Botium Toys - Internal IT Security Audit

Controls and Compliance Checklist

Prepared as part of an internal IT audit conducted using the NIST Cybersecurity Framework (CSF). This document assesses Botium Toys' current controls and compliance posture against the scope, goals, and risk assessment findings, and provides recommendations to reduce risk.

1. Audit Scope and Goals

Scope: The entire security program at Botium Toys, including employee equipment/devices, the internal network, and all managed systems.

Goal: Assess existing assets and complete the controls and compliance checklist to determine which controls and best practices need to be implemented to improve Botium Toys' security posture.

2. Controls Assessment Checklist

Does Botium Toys currently have this controls in place?

Item	Yes/No	Evidence from Scenario
Least Privilege	No	Access controls pertaining to least privilege have not been implemented
Disaster recovery plans	No	There are no disaster recovery plans currently in place
Password policies	Yes	Although a password policy exists is weak (It exists, even though it is weak).
Separation of duties	No	Separation of duties has not been implemented.
Firewall	Yes	The IT department has a firewall.
Intrusion Detection System (IDS)	No	The IT department has not installed an Intrusion Detection System (IDS)
Backups	No	The company does not have backups of critical data.
Antivirus software	Yes	Antivirus software is installed and monitored regularly.
Manual monitoring, maintenance, and intervention for legacy systems	Yes	Legacy systems are monitored and maintained although there is no regular schedule.
Encryption	No	Encryption is not currently used.
Password management system	No	There is no centralized password management system.
Locks (offices, storefront, warehouses)	Yes	The store's physical location has sufficient locks.
Close-circuit television (CCTV) surveillance	Yes	Up-to-date CCTV surveillance
Fire detection/prevention	Yes	Functioning fire detection and prevention systems.

3. Compliance Checklist

Payment Card Industry Data Security Standard (PCI DSS)

Does Botium Toys currently adhere to this compliance best practices?

Item	Yes/No	Evidence
Only authorized users have access to customers' credit card information.	No	All employees currently have access to stored data and may access cardholder data.
Credit card information is stored, accepted, processed, and transmitted internally in a secure environment.	No	Lack of least privilege and no encryption means the environment is not adequately secured.
Implement data encryption procedures.	No	Encryption is not currently used.
Adopt secure password management policies.	No	Password policy is weak and there is no centralized password management system.

General Data Protection Regulation (GDPR)

Does Botium Toys currently adhere to this compliance best practices?

Item	Yes/No	Evidence
E.U. customers' data is kept private/secured.	No	Customers' data lacks encryption and proper access controls.
72-hour breach notification plan.	Yes	Sufficient for the scenario but insufficient for the actual GDPR – Article 33 and 34 which required further attention and more rigorous compliance.
Ensure data is properly classified and inventoried.	No	The risk assessment states inadequate asset management and recommends identifying and classifying assets.
Enforce privacy policies, procedures, and processes to properly document and maintain data.	Yes	The scenario states privacy policies, procedures, and processes have been developed and enforced.

System and Organization Control (SOC Type 1 /SOC Type 2)

Does Botium Toys currently adhere to this compliance best practices?

Item	Yes/No	Evidence
User access policies are established.	No	Least privilege and separation of duties are not implemented, and all employees have broad access.
Sensitive data (PII/SPII) is confidential/private.	No	Encryption is absent and excessive user access exists.
Data integrity is ensured.	Yes	The IT department has implemented integrity controls.

Data is available to authorized individuals.	Yes	The scenario states the IT department has ensured availability controls.

4. Executive Summary

Botium Toys' overall risk score is 8/10 — **high** — driven primarily by missing technical and administrative controls rather than physical controls, which are largely in place (locks, CCTV, fire detection).

- **Strengths:** Firewall, antivirus, physical security controls, GDPR breach-notification plan and privacy policy enforcement, and data integrity/availability controls are all in place.
- **Gaps:** No least privilege or separation of duties, no encryption of stored/transmitted cardholder data, no IDS, no backups or disaster recovery plan, no centralized password management, and no formal data classification/inventory process.
- **Compliance exposure:** Botium Toys does not fully comply with **PCI DSS requirements, GDPR, or SOC best practices.** The most significant concerns include unrestricted employee access to customer payment information, unencrypted credit card data, weak password controls, and an inadequate asset inventory and classification process. These deficiencies create significant financial, legal, and operational risks, particularly because the company processes online payments.

Part 3 – Recommendations (Optional)

Below is a prioritized checklist to help address the identified vulnerabilities. These recommendations should be the organization's highest priorities to reduce the likelihood of data breaches, maintain business continuity, protect customer information, and strengthen compliance with applicable security standards and regulatory requirements.

Priority 1 (Critical)

- Implement least privilege and role-based access control (RBAC).
- Implement separation of duties.
- Encrypt all stored, transmitted, and processed payment card information.
- Install an Intrusion Detection System (IDS).
- Create and regularly test backup procedures.
- Develop and document a disaster recovery plan.

Priority 2 (High)

- Deploy a centralized password management system.
- Strengthening password policy requirements:

    - Minimum 8–12 characters
    - Uppercase and lowercase letters
    - Numbers
    - Special characters
    - Multi-factor authentication (MFA), where possible
- Conduct a complete asset inventory and classify all critical assets according to the NIST Cybersecurity Framework (Identify function).

Priority 3 (Medium)

- Establish scheduled maintenance procedures for legacy systems.
- Review employee permissions regularly.
- Perform periodic security awareness training.
- Conduct routine internal audits and vulnerability assessments.
- Continue maintaining firewalls, antivirus, CCTV, locks, and fire prevention systems.