

















CyberSecurity Guide (PART I)

- **Confidentiality:** Protects information and systems from unauthorized access.
- **Integrity:** Protects information and systems from unauthorized modification.
- **Availability:** Ensures information and systems are available for authorized users when needed.

	Identification: You enter your username.
	Authentication: You enter your password (or use another method like a fingerprint).
	Authorization: The system checks if you have permission to access certain files or systems.
	Accounting: The system logs your activities for future reference.

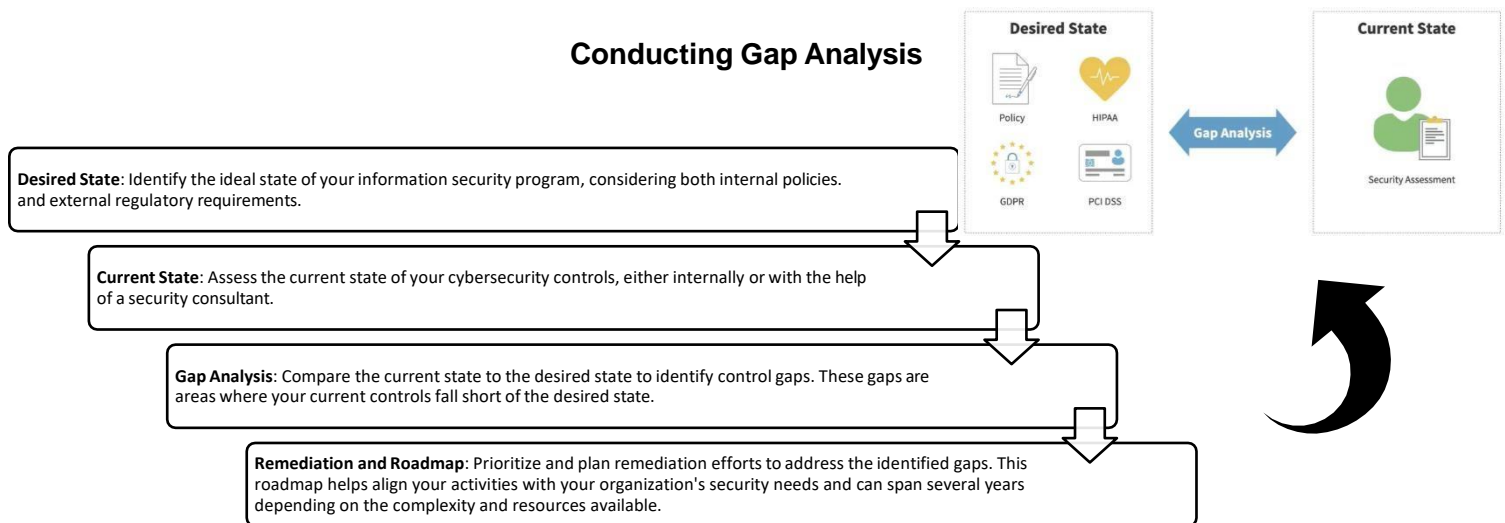
Security Controls:

Security controls are measures put in place to protect an organization from security risks. Let's think of them as different tools and strategies to keep your home safe.

	Preventive Controls: These aim to stop security issues before they happen. For example, a firewall that blocks unwanted traffic is like a lock on your door.	
	Detective Controls: These identify potential security breaches. An intrusion detection system is like a burglar alarm that alerts you if someone tries to break in.	
	Corrective Controls: These fix issues after they occur. Restoring data from a backup after an attack is like fixing a broken window after a burglary.	
	Deterrent Controls: These discourage attackers from trying. Guard dogs or security cameras act as deterrents.	
	Directive Controls: These provide guidelines on what to do. Policies and procedures are like instructions for using your home security system.	
	Compensating Controls: These fill gaps in your security. If a gate is easy to jump over, placing a guard there compensates for that weakness.	

- **Technical Controls:** These use technology to achieve security. Examples include firewalls, encryption, and antivirus software.
- **Operational Controls:** These are processes carried out by people to manage security. Examples include user access reviews and security training.
- **Managerial Controls:** These focus on managing risks. Conducting regular risk assessments and security planning are examples.
- **Physical Controls:** These protect the physical environment. Examples include locks, fences, and fire suppression systems.

Conducting Gap Analysis



Zero Trust Network Access (ZTNA) and **Secure Access Service Edge (SASE)** are modern approaches to network security.

Zero Trust Network Access (ZTNA)

- **Core Principle:** Trust no one by default, whether inside or outside the network. Every user and device must be verified before accessing resources.
- **Least Privilege:** Users only get access to the resources they need for their role, nothing more.
- **Network Location Irrelevant:** It doesn't matter if users are in the office, at home, or on the road. Location alone doesn't grant access.

How ZTNA Works

Control Plane vs. Data Plane:

- **Control Plane:** Where decisions about access are made.
- **Data Plane:** Where access is granted based on those decisions.

Key Capabilities:

- **Adaptive Identity:** Supports various user roles and identities that may change over time.
- **Threat Scope Reduction:** Keeps the environment simple to minimize risks.
- **Policy-Driven Access Control:** Flexible access control that adapts to changing needs.
- **Implicit Trust Zones:** Zones for sensitive data, like personal information or credit card data, that require extra protection.

NIST Model:

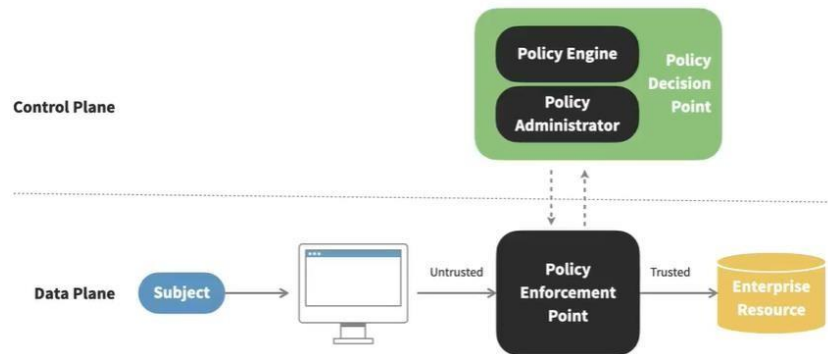
- **Policy Enforcement Point (PEP):** Intercepts access requests and enforces decisions.
- **Policy Decision Point (PDP):** Consists of:
 - **Policy Engine:** Decides whether to grant or deny access.
 - **Policy Administrator:** Configures the PEP based on the decision.

Secure Access Service Edge (SASE)

- **Higher-Level Design:** Combines ZTNA with other network security services like cloud access security brokers and firewalls.
- **Long-Term Goal:** Organizations gradually evolve their networks to support SASE, integrating outdated and new technologies.

Practical Implications

- **Short-Term:** Adopt Zero Trust principles to secure remote workforces and cloud services.
- **Long-Term:** Plan new networking projects with SASE in mind for future integration.



Physical Access Control

Types of Locks:

- **Preset Locks:** Traditional locks that require a specific physical key.
- **Cipher Locks:** Use a keypad where you enter a combination.
- **Biometric Locks:** Use physical characteristics like fingerprints or retinal patterns.
- **Card-Based Locks:** Use cards (magnetic stripe or proximity) to grant access.

Key Management:

- It's crucial to keep track of who has which keys and change locks if keys are lost or stolen.

Tailgating:

- This occurs when an unauthorized person follows an authorized person through a door. Access control vestibules (two-door systems) help prevent this by verifying only one person enters at a time.

Sensors for Monitoring:

- **Motion Sensors:** Detect movement.
- **Noise Sensors:** Monitor unexpected sounds like glass breaking.
- **Pressure Sensors:** Detect footsteps.
- **Microwave and Ultrasonic Sensors:** Use advanced technology to detect presence.

Video Surveillance:

- Acts as both a deterrent and a detective control. Cameras can be monitored by security personnel or software to detect unauthorized access.

Physical Barriers:

- **Fences and Cages:** Prevent unauthorized access to areas.
- **Bollards:** Prevent vehicles from crashing into buildings.
- **Lighting and Signs:** Increase visibility and provide legal grounds for trespassing charges.

Industrial Camouflage:

- Hiding sensitive facilities to make them look like ordinary buildings, which is increasingly challenging with drones.

Physical Security personnel

Role of Human Guards:

- **Human Judgment:** Security personnel use their judgment to evaluate visitor requests and grant access. This human element is crucial as technology alone can't always make these decisions.
- **Welcoming Presence:** Guards can serve as a welcoming face to visitors while still performing important security functions. They might appear as receptionists but are ensuring security.

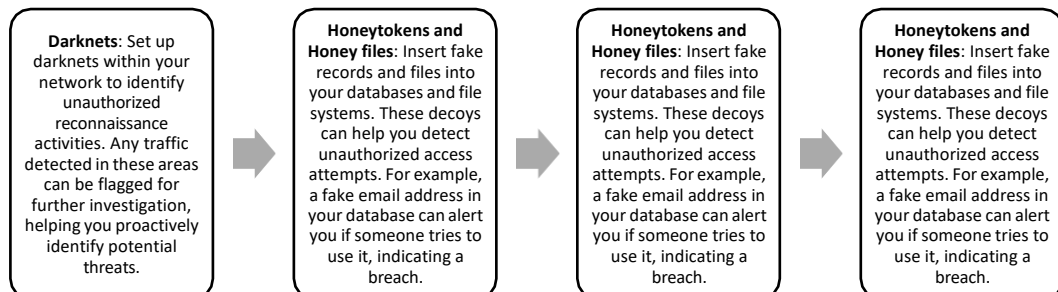
Types of Security Guards:

- **Overt Uniformed Guards:** These guards are visible and project an air of security and authority. Depending on local regulations, they can be armed.
- **Robot Sentries:** These are automated guards that patrol facilities, looking for abnormal activities and either challenging intruders or summoning human responses.

Two-Person Rule:

- **Two-Person Integrity:** This policy requires two people to be present for access to sensitive areas, deterring unauthorized activity by a single person.
- **Two-Person Control:** Requires the agreement of two individuals to perform a sensitive action, like launching a nuclear missile. This ensures that no single person can perform the action alone.

Deception Technologies



Change Management

What is Change Management?

- It's a way to plan, implement, and monitor organizational IT system changes to minimize risks and maximize benefits.

Key Steps in Change Management:

- **Approval Process:** Before making any changes, they must be reviewed and approved to avoid unauthorized modifications.
- **Assigned Owner:** Each change has a person responsible for it, ensuring accountability.
- **Stakeholder Involvement:** Involve the right people (like IT staff and department heads) to understand the impact of changes.
- **Impact Analysis:** Assess potential risks and consequences of the change.
- **Testing:** Verify the change works as intended without causing issues.
- **Back-Out Plan:** Have a plan to revert the change if something goes wrong.

- **Scheduling:** Implement changes during maintenance windows to minimize disruptions.
- **Standard Operating Procedures (SOPs):** Follow consistent guidelines to ensure changes are made correctly.

Technical Considerations:

- **Allow/Deny Lists:** Control what actions are permitted or blocked.
- **Restrictions:** Limit certain activities to enhance security.
- **Downtime:** Plan for temporary service interruptions.
- **Service Restarts:** Restart applications to apply changes.
- **Legacy Applications:** Ensure changes don't affect older systems.
- **Dependencies:** Understand how changes affect other systems.

Documentation and Version Control:

- **Version Control:** Keep records of all changes for traceability.
- **Update Documentation:** Revise diagrams, procedures, and policies to reflect the new state after changes.