# Internal Security Audit Report – Botium Toys

## 1. Project Scope and Objectives

The purpose of this document is to outline the internal audit conducted for Botium Toys’ cybersecurity program.   
The audit covers asset identification, current security posture, risk assessment, and recommendations for control improvements aligned with NIST CSF best practices.

* **Scope**:

The audit scope includes all IT-managed assets, internal systems, networks, employee devices, data storage,   
and the physical store and warehouse environments.

* **Objectives**:
* Identify and classify current assets and systems.
* Assess compliance with U.S. and international regulations.
* Evaluate existing controls and policies.
* Recommend administrative, technical, and physical controls to improve posture.
* Complete a controls and compliance checklist based on industry best practices.

## 2. Current Assets Overview and Risk Assessment

The following assets were identified as part of the Botium Toys infrastructure:

* On-premises office equipment
* Employee end-user devices (laptops, phones, accessories)
* Storefront retail inventory and warehouse stock
* Internal systems (accounting, database, ecommerce, security, telecom)
* Internet access and internal networks
* Legacy systems requiring manual maintenance
* Data retention and storage

**Risk Assessment Summary:**

- Risk Score: 8/10 (High)  
- Primary Risks: Inadequate access control, lack of encryption, no backups or disaster recovery plan, weak password enforcement.  
- Potential Impacts: Compliance fines, data breaches, insider threats, business disruption.

## Controls Assessment Checklist

[ ] Yes [ •] No - Least Privilege

[ ] Yes [• ] No - Disaster recovery plans

[ ] Yes [• ] No - Password policies

[ ] Yes [• ] No - Separation of duties

[• ] Yes [ ] No - Firewall

[] Yes [ •] No - Intrusion detection system (IDS)

[ ] Yes [• ] No - Backups

[ •] Yes [ ] No - Antivirus software

[ ] Yes [ •] No - Manual monitoring, maintenance, and intervention for legacy systems

[ ] Yes [• ] No - Encryption

[ ] Yes [• ] No - Password management system

[ ] Yes [ ] No - Locks (offices, storefront, warehouse)

[ •] Yes [ ] No - Closed-circuit television (CCTV) surveillance

[ •] Yes [ ] No - Fire detection/prevention (fire alarm, sprinkler system, etc.)

## Compliance Checklist

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

[ ] Yes [ •] No - Only authorized users have access to customers’ credit card information.

[ ] Yes [• ] No - Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.

[ ] Yes [ •] No - Implement data encryption procedures to better secure credit card transaction touchpoints and data.

[ ] Yes [• ] No - Adopt secure password management policies.

**General Data Protection Regulation (GDPR)**

[ ] Yes [ ] No - E.U. customers’ data is kept private/secured.

[ ] Yes [ ] No - There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.

[ ] Yes [ ] No - Ensure data is properly classified and inventoried.

[ ] Yes [ ] No - Enforce privacy policies, procedures, and processes to properly document and maintain data.

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

[ ] Yes [ •] No - User access policies are established.

[ ] Yes [ •] No - Sensitive data (PII/SPII) is confidential/private.

[ •] Yes [ ] No - Data integrity ensures the data is consistent, complete, accurate, and has been validated.

[• ] Yes [ ] No - Data is available to individuals authorized to access it.

## Conclusion

To strengthen Botium Toys’ IT security, we recommend implementing strict access controls, using encryption for customer credit card data, installing an intrusion detection system (IDS), and developing a disaster recovery plan with regular backups. Additionally, we should enhance the password policy, establish a centralized password management system, and create a maintenance schedule for legacy systems.  
  
Best regards,  
Muhammed Afnaan  
afnaanspy@gmail.com