Control categories

Control categories

1. Administrative/Managerial controls:

- Developing and implementing security policies and procedures to govern the organization's security practices.
- Conducting regular security training and awareness programs for employees to educate them on security best practices.
- Implementing access control mechanisms such as user privileges and role-based access controls to restrict unauthorized access to sensitive information.
- Implementing incident response and management protocols to enable prompt response to security incidents and minimize their impact.

2. Technical controls:

- Implementing network security measures such as firewalls, intrusion detection/prevention systems, and encryption to protect data in transit and at rest.
- Implementing endpoint security solutions such as antivirus software, endpoint detection and response tools, and mobile device management to secure devices and prevent malware infections.
- Implementing secure coding practices and conducting regular security assessments of applications to identify and remediate vulnerabilities.
- Implementing data loss prevention (DLP) solutions to monitor and prevent unauthorized data exfiltration.

3. Physical/Operational controls:

- Implementing access control measures such as biometric authentication, access badges, and security guards to restrict physical access to sensitive areas.
- Implementing surveillance systems and alarms to monitor and detect unauthorized access or security breaches.
- Implementing environmental controls such as temperature and humidity monitoring to protect sensitive equipment and data centers.
- Implementing disaster recovery and business continuity plans to ensure the organization can recover from security incidents and maintain operations in the event of a disruption.

Control types

Administrative/Managerial Controls		
Control Name	**Control Type**	**Control Purpose**
Least Privilege	Preventative	Reduce risk and overall impact of malicious insider or compromised accounts
Disaster recovery plans	Corrective	Provide business continuity
Password policies	Preventative	Reduce likelihood of account compromise through brute force or dictionary attack techniques
Access control policies	Preventative	Bolster confidentiality and integrity by defining which groups can access or modify data
Account management policies	Preventative	Managing account lifecycle, reducing attack surface, and limiting overall impact from disgruntled former employees and default account usage
Separation of duties	Preventative	Reduce risk and overall impact of malicious insider or compromised accounts

Technical Controls		
Control Name	**Control Type**	**Control Purpose**

Firewall	Preventative	To filter unwanted or malicious traffic from entering the network
IDS/IPS	Detective	To detect and prevent anomalous traffic that matches a signature or rule
Encryption	Deterrent	Provide confidentiality to sensitive information
Backups	Corrective	Restore/recover from an event
Password management	Preventative	Reduce password fatigue
Antivirus (AV) software	Preventative	Scans to detect and quarantine known threats
Manual monitoring, maintenance, and intervention	Preventative	Necessary to identify and manage threats, risks, or vulnerabilities to out-of-date systems

Physical/Operational Controls		
Control Name	**Control Type**	**Control Purpose**
Time-controlled safe	Deterrent	Reduce attack surface and overall impact from physical threats
Adequate lighting	Deterrent	Deter threats by limiting “hiding” places
Closed-circuit television (CCTV)	Preventative/Detective	Closed circuit television is both a preventative and detective control because it’s presence can reduce

		risk of certain types of events from occurring, and can be used after an event to inform on event conditions
Locking cabinets (for network gear)	Preventative	Bolster integrity by preventing unauthorized personnel and other individuals from physically accessing or modifying network infrastructure gear
Signage indicating alarm service provider	Deterrent	Deter certain types of threats by making the likelihood of a successful attack seem low
Locks	Deterrent/Preventative	Bolster integrity by deterring and preventing unauthorized personnel, individuals from physically accessing assets
Fire detection and prevention (fire alarm, sprinkler system, etc.)	Detective/Preventative	Detect fire in physical location and prevent damage to physical assets such as inventory, servers, etc.