# Analyze the audit scope, goals, and risk assessment

After you review the audit scope, goals, and risk assessment, consider the following questions:

* What are the biggest risks to the organization?
  + **Inadequate Asset Management**: The organization lacks proper management of its assets, which could lead to vulnerabilities and security gaps going unnoticed.
  + **Lack of Controls**: Insufficient controls are in place, leaving the organization susceptible to security breaches and unauthorized access.
  + **Non-Compliance**: Botium Toys might not be compliant with U.S. and international regulations and standards. This could result in legal consequences, fines, and damage to the organization's reputation.
* Which controls are most essential to implement immediately versus in the future?
  + **Asset Management Control**: Establish proper procedures for tracking and managing all assets, ensuring an accurate inventory of equipment, software, and services.
  + **Access Control**: Implement robust access controls to restrict user permissions based on the principle of least privilege, ensuring users have only the access they need.
  + **Compliance Control**: Begin aligning the organization's processes, procedures, and systems with necessary compliance requirements.
* Which compliance regulations does Botium Toys need to adhere to, to ensure the company keeps customer and vendor data safe, avoids fines, etc.?
  + **Payment Card Industry Data Security Standard** (PCI DSS): If Botium Toys accepts credit card payments, it must comply with PCI DSS to ensure the security of payment card data.
  + **General Data Protection Regulation** (GDPR): If Botium Toys handles personal data of European Union citizens, it must comply with GDPR to protect individual privacy and data rights.
  + **Industry-Specific Regulations**: Depending on the industry in which Botium Toys operates, there may be specific regulations to follow.

# 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 |
| 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 |
| Password policies | Preventative; establish password strength rules to improve security/reduce likelihood of account compromise through brute force or dictionary attack techniques |  | NA |
| Access control policies | Preventative; increase confidentiality and integrity of data |  | NA |
| Account management policies | Preventative; reduce attack surface and limit overall impact from disgruntled/former employees |  | NA |
| Separation of duties | Preventative; ensure no one has so much access that they can abuse the system for personal gain |  | NA |

|  |  |  |  |
| --- | --- | --- | --- |
| **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 | X | Medium |
| Encryption | Deterrent; makes confidential information/data more secure (e.g., website payment transactions) | X | Medium |
| 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 | Medium |
| Antivirus (AV) software | Corrective; detect and quarantine known threats | X | Medium |
| Manual monitoring, maintenance, and intervention | Preventative/corrective; required for legacy systems to identify and mitigate potential threats, risks, and vulnerabilities | X | Medium |

|  |  |  |  |
| --- | --- | --- | --- |
| **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 |  | NA |
| Adequate lighting | Deterrent; limit “hiding” places to deter threats |  | NA |
| 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 |  | 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 |

# Compliance checklist

To review compliance regulations and standards, read the [controls, frameworks, and compliance](https://www.coursera.org/learn/foundations-of-cybersecurity/supplement/xu4pr/controls-frameworks-and-compliance) document.

**The Federal Energy Regulatory Commission - North American Electric Reliability Corporation (FERC-NERC)**

The FERC-NERC regulation applies to organizations that work with electricity or that are involved with the U.S. and North American power grid. Organizations have an obligation to prepare for, mitigate, and report any potential security incident that can negatively affect the power grid. Organizations are legally required to adhere to the Critical Infrastructure Protection Reliability Standards (CIP) defined by the FERC.

**Explanation:**

**General Data Protection Regulation (GDPR)**

GDPR is a European Union (E.U.) general data regulation that protects the processing of E.U. citizens’ data and their right to privacy in and out of E.U. territory. Additionally, if a breach occurs and an E.U. citizen’s data is compromised, they must be informed within 72 hours of the incident.

**Explanation:** Adherence to GDPR is important for Botium Toys if they handle personal data of European Union citizens. Even though Botium Toys is not explicitly mentioned as an EU-based company, if they sell products or services to EU citizens or process their data, they need to follow GDPR rules to protect individuals' privacy rights and notify them of data breaches within 72 hours.

**Payment Card Industry Data Security Standard (PCI DSS)**

PCI DSS is an international security standard meant to ensure that organizations storing, accepting, processing, and transmitting credit card information do so in a secure environment.

**Explanation**: Botium Toys needs to adhere to PCI DSS if they store, process, or transmit credit card information. Compliance with PCI DSS ensures that credit card data is handled securely, protecting both the customers' financial information and the reputation of the organization.

**The Health Insurance Portability and Accountability Act (HIPAA)**

HIPAA is a federal law established in 1996 to protect U.S. patients' health information. This law prohibits patient information from being shared without their consent. Organizations have a legal obligation to inform patients of a breach.

**Explanation:**

**System and Organizations Controls (SOC type 1, SOC type 2)**

The SOC1 and SOC2 are a series of reports that focus on an organization's user access policies at different organizational levels. They are used to assess an organization’s financial compliance and levels of risk. They also cover confidentiality, privacy, integrity, availability, security, and overall data safety. Control failures in these areas can lead to fraud.

**Explanation:**