

# **Internal Security Audit Report: Botium Toys**

## **1. Introduction**

This internal security audit was conducted to assess Botium Toys' security posture, identify gaps, and recommend improvements. The audit follows the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and evaluates controls and compliance best practices.

---

## **2. Scope and Goals**

### **Scope:**

The audit covers the entire security program at Botium Toys, including employee equipment, internal networks, data storage, and compliance with U.S. and international security standards.

### **Goals:**

- Assess existing assets and security measures.
  - Identify missing controls and compliance gaps.
  - Provide recommendations to improve security and compliance.
- 

## **3. Current Assets Managed by IT**

- On-premises office and retail store equipment.
  - Employee devices (desktops, laptops, smartphones, etc.).
  - Storefront products (retail and online inventory).
  - Systems and software (accounting, telecommunication, security, e-commerce, etc.).
  - Internal network, data storage, and legacy system maintenance.
- 

## **4. Risk Assessment Summary**

- **Risk Score:** 8/10 (High Risk)

- **Key Issues Identified:**

- Inadequate asset management.
  - Lack of encryption for credit card data.
  - No enforcement of least privilege and separation of duties.
  - No intrusion detection system (IDS) or disaster recovery plan.
  - Weak password policies.
  - Unrestricted employee access to sensitive data.
  - No regular maintenance schedule for legacy systems.
- 





## 5. Controls and Compliance Checklist

### Controls Assessment





<u>Control</u>	<u>Implemented?</u>
Least Privilege	✗ No
Disaster Recovery Plans	✗ No
Password Policies	✓ Yes (but weak)
Separation of Duties	✗ No
Firewall	✓ Yes
Intrusion Detection System (IDS)	✗ No
Backups	✗ No
Antivirus Software	✓ Yes
Manual Monitoring for Legacy Systems	✓ Yes (but no schedule)
Encryption	✗ No
Password Management System	✗ No
Locks (Offices, Storefront, Warehouse)	✓ Yes
CCTV Surveillance	✓ Yes
Fire Detection/Prevention	✓ Yes

## Compliance Assessment





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

<u>Requirement</u>	<u>Compliant?</u>
Authorized access to credit card data	 No
Secure storage/processing of credit card data	 No
Data encryption for credit card transactions	 No
Secure password management policies	 No

### General Data Protection Regulation (GDPR)

<u>Requirement</u>	<u>Compliant?</u>
E.U. customer data protection	 No
Breach notification within 72 hours	 Yes
Proper data classification and inventory	 No
Privacy policies and enforcement	 Yes

### System and Organization Controls (SOC 1, SOC 2)

<u>Requirement</u>	<u>Compliant?</u>
User access policies	 No
PII/SPII confidentiality	 No
Data integrity	 Yes
Authorized data access	 Yes

---

## 6. Recommendations

1. **Implement Least Privilege & Separation of Duties** – Restrict access to sensitive data based on job roles.
  2. **Strengthen Password Policies & Introduce a Password Management System** – Enforce multi-factor authentication (MFA) and implement a centralized password manager.
  3. **Enable Data Encryption for Payment Processing** – Encrypt all stored and transmitted credit card information.
  4. **Deploy an Intrusion Detection System (IDS)** – Monitor and detect network anomalies.
  5. **Establish a Disaster Recovery Plan & Backup Strategy** – Implement regular, offsite backups and a tested recovery plan.
  6. **Create a Scheduled Maintenance Plan for Legacy Systems** – Ensure outdated systems do not pose security risks.
  7. **Improve GDPR Compliance** – Inventory and classify customer data, and enforce stronger privacy controls.
- 

## 7. Conclusion

Botium Toys currently has significant security gaps that need to be addressed to reduce risks and improve compliance. The company should prioritise implementing encryption, access controls, and backup strategies while strengthening password and compliance policies. By following the recommended actions, Botium Toys can enhance its cybersecurity posture and align with industry best practices.

---

### Prepared by:

Sameera Mohamed

21<sup>st</sup> March 2025