Internal Security Audit Report

Organization Name: Botium Toys
Audit Date: 27/2/2025
Auditor(s): Rina Razali

---

1. Executive Summary

This internal security audit assesses the organization's adherence to security controls and compliance requirements. The objective is to identify vulnerabilities, ensure regulatory compliance, and recommend security improvements.

---

2. Compliance and Controls Checklist

2.1 Controls assessment checklist

Administrative Control

Control	Compliance Status	Notes/Findings
Principle of least privilege in place	❌ Non-compliant	Currently, all Botium Toys employees have access to internally stored data. Principle of least privilege have not been implemented
Separation of duties are in place	❌ Non-compliant	Separation of duties have not been implemented.
Password policy exists	❌ Non-compliant	Although a password policy exists, its requirements are nominal and not in line with current minimum password complexity requirements (e.g., at least eight characters, a combination of letters and at least one number; special characters).
Password management system	❌ Non-compliant	There is no centralized password management system that enforces the password policy's minimum requirements, which sometimes affects productivity when employees/vendors submit a ticket to the IT department to recover or reset a password.

Technical control

Control	Compliance Status	Notes/Findings
Firewall are in place	✅ Compliant	The IT department has a firewall that blocks traffic based on an appropriately defined set of security rules.
IDS are actively monitoring traffic	❌ Non-compliant	The IT department has not installed an intrusion detection system (IDS).
Antivirus is installed	✅ Compliant	Antivirus software is installed and monitored regularly by the IT department
Data is encrypted	❌ Non-compliant	Encryption is not currently used to ensure confidentiality of customers' credit card information that is accepted, processed, transmitted, and stored locally in the company's internal database.
Backup and disaster recovery plans are in place	❌ Non-compliant	There are no disaster recovery plans currently in place, and the company does not have backups of critical data.
Manual monitoring, maintenance, and intervention for legacy systems	❌ Non-compliant	While legacy systems are monitored and maintained, there is no regular schedule in place for these tasks and intervention methods are unclear.

Physical Control

Control	Compliance Status	Notes/Findings
Locks	✅ Compliant	The store's physical location, which includes Botium Toys' main offices, store front, and warehouse of products, has sufficient locks, up-to-date closed-circuit television (CCTV) surveillance, as well as functioning fire detection and prevention systems.
CCTVs	✅ Compliant	
Fire detection and prevention systems	✅ Compliant	

2.2 Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

Compliance	Compliance Status	Notes/Findings
Only authorized users have access to customers' credit card information.	❌ Non-compliant	Currently, all Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers' PII/SPII.
Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.	❌ Non-compliant	Encryption is not currently used to ensure confidentiality of customers' credit card information that is accepted, processed, transmitted, and stored locally in the company's internal database.
Implement data encryption procedures to better secure credit card transaction touchpoints and data.	❌ Non-compliant	No encryption in place to ensure the transactions is secured
Adopt secure password management policies.	❌ Non-compliant	Current password policy is not in line with current minimum password complexity requirements (e.g., at least eight characters, a combination of letters and at least one number; special characters).

General Data Protection Regulation (GDPR)

Compliance	Compliance Status	Notes/Findings
E.U. customers' data is kept private/secured.	❌ Non-compliant	Encryption is not used to protect the confidentiality of the data
There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.	✅ Compliant	The IT department has established a plan to notify E.U. customers within 72 hours if there is a security breach.

Ensure data is properly classified and inventoried.	❌ Non-compliant	Data has been inventoried and listed but not classified.
Enforce privacy policies, procedures, and processes to properly document and maintain data.	✅ Compliant	

System and Organizations Controls (SOC type 1, SOC type 2)

Compliance	Compliance Status	Notes/Findings
User access policies are established.	❌ Non-compliant	Access controls pertaining to least privilege and separation of duties have not been implemented.
Sensitive data (PII/SPII) is confidential/private.	❌ Non-compliant	Currently, all Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers' PII/SPII
Data integrity ensures the data is consistent, complete, accurate, and has been validated.	✅ Compliant	The IT department has ensured availability and integrated controls to ensure data integrity.
Data is available to individuals authorized to access it.	❌ Non-compliant	Currently, all employees have access to the data and it needs to only be made available to those who are authorized to have access.

3. Findings & Recommendations

High-Risk Issue #1: Weak Password Policies and Absence of Centralized Password Management System

Recommendations:

✔ Enforce a strong password policy (minimum 12 characters, mix of upper/lowercase letters, numbers, and special characters).
✔ Deploy a Centralized Password Management System (e.g., enterprise password vaults like CyberArk, LastPass, or Bitwarden) to enforce consistent password policies across all systems.
✔ Require the use of Password Managers for employees to securely store and manage credentials.
✔ Disable password reuse and enforce expiration policies to mitigate password-related risks.

High-Risk Issues #2: Lack of Proper Access Control for Sensitive Data

Recommendations:

✔ Apply the Principle of Least Privilege (PoLP) in order to restrict access based on job responsibilities.

✔ Implement a formal Separation of Duties (SoD) policy to ensure no single individual has end-to-end control over critical processes.

✔ Conduct quarterly access reviews to remove unnecessary or outdated privileges.

High-Risk Issues #2: Absence of Encryption for Sensitive Data

Recommendations:

✔ Enforce encryption to ensure confidentiality of customers' credit card information that is accepted, processed, transmitted, and stored locally in the company's internal database.

✔ Using industry-standard encryption algorithms such as Advanced Encryption Standard (AES) with a key size of at least 256 bits for encrypting credit card information.

✔ Encrypt Data in Transit and at Rest.

✔ Implement Proper Key Management.

✔ Train employees on the importance of encryption and how to handle sensitive data securely.

High-Risk Issues #3: Absence of Backups for Critical Data

Recommendations:

✔ Implement a backup strategy with daily incremental and weekly full backups of critical systems.

✔ Secure offsite or cloud backups with encryption.

✔ Regular backup testing and restoration drills to verify data integrity.

Medium-Risk Issue: Absence of Intrusion Detection System (IDS)

Recommendations:

✔ Deploy an Intrusion Detection System (IDS) to monitor network traffic for suspicious activities and threats.

✔ Implement host-based IDS (HIDS) for servers and network-based IDS (NIDS) for perimeter security.

✔ Integrate IDS with Security Information and Event Management (SIEM) for centralized monitoring.

Low-Risk Issues #1: Lack of Structured Schedule for Manual Monitoring, Maintenance, and Intervention for Legacy Systems

Recommendations:

✓ Establish a structured schedule and clear intervention guidelines for legacy system monitoring, by having a regular maintenance & monitoring schedule.

Low-Risk Issues #2: Absence of a Disaster Recovery (DR) Plan

Recommendations:

✓ Develop and document a Disaster Recovery (DR) Plan with Defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).
✓ Develop A Business Continuity Plan (BCP) for operational resilience.

---

4. Conclusion

Overall, the audit identified key areas of compliance and gaps requiring remediation. Implementing the recommended actions will improve security posture and compliance alignment.