

Botium Toys Internal Security Audit

Conducted by Antonio Jones | April 2025

Botium Toys Internal Security Audit

Audit Fictional Focus Internal Security Framework NIST CSF

Simulated internal security audit report showcasing cybersecurity assessment, risk analysis, and compliance evaluation.

Jump to section:

Executive Summary

Scope & Objectives

Risk Assessment Summary

Key Findings

Existing Security Controls

Recommendations

Compliance & Framework Alignment

Controls & Compliance Checklist

Next Steps

Executive Summary

This internal audit evaluates the security posture of Botium Toys, focusing on asset inventory, data protection, access control, and compliance. Several high-risk vulnerabilities were identified, and specific mitigation steps are recommended to strengthen overall resilience.

Scope & Objectives

Scope: The audit includes employee devices, internal network infrastructure, enterprise systems (accounting, telecom, ecommerce, inventory), data retention systems, legacy systems, and physical locations (warehouse and storefront).

Objectives:

- Identify and classify all organizational assets
- Evaluate the effectiveness of current security controls
- Assess compliance with U.S. and international standards
- Provide actionable recommendations to improve security posture

Risk Assessment Summary

- **Asset Management:** Poor inventory practices; untracked assets (High – 8/10)
- **Access Control:** No least privilege enforcement or RBAC (High)
- **Data Protection:** No encryption of credit card/PII data (High)
- **Incident Detection:** No IDS/IPS in place (High)
- **Disaster Recovery:** No DR plans or backup processes (High)
- **Password Management:** Weak, outdated policies (Medium)
- **Physical Security:** Locks, CCTV, and fire systems are in place (Low)
- **Legacy Systems:** Maintained, but lacking scheduled oversight (Medium)

Key Findings

- Excessive internal access to PII and cardholder data

- No encryption of sensitive data
- No IDS/IPS or disaster recovery plans in place
- Weak password policies and legacy systems without schedules

Existing Security Controls

- Firewall configured with rule sets
- Antivirus software installed and regularly monitored
- Physical security measures including locks, CCTV, and fire prevention systems
- GDPR breach notification processes in place

Recommendations

- Implement encryption and centralized password management
- Deploy intrusion detection/prevention systems
- Establish and test disaster recovery procedures
- Enforce least privilege and asset classification

Compliance & Framework Alignment

This audit aligns with the NIST Cybersecurity Framework (CSF):

- **Identify:** Gaps in asset inventory and classification
- **Protect:** Issues with encryption, password policy, and access controls
- **Detect:** No IDS/IPS or centralized logging
- **Respond/Recover:** No DR plans or response playbooks

Standards Covered: PCI DSS, GDPR, SOC Type 1 & 2

Controls & Compliance Checklist

Controls Assessment Checklist

Control	Implemented?
Least Privilege	No
Disaster Recovery Plans	No
Password Policies	Yes (outdated)
Separation of Duties	No
Firewall	Yes
Intrusion Detection System (IDS)	No
Backups	No
Antivirus Software	Yes
Legacy System Maintenance	Partial
Encryption	No
Password Management System	No
Physical Locks	Yes
CCTV Surveillance	Yes
Fire Detection/Prevention	Yes

PCI DSS

Best Practice	Adhered?
Only authorized users access credit card info	No
Credit card info stored securely	No
Data encryption at transaction touchpoints	No
Secure password management policies	No

GDPR

Best Practice	Adhered?
E.U. customer data is secure	Yes
Breach notification within 72 hours	Yes
Proper classification & inventory of data	No
Privacy policies enforced	Yes

SOC (Type 1 & 2)



Best Practice	Adhered?
User access policies established	No
Confidentiality of PII/SPII	No
Data integrity ensured	Yes
Authorized data access maintained	Yes

IT Management Recommendations

- Implement encryption and backup procedures immediately.
- Deploy an IDS/IPS solution for real-time monitoring.
- Upgrade and enforce a strong password policy with centralized management.
- Enforce least privilege and separation of duties.
- Inventory and classify all data for better compliance.

Visuals

Visual content such as network diagrams and threat models is included below:

 Network Diagram  Threat Model

Next Steps

- Finalize visual content uploads
- Include real-world logs and sample scans
- Create downloadable PDF version of report
- Enhance interactivity using GitHub Pages or Jekyll themes