



Types of Controls

Security Architecture & Tool Sets

Types of Controls

- Controls prevent, detect, counteract, or limit certain security risks
 - Technical Controls
 - Administrative Controls
 - Legal Controls
 - Physical Controls
 - Preventive Controls
 - Detective Controls
 - Corrective Controls
 - Compensating Controls

Based on their Implementation

Based on when the control acts



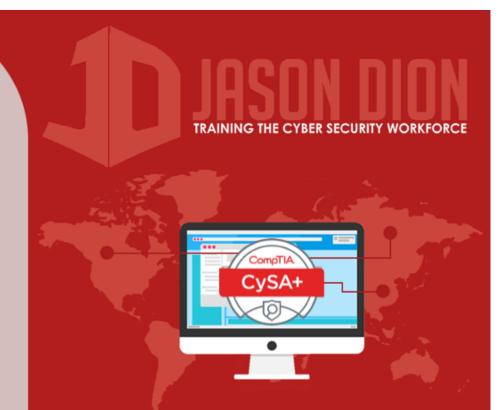


Technical Controls

 Designed to provide security through technical measures

- Examples
 - Firewalls
 - IDS/IPS
 - Authentication Systems
 - Network Segmentation





Administrative Controls (or Procedural Controls)

- Designed to provide security through processes and procedures
- Legal controls are a type of these controls that are put in place by the law
- Examples
 - Incident Response Plans
 - User Awareness Training
 - Account Creation Policy
 - Acceptable Use Policy







Physical Controls

 Designed to provide security by preventing physical access or harm to the organization's systems or facilities

- Examples
 - Fences
 - Mantraps
 - Security Guards
 - Fire Suppression Systems







Preventative Controls

- Designed to stop an incident before it has occurred
- Proactive measures
- Examples
 - Firewalls
 - Antivirus
 - Training
 - Security Guards







Detective Controls

 Designed to detect when an incident occurs, capture details about it, and send an alarm/notification so someone can act

- Examples
 - Intrusion Detection System
 - Security Cameras
 - Logs







Corrective Controls

- Designed to fix an issue after an incident has occurred
- Part of incident response process
- Reactive measures
- Examples
 - Security Patching
 - System Rebuilding
 - Restore from Backups





RAINING THE CYBER SECURITY WORKFORCE



Compensating Controls

 Designed to satisfy a security requirement not being met by other controls

 Minimizes threat down to an acceptable level of risk (based on risk appetite)

Examples

- Blocking certain ports instead of upgrading all of the operating systems
- Segmenting vulnerable software to a separate part of the network

