# Internal IT Security Audit Report: Botium Toys

Date: April 10, 2025

Prepared by: Bobby Hoskins

## 1. Executive Summary

This internal audit was carried out to take a closer look at the current security practices at Botium Toys. We reviewed the company's IT-managed assets, security controls, and how well they align with important industry standards like PCI DSS, GDPR, and SOC 1/SOC 2. During our review, we identified several areas of concern, including high-risk vulnerabilities caused by missing or underdeveloped security controls.

## 2. Audit Scope and Objectives

Scope:

We looked at everything that falls under Botium Toys' security umbrella—this includes employee devices, internal networks, physical spaces like the office and warehouse, business software, and legacy systems that are still in use.

Goals:

- Identify and assess current IT-managed assets
- Complete the security controls and compliance checklist
- Highlight vulnerabilities and propose security improvements
- Improve the organization's security posture and regulatory compliance

## 3. Assets Managed by IT

- Employee equipment: laptops, desktops, smartphones, peripherals
- On-premises infrastructure and surveillance systems
- Storefront and warehouse product inventory systems
- Business software: accounting, inventory, e-commerce, telecom
- Internal network and internet services
- Legacy systems requiring manual monitoring

## 4. Risk Assessment Summary

The overall risk score is 8 out of 10, which means the risk level is considered high.

Here are the most pressing issues we found: no encryption on sensitive customer data, lack of access controls or role separation, no intrusion detection system (IDS), no backup or disaster recovery plan, and weak password practices without a password manager. These issues expose Botium Toys to serious security threats and regulatory fines.

- No encryption for customer/cardholder data
- No access control or separation of duties
- No IDS or disaster recovery plan
- Weak password practices and lack of password management
- High exposure to regulatory penalties (PCI/GDPR/SOC)

## 5. Controls Checklist Summary

| Control | Implemented? |
|---|---|
| Least Privilege | No |
| Disaster Recovery Plan | No |
| Password Policies | No |
| Separation of Duties | No |
| Firewall | Yes |
| Intrusion Detection System (IDS) | No |
| Backups | No |
| Antivirus Software | Yes |
| Legacy System Monitoring | Partial |
| Encryption | No |
| Password Management System | No |
| Physical Locks | Yes |
| CCTV Surveillance | Yes |
| Fire Detection and Prevention | Yes |

## 6. Compliance Checklist Summary

**PCI DSS:** Botium Toys is currently not compliant with PCI DSS requirements. Access control, encryption, and secure password policies need to be put in place to meet the standards.

**GDPR:** The company is partially compliant. While there are policies in place to protect data and handle breaches, the absence of encryption puts customer privacy at risk.

**SOC 1/SOC 2:** Botium Toys meets some of the requirements, like maintaining data integrity and availability. However, access to sensitive data is too open. Implementing role-based access would help meet these standards more fully.

## 7. Recommendations

Here’s what we recommend doing right away: start encrypting sensitive data, set up access controls and separation of duties, install an IDS, implement regular data backups and a disaster recovery plan, and put a strong password policy in place using a centralized manager.

- Implement encryption for sensitive customer/cardholder data
- Apply access controls based on least privilege and separation of duties
- Install and configure an Intrusion Detection System (IDS)
- Establish automated backup procedures and disaster recovery planning
- Enforce a secure password policy with a centralized password manager

Next, focus on scheduling regular maintenance for legacy systems and improving how data is organized and classified.

- Establish regular legacy system maintenance schedules
- Improve data classification and inventory processes

Over the long run, the company should conduct regular compliance audits, provide ongoing training for employees about cybersecurity, and make sure all security policies are kept up-to-date.

- Regular compliance audits
- Employee security awareness training
- Maintain and update all security policies and procedures