# **Controls Assessment**

Refer to the information in the [scope, goals, and risk assessment report](https://docs.google.com/document/d/1s2u_RuhRAI40JSh-eZHvaFsV1ZMxcNSWXifHDTOsgFc/template/preview#heading=h.evidx83t54sc). For more details about each control, refer to the [control categories](https://docs.google.com/document/d/1btezuy_bMKWoK8pd97ZuzdWB9y6au_zfkrpkfVf8ktI/template/preview) 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)** |
| 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 |
| Disaster recovery plans | Corrective; business continuity to ensure systems are able to run in the event of an 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 | X |
| Password policies | Preventative; establish password strength rules to improve security/reduce likelihood of account compromise through brute force or dictionary attack techniques | X |
| Separation of duties | Preventative; ensure no one has so much access that they can abuse the system for personal gain | X |

| **Technical Controls** | | |
| --- | --- | --- |
| **Control Name** | **Control type and explanation** | **Needs to be implemented**  **(X)** |
| 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 |
| Encryption | Deterrent; makes confidential information/data more secure (e.g., website payment transactions) | X |
| Backups | Corrective; supports ongoing productivity in the case of an event; aligns to the disaster recovery plan | X |
| Password management system | Corrective; password recovery, reset, lock out notifications | X |
| Antivirus (AV) software | Corrective; detect and quarantine known threats | NA |
| Manual monitoring, maintenance, and intervention | Preventative/corrective; required for legacy systems to identify and mitigate potential threats, risks, and vulnerabilities | X |

| **Physical Controls** | | |
| --- | --- | --- |
| **Control Name** | **Control type and explanation** | **Needs to be implemented**  **(X)** |
| Closed-circuit television (CCTV) surveillance | Preventative/detective; can reduce risk of certain events; can be used after event for investigation | NA |
| Locks | Preventative; physical and digital assets are more secure | NA |
| 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. | NA |