REPORT
Botium Security Audit

v1.0.0

Author:

Eldon Gabriel

July 11, 2025

TABLE OF CONTENTS

REVISION HISTORY

Version	Date	Author	Description of Changes
v1.0.0	02/15/2025	Eldon G.	Initial draft
v.1.1.0	07/11/2025	Eldon G.	Added structured sections and a conclusion

SECTION 1.0: PROJECT OVERVIEW

1.1 Scenario Summary

Botium Toys, a U.S.-based toy company, is experiencing increased cybersecurity challenges as its digital footprint expands. Concerned about regulatory and operational risk, the IT Manager initiated a security audit aligned with the NIST Cybersecurity Framework (CSF). This assessment aimed to evaluate vulnerabilities, validate compliance (PCI DSS, GDPR, SOC 1/2), and safeguard business continuity.

1.2 Assessment Objectives

The primary goal was to review Botium Toys' existing security controls to:

- Identify gaps and misconfigurations
- Validate compliance with regulatory standards
- Recommend prioritized improvements to mitigate risk

1.3 Key Areas Assessed

The following security domains were evaluated:

Control Area	Implemented (✓/✗)
Least Privilege	✗
Disaster Recovery Plans	✗
Password Policies	✗
Separation of Duties	✓
Firewall	✓
Intrusion Detection System (IDS)	✗
Backups	✓
Antivirus Software	✓
Manual Intervention for Legacy Systems	✗
Encryption	✗
Password Management System	✗
Physical Locks (Offices/Warehouse)	✓
CCTV Surveillance	✓
Fire Detection & Suppression	✓

1.4 Compliance Checklists

Payment Card Industry Data Security Standard (PCI DSS)

Best Practice	Compliant (✓/✗)
Restricted credit card access	✓
Secure handling and transmission	✓
Encryption procedures are in place	✗
Password management policy	✗

General Data Protection Regulation (GDPR)

Best Practice	Compliant (✓/✗)
E.U. data privacy and security	✓
Breach notification	✗
Data classification & inventory	✗
Enforced privacy procedures	✓

SOC 1 & SOC 2

Best Practice	Compliant (✓/✗)
User access policies established	✓
Sensitive data confidentiality	✓
Data integrity controls	✗
Data availability to authorized users	✓

1.5 Recommendations

- **Access Control**: Enforce Role-Based Access Control (RBAC) with regular access reviews to ensure effective security.
- **Password Management**: Strengthen password policies and adopt password vaulting tools.
- **Network Security**: Upgrade firewalls and deploy IDS/IPS solutions.
- **Encryption**: Implement AES-256 encryption for data in transit and at rest.
- **Disaster Recovery**: Establish a tested, up-to-date recovery plan with off-site backups.

Regulatory Compliance

- **PCI DSS:** Encrypt cardholder data and adopt stronger password practices.
- **GDPR:** Classify data, document privacy policies, and formalize breach notification.
- **SOC 2**: Enforce user access controls and validate data integrity mechanisms.

SECTION 2.0: CONCLUSION

2.1 Key Takeaways

- Critical gaps were identified in access control, encryption, and detection capabilities.
- Physical security controls were generally strong, but logical controls require immediate improvement.
- PCI DSS and SOC 2 controls are partially in place but need enhancements to meet full compliance.
- GDPR compliance shows progress but lacks formal breach response planning.

2.2 Security Implications and Recommendations

Ignoring these control gaps can cause data leaks, regulatory fines, and damage to your reputation. Focusing on access management, encryption, and monitoring lowers the risk of attacks and meets global data protection standards. Support from management and stakeholder awareness is crucial for sustaining security improvements.