# Controls assessment

To review control categories, types, and the purposes of each, read the [control categories](https://docs.google.com/document/d/1Ut_H5A9FHwuQEy6_qG6Lfy3zwF6GSJnj3DZTMaNRWEE/template/preview?usp=sharing&resourcekey=0-i4dR5qZFqQyfzr8uk3OOmA) 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, one of the major goals is to implement Least Access. |
| 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 | High, NIST CSF includes recovery. |
| Password policies | Preventative; establish password strength rules to improve security/reduce likelihood of account compromise through brute force or dictionary attack techniques | X | High, GDPR is heavy on user protection. This would lower risk of compromises. |
| Access control policies | Preventative; increase confidentiality and integrity of data | X | Medium, Company wants to use least permissions, but is focusing on NIST and not CIA framework. |
| Account management policies | Preventative; reduce attack surface and limit overall impact from disgruntled/former employees | X | Medium, Company is still fairly small, so attacks from former employees are unlikely. |
| Separation of duties | Preventative; ensure no one has so much access that they can abuse the system for personal gain | X | High,  Company wants to strengthen least permissions |

| **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 |  | UnnecessaryAlready in place |
| Intrusion Detection System (IDS) | Detective; allows IT team to identify possible intrusions (e.g., anomalous traffic) quickly | X | High, GDPR values monitoring. Would aid in detecting for the NIST CSF framework. |
| Encryption | Deterrent; makes confidential information/data more secure (e.g., website payment transactions) | X | High, GDPR wants to protect customers rights. Especially for data relating to payments which is also related to the PCI DSS |
| Backups | Corrective; supports ongoing productivity in the case of an event; aligns to the disaster recovery plan | X | Medium, would help to recover/respond for the NIST CSF framework |
| Password management system | Corrective; password recovery, reset, lock out notifications | X | High, protects customers rights for the GDPR |
| Antivirus (AV) software | Corrective; detect and quarantine known threats | X | High, big role in responding and detecting problems in the NIST CSF framework. |
| Manual monitoring, maintenance, and intervention | Preventative/corrective; required for legacy systems to identify and mitigate potential threats, risks, and vulnerabilities | X | High, GDPR states that systems must be monitored heavily |

| **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 | Low, main threat is the online business. Still would help to fortify controls |
| Adequate lighting | Deterrent; limit “hiding” places to deter threats |  | Unnecessary |
| Closed-circuit television (CCTV) surveillance | Preventative/detective; can reduce risk of certain events; can be used after event for investigation | X | Low, main threat is the online business. Still would help to fortify controls |
| Locking cabinets (for network gear) | Preventative; increase integrity by preventing unauthorized personnel/individuals from physically accessing/modifying network infrastructure gear | X | Medium, gaining unauthorized access network gear could be catastrophic to business continuity. |
| Signage indicating alarm service provider | Deterrent; makes the likelihood of a successful attack seem low |  | Unnecessary |
| Locks | Preventative; physical and digital assets are more secure |  | Unnecessary |
| 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, would help comply with physical safety regulations. Protection from lawsuits and would save inventory. |