and distribution of data.
- Data Owner: the person who can access, edit, use, or destroy their information.
- Data Custodian: anyone or anything that's responsible for the safe handling, transport, and storage of information.
- Data Steward: the person or group that maintains and implements data governance policies set by an organization.
- The principle of least privilege: a security concept in which a user is only granted the minimum level of access and authorization required to complete a task or function.
- Data lifecycle consists of 5 main stages: Collection, Storage, Usage, Archival, and Destruction.

- **Three of the most influential industry regulations that every security professional should know about are:**
  - **General Data Protection Regulation (GDPR)**
    - A set of rules and regulations developed by the European Union (EU) that puts data owners in total control of their personal information.
    - Under GDPR, types of personal information include a person's name, address, phone number, financial information, and medical information.
  - **Payment Card Industry Data Security Standard (PCI DSS)**
    - A set of security standards formed by major organizations in the financial industry.
    - Aims to secure credit and debit card transactions against data theft and fraud.
  - **Health Insurance Portability and Accountability Act (HIPAA)**
    - A U.S. law that requires the protection of sensitive patient health information.

- Security audit: a review of an organization's security controls, policies, and procedures against a set of expectations.
- Security assessment: a check to determine how resilient current security implementations are against threats.
- Encryption: the process of converting data from a readable format to an encoded format
- Cipher: an algorithm that encrypts information
- Public key infrastructure (PKI): an encryption framework that secures the exchange of online information
- **Types of encryption:**
  - **Symmetric encryption**
    - The use of a single secret key to exchange information.
    - Fast, but less secure.
    - Algorithms:
      - **Triple DES (3DES)**
        - Known as a block cipher because of the way it converts plaintext into cipher text in "blocks."
        - Generates keys that are 192 bits
        - Many organizations are moving away from using Triple DES due to limitations on the amount of data that can be encrypted
      - **Advanced Encryption Standard (AES)**
        - One of the most secure symmetric algorithms today
        - Generates keys that are 128, 192, or 256 bits.

Created By: Abdelrahim Alsadiq

    - **Asymmetric algorithms**
        - The use of a public and private key pair for encryption and decryption of data. It uses two separate keys: a public key and a private key.
        - The public key is used to encrypt data, and the private key decrypts it. The private key is only given to users with authorized access.
        - **Algorithms:**
            - **Rivest Shamir Adleman (RSA):**
                - Key sizes are 1,024, 2,048, or 4,096 bits
                - Mainly used to protect highly sensitive data.
            - **Digital Signature Algorithm (DSA)**
                - Generates key lengths of 2,048 bits
                - Widely used today as a complement to RSA in public key infrastructure.

- OpenSSL: an open-source command line tool that can be used to generate public and private keys.

- Non-repudiation: the concept that the authenticity of information can't be denied
- Hash functions: algorithms that produce a code that can't be decrypted
- Rainbow table: a file of pre-generated hash values and their associated plaintext
- Hash collision: An instance when different inputs produce the same hash value
- Salting: An additional safeguard that's used to strengthen hash functions
- Single sign-on (SSO): a technology that combines several different logins into one.
- Access Controls: security controls that manage access, authorization, and accountability of information.
- AAA Framework: a security framework that controls access to computer resources, enforces policies, and audits usage. Includes:
    - Authentication
    - Authorization.
    - Accountability.
- **Authentication factors:**
    - Knowledge: something the user knows, such as password or security question.
    - Ownership: something the user possesses, such as OTP.
    - Characteristics: something the user is, such as biometrics.
- Basic auth: The technology used to establish a user's request to access a server
- OAuth: An open-standard authorization protocol that shares designated access between applications

- Application programming interface (API) token: A small block of encrypted code that contains information about a user
- Session: A sequence of network HTTP basic auth requests and responses associated with the same user
- Session ID: A unique token that identifies a user and their device while accessing a system
- Session cookie: A token that websites use to validate a session and determine how long that session should last
- Session hijacking: An event when attackers obtain a legitimate user's session ID
- User provisioning: the process of creating and maintaining a user's digital identity.
- **Granting authorization Frameworks:**
    - **Mandatory access control (MAC)**
        - Based on a strict need-to-know basis
        - Access to information must be granted manually by a central authority or system administrator.
    - **Discretionary access control (DAC)**
        - Applied when a data owner decides appropriate levels of access
    - **Role-based access control (RBAC)**
        - When authorization is determined by a user's role within an organization.