# Botium Toys: Scope, goals, and risk assessment report

## Scope and goals of the audit

**Scope:** The scope is defined as the entire security program at Botium Toys. This means all assets need to be assessed alongside internal processes and procedures related to the implementation of controls and compliance best practices.

**Goals:** Assess existing assets and complete the controls and compliance checklist to determine which controls and compliance best practices need to be implemented to improve Botium Toys’ security posture.

## 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.
* Storefront products available for retail sale on site and online; stored in the company’s adjoining warehouse
* Management of systems, software, and services: accounting, telecommunication, database, security, ecommerce, and inventory management
* Internet access
* Internal network
* Data retention and storage
* Legacy system maintenance: end-of-life systems that require human monitoring

## Risk assessment

### Risk description

Currently, there is inadequate management of assets. Additionally, Botium Toys does not have all of the proper controls in place and may not be fully compliant with U.S. and international regulations and standards.

### Control best practices

The first of the five functions of the NIST CSF is Identify. Botium Toys will need to dedicate resources to identify assets so they can appropriately manage them. Additionally, they will need to classify existing assets and determine the impact of the loss of existing assets, including systems, on business continuity.

### Risk score

On a scale of 1 to 10, the risk score is 8, which is fairly high. This is due to a lack of controls and adherence to compliance best practices.

### Additional comments

The potential impact from the loss of an asset is rated as medium, because the IT department does not know which assets would be at risk. The risk to assets or fines from governing bodies is high because Botium Toys does not have all of the necessary controls in place and is not fully adhering to best practices related to compliance regulations that keep critical data private/secure. Review the following bullet points for specific details:

* Currently, all Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers’ PII/SPII.
* Encryption is not currently used to ensure confidentiality of customers’ credit card information that is accepted, processed, transmitted, and stored locally in the company’s internal database.
* Access controls pertaining to least privilege and separation of duties have not been implemented.
* The IT department has ensured availability and integrated controls to ensure data integrity.
* The IT department has a firewall that blocks traffic based on an appropriately defined set of security rules.
* Antivirus software is installed and monitored regularly by the IT department.
* The IT department has not installed an intrusion detection system (IDS).
* There are no disaster recovery plans currently in place, and the company does not have backups of critical data.
* The IT department has established a plan to notify E.U. customers within 72 hours if there is a security breach. Additionally, privacy policies, procedures, and processes have been developed and are enforced among IT department members/other employees, to properly document and maintain data.
* Although a password policy exists, its requirements are nominal and not in line with current minimum password complexity requirements (e.g., at least eight characters, a combination of letters and at least one number; special characters).
* There is no centralized password management system that enforces the password policy’s minimum requirements, which sometimes affects productivity when employees/vendors submit a ticket to the IT department to recover or reset a password.
* While legacy systems are monitored and maintained, there is no regular schedule in place for these tasks and intervention methods are unclear.
* The store’s physical location, which includes Botium Toys’ main offices, store front, and warehouse of products, has sufficient locks, up-to-date closed-circuit television (CCTV) surveillance, as well as functioning fire detection and prevention systems.

**CONTROL ASSESSMENT**

ADMINISTRATIVE CONTROLS

|  |  |  |
| --- | --- | --- |
| CONTROL NAME | CONTROL TYPE AND EXPLANATION | PRIORITY |
| LEAST PRIVILEDGE | Preventative  Reduce risk and overall impact of malicious insider or compromised accounts. | HIGH |
| DISASTER RECOVERY | Corrective  Provide business continuity. | HIGH |
| PASSWORD POLICIES | Preventative  Reduce likelihood of account compromise through brute force or dictionary attack techniques. | HIGH |
| ACCESS CONTROL POLICIES | Preventative  Bolster confidentiality and integrity by defining which groups can access or modify data. | HIGH |

TECHNICAL CONTROLS

|  |  |  |
| --- | --- | --- |
| CONTROL NAME | CONTROL TYPE AND EXPLANATION | PRIORITY |
| ENCRYPTION | Deterrent  Provide confidentiality to sensitive information. | HIGH/MEDIUM |
| IDS/IPS | Detective  To detect and prevent anomalous traffic that matches a signature or rule. | HIGH |
| BACKUPS | Corrective  Restore/recover from an event | HIGH |
| PASSWORD MANAGEMENT | Preventative  Reduce password fatigue | HIGH |

**Compliance Checklist**

General Data Protection Regulation (GDPR)

The Organisation is aware and have plans in motion in adhering to GDPR because we conduct business and collect personal information from people in the EU.

Payment Card Industry Data Security Standard (PCI DSS)

The organization is aware and have plans adhere to PCI DSS because we store, accept, process, and transmit credit card information in person and online