# Controls assessment

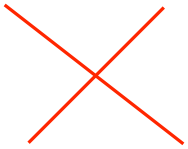
To review control categories, types, and the purposes of each, read the control categories document.

## Current assets

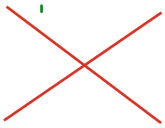
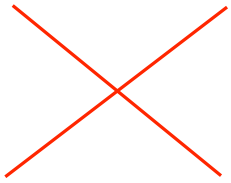
Assets managed by the IT Department include:

- On-premises equipment for in-office business needs
- Employee equipment: end-user devices (desktops/laptops, smartphones), remote workstations, headsets, cables, keyboards, mice, docking stations, surveillance cameras, etc.
- Management of systems, software, and services: accounting, telecommunication, database, security, ecommerce, and inventory management
- Internet access
- Internal network
- Vendor access management
- Data center hosting services
- Data retention and storage
- Badge readers
- Legacy system maintenance: end-of-life systems that require human monitoring

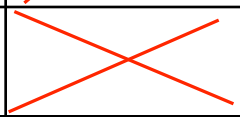
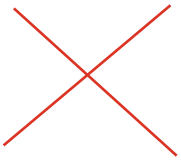
| Administrative Controls | | | |
|---|---|---|---|
| **Control Name** | **Control type and explanation** | **Needs to be implemented (X)** | **Priority** |
| Least Privilege | Preventative; reduces risk by making sure vendors and non-authorized staff only have access to the assets/data they need to do their jobs | X | High |
| Disaster recovery plans | Corrective; business continuity to ensure systems are able to run in the event of an | X | Medium/ High |

| Administrative Controls | | | |
|---|---|---|---|
| | incident/there is limited to no loss of productivity downtime/impact to system components, including: computer room environment (air conditioning, power supply, etc.); hardware (servers, employee equipment); connectivity (internal network, wireless); applications (email, electronic data); data and restoration | | |
| Password policies | Preventative; establish password strength rules to improve security/reduce likelihood of account compromise through brute force or dictionary attack techniques |  | High |
| Access control policies | Preventative; increase confidentiality and integrity of data |  | High |
| Account management policies | Preventative; reduce attack surface and limit overall impact from disgruntled/former employees |  | Medium/ High |
| Separation of duties | Preventative; ensure no one has so much access that they can abuse the system for personal gain |  | High |

| Technical Controls |
|---|

| Control Name | Control type and explanation | Needs to be implemented (X) | Priority |
|---|---|---|---|
| Firewall | Preventative; firewalls are already in place to filter unwanted/malicious traffic from entering internal network | | NA |
| Intrusion Detection System (IDS) | Detective; allows IT team to identify possible intrusions (e.g., anomalous traffic) quickly |  | High |
| Encryption | Deterrent; makes confidential information/data more secure (e.g., website payment transactions) |  | High |
| Backups | Corrective; supports ongoing productivity in the case of an event; aligns to the disaster recovery plan |  | High |
| Password management system | Corrective; password recovery, reset, lock out notifications |  | Medium |
| Antivirus (AV) software | Corrective; detect and quarantine known threats |  | High |
| Manual monitoring, maintenance, and intervention | Preventative/corrective; required for legacy systems to identify and mitigate potential threats, risks, and vulnerabilities |  | High |

| Physical Controls |
|---|

| Control Name | Control type and explanation | Needs to be implemented (X) | Priority |
|---|---|---|---|
| Time-controlled safe | Deterrent; reduce attack surface/impact of physical threats |  | Low |
| Adequate lighting | Deterrent; limit “hiding” places to deter threats |  | Low |
| Closed-circuit television (CCTV) surveillance | Preventative/detective; can reduce risk of certain events; can be used after event for investigation |  | High |
| Locking cabinets (for network gear) | Preventative; increase integrity by preventing unauthorized personnel/individuals from physically accessing/modifying network infrastructure gear |  | Low/ Medium |
| Signage indicating alarm service provider | Deterrent; makes the likelihood of a successful attack seem low |  | Low |
| Locks | Preventative; physical and digital assets are more secure |  | High |
| Fire detection and prevention (fire alarm, sprinkler system, etc.) | Detective/Preventative; detect fire in the toy store’s physical location to prevent damage to inventory, servers, etc. |  | Medium |