Botium Toys

Conduct Security Audit Report

Prepared by: [Your Name]
Date: [Insert Date]

1. Executive Summary

Botium Toys has experienced significant growth in its online presence, expanding its customer base both within the United States and internationally. As the company scales, the IT department is under pressure to ensure its systems, processes, and data handling remain secure, compliant, and resilient. This security audit was conducted using the NIST Cybersecurity Framework (CSF) as guidance. The goal was to assess current security controls, evaluate compliance with PCI DSS, GDPR, and SOC requirements, and identify risks. The audit revealed strengths in physical security but major gaps in encryption, compliance, and disaster recovery planning.

2. Audit Scope and Goals

Scope: Review IT-managed assets, policies, controls, and compliance posture.
Goals: Identify risks and vulnerabilities, assess compliance, and provide mitigation recommendations.

3. Controls Assessment Findings

Control	In Place?
Least Privilege	No
Disaster Recovery Plans	No
Password Policies	No
Separation of Duties	No
Firewall	Yes
Intrusion Detection System (IDS)	No
Backups	No
Antivirus Software	Yes
Manual Monitoring of Legacy Systems	Yes
Encryption	No
Password Management System	No
Locks (offices, storefront, warehouse)	Yes
CCTV Surveillance	Yes
Fire Detection/Prevention	Yes

4. Compliance Assessment Findings

PCI DSS

PCI DSS Best Practice	In Place?
Only authorized users access cardholder data	No
Credit card data securely stored/processed	No
Encryption for credit card data	No
Secure password policies	No

GDPR

GDPR Best Practice	In Place?
EU data kept private/secure	No
Breach notification plan (72 hrs)	Yes
Data properly classified/inventoried	No
Privacy policies enforced	Yes

SOC (Type 1 & 2)

SOC Best Practice	In Place?
User access policies established	No
Sensitive data kept confidential	No
Data integrity maintained	Yes
Data availability ensured	Yes

5. Recommendations

High Priority:
- Implement encryption for credit card and customer data.
- Develop and test a disaster recovery plan with backups.
- Adopt stronger password policies and deploy a password management system.
- Enforce least privilege and separation of duties.
- Deploy IDS/IPS for proactive monitoring.

Medium Priority:
- Classify and inventory all customer and employee data.
- Assign a Data Protection Officer (DPO) for GDPR compliance.
- Provide security awareness training for all staff.
- Secure software development for the online storefront.

Long-Term:
- Work toward SOC 2 certification.
- Implement centralized SIEM logging.
- Conduct periodic policy reviews as business scales.

6. Conclusion

Botium Toys has foundational security controls in place but lacks critical elements to safeguard sensitive data, ensure compliance, and support global operations. Immediate action is required to close compliance gaps, reduce risk exposure, and protect customer trust. Implementing the recommended measures will enable Botium Toys to strengthen its cybersecurity posture and confidently support its expanding online presence.