Control Categories

Cybersecurity controls at SafeInvest are grouped into three primary categories: Administrative, Technical, and Physical/Operational. Each category is designed to address different aspects of the security posture to mitigate identified risks and ensure compliance with relevant regulations.

1. Administrative/Managerial Controls: These controls address the human element of cybersecurity within SafeInvest. They involve establishing policies and procedures that define how data should be managed and outline the responsibilities of each employee in protecting the organization. While these controls are policy-based, enforcing them often requires support from technical or physical measures.

2. Technical Controls: these controls involve the use of technology and software solutions to protect SafeInvest's digital assets. These controls are implemented within the IT infrastructure and applications to enforce security policies and procedures. This includes solutions such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), antivirus software, and encryption technologies. These tools help us prevent, detect, and respond to security incidents, ensuring our technology aligns with organizational goals and security requirements.

3. Physical/Operational Controls: these controls are implemented to limit physical access to SafeInvest's physical assets, such as servers, data centers, and office spaces, by unauthorized personnel. They include measures such as door locks, cabinet locks, surveillance cameras, and badge readers. The goal is to restrict physical access to critical systems and data centers, ensuring that only authorized personnel can access sensitive areas.

Control Types

Cybersecurity controls can also be categorized by their function:

- **Preventative Controls:** These controls are designed to prevent security incidents from occurring in the first place.
- **Corrective Controls:** These controls are implemented to restore systems and data to a normal state after a security incident has occurred.
- **Detective Controls:** These controls are used to identify and alert security personnel about security incidents that have occurred or are in progress.
- **Deterrent Controls:** These controls are designed to discourage potential attackers from attempting to exploit vulnerabilities or initiate attacks.

Detailed descriptions of each type of control can be found in the following charts.

Administrative/Managerial Controls

Control Name	Control Type	Control Purpose
Least Privilege	Preventative	Reduce the risk and impact of malicious insiders or compromised accounts by limiting access.
Disaster Recovery Plans	Corrective	Provide business continuity and restore operations after an incident.
Password Policies	Preventative	Lower the risk of account compromise by enforcing strong password practices and periodic updates.
Access Control Policies	Preventative	Define which groups can access or modify data, thereby safeguarding confidentiality and integrity.
Account Management Policies	Preventative	Manage account lifecycles to reduce attack surfaces and limit risks from default or stale accounts.
Separation of Duties	Preventative	Prevent misuse of access by dividing responsibilities among multiple individuals.

Technical Controls

Control Name	Control Type	Control Purpose
Firewall	Preventative	Filter out unwanted or malicious traffic from entering the network.
IDS/IPS	Detective	Identify and block anomalous or suspicious activity by monitoring network traffic.
Encryption	Deterrent	Protect sensitive information by converting it into unreadable code for unauthorized users.
Backups	Corrective	Ensure that data can be restored and operations resumed after an incident.
Password Management	Preventative	Encourage secure practices by reducing password fatigue and enforcing strong, unique passwords.
Antivirus (AV) Software	Corrective	Detect and quarantine known threats to prevent malware infections.

Control Name	Control Type	Control Purpose
Manual Monitoring, Maintenance, and Intervention	Preventative	Identify and manage risks, especially for legacy systems or areas where automated solutions fall short.

Physical/Operational Controls

Control Name	Control Type	Control Purpose
Time-Controlled Safe	Deterrent	Limit physical access over time, reducing risk from unauthorized attempts during vulnerable periods.
Adequate Lighting	Deterrent	Deter potential threats by eliminating dark areas that could provide cover for unauthorized activities.
Closed-Circuit Television (CCTV)	Preventative/Detective	Deter incidents with visible surveillance and assist in investigating events if they occur.
Locking Cabinets (for network gear)	Preventative	Prevent unauthorized physical access or tampering with critical network infrastructure.
Signage Indicating Alarm Service Provider	Deterrent	Discourage potential attackers by signaling that rapid response measures are in place.
Locks	Deterrent/Preventative	Prevent unauthorized access to physical assets and secure sensitive areas.
Fire Detection and Prevention (Fire alarms, sprinkler systems, etc.)	Detective/Preventative	Detect fires early and mitigate damage to physical assets such as servers, inventory, and critical equipment.

These control categories and types work together to create a layered security approach, often referred to as "defense in depth," to protect SafeInvest's valuable assets.