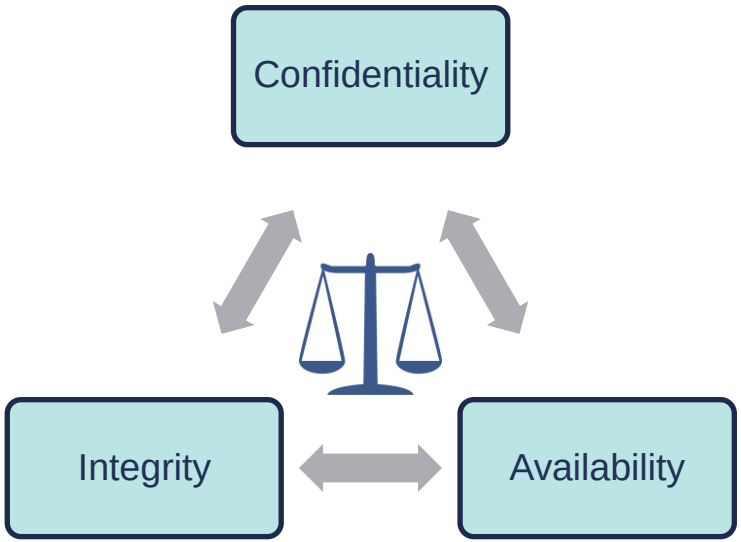
The CIA Triad

The CIA Triad

- **C**onfidentiality
- **I**ntegrity
- **A**vailability

All 3 Equally Important & Intertwined



Authentication, Authorization, and Accounting (AAA)

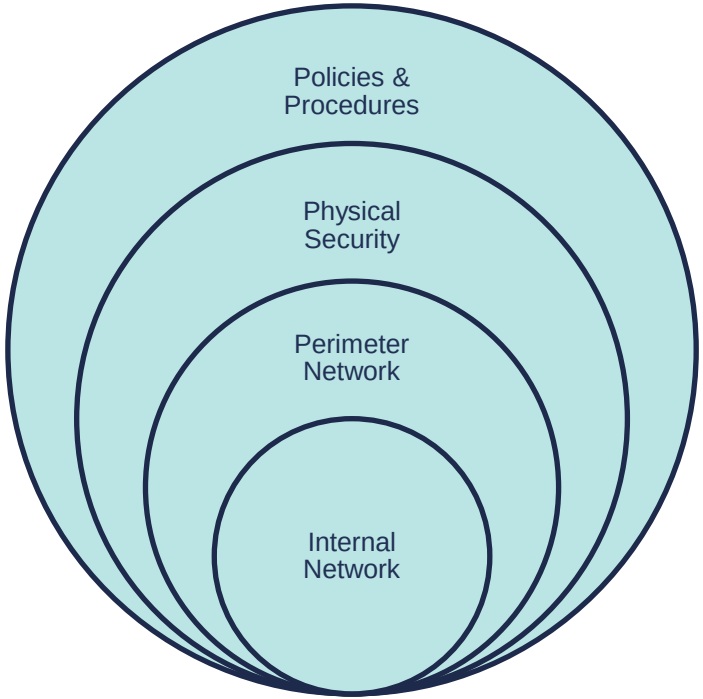
Authentication, Authorization & Accounting (AAA)

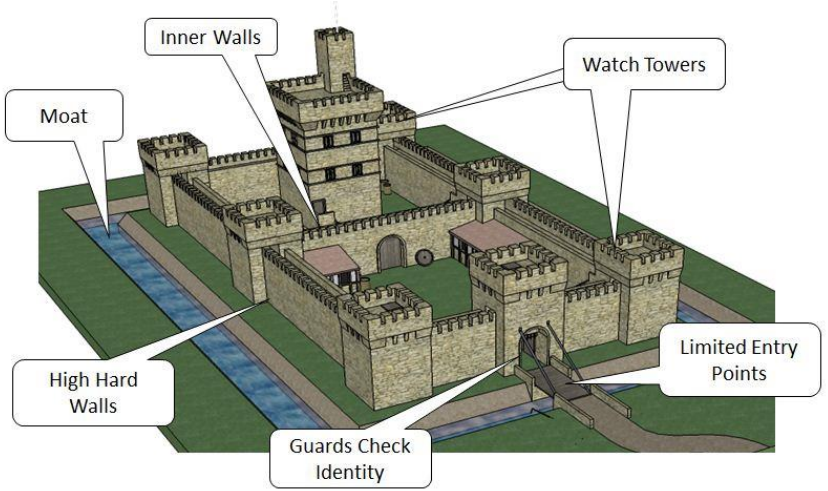
AAA is an information security framework for controlling access to data and system resources, enforcing policies, and auditing actions.

- **Authentication**
  - ✓ Verifies a user's identification via the process of logging into a system.
- **Authorization (Access Control)**
  - ✓ Determines what a user has the authority to do and have access to.
- **Accounting**
  - ✓ Tracks and records user access and actions with system logs.

Defense in Depth

Defense in Depth





Least Privilege

Least Privilege

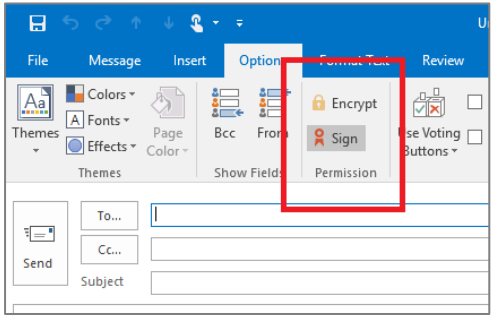
Definition: A user, system, process, or application is only given the permissions necessary to complete its assigned tasks or functions and nothing more.

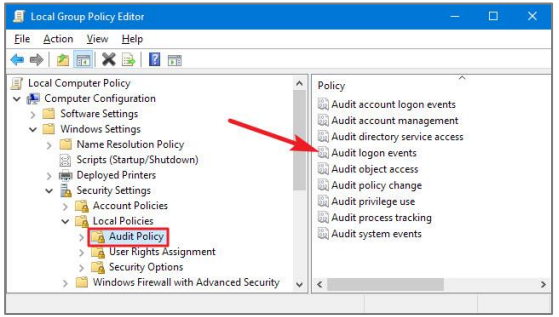
- Implementing Least Privilege:
  - Security Groups
  - Account Standardization
  - Account Management Processes & Procedures

Non-Repudiation

Non-Repudiation

- Used to prevent an entity from denying an action took place.
- **Examples**: Digitally Signed Documents & Auditing System Logs





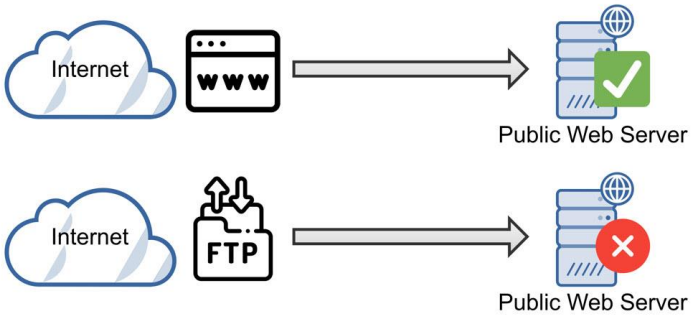
Implicit Deny

Implicit Deny

- Indicates that unless something is explicitly allowed, it is denied.
  - Implemented with Access Control Lists (ACLs)

Definition: An ACL rule that blocks all traffic that hasn't been explicitly allowed via another ACL rule.

- **Example**:
  - All Internet traffic to a company's web server is blocked, unless it is directed to port 443 for HTTPS.



Legal and Regulatory Issues

Legal & Regulatory Issues

- Compliance with laws and regulations is a must.
  - Federal Information Security Management Act (FISMA)
  - Health Insurance Portability & Accountability Act (HIPPA)
  - Gramm-Leach-Bliley Act
  - Payment Card Industry Data Security Standards (PCI-DSS)

- Ignorance of a law is not a valid excuse.
- If you're not in compliance, you could be held legally liable for your inactions.

Due Care and Due Diligence

- **Due Care** is often called the “prudent man” rule, which is doing what any responsible person would do. In other words, this is implementing a security measure to mitigate against certain risks.

- **Due Diligence** is essentially the management of due care. In other words, ensuring the implemented security measure was done correctly.

- **Gross Negligence** is the opposite of due care. If you’re not performing due care, what a “prudent man” would do, and you suffer a negative loss, you could be held legally liable, i.e., you acted with gross negligence.

Information Security Governance

Information Security Governance

- **Information Security Governance** is the process of how an organization manages its information security program via policies, procedures, roles, and responsibilities.
- It provides strategic direction for **security** activities and ensures that **cybersecurity** objectives such as effective risk management are achieved.
- Determines **how much** security is **enough** security.

- **Senior Management** plays an essential role in information security governance because they:
  - ✓ Craft and mold the higher-level policies
  - ✓ Drive the direction of IT security based on business needs
  - ✓ Have the final say in all major decisions that impact the business

- Effective IT security management needs to be a top-down driven approach, not bottom-up.

Authentication Basics

Authentication Basics

- Authentication is used to prove identity by using some type of credential that is previously known by the authenticator.
  - **Common Example**: Username & Password
- Can be used to prove the identity of:
  - A User
  - A Service or Process Running on a Computer or Server
  - A Workstation or Server Itself
  - A Network Device
- In IT security, we need to authenticate more than just the people accessing the network and IT systems
- We want to authenticate everything!

INSTRUCTOR
ALTON

Three Factors of Authentication

Something You Know

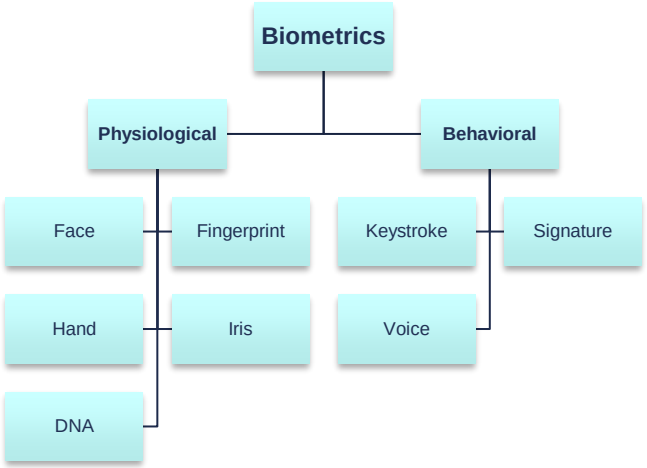
- Password
- PIN

Something You Have

- Smart Card
- RSA Token

Something You Are

- Biometrics



Two-Factor Authentication

- Common Practice to Increase Security
- Uses a combination of two of the three factors of authentication
  - Something You Have
  - Something You Know
  - Something You Are

- **Examples**:
  - **Banks**: ATM Card & PIN
  - **Gym Access**: Biometrics Palm Scan & ID Card
  - **Work ID Badges**: SmartID Card & PIN Number

Identify Proofing

INSTRUCTOR
ALTON

Identity Proofing

- Not the same as authentication.
- Before you give out credentials, you “Identity Proof” somebody.
- Validates someone’s identity before credentials are issued
  - Driver’s License, Passport, etc.

Identity Proofing Example

- **Online Banking Login**
  - You've forgotten your password and request a new password.
  - Your bank will identity proof your identity by one of the following methods:
    - Texting your registered cell phone number a temporary login PIN
    - E-mailing your registered e-mail account a temporary password
    - Asking you to answer security questions
  - You can't log into your account unless your identity is proofed.

General Password Rules

General Password Rules

- Passwords should be strong
  - 8 Characters Minimum
  - Combination of Upper Case & Lower Case Letters, Numbers, and Special Characters
- Passwords should not be written down
- Passwords should not be shared
- Passwords should be regularly changed
  - Every 60 to 90 days

General Password Rules

- Passwords should not be reused
  - Don’t allow reuse of last 4 passwords
- Account lockout policies should be used
  - Lockout user after 3 failed login attempts
- Default passwords should be changed
  - New user default password expires after 1st use