

CIA

Confidentiality -> ensure that sensitive information is not disclosed to unauthorized individuals, entities or processes

- Access Controls -> Passwords, Biometric Verification, limit resource access
- Encryption -> The process of encoding information so only authorized parties can read it. If in case unauthorized party intercepts the data would not be able to interpret without the encryption key
- Secure Communication -> Use secure protocols as TLS on transfer data to prevent interception

Integrity -> Protecting data from unauthorized changes (accuracy of data)

- Data Accuracy
- Data Consistency
- Data Trustworthiness (you can trust)

Methods:

- Cryptographic hash Functions
- Digital Signatures
- Access Controls (edit permission)

Availability -> Ensure that data, systems and services are accessible to authorized users when needed

- Fault Tolerance -> Even if a component fail the system would still be accessible (multi region, cluster, HA (Active-Passive OR Active-Active))
- Backup System -> Regularly backing up data to enable recovery in case of data loss or corruption

Disclosure X Confidentiality

Alteration X Integrity

Denial X Availability

AAA - Authentication x Authorization x Auditing

Authentication -> Process of verifying the identity of a user, device or other entity in a computer, typically as a prerequisite to granting access to a resource (user can login)

Authorization -> Once a user is authenticated, the authorization determines what that user is permitted to do by matching user credentials against an access control list (user permission based on ACL)

Auditing (or accounting) -> Ensured by keeping a track of activities, logging and monitoring all user actions

Accountability is key for non-repudiation, it ensures individuals or entities are held responsible for their actions

1. Identification
2. Authentication
3. Authorization
4. Accounting
5. Accountability

Non-repudiation -> Ensure that a party in a communication cannot deny the authenticity of their actions (always have proof of a action)

To monitor this:

- Digital signatures
- Logs
- Audit

Solutions:

- TACACS+ -> TCP routers, switches, and firewalls -> for environments requiring strict control
- RADIUS -> UDP Wi-Fi, VPN, dial-in -> where speed and scalability are important

Authentication people:

- Usernames and passwords
- Biometrics
- MFA

Authentication device:

- Digital certificates
- IP addresses
- MAC addresses

Controls Categories

Technical Security Controls -> Logical controls implemented in hardware, software or firmware that automat the process of preventing, detecting and responding to security threats (things that go to a paper or PDF)

- ACL
- Firewalls
- Intrusion Detection System (IDS) -> SIEM
- Intrusion prevention Systems (IPS)
- Encryption
- Antimalware
- VPN

Managerial security controls -> Administrative Controls are polices, procedures and guidelines

- Security Polices and Procedures
- Risk Management
- Incident Response and Recovery Plans
- Business Continuity and Disaster Recovery Plan
- Security Awareness Training

Operational Security Controls -> Are the day-to-day methods and procedures that are implemented to ensure and maintain the security of its information and assets (done by the people in the org)

- Physical media protection
- The execution of Incident response plan

Physical security Controls -> protect the actual hardware and facilities, these controls are designed to prevent unauthorized access, damage, and interference to the organizations physical resources

- Lighting
- Signs
- Fences
- Security guards
- Cameras

Technical Security Controls -> Could be configured

Managerial security controls -> Could be in a paper or a PDF

Operational Security Controls -> Day-to-day security

Physical security Controls -> Protect the integrity of the hardware in a physical environment

Controls Types

Preventive Controls -> Attempt to stop a security incident

- IPS
- Firewalls
- Encryption
- Access Control

Detective Controls -> Attempt to detect events that resulted or could result in a security incident

- IDS
- SIEM
- Video surveillance/CCTV
- Motion Detection
- Vulnerability Scanning

Corrective Controls -> Attempts to remediate an incident that has occurred

- UPS (Uninterruptible Power Supply)
- Restoring backups
- Incident Response Procedures

Deterrent Controls -> Attempts to discourage a threat

- Guard dogs
- Cameras
- Barbed wire
- Lighting
- Fencing/Bollards

Directive Controls -> provide directions on how to systems

- Policies
- Procedures

Compensating Controls -> Provide alternate controls when the primary control may not be sufficient

- Segregation of duties

Zero Trust

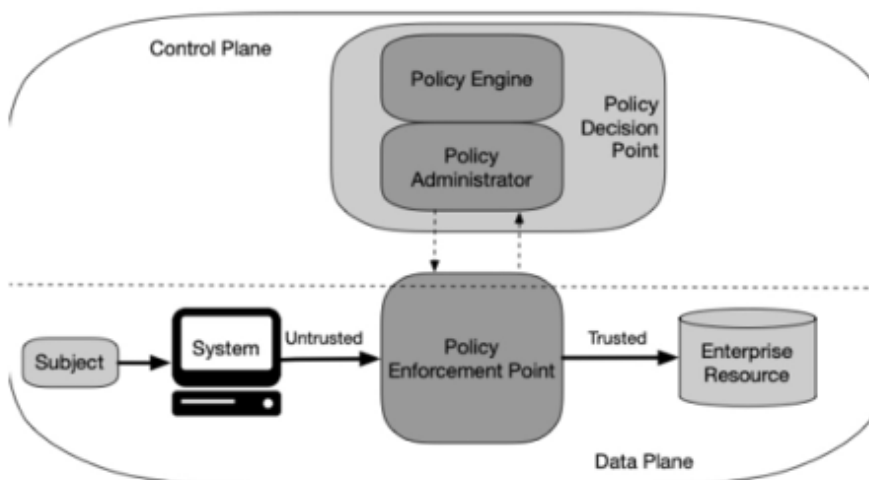
Centers on the belief that organizations should not automatically trust anything inside or outside their perimeters and instead must verify everything trying to connect to its systems before grant access

Control Plane -> Manage all actions of data plane deciding how data packets should be forwarded

- Adaptive Identity -> Based on context adjust dynamically user/system identity verification (adjusts authentication requirements based on user behavior, context, and risk factors)
- Police-driven Access Control -> Access granted based on policies
- Policy Administrator -> Responsible to establish and shut down the communication path based on Police Engine decision
- Police Engine -> Responsible for the decision to grant access to resource for a given subject
- Threat Scope Reduction -> Minimize the attack Surface

Data Plane -> What process the connection with security

- Subject -> Entity requesting access
- Implicit Trust Zone -> Place with Zero Trust
- Policy Enforcement Point (PEP) -> Enable/Disable (based on policies from Control Plane) and monitor connections between subject and resource



No Zero Trust

Connect computer to switch -> Get access to intranet

Zero Trust

Connect computer to switch -> Get log in while the minimum access -> Get access to intranet -> Logs of actions done Admin

Strict Identity Verification (identify users)

Least Privilege Access (minimum access needed, if you just need to read the info, you will not get edit permission)

Multi-Factor Authentication (MFA)

Monitor and Log All Traffic

Cryptography

Is the practice and study of techniques for securing communication and data in the presence of adversaries. It involves creating written or generated codes that allow information to be kept secret.

Focus in confidentiality + integrity (hash)

Algorithms -> Methods or procedures used to encrypt and decrypt data, also defines how the encryption and decryption processes are to be carried out

Key -> Used by the cryptographic algorithms to transform the data, it is what makes your encrypted data unique

Symmetric Encryption -> Faster than asymmetric used for VPNs, Wireless Networks, files and databases, the security depends on the key length, not recommended to large companies

Symmetric Algorithms -> Use the same key for both encryption and decryption

$N(N-1)/2$ -> math formula to get the keys you need depends on the number of the people

Asymmetric Encryption -> Get you a digital signature because it is unique

Asymmetric Algorithms -> Public key cryptography, system that uses pairs of keys: a public key (shared with anyone) and a private key (kept with the owner)

If the public key encrypts the private decrypt (make sure the data was received by you)

If the private key encrypts the public decrypt (make sure the data was sent by you)

Trusted Platform Module (TPM) -> Provide a hardware-based (laptops and computers) root of trust for a system, ensuring hardware-level security for encryption and authentication processes ensuring the integrity of the boot process in computing devices by verifying the integrity of the firmware and boot components.

Secure enclave -> Secure environment for sensitive operations like mobile payments

Key management system (KMS) -> Key management for encryption and decryption tasks. It does not handle certificate issuance or management

Hardware security module (HSM) -> It is like KMS but with physical separation (most used in large scale servers than TPM)

Key escrow -> Secure storage mechanism where cryptographic keys are held to ensure they can be recovered if lost

Key stretching -> technique that slow down the hashing process by repeatedly applying a cryptographic hash function to a password or key. Making it more difficult for attackers to perform brute-force attacks.

- HSM -> Physical device that manage digital keys for strong authentication
- TPM -> A specialized CHIP on an endpoint device that stores RSA encryption keys specific to the host system for hardware authentication
- EFS -> Windows Feature for individual files
- SED -> Storage drives that automatically and continuously encrypt the data on the drive without any user interaction
- FDE -> Full Disk Encryption
- BitLocker -> Windows Feature for full disk
- GPG -> FREE program used to encrypt and decrypt data, messages, and emails
- PGP -> PAID program used to encrypt and decrypt data, messages, and emails
- STARTTLS -> Upgrade the unsecure connection to TLS/SSL
- SMTPS -> OBSOLETE OF SSL/TLS
- SRTP -> Encryption for VOIP
- SHTTP -> Secure Hypertext Transfer Protocol it is the obsolete version of HTTPS

Certificates

Digital Signature -> Cryptographic technique used to validate the authenticity and integrity of a message

- Authenticity -> Confirm that the signature was created by the known sender (non-repudiation)
- Integrity -> Ensure the message was not altered in transit

Creation of Digital Signature -> Hash a message and then encrypt the hash with private key of the sender

Verify Digital Signature -> Use the sender public key to decrypt the hash so could validate the message it is integer

PKI (Public Key Infrastructure) -> A framework used to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption. It is used to facilitate the secure electronic transfer of information for a range of network activities.

- Encryption and Decryption -> PKI allows users to encrypt and decrypt data using public and private keys
- Digital Signatures -> PKI provides for the creation and verification of digital signatures, ensuring the authenticity and integrity of data
- Certificate management -> The CA issues and revokes certificates as needed
- Certificate Signing Request (CSR) -> It is a request sent by an entity to a Certificate Authority to obtain a digital certificate (contains the entity's public key and identifying information, which the CA uses to create the digital certificate)
- Certificate revocation lists (CRLs) -> Lists maintained by CAs that contain the serial numbers of certificates that have been revoked before their expiration date
- Online Certificate Status Protocol (OCSP) -> Check the revocation status of a digital certificate in real-time. (It provides a faster and more efficient method than traditional CRLs)

Root of Trust -> Is just the very beginning or the most trusted part of this chain. If the Root CA is trusted, everything it vouches for can be trusted as well (it is typically a trusted entity or mechanism that is used to verify the authenticity of certificates and ensure the security of communications)

Threats

1. Data Exfiltration (steal data)
2. Espionage
3. Service Disruption (disable or disturb a service)
4. Blackmail
5. Financial Gain
6. Philosophical/Political Beliefs
7. Ethical
8. Revenge
9. Disruption/Chaos
10. War

Shadow IT -> Systems/Hardware/Cloud Providers used/built without org approval, being not approved could not have the certain controls

Vulnerabilities

A weakness in a system that can be exploited by a threat actor to gain unauthorized access

Memory injection

Inserting Malicious code into a program's memory. The attacker leverages vulnerabilities that allow them to execute arbitrary code.

- Code Injection
- Buffer Overflow
- DLL Injection

Fixed by secure coding practices such as input validation, to find miss configured inputs use vulnerability scans

Virtualization Vulnerabilities

Virtual machine Escape -> An attacker runs code on a VM which allows them to break out and interact with the host or other VMs

Resource Reuse -> Sensitive data can remain in system resources and be accessed by other processes

API Vulnerability

Insecure Interfaces and APIs -> Cloud Services are accessed through interfaces and APIs, which, if not properly secured, can be exploited

Mobile Vulnerabilities

- Jailbreaking -> Process of removing software restrictions imposed by the OS (get the root of the phone)

Malware/Attacks

Worm -> Replicate itself in the network infected

Trojans -> Fake being legitimate software but it is a virus

Ransomware -> Steal data (hostage data for money)

Spyware -> Collect data without having any alert (try to be stealth)

Rootkit -> Get admin/escalate permission (SUID) after get access to the machine (try to be stealth)

Logic Bomb -> Malicious code and after some time do a action (try to be stealth)

DNS Hijack -> Manipule DNS server or hosts file to send you to malicious website

On Path Attack -> The new Man in the middle

CSRF -> Trojan but for unwanted actions on a website

Social Engineering

malicious activities accomplished through human interactions

Phishing -> Type of attack that attempts to trick individual into providing sensitive information

Vishing -> Phishing through voice

Smishing -> Phishing through SMS

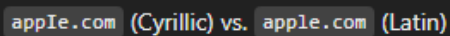
Misinformation -> false/inaccurate information WITHOUT malicious intention

Disinformation -> false/inaccurate information WITH malicious intention

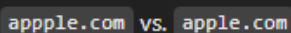
Impersonation -> Spoof a e-mail to pretend to be someone

Pretexting -> Technique where an attacker creates a fabricated scenario or pretext to manipulate individuals

Homograph attacks -> Use similar-looking characters from different writing systems to create deceptive domains

A screenshot of a text box containing the text "appIe.com (Cyrillic) vs. apple.com (Latin)". The text is in a monospaced font, with "appIe.com" in a lighter color and "(Cyrillic)" in a darker color, followed by "vs.", "apple.com", and "(Latin)".

Typosquatting -> Takes advantage of common typos or misspellings in domain names

A screenshot of a text box containing the text "appple.com vs. apple.com". The text is in a monospaced font, with "appple.com" in a lighter color and "vs." in a darker color, followed by "apple.com".

User training:

- Phishing campaign
- Look for links
- Look for the e-mail sender
- Everything urgent

Securing IT Assets

Access Control -> Granting or deny specific requests to obtain and use information an related information processing services. Users are identified and granted certain rights to access and perform functions with information systems, networks or databases

Least Privilege -> Only have access to you need, if you just use the read administration to work you do not need edit administration (necessary to perform their duties)

Application Allow List -> Only approved applications could be installed

Decommissioning -> It involves safely and systematically retiring theses assets to ensure that no security vulnerabilities are introduced during or after the process

Hardening -> Measures and practices taken to reinforce the security of a system or network, the goal it to reduce vulnerabilities and minimize the attack surface

- Encryption
- Disabling Ports/Protocols -> Disable unused or unsecure ports/protocols (Think like Least Privileges but for ports/protocols)
- Endpoint Protection -> Antimalware and EDR
- HIPS (Host Intrusion Prevention System) -> It monitors and analyzes systems behavior and configuration
- Change Default Passwords
- Removal of Unnecessary Software -> Think like Least Privileges but for software installed in the device

Uninterruptible power supply (UPS) -> Backup power in case of sudden power loss, allowing critical systems to remain operational for a short period

Generators -> Ensuring operational continuity during extended power outages by providing a reliable source of backup power

Power converters -> Convert electrical power from one form to another (AC to DC or vice versa)

Power regulators -> Stabilize voltage levels to protect sensitive equipment from power surges or fluctuations

Network Security Principles

Network Segmentation -> Splitting a network into multiple segments or subnets

Network Isolation -> Isolate a system, a computer for all network, have no contact with any other device, this is used in a security incident

Security Zones -> Segments within a network that have distinct levels of security controls

- External
- Internal
- DMZ

Attack Surface -> Total number of points where an unauthorized user can try to enter or extract data, all areas that are vulnerable to cyber attacks

Device Attribute:

Active -> Can block or change the traffic flow -> Firewall/Endpoint

Passive -> Only monitor the traffic flow -> SIEM

Jump Server -> It is a secure computer that acts as a controlled entry point into a remote network or server group, it's a gateway between two networks to manage and access devices in a separate security zone

Proxy Server -> Acts as an intermediary between a user's computer and the internet.

- It mask the user's IP address
- Control internet usage blocking access to specific websites
- Can cache frequently accessed content
 1. Forward Forward -> No direct connection is made between the client and the internet
 2. Reverse Proxy -> Sits in front of web servers and directs client requests to the appropriate backend server, used for load balancing, caching or SSL encryption
 3. Open Proxy -> Conceals your IP address from the websites you visit, providing a degree of anonymity

SD-WAN -> Approach to simplify branch office networking and assure optimal application performance, centralized control function to securely and intelligently direct traffic across the WAN (Company use part of the data from On prem and part from Cloud)

IAM

Identity Proofing

- Verification of personal information
- KBA
- Document Verification
- Biometric
- Use third-party services

SAML -> Authentication and Authorization (Federation when it in websites)

OAuth -> Only Authorization (don't share credentials)

OpenID -> Add Authentication to OAuth

Mandatory Access Control (MAC) -> Central authority based on different levels of security clearance, users can not change access permissions, they are set and enforced by administrator

LINUX SE

- Government
- Military

Discretionary Access Control (DAC) -> Resource owner decides on access levels (more flexible), this can be risk because users could grant excessive access

Windows + MAC + Common Linux

- Where users need control over the resource they own (setting file permissions on OS)

Role-Based Access Control (RBAC) -> Assign permissions based on user's role (assign permission to group and the group to the users)

- Corporate environments

Rule-Based Access Control (RuBAC) -> Permissions based on rules

FIREWALLS

Attribute-Based Access Control (ABAC) -> Uses policies that evaluate attributes (more granular)

NETFLIX

- Complex environments with divers and dynamic users
- Attributes:
 - Screen size

- Localization
- Age

Secure Techniques

Baseline -> Security standards and configurations that an organization establishes to protect data and systems with the industry best practices, regulatory requirements and organization's needs

1. Establish
 - a. Assessment -> Understanding the specific needs
 - b. Define Standards -> Set configuration and controls
 - c. Documentation -> Create policies and procedures to implement these baselines
2. Deploy
 - a. Implementation -> Make sure the configurations are implemented in every device/software
 - b. Automate (if possible)
 - c. Verification -> Compliance check if the baseline it's well implemented
3. Maintain
 - a. Monitoring -> Audit logs
 - b. Updating -> Well patched
 - c. Training and Awareness -> Users trained how to work with the device/software

MDM (Mobile Device management) -> Software application that allow it administrators to control, secure and enforce policies on mobile devices (EDR for mobile)

BYOD (Bring your own device) -> Use personal device for work purpose

COPE (Corporate-Owned, Personally Enabled) -> Corporate device but the organization allow for some personal use

CYOD (Choose your own device) -> Employee choose from a selection of devices provided by the organization, it is the balance between personal preference and corporate control

AppSec -> Ensure that software applications are secure

- Input Validation -> Validate the input text are validated so you cannot put characters to explore XSS or SQLi
- Secure Cookies -> Key attributes include Secure (indicating that the cookie should only be sent over HTTPS connection)
- SAST/DAST -> Scans that review the code to find possible vulnerabilities, code flaws and ensure compliance
- Code Signing -> Use certificate
- Sandboxing -> Isolate application, processes or programs to simulate the end-user

Data Protection

Intellectual Property -> Creation of the mind like inventions, designs, symbols, literary works, artistic works, protection involves right management, strict access controls, and potentially watermark.

Copyright protects:

- Literary works
- Musical works
- Dramatic works
- Pantomimes and choreographic works
- Pictorial, graphical, and sculptural works
- Motion pictures and audiovisual works
- Sound recordings
- Architectural works

Regulated Data -> Data that is subject to regulatory requirements, such as personal data protected under laws like GDPR, health information covered by HIPAA, or financial data under PCI-DSS.

Compliance with legal and regulatory standards is crucial.

Legal Data -> Information pertaining to legal matters, including case files, legal advice, and other sensitive legal documents

Financial Data -> Financial records, credit information and other monetary data

Human-Readable Data -> Easily interpretable by humans

Non-Human Readable Data -> Require specific software to help read (0 and 1 language)

Data Classification -> Help in determining the level of security controls and handling protocols that should be applied. The owner of the data must assign to information

Classification level by military and government:

- Unclassified -> No protection needed
- Confidential -> Filing cabinet with a metal bar and lock
- Secret -> An approved safe
- Top Secret -> A vault

Other example:

- Public -> Public information on the website
- Sensitive -> Profit earning and forecasts, financial information
- Private/Restricted -> Work history, human resource information

- Confidential/Proprietary -> Trade Secret, Health care information, technical specification of a product
- Critical -> If compromised, could lead to severe harm or damage to an organization

Data Sovereignty -> Follow the law of the people/system you collect data, if you collect data from people from US and store in Brazil you will need to follow US privacy data laws

Methods to secure data:

- Encryption
- Hashing
- Masking -> Process that protect sensitive data by replacing, hiding, or scrambling data with fictional or anonymized data (123-xxx-7890) data is modified forever, this makes more appropriated for DEV env IT IS NOT CONSIDER ENCRYPTION
- Salting -> Add random values to a password before hash to prevent the same input from generating the same hash value
- Tokenization -> Replace sensitive data with non-sensitive substitutes (randomly generated), knows as token data is NOT modified forever, this makes more appropriated for PROD env
- Obfuscation -> Make data ambiguous or unclear to obscure, it involves techniques such as renaming variables, adding unnecessary code, and restructuring the code
- Steganography -> Concealing a message, image or file within another message, image or file (secret messages in files) add message in the metadata of a image
- Segmentation
- Permission restriction

Data controller -> Organizations that determine the purposes and means of processing personal data - YOU

Data processor -> Process personal data on behalf of data controllers - GOOGLE

Data subjects -> Individuals whose personal data is being processed by organizations - USERS

Data custodians/stewards -> Responsible for the day-to-day management and protection of data assets, as directed by the owner

Visitor (Data subject) visit your website (Data controller) because of Google Analytics (Data processor) ad.

Incident Response

Process:

1. Preparation -> Training personnel, conducting regular security assessments, and have all necessary resources to handle a security incident
2. Detection -> Identifying potential security incidents (network monitoring, IDS and security audit)
3. Analysis -> Understand its nature and scope (type of attack, systems affected, data compromised, attack tactics/techniques/procedures (TTPS))
4. Containment -> Limit the scope and magnitude of the incident
5. Eradication -> Removing malware, closing security gaps, implementing patches
6. Recovery -> Ensure all systems are cleaned and secure before bringing back online
7. Lessons learned -> Post-incident review, lessons learned are documented and used to improve the incident response plan

Tabletop exercise -> Walk through various incident scenarios in a structured manner (validate the effectiveness of the incident response plan)

Security Governance

Policies -> Providing a framework for consistent and secure operations across the organization

- Business Continuity Policies -> Procedures and instructions an organization must follow in the face of major disruptions or disasters
- SDLC (Software Development Lifecycle Policy) -> Developing, deploying and maintaining software

Standards -> Established benchmarks or criteria against which security measures are designed, they guide organizations in implementing organization policies

- Password standards -> Criteria for creating and managing passwords
- Access Control Standards -> How access to information systems and data should be controlled and managed
- Encryption Standards -> Requirements for encryption data

Guidelines -> Recommendations and best practices that help shape organization's security posture, they provide the roadmap for organizations to develop, implement and maintain robust security practices (Good practices to guide the standards be well funded)

Procedures -> Detailed, operation-level instructions that guide the day-to-day activities of maintaining security

Playbooks -> Procedures for a incident response

PII (Personal Identifiable Information) -> When used alone or with other relevant data, can identify an individual

PHI (Protected health information) -> Personal health information, demographic information, medical histories, laboratory results

Gap Analysis -> Validate current state of security posture against security best practices of the market

Security Delta -> It represents the gap that needs to be addressed to improve security posture.

Committees -> Formed to address specific topics or areas of interest within an organization (experts providing guidance on specific topics)

Boards -> High-level executives and stakeholders who make strategic decisions and provide oversight for the organization as a whole

Government Entities -> Regulatory bodies or agencies that oversee compliance with laws, regulations, and standards

Decentralized Entities -> Organizations or structures where decision-making authority is distributed across various levels or locations

Risk Management

Continuous Assessment -> Constantly monitoring and evaluating risks in real-time

Ad hoc Assessment -> Conducted after a major security breach, useful for addressing immediate and emerging risks

one-time Assessment -> Conducted only once, usually in response to a specific project or initiative

Recurring Risk Assessment -> Systematic approach (regular intervals -> quarterly or annually) and ensure that changes in the environment, assets, and threat landscape are consistently accounted for and addressed

Asset Value (AV) -> The total value of the asset being evaluated (in monetary terms). In this case, it is \$100,000.

Exposure Factor (EF) -> The percentage of the asset's value that would be lost or damaged if a specific threat occurs. In this case, it is 40%, or 0.40.

Annualized Rate of Occurrence (ARO) -> The estimated number of times the threat is expected to occur in a year. In this case, it is 2

SLE (Single Loss Expectancy) is the expected loss from a single occurrence of the event.

$$SLE = AV \times EF$$

$$SLE = 100,000 \times 0.40 = 40,000$$

$$ALE = SLE \times ARO$$

$$ALE = 40,000 \times 2 = 80,000$$

Risk Register -> Essential component of effective risk management, serving as a centralized repository for information, is a document that typically provides a comprehensive view of all identified risks, their status and the mitigation strategies

- Key Risk Indicators (KRI) -> metrics used to measure and monitor the likelihood and impact of risks
- Risk Threshold/Tolerance -> Level of risk that the organization will accept, setting limits on risk
- Risk Appetite -> Amount of risk that an organization is willing to accept in order to achieve its goals and objectives
 - Neutral -> Organization that prefers to maintain its current position and avoid taking unnecessary risks
 - Aggressive/Expansionary -> Organization that is willing to take on high levels of risk in pursuit of aggressive growth and competitive advantages
 - Conservative -> Organization that is very risk-averse and prefers to maintain a low level of risk exposure

- **Risk identification:** This includes the risk name or identification number.
- **Risk description:** This is a brief description of the risk and why it's an issue.
- **Risk category:** Categorizing your risks can help your team identify the risk within the risk register, making it easier to understand who will be responsible for mitigation. For example, you categorize your risk register by departments
- **Risk ownership:** This includes the person or persons who will be responsible for managing and overseeing the risk response.
- **Risk probability:** How likely the risk is to occur. You can categorize each risk as highly unlikely, unlikely, likely, or very likely. You can also use a numerical scale.
- **Risk impact:** This highlights and measures the potential impact of the risk, helping your team understand which risks take precedence. When rating the potential impact, use a simple scale that includes ratings like extremely low, low, medium, high, and extremely high.
- **Risk priority:** This takes risk probability and risk analysis into account to measure the priority level of the risk.
- **Risk response:** Your response or mitigation plan will detail how you plan to handle the risk. Your solution should be clearly outlined.
- **Risk status:** This field of your risk register includes the status of the risk—open, in progress, ongoing, or closed.
- **Notes:** You can also include a notes section to include any additional notes or details that will help team members better understand the risk and mitigation plan.

Risk Avoidance -> Changing plans or procedures to eliminate the risk (eliminating the risk entirely)

Risk Mitigation -> Reduce the likelihood or impact of the risk (not necessarily eliminate the risk entirely)

Risk Transfer -> Sifting the impact of a risk to a third party

Risk Acceptance -> Just accept the risk

Risk Exploitation -> Taking advantage of the potential positive impacts

Risk Reporting -> Communicating information about identified risk

Risk Owner -> Typically responsible for ensuring that risks are addressed in line with the organization's risk strategy and appetite

Risk Assessor -> Identify, assess, and analyze risks within an organization

Risk Communicator -> Effectively communicating risk-related information to stakeholders within the organization

BIA -> How a risk will impact the business

- Maximum Tolerable Downtime (MTD) / Maximum Tolerable Outage (MTO) -> Downtime acceptable before causing irreparable harm
- Recovery Time Objective (RTO) -> Maximum acceptable downtime (This need to be less than MTD/MTO)
- Recovery Point Objective (RPO) -> The maximum acceptable amount of data loss measured in time
- Mean Time to Repair (MTTR) -> Average time taken to repair

Vendor Management

Vendors -> Typically refer to companies or individuals that supply goods or services to an organization

Suppliers -> Entities that provide goods or services to an organization

Managed service providers (MSPs) -> Third-party companies that manage and assume responsibility for providing a defined set of services to their clients

Distributors -> Entities that distribute goods or services from manufacturers to retailers or end-users

SUPPLIER create/provide raw material to VENDORS to create products and sell to the customers, the DISTRIBUTOR handle the intermediaries managing the logistics of getting products

The MSP it is a different case, it manage services and systems on behalf of the customer but typically don't sell hardware or software directly

Vendor Assessment -> Evaluating and monitoring the security risks associated with third-party service providers, it involves scrutinizing the vendor's cybersecurity practices, policies and compliance

Rules of Engagement -> How an organization interacts and cooperates with third-party vendors, these rules of expectations, responsibilities and boundaries

Due Diligence -> Comprehensive appraisal of vendor's business practices, aims to uncover any potential security vulnerabilities or weakness in the vendor's offerings

SLA -> Establishing performance benchmarks and consequences for not meeting agreed standards

Memorandum of Agreement (MOA) -> Joint initiatives for information sharing, collaborative development of security protocols, etc.

Memorandum of Understanding (MOU) -> Less formal way of MOA

Master Service Agreement (MSA) -> Streamline future agreements and often includes clauses on confidentiality, dispute resolution and data security standards

Statement of Work (SOW)/ Work Order (WO) -> Document that provides specific details about the work to be performed under a contract

NDA -> Agree not to disclose information covered by the agreement

Business Partners Agreement (BPA) -> Specify roles, responsibilities and security requirements when sharing resources, joint ventures, or collaborative projects

Vendor Monitoring -> The primary goal is to ensure that vendors consistently deliver quality as agreed upon in the contract

Change Management Process

Business processes impacting security operation -> Processes or operations that could be impacted by a change, potentially leading to security issues

Maintenance Window -> Designated time frame during which changes can be implemented without disrupting normal operations

Backout Plan -> contingency plan that outlines the steps to revert to the previous state in case a change causes unexpected issues

Stakeholders -> individuals or groups with an interest in the outcome of a change