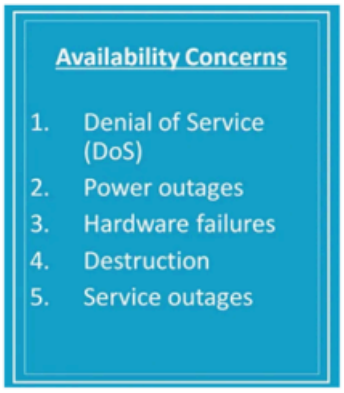
cc - certified in cybersecurity

rana chouchen

Domain 1 : SECURITY PRINCIPLES

- Confidentiality is about limiting access to information/assets and is therefore most similar to **secrecy**.



- **Snooping:** Unauthorized people looking for visible information.
- **Dumpster Diving:** Searching trash for sensitive papers.
- **Eavesdropping:** Listening to conversations (physical or electronic).
- **Wiretapping :**A specific form of eavesdropping focused on **network or electronic communication**, such as telephone lines, internet traffic, or emails.
- **Social Engineering :** Tricking people into revealing sensitive information.

- **Impersonation Attacks:** Attackers pretend to be trusted people (e.g., a boss or IT staff) to trick others and manipulate data.
- **Replay Attacks**: Attackers intercept and reuse valid login details to access systems without permission.

Privacy :is the right of an individual to control the distribution of information about themselves.

In 2016, the European Union passed comprehensive legislation addressing personal privacy, deeming it an individual human right

- **The European Union's General Data Protection Regulation (GDPR)** is a comprehensive data privacy law designed to protect individuals' personal data and regulate its collection, processing, and storage within the EU and beyond (2016).
- In the United States, **HIPAA** controls how the privacy of medical information must be maintained.
- Security controls are implemented in the risk management process to mitigate the risk to a level that is deemed acceptable by the entity.

Threat Actor : An individual or a group that attempts to exploit vulnerabilities to cause or force a threat to occur.

Threat Vector : The means by which a threat actor carries out their objectives.

- if a pickpocket is a threat, the attack vector would be their technique and approach.

Personally Identifiable Information (PII) : is the term used to describe information that, when combined with other pieces of data, significantly narrows the possibility of association with more individuals.

An asset : is something in need of protection. Anything of value that is owned by an organization. Assets include both tangible items such as information systems and physical property and intangible assets such as intellectual property.

A vulnerability: is a gap or weakness in those protection efforts.

A threat: is something or someone that aims to exploit a vulnerability to thwart protection efforts.

- **When making decisions based on risk priorities organizations must evaluate the likelihood and impact of the risk as well as their tolerance for different sorts of risk**
- Determining risk tolerance is up to **the executive management and board of directors**.
- In order to mitigate the risk associated with a threat, it is recommended to evaluate how likely an event is to take place and take appropriate actions to mitigate the risk associated with the threat.
- **Employees at all levels of the organization are responsible for identifying risk.**
- Security professionals are likely to assist in risk assessment at a system level, focusing on process, control, monitoring, or incident response and recovery activities.

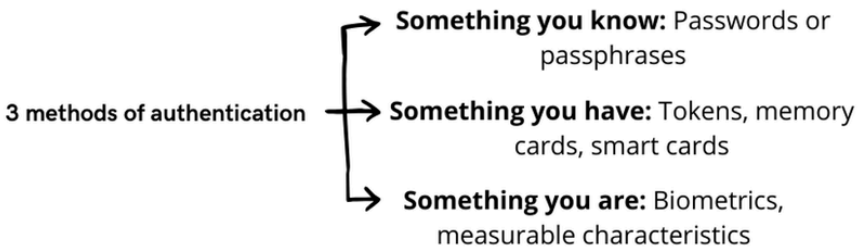
Security Controls		
Physical Controls	**Technical Controls**	**Administrative Controls**
Physical controls address security needs using physical hardware devices, such as badge readers, architectural features of buildings and facilities, and specific security actions taken by staff.	Technical controls (also called logical controls) are security controls that computer systems and networks directly implement	Administrative controls (also known as managerial controls) are directives, guidelines, or advisories aimed at the people within the organization. They provide frameworks, constraints, and standards for human behavior and should cover the entire scope of the organization's activities and its interactions with external parties and stakeholders.

Governance : The process of how an organization is managed; usually includes all aspects of how decisions are made for that organization, such as policies, roles and procedures the organization uses to make those decisions.

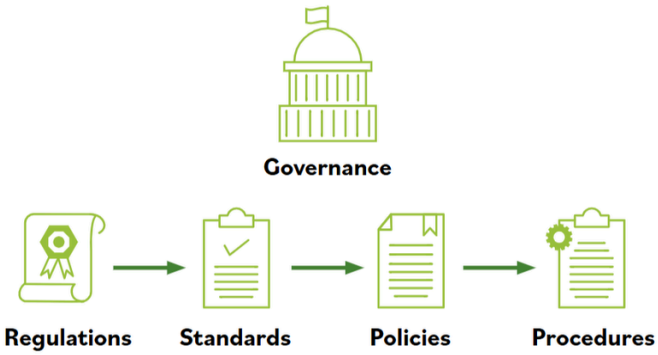
- Information security professionals are expected to uphold **honorable, honest, just, responsible, and legal conduct,** as mentioned in the code of ethics.

Access Control Steps for IT Professionals:

1. **Identification**
   - The user claims an identity (e.g., providing a username).
2. **Authentication**
   - The user verifies their identity, typically using credentials like a password, PIN, or biometrics.
3. **Authorization**
   - Permissions are checked to confirm what the user is allowed to access.



- The use of an ATM card (something you have) and a PIN (something you know) at the bank, providing two different factors of authentication.
- Knowledge-based authentication involves using a passphrase or secret code (e.g., PIN or password) to differentiate between authorized and unauthorized users.



Governance Elements			
Procedures	**Policies**	**Standards**	**Regulations**
Procedures are the detailed steps to complete a task that support departmental or organizational policies.	Policies are put in place by organizational governance, such as executive management, to provide guidance in all activities to ensure that the organization supports industry standards and regulation.	Standards are often used by governance teams to provide a framework to introduce policies and procedures in support of regulations.	Regulations are commonly issued in the form of laws, usually from government (not to be confused with governance) and typically carry financial penalties for non-compliance

- Laws are the explicit authority of the jurisdiction where any organizations operate; laws cannot be violated, regardless of internal company governance. Laws supersede everything else.
- **Policies, standards, processes, procedures and guidelines** set by corporate administrative entities (e.g., executive- and/or mid-level management) **are management/administrative controls.**

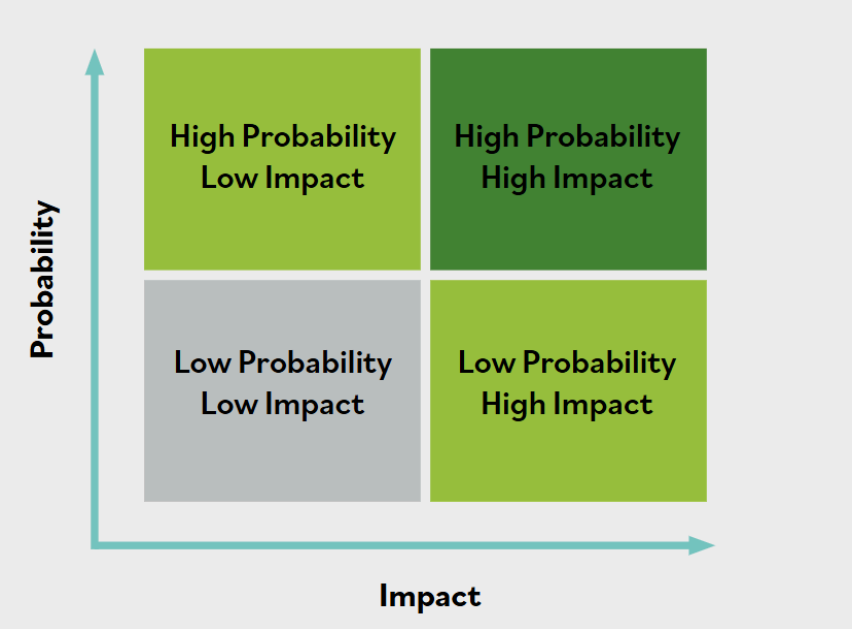
Baseline: A documented, lowest level of security configuration allowed by a standard or organization.

Non-repudiation: The inability to deny taking an action such as creating information, approving information, or sending or receiving a message.

Prioritizing Risk :

One effective method to prioritize risk is to use a risk matrix, which helps identify priority as the intersection of likelihood of occurrence and impact.

- You can use this simple probability and impact model to determine the level of risk and therefore prioritize risk.
- Level of Risk = Probability + Impact



Risk Treatment Options:

1. **Risk Avoidance**: Stop activities that pose high risks.
2. **Risk Mitigation**: Implement controls to reduce risk likelihood or impact.
3. **Risk Acceptance**: Accept the risk if impact is negligible or benefits outweigh risks.
4. **Risk Transference**: Transfer risk to a third party (e.g., insurance)

What is risk tolerance often likened to? → **Risk appetite**

Risk assessment: is the process of identifying, analyzing, and evaluating potential risks to determine their impact and likelihood.

- The result of the risk assessment process is often documented as a report or presentation given to management for their use in prioritizing the identified risks.

Domain 2 : INCIDENT RESPONSE, BUSINESS CONTINUITY AND DISASTER RECOVERY CONCEPTS

Event: Any observable occurrence in a network or system.

Incident: An event that jeopardizes the confidentiality, integrity, or availability of information or systems.

Threat: Any circumstance or event with the potential to harm organizational operations, assets, individuals, or systems.

Vulnerability: Weakness in a system, procedures, controls, or implementation that could be exploited by a threat.

Breach: The loss, compromise, or unauthorized access of personally identifiable information (PII) or similar sensitive data.

Exploit: A specific attack leveraging vulnerabilities in systems.

Intrusion: A deliberate security incident where an intruder gains, or attempts to gain, unauthorized system access.

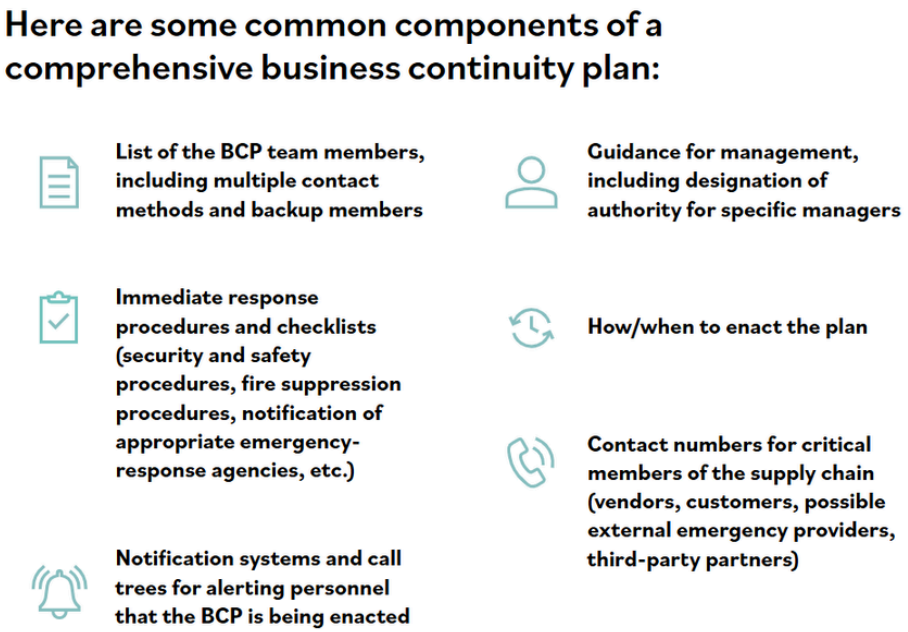
Zero Day: A previously unknown vulnerability exploited before detection or mitigation is possible.

Business Continuity (BC): Actions, processes and tools for ensuring an organization can continue critical operations during a contingency~ ensures operations can sustain and recover from significant disruptions.

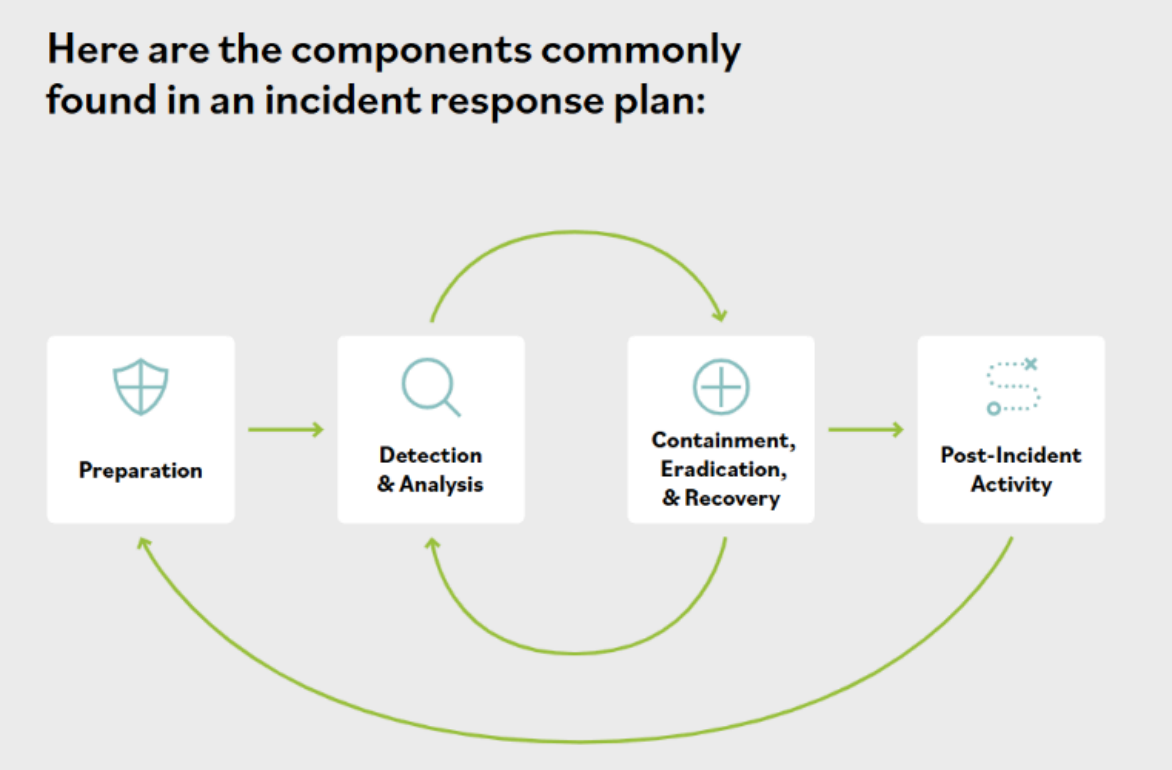
Business Continuity Plan (BCP): The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption.

- What term is sometimes used interchangeably with "incident management"?-->Crisis Management
- Some organizations use the term "**crisis management**" to describe the incident management process.

The red book serves as a **hard copy backup** accessible outside the facility, containing outlined procedures in case electronic access is unavailable.



- One key outcome of a **Business Impact Analysis (BIA)** is the identification of functions and dependencies.
- In the United States, specific numbers in specific networks, like military-grade networks, can be used during a severe cyberattack to maintain essential activity, especially for critical infrastructures such as hospitals.



Preparation	Detection and Analysis	Containment	Post-Incident Activity
Develop a management-approved policy, identify critical assets, train staff, establish an incident response team, define roles, plan stakeholder communication, and ensure alternative communication methods.	-Monitor all possible attack vectors. -Analyze the incident using known data and threat intelligence. -Prioritize incident response. -Standardize incident documentation.	-Gather evidence - choose an appropriate containment strategy. -Identify the attacker. -Isolate the attack	-Identify evidence that may need to be retained. -Document lessons learned.

Incident Response Team (IRT):

- Cross-functional team includes senior management, security professionals, legal, public affairs, and engineering representatives.
- The four primary responsibilities of a response team when an incident occurs are **determining damage**, **assessing compromise**, **implementing recovery procedures**, and **supervising security measures**.
- The incident response team is responsible for **assessing and scoping out any damage** when an incident occurs.

Disaster Recovery Planning (DRP):DRP is about restoring IT, while BCP focuses on business operations

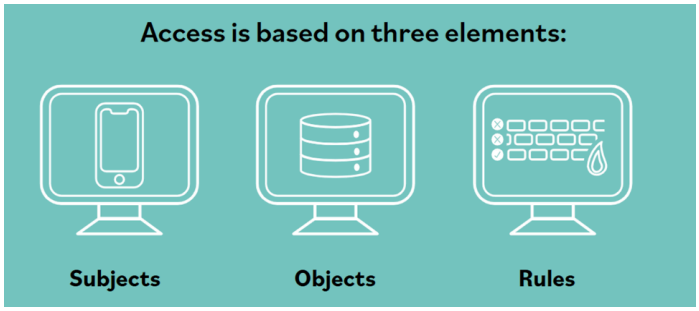
Business continuity planning (BCP) centers on maintaining critical business functions, while disaster recovery planning (DRP) specifically targets the restoration of IT and communications services essential for business operations.

- The purpose of the Executive Summary in a Disaster Recovery Plan is to provide a high-level overview of the plan.
- Organizational support for business continuity planning efforts must be provided by executive management or an executive sponsor.
- Backups are pivotal components of any disaster recovery (DR) effort, serving as essential resources for swift restoration of critical data post-disaster, ensuring operational continuity, and mitigating risks effectively.
- It is necessary to consider the database and dependencies on other systems to address the intricate dependencies of complex systems, ensuring a successful disaster recovery plan.

Domain 3 : Access Control Concepts

Access control involves limiting what objects can be available to what subjects according to what rules.

- Access controls are not just about restricting access to information systems and data, but also about allowing access. It is about granting the appropriate level of access to authorized personnel and processes and denying access to unauthorized functions or individuals.



Element	Definition	Characteristics
Subjects	can be defined as any entity that requests access to assets	Is **active**: It initiates a request for access to resources or services
Objects	anything that a subject attempts to access is referred to as an object An object is defined as an entity that responds to a request for service.	Is **passive**
Rules	is an instruction developed to allow or deny access to an object by comparing the validated identity of the subject to an access control list.	

Defense in depth(Layered Defense) describes an information security strategy that integrates people, technology, and operations capabilities to establish **variable barriers across multiple layers** and missions of the organization.

- When a company has information at multiple sensitivity levels, it might require the network traffic to be validated by rules on more than one firewall, with the most sensitive information being stored behind multiple firewalls.

Least Privilege: To preserve the confidentiality of information and ensure that it is only available to personnel who are authorized to see it, we use privileged access management, which is based on the principle of least privilege. That means each user is granted access to only the items they need and nothing further.

- Privileged access management implements the principle of least privilege by granting each user access only to the items they need.

---> The more critical information a person has access to, the greater the security should be around that access. They should definitely have multi-factor authentication, for example.

physical access control	logical access control
tangible methods or mechanisms that limit someone from getting access to an area or asset	electronic methods that limit someone from getting access to systems, and sometimes even to tangible assets or areas

User provisioning in identity management involves creating and managing access to resources and information systems.

Access Control Model	Definition	Key Features	Use Cases
Mandatory Access Control (MAC)	Mandatory Access Control (MAC) is a strict security policy where only authorized security administrators can manage access rules for users (subjects) and resources (objects) in a system. These rules are consistently applied across the system, and users cannot modify them or share their privileges.	**Restricted User Actions**: ● Users cannot share access with others. ● Users cannot alter security settings or rules. ● Users cannot choose security levels for new files or data. **Centralized Control**: ● Only security administrators can change security rules or permissions.	Government agencies (e.g., military systems) where confidentiality and sensitivity are critical.
Role-Based Access Control (RBAC)	Role-based access control provides each worker privileges based on what role they have in the organization.	- Users are assigned roles, and each role has specific permissions. - Simplifies management by grouping permissions. - Access changes when roles change.	● Businesses and organizations with structured roles (e.g., HR systems, finance departments) ● Role-based access control works well in an environment with high staff turnover and multiple personnel with similar access requirements.
Discretionary Access Control (DAC)	A flexible model where access is determined by the resource owner.	- Resource owners can grant or revoke access to others. - Permissions can be customized for individual users. - Less restrictive but prone to security risks (e.g., accidental sharing).	- Personal systems or collaborative environments where resource sharing is common (e.g., file-sharing systems).

- The level of access to certain areas in certain government agencies is determined by government policy and security clearance in the context of Mandatory Access Control (MAC).
- **Privilege creep** (or **permissions creep**) is the term which refers to someone inheriting expanded permissions that are not appropriate for their role in RBAC.
- Discretionary Access Control (DAC) is not considered very scalable because it relies on the discretion of individual object owners.

Which of these combinations of physical security controls share a single point of failure? --->Both lighting and cameras require power. A power failure will disable both the cameras and the lights.

- The key feature of just-in-time privileged access management is role-based subsets of privileges.
- It is recommended to disable accounts for a period before deletion to preserve the integrity of audit trails or files that may be owned by the user.

Privileged Accounts : Privileged accounts are those with permissions beyond those of normal users, such as managers and administrators.

- Systems administrators with privileged accounts have the principal responsibilities for operating systems, application deployment, and performance management.
- Small and medium businesses often face a challenge in implementing technical controls due to insufficient personnel for duty separation.

Separation of duties is based on the security practice that no one person should control an entire high risk transaction from start to finish.

- It is possible, of course, that two individuals can willfully work together to bypass the separation of duties to jointly commit fraud. This is called **collusion**.

Two-Person Integrity : The two-person rule is a security strategy that requires a minimum of two people to be in an area together, making it impossible for a person to be in the area alone.

- The two-person rule in the context of security strategy means that two people must be in an area together.

Crime Prevention Through Environmental Design (CPTED): is a strategy used to create safer spaces by designing environments in a way that discourages crime. Instead of relying solely on alarms or security guards, CPTED focuses on using **passive design elements** to enhance security naturally.

- CPTED provides direction to solve the challenges of crime with organizational (people), mechanical (technology and hardware), and natural design (architectural and circulation flow) methods. By directing the flow of people using passive techniques to signal who should and should not be in a space and providing visibility to otherwise hidden spaces, the likelihood that someone will commit a crime in that area decreases

Biometric Authentication:

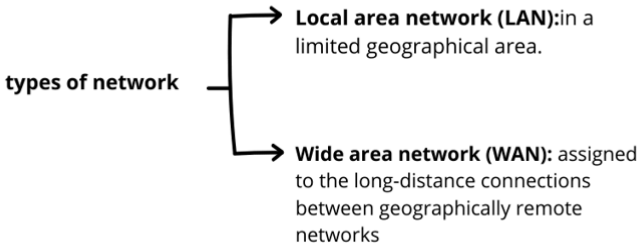
- **Types of Biometrics**:
  - **Physiological**: Fingerprints, iris scans, retinal scans, palm scans, venous scans.
  - **Behavioral**: Voiceprints, signature dynamics, keystroke dynamics.

Monitoring tools :

Cameras	Tools for surveillance, deterrence, and forensic evidence.
Logs	Records of events for compliance, forensics, and auditing.
Alarm Systems	Devices that alert when unauthorized or emergency situations occur.
Security Guards	Human presence to deter and monitor unauthorized access.
Motion Sensors	Detect movement or breaches in secure areas.

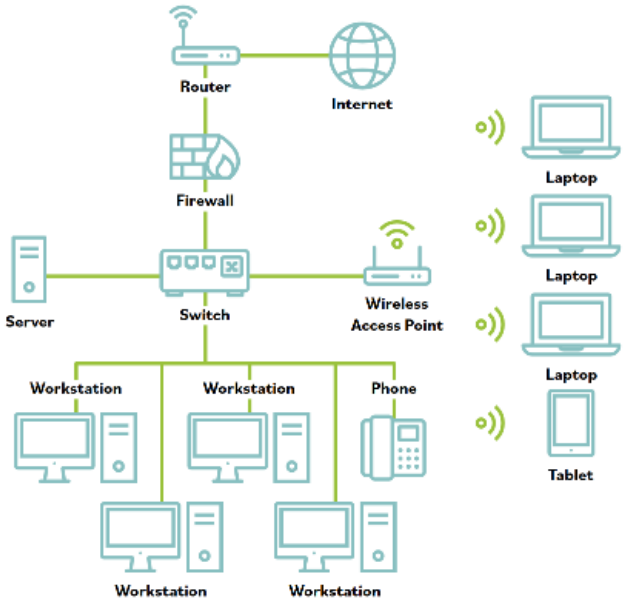
- A turnstile typically uses a revolving mechanism that allows only one person to be admitted at a time, reducing the possibility of an unauthorized person following an authorized person into a controlled area. **("piggybacking" or "tailgating")**

Domain 4 : Network Security



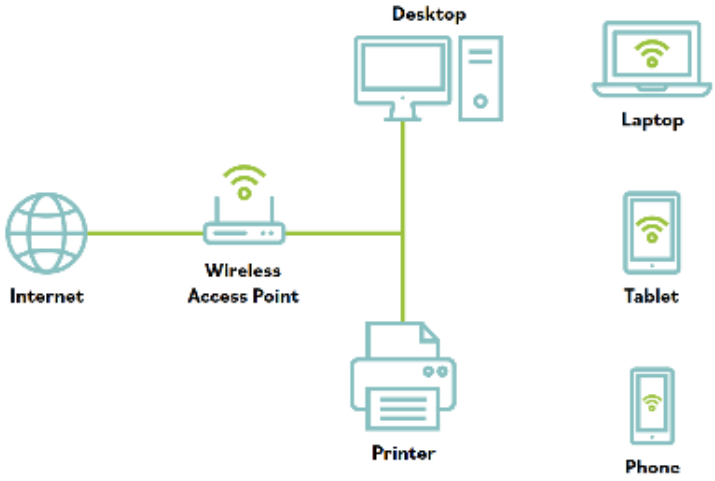
Ethernet (IEEE 802.3): This standard defines the way data is formatted over the wire to ensure disparate devices can communicate over the same cables.

A Small Business Network:



- Notice how all devices behind the firewall connect via the network switch, and the firewall lies between the network switch and the internet

A Typical Home Network



- firewall, and network switch are often combined into one device supplied by your internet provider and shown here as the wireless access point
- **Wi-Fi :**In a LAN, threat actors need to enter the physical space or immediate vicinity of the physical media itself. For wired networks, this can be done by placing sniffer taps onto cables, plugging in USB devices, or using other tools that require physical access to the network. By contrast, wireless media intrusions can happen at a distance.
- **Additional vulnerabilities** is a potential drawback associated with the freedom provided by wireless networking.
- **micro-segmentation** aid in protecting against **Advanced persistent threats (APTs)**
- micro-segmentation enforce in terms of business functions/units/offices/departments the concept of least privilege.

Tools to Identify and Prevent Threats

Tools	Description	Identifies Threats	Prevent Threats
Intrusion Detection System (IDS)	A form of monitoring to detect abnormal activity; it detects intrusion attempts and system failures.	✓	
Host-basaed IDS (HIDS)	Monitors activity on a single computer.	✓	
Network-based IDS (NIDS)	Monitors and evaluates network activity to detect attacks or event anomalies.	✓	
SIEM	Gathers log data from sources across an enterprise to understand security concerns and apportion resources.	✓	
Anti-malware/Antivirus	Seeks to identify malicious software or processess.	✓	✓
Scans	Evaluates the effectiveness of security controls.	✓	
Firewall	Filters network traffic - manages and controls network traffic and protects the network.	✓	✓
Intrusion Protection System (IPS-NIPS/HIPS)	An active IDS that automatically attempts to detect and block attacks before they reach target systems.	✓	✓

demilitarized zone (DMZ) : What is a DMZ? (Demilitarized Zone)

a portion of the organization's network that interfaces directly with the outside world and typically has more security controls and restrictions compared to the rest of the internal IT environment

Web Application Firewall (WAF): It monitors all traffic from the outside for malicious behavior before passing commands to a web server.

- A virtual private network (VPN) is **not necessarily an encrypted tunnel**. It is simply a point-to-point connection between two hosts that allows them to communicate. Secure communications can, of course, be provided by the VPN, but only if the security protocols have been selected and correctly configured to provide a trusted path over an untrusted network, such as the internet.
- **Gateway-to-gateway VPNs** is a potential alternative to **expensive dedicated point-to-point connections.**

basic steps you can take that help reduce the risk of many types of threat:

-->Keep systems and applications up to date.

-->Remove or disable unneeded services and protocols.

-->Use intrusion detection and prevention systems.

-->Use firewalls.

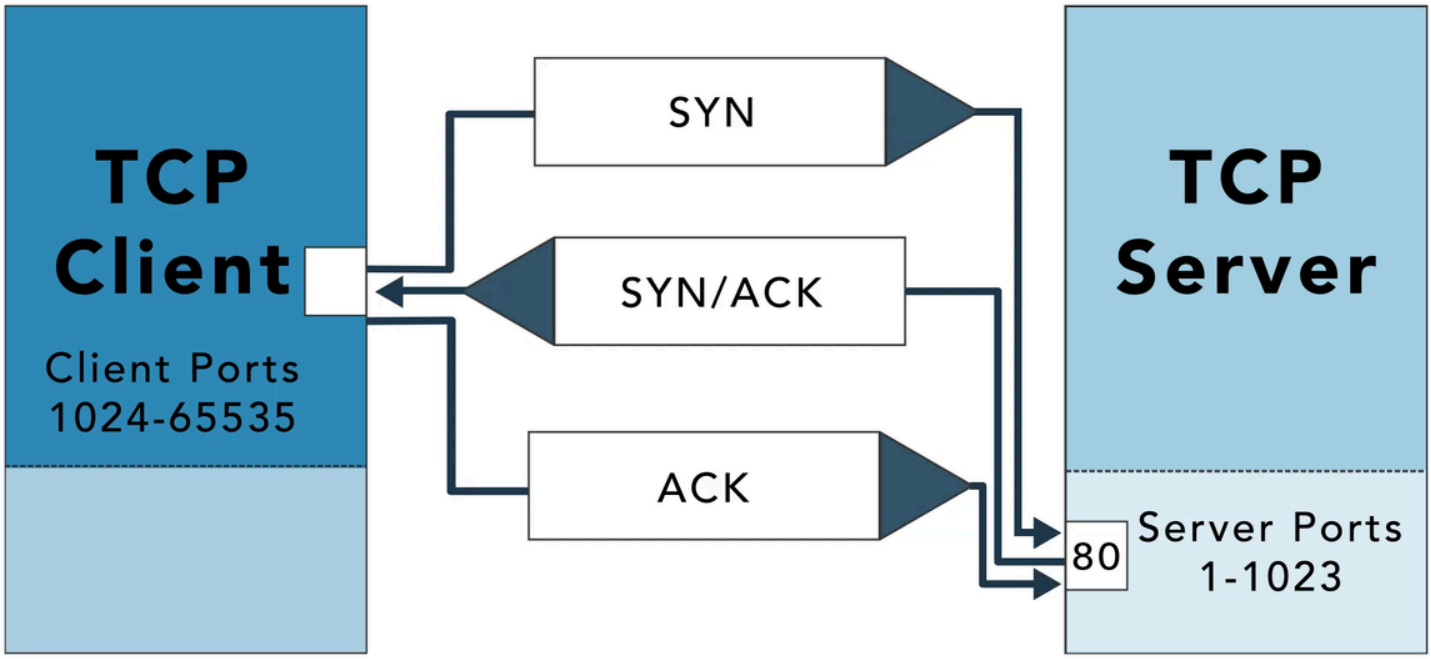
-->Use up-to-date anti-malware software

- A distinguishing difference between an IDS and an IPS is that the IPS is placed in line with the traffic In other words, all traffic must pass through the IPS and the IPS can choose what traffic to forward and what traffic to block after analyzing it.

Host-based Intrusion Detection System (HIDS)	Network Intrusion Detection System (NIDS)
monitors activity on a single computer	monitors and evaluates network activity to detect attacks or event anomalies
examine events in more detail than a NIDS can, and it can pinpoint specific files compromised in an attack	It cannot monitor the content of encrypted traffic but can monitor other packet details.
HIDSs over NIDSs is that HIDSs can detect anomalies on the host system that NIDSs cannot detect	A NIDS is usually able to detect the initiation of an attack or ongoing attacks, but they can't always provide information about the success of an attack.
HIDSs are more costly to manage than NIDSs because they require administrative attention on each system, whereas NIDSs usually support centralized administration.	centralized administration

network monitoring or sniffing: Monitoring traffic patterns to obtain information about a network

SYN, SYN-ACK, ACK Handshake



Well-known ports (0–1023)	These ports are related to the common protocols that are at the core of the Transport Control Protocol/Internet Protocol (TCP/IP) model, Domain Name Service (DNS), Simple Mail Transfer Protocol (SMTP), etc
Registered ports (1024–49151)	These ports are often associated with proprietary applications from vendors and developers. While they are officially approved by the Internet Assigned Numbers Authority (IANA), in practice many vendors simply implement a port of their choosing. Examples include Remote Authentication Dial-In User Service (RADIUS) authentication (1812), Microsoft SQL Server (1433/1434) and the Docker REST API (2375/2376)
Dynamic or private ports (49152–65535)	Whenever a service is requested that is associated with well-known or registered ports, those services will respond with a dynamic port that is used for that session and then released.

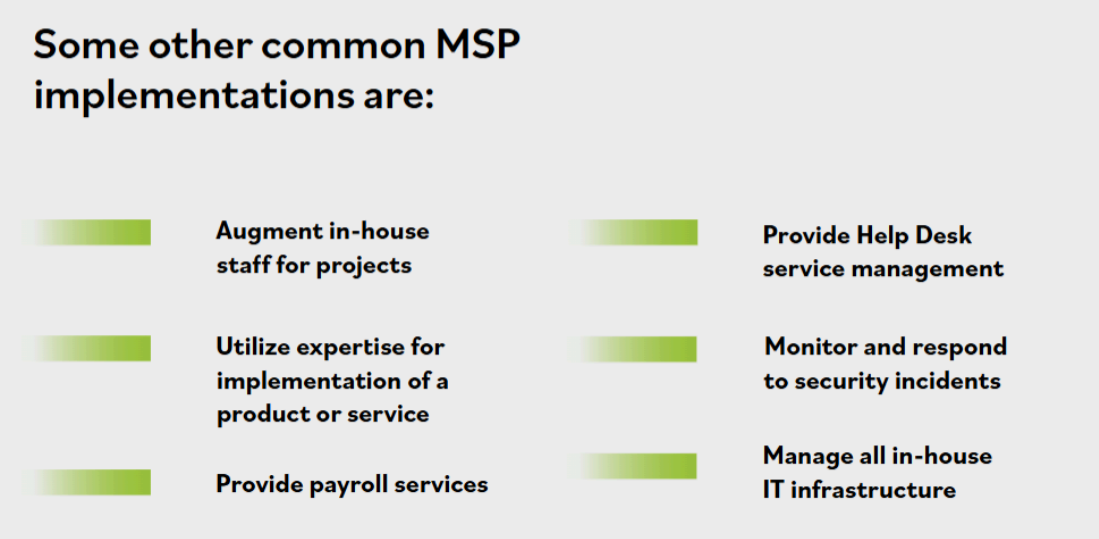
The concept of redundancy: is to design systems with duplicate components so that if a failure were to occur, there would be a backup.

What is the function of transfer switches or transformers in a redundant power system?-->Enable seamless transition between power sources

Why is an abnormal system shutdown in a data center a concern?-->It may result in the loss or corruption of data

What is resource pooling in the context of cloud computing?-->Sharing physical servers with other organizations

A managed service provider (MSP) is a company that manages information technology assets for another company.



What is one of the services offered by many MSPs, where they monitor firewalls and other security tools to provide expertise in triaging events?-->Managed Detection and Response (MDR) Service

- Cloud computing refers to on-demand access to computing resources available from almost anywhere, and cloud computing resources are highly available and easily scalable.
- Cloud computing is usually associated with an internet-based set of computing resources, and typically sold as a service provided by a cloud service provider (CSP)
- The cloud computing service-level agreement (cloud SLA) is an agreement between a cloud service provider and a cloud service customer based on a taxonomy of cloud computing–specific terms to set the quality of the cloud services delivered.

Model	Definition	Primary Users	Control Level	Examples	Key Features
SaaS	**Software as a Service** – Provides fully functional applications over the internet.	End users (businesses and individuals)	Minimal control (users only interact with the application)	Google Workspace, Microsoft 365, Dropbox	- Ready-to-use applications - No installation or maintenance required - Subscription-based pricing
PaaS	**Platform as a Service** – Provides a platform for developers to build, deploy, and manage applications.	Developers and IT teams	Control over applications, but not infrastructure	Heroku, Google App Engine, Microsoft Azure App Services	- Develop, test, and deploy applications - Platform management (e.g., OS, servers) is handled by the provider
IaaS	**Infrastructure as a Service** – Provides virtualized computing resources over the internet	IT admins, Developers, Enterprises	Full control over infrastructure (e.g., virtual machines)	Amazon Web Services (AWS), Microsoft Azure, Google Cloud	- Flexible infrastructure (e.g., storage, compute power) - Users manage the OS, applications, and data

- Which cloud computing model allows an enterprise to scale up new software or data-based services/solutions quickly without massive hardware installation?-->Platform as a Service (PaaS)

Some organizations seeking to minimize downtime and enhance BC (Business Continuity) and DR (Disaster Recovery) capabilities will create agreements with other, similar organizations. They agree that if one of the parties experiences an emergency and cannot operate within their own facility, the other party will share its resources and let them operate within theirs to maintain critical functions. These agreements often include competitors, because their facilities and resources meet the needs of their particular industry.-->**These agreements are called joint operating agreements (JOA), memoranda of understanding (MOU), or memoranda of agreement (MOA)**

What distinguishes Memoranda of Understanding (MOU) or Memoranda of Agreement (MOA) from Service Level Agreements (SLA)?-->MOUs/MOAs are more directly related to what can be done with a system or information, while SLAs specify more intricate aspects of services

Network Segmentation: Network segmentation involves controlling traffic among networked devices. Complete or physical network segmentation occurs when a network is isolated from all outside communications, so transactions can only occur between devices within the segmented network

Demilitarized Zone (DMZ): A DMZ is a network area that is designed to be accessed by outside visitors but is still isolated from the private network of the organization. The DMZ is offen the host of public web, email, file and other resource servers.

Virtual Local Area Network (VLAN) : VLANs are created by switches to logically segment a network without altering its physical topology**.**

Virtual Private Network (VPN) : A virtual private network (VPN) is a communication tunnel that provides point-to-point transmission of both authentication and data traffic over an untrusted network.

Defense in depth: Defense in depth uses multiple types of access controls in literal or theoretical layers to help an organization avoid a monolithic security stance.

Network Access Control (NAC): Network access control (NAC) is a concept of controlling access to an environment through strict adherence to and implementation of security policy.

Types of Threats:

- **Spoofing:** This is an attack with the goal of gaining access to a target system through the use of a falsified identity. Spoofing can be used against IP addresses, MAC address, usernames, system names, wireless network SSIDs, email addresses, and many other types of logical identification.
- **phishing**
- **DOS/DDOS**
- **VIRUS :** a user must click on a link or open a file.
- **Worm:** they propagate themselves without requiring any human intervention.
- **Trojan**
- **On-path Attack (Man in the middle)**
- **Side channel :** A side-channel attack is a passive, non invasive attack to observe the operation of a device. Methods include power monitoring, timing and fault analysis attack.
- **Advanced Persistent Threat (APT):** refers to threats that demonstrate an unusually high level of technical and operational sophistication spanning months or even years. APT attacks are often conducted by highly organized groups of attackers.
- **Insider Threat**
- **Malware**
- **Ransomware**

Virtual local area networks (VLANs) allow network administrators to use switches to create software-based LAN segments, which can segregate or consolidate traffic across multiple switch ports.

- Devices that share a VLAN communicate through switches as if they were on the same Layer 2 network.
- there are attacks that allow a malicious user to see traffic from other VLANs (so-called "**VLAN hopping**").

Which of the following tools can be used to grant remote users access to the internal IT environment?-->VPN (virtual private network)

What might a user typically need to acknowledge before being allowed to access the internet in a hotel network?-->Acceptable use policy

How are VLANs used in Network Access Control (NAC) systems?-->VLANs control whether devices connect to the corporate network or a guest network

<table>
<tr><th>OSI Model Layers</th><th>TCP/IP Protocol Architecture</th><th colspan="4">TCP/IP Protocol Suite</th></tr>
<tr><td>Application Layer</td><td rowspan="3">Application Layer</td><td>FTP</td><td>Telnet</td><td>SNMP</td><td>LPD</td></tr>
<tr><td>Presentation Layer</td><td rowspan="2">TFTP</td><td rowspan="2">SMTP</td><td rowspan="2">NFS</td><td rowspan="2">X Window</td></tr>
<tr><td>Session Layer</td></tr>
<tr><td>Transport Layer</td><td>Transport Layer</td><td colspan="2">TCP</td><td colspan="2">UDP</td></tr>
<tr><td>Network Layer</td><td>Internet Layer</td><td>IGMP</td><td colspan="2">IP</td><td>ICMP</td></tr>
<tr><td>Data Link Layer</td><td rowspan="2">Network Interface Layer</td><td rowspan="2">Ethernet</td><td rowspan="2">Fast Ethernet</td><td rowspan="2">Token Ring</td><td rowspan="2">FDDI</td></tr>
<tr><td>Physical Layer</td></tr>
</table>

What is the primary responsibility of the upper layer (host or application layer) in a network model?-->Transforming data into a format that any system can understand

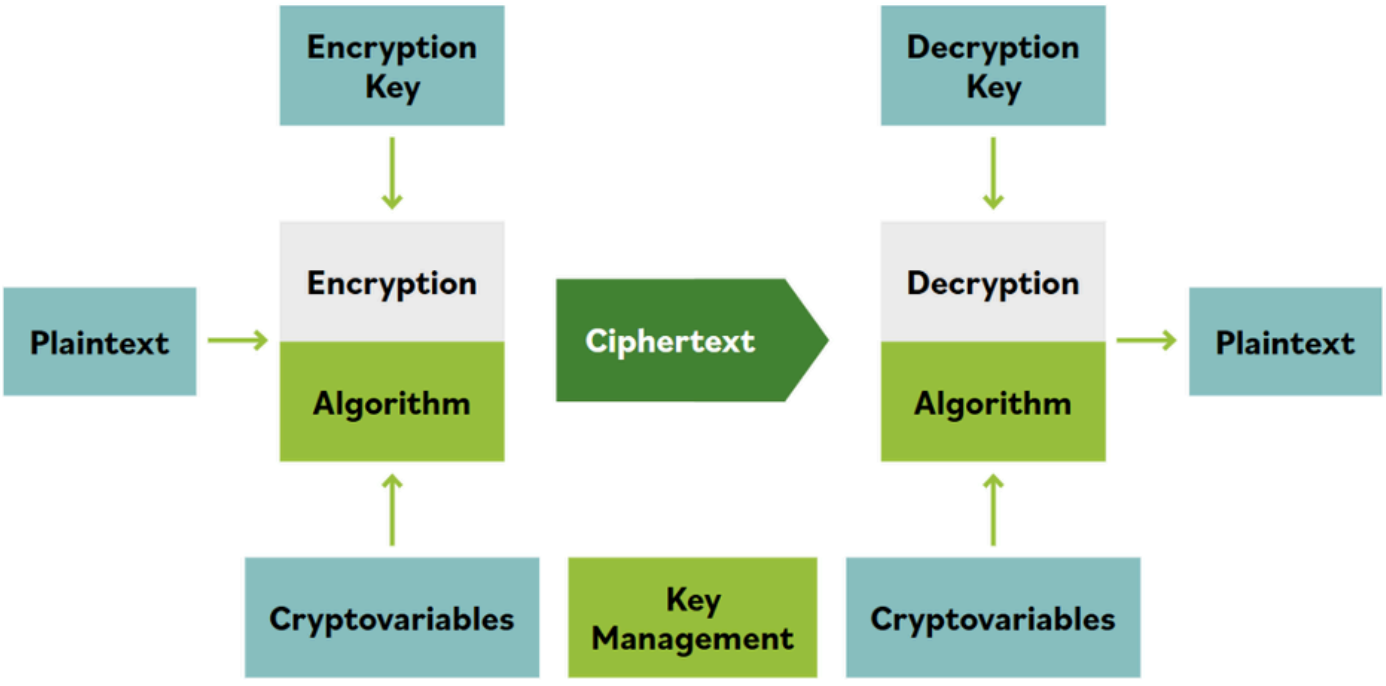
Which layer of the OSI model corresponds to the Internet Layer in the TCP/IP protocol architecture?-->Network Layer

Domain 5 :Security Operations

Data Handling:

- retention is how long we store the information and where based on the requirements of our organization and perhaps regulatory agencies as well.
- Degaussing : process of reducing or eliminating an unwanted magnetic field (or data) stored on tape and disk media.

Encryption System: An encryption system is a set of hardware, software, algorithms, control parameters, and operational methods that provide a set of encryption services.



What do integrity services, provided by hash functions and digital signatures, allow a recipient to verify?-->That a message has not been altered by malice or error

Security Awareness Training: The purpose of awareness training is to make sure everyone knows what is expected of them, based on responsibilities and accountabilities, and to find out whether there is any carelessness or complacency that may pose a risk to the organization

by : → education → training → awareness

How long does it take to crack a 10-number password using software with cryptographic calculation?-->5 seconds

What is something which every security policy should have?--> Consequences for non-compliance

Phishing attacks that attempt to trick highly placed officials or private individuals with sizable assets into authorizing large fund wire transfers to previously unknown entities are known as **whaling attacks.**

What task is recommended for employees to practice what they've learned?-->Sending simulated phishing emails

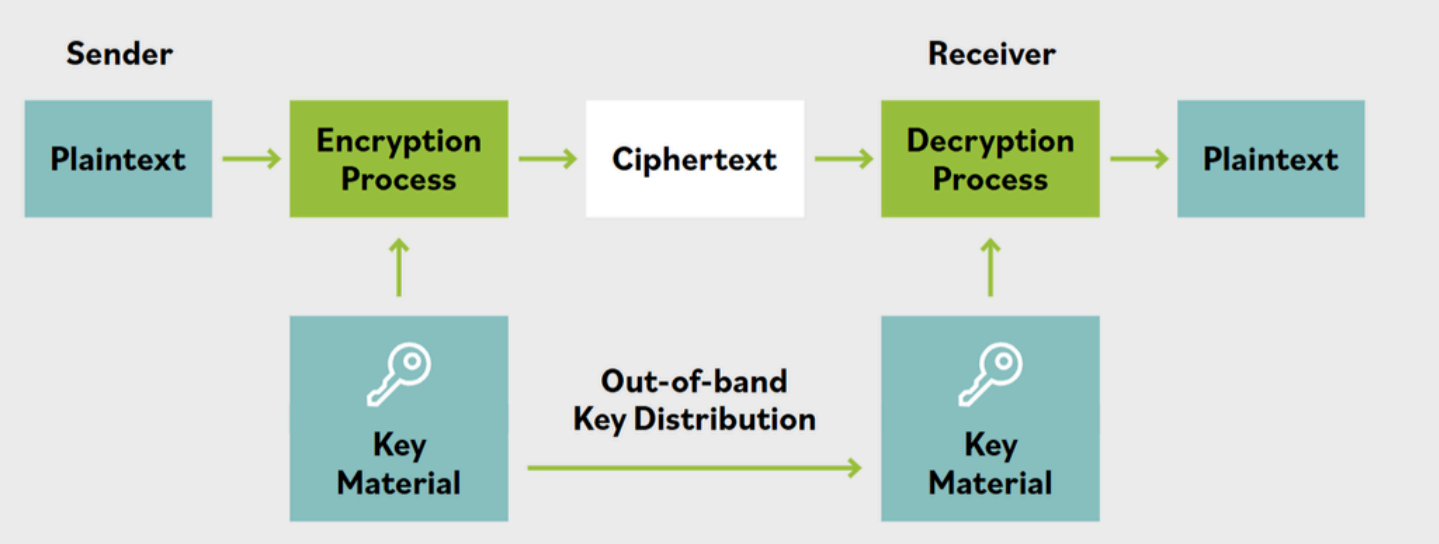
Why is asymmetric encryption considered more secure?-->It involves a unique code for the sender and receiver

Hashing puts data through a hash function or algorithm to create an alphanumeric set of figures, or a digest that means nothing to people who might view it

- No matter how long the input is, the hash digest will be the same number of characters.

symmetric algorithm

The central characteristic of a symmetric algorithm is that it uses the same key in both the encryption and the decryption processes. It could be said that the decryption process is a mirror image of the encryption process



Other names for symmetric algorithms:

- **shared key**
- **single key**
- **same key**
- **secret key**
- **session key**

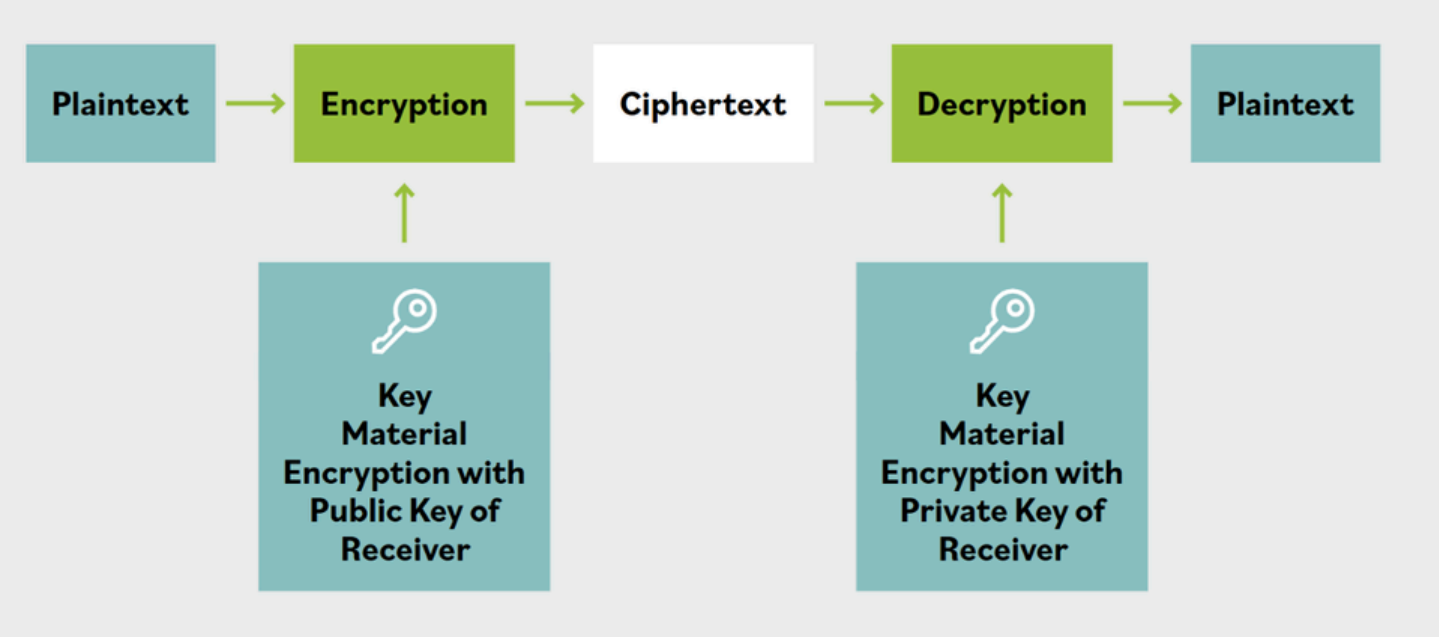
An example of symmetric encryption is a **substitution cipher,** which involves the simple process of substituting letters for other letters, or more appropriately, substituting bits for other bits, based upon a cryptovariable. These ciphers involve replacing each letter of the plaintext with another that may be further down the alphabet.

What is a mode of encryption which ensures confidentiality efficiently, with a minimum amount of processing overhead?-->**Symmetric**

Asymmetric encryption:

Asymmetric encryption uses one key to encrypt and a different key to decrypt the input plaintext. This is in stark contrast to symmetric encryption, which uses the same key to encrypt and decrypt.

- The problem, however, has been that asymmetric cryptography is extremely slow compared with its symmetric counterpart. Asymmetric cryptography is impractical for everyday use in encrypting large amounts of data or for frequent transactions where speed is required.
- Similarly, signing a message with a sender's private key can only be verified by the recipient decrypting its signature with the sender's public key. Therefore, as long as the key holder keeps the private key secure, there exists a method of transmitting a message confidentially.



Common Security Policies:

- **Data Handling Policy**
- **Password Policy**
- **Acceptable Use Policy (AUP):** defines acceptable use of the organization's network and computer systems and can help protect the organization from legal action.
- **Bring Your Own Device (BYOD) Policy**
- **Privacy Policy**
- **Change Management Policy:** Change management is the discipline of transitioning from the current state to a future state. It consists of three major activities: deciding to change, making the change, and confirming that the change has been correctly accomplished.

A roolback Restoring the system to its previous state before a change.

Who is often tasked with coordinating the change management effort?-->Information Security professionals

Three Major Components of Change Management

1. **Request for Change (RFC)**
   Initiates the process; stakeholders submit a detailed request for the proposed change.
2. **Approval**
   Evaluates and approves or rejects the change based on risk analysis, stakeholder input, and organizational practices.
3. **Rollback**
   Defines a plan to revert the change if issues arise, ensuring minimal disruption to operations.

Logging and monitoring the health of the information environment is essential to identifying inefficient or improperly performing systems, detecting compromises and providing a record of how systems are used.

- Logs should be stored separately from the systems they're logging