

# Controls assessment

## 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                           | High     |

| Administrative Controls     |  |   |      |
|-----------------------------|--|---|------|
|                             | incident/there is limited to no loss of productivity<br>downtime/impact to system components, including:<br>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  | X | High |
| Access control policies     | Preventative; increase confidentiality and integrity of data   | X | High |
| Account management policies | Preventative; reduce attack surface and limit overall impact from disgruntled/former employees   | X | High |
| Separation of duties        | Preventative; ensure no one has so much access that they can abuse the system for personal gain  | X | High |

|                           |
|---------------------------|
| <b>Technical Controls</b> |
|---------------------------|

| 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                                 | X                           | High     |
| Encryption                                       | Deterrent; makes confidential information/data more secure (e.g., website payment transactions)                             | X                           | High     |
| Backups  | Corrective; supports ongoing productivity in the case of an event; aligns to the disaster recovery plan                     | X                           | High     |
| Password management system                       | Corrective; password recovery, reset, lock out notifications  | X                           | High     |
| Antivirus (AV) software                          | Corrective; detect and quarantine known threats   | X                           | High     |
| Manual monitoring, maintenance, and intervention | Preventative/corrective; required for legacy systems to identify and mitigate potential threats, risks, and vulnerabilities | X                           | 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   | X                           | Medium   |
| Adequate lighting  | Deterrent; limit “hiding” places to deter threats   | X                           | Med/Low  |
| Closed-circuit television (CCTV) surveillance                      | Preventative/detective; can reduce risk of certain events; can be used after event for investigation  | X                           | Medium   |
| Locking cabinets (for network gear)                                | Preventative; increase integrity by preventing unauthorized personnel/individuals from physically accessing/modifying network infrastructure gear | X                           | Medium   |
| Signage indicating alarm service provider                          | Deterrent; makes the likelihood of a successful attack seem low   | X                           | Medium   |
| Locks  | Preventative; physical and digital assets are more secure   | X                           | 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.                            | X                           | High     |