# Control categories

## Control categories

- Administrative/Managerial controls
- Technical controls
- Physical/Operational controls

| **Administrative/Managerial Controls** | | | |
|---|---|---|---|
| **Control Name** | **Control Type** | **Implemented** | **Gaps & Recommendations** |
| Least Privilege | Preventative | No | Restrict access to only necessary personnel. Implement role-based access control (RBAC). |
| Disaster recovery plans | Corrective | No | Create business continuity and disaster recovery (DR) plans to restore systems after incidents. |
| Password policies | Preventative | Yes (but weak) | Strengthen the policy to require longer, more complex passwords. Enforce multi-factor authentication (MFA). |
| Access control policies | Preventative | No | Define who can access or modify data. Implement access review processes |

| Administrative/Managerial Controls | | | |
|---|---|---|---|
| Account management policies | Preventative | No | Implement automated account deactivation for former employees and enforce least privilege. |
| Separation of duties | Preventative | No | Define job roles to separate critical tasks and prevent fraud or misuse. |

| Technical Controls | | | |
|---|---|---|---|
| **Control Name** | **Control Type** | **Implemented** | **Control Purpose** |
| Firewall | Preventative | Yes | Ensure firewall rules are regularly reviewed and updated. |
| IDS/IPS | Detective | No | Deploy an IDS to monitor and alert on suspicious traffic. |
| Encryption | Deterrent | No | Encrypt stored and transmitted sensitive data, including credit card details. |
| Backups | Corrective | No | Implement regular backups with offsite storage for redundancy. |
| Password management | Preventative | No | Deploy a centralized |

| | | | |
|---|---|---|---|
| | | | password manager to enforce strong policies and reduce password fatigue. |
| Antivirus (AV) software | Preventative | Yes | Ensure AV is updated and monitored continuously. |
| Manual monitoring, maintenance, and intervention | Preventative | Yes (but lacks schedule) | Implement scheduled maintenance and upgrade plan for legacy systems. |

| **Physical/Operational Controls** | | | |
|---|---|---|---|
| **Control Name** | **Control Type** | **Implemented** | **Control Purpose** |
| Time-controlled safe | Deterrent | Yes | Periodically review safe access logs and ensure security policies are updated. |
| Adequate lighting | Deterrent | Yes | Ensure proper lighting in all entry/exit points and critical areas to deter unauthorized access. |
| Closed-circuit television (CCTV) | Preventative/Detective | Yes | Ensure recordings are stored securely and monitored. |
| Locking cabinets (for network gear) | Preventative | No | Install locking cabinets for critical |

| | | | |
|---|---|---|---|
| | | | network equipment to prevent unauthorized access. |
| Signage indicating alarm service provider | Deterrent | No | Add visible alarm system signage to deter potential intruders. |
| Locks | Deterrent/Preventative | No | Ensure regular security audits of physical access points. |
| Fire detection and prevention (fire alarm, sprinkler system, etc.) | Detective/Preventative | No | Regularly test fire alarms and update fire safety protocols |