Introduction to Access Control

Access Control protects against a wide variety of threats

- Unauthorized Access
- Unapproved Modification of Data
- Lack of Data Confidentiality

Physical & Logical Access Control

Physical security includes implementing different access control methods with technology you can touch. Physically locking down the equipment and securing the building.

Logical security methods include those elements that are implemented through technological means. Password policies, logical access control lists, etc.

Common Physical Access Control Measures

- Employee ID Badges
- Physical Access Logs
- Door Access Systems
- Proximity Cards
- Mantraps
- Hardware Locks
- Video Surveillance
- Security Guards
- Building Alarms
- Fences

Common Logical Access Control Measures

- Access Control Lists
- NTSF Permissions
- Windows Group Policies
- Password Policies
- Account Policies
- Device Policies

Access Control Categories & Types

- Preventive
- Detective
- Corrective
- Recovery
- Deterrent
- Compensating

Preventative Access Controls

- **Preventive controls** prevent actions.
  - Background check before approving a tenant ensure a qualified tenant.
  - Drug test before employment prevents hiring of employees that use illegal drugs.

Detective Access Controls

- **Detective controls** send alerts during or after an attack.
  - Building alarm triggered during a break-in.
  - Network intrusion detection system (IDS) alerting network administrators of an attack.

Corrective Access Controls

- **Corrective controls** “correct” a damaged system or process.
  - Anti-virus can quarantine and delete malicious software from a computer system.
  - Intrusion prevention system (IPS) can stop a network attack by blocking it.

Recovery Access Controls

- **Recovery controls** are needed to restore functionality.
  - Restoring corrupted data with a data back-up.
  - A secondary office site can restore business functionality after a natural disaster to the business's primary site.

Deterrent Access Controls

- **Deterrent controls** deter users from performing actions.
  - Security guards.
  - A “beware of dog” sign.
  - A fence around your building.

Compensating Access Controls

- **Compensating controls** add additional security by compensating other control's weaknesses.
  - Defense In Depth
  - Multiple Layers of Security