Botium Toys: Detailed Internal Security Audit Report

# Introduction

Botium Toys is a small U.S.-based company specializing in the design, manufacture, and sale of toys. Operating from a single location that functions as an office, storefront, and warehouse, Botium Toys has experienced increasing demand from both domestic and international markets, particularly through its online platform. To support ongoing growth, the IT department is responsible for securing the company's infrastructure, maintaining regulatory compliance, and preparing for future expansion. An internal audit was conducted to evaluate Botium Toys’ current security controls and compliance with applicable standards. The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) served as the foundation for this audit.

# Audit Scope and Goals

The internal audit encompassed all IT-managed assets, including the company’s website, customer databases, payment systems, internal network infrastructure, and physical security systems. The primary objectives of the audit were to:

* Assess current security controls
* Identify gaps or weaknesses in compliance and control implementation
* Recommend improvements to reduce risk and align with applicable regulatory standards

# Methodology

The audit was conducted using the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). This process included a review of Botium Toys’ risk assessment, evaluation of current control implementations, and assessment of adherence to industry-standard compliance practices such as Payment Card Industry Data Security Standard (PCI DSS), General Data Protection Regulation (GDPR), and System and Organizations Controls (SOC Type 1 and 2).

# Controls Assessment Summary

The following controls were evaluated to determine whether Botium Toys currently has each in place. Each control was marked 'Yes' or 'No' based on internal documentation, interviews with IT staff, and system review. Refer to the checklist below for the full evaluation of each control.

# Compliance Assessment Summary

Compliance best practices were assessed using three key standards:

* Payment Card Industry Data Security Standard (PCI DSS)
* General Data Protection Regulation (GDPR)
* System and Organizations Controls (SOC Type 1 and 2)

Botium Toys shows partial adherence across each compliance area. Detailed adherence information is provided in the checklists below.

## Controls Assessment Checklist

|  |  |
| --- | --- |
| Control | Implemented (Yes/No) |
| Least Privilege | Yes |
| Disaster recovery plans | No |
| Password policies | Yes |
| Separation of duties | Yes |
| Firewall | Yes |
| Intrusion detection system (IDS) | No |
| Backups | Yes |
| Antivirus software | Yes |
| Manual monitoring, maintenance, and intervention for legacy systems | No |
| Encryption | Yes |
| Password management system | No |
| Locks (offices, storefront, warehouse) | Yes |
| Closed-circuit television (CCTV) surveillance | Yes |
| Fire detection/prevention (fire alarm, sprinkler system, etc.) | No |

## Compliance Checklist

### Payment Card Industry Data Security Standard (PCI DSS)

|  |  |
| --- | --- |
| Best Practice | Adhered (Yes/No) |
| Only authorized users have access to customers’ credit card information. | Yes |
| Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment. | Yes |
| Implement data encryption procedures to better secure credit card transaction touchpoints and data. | Yes |
| Adopt secure password management policies. | No |

### General Data Protection Regulation (GDPR)

|  |  |
| --- | --- |
| Best Practice | Adhered (Yes/No) |
| E.U. customers’ data is kept private/secured. | Yes |
| There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach. | No |
| Ensure data is properly classified and inventoried. | No |
| Enforce privacy policies, procedures, and processes to properly document and maintain data. | Yes |

### System and Organizations Controls (SOC Type 1, SOC Type 2)

|  |  |
| --- | --- |
| Best Practice / Statement | Adhered / Response |
| User access policies are established. | Yes |
| Sensitive data (PII/SPII) is confidential/private. | Yes |
| Data integrity ensures the data is consistent, complete, accurate, and has been validated. | Yes |
| Data is available to individuals authorized to access it. | Yes |

# Conclusion

Botium Toys has taken an important first step in strengthening its IT security and regulatory compliance by conducting this internal audit. Addressing the identified gaps will significantly improve the company’s ability to manage risk, protect customer data, and ensure the continuity of business operations as the company continues to grow.

# Recommendations

* Develop and document a disaster recovery plan to ensure resilience during unexpected outages or disasters.
* Implement an intrusion detection system (IDS) to detect and respond to unauthorized access attempts.
* Establish a formal password management system to support policy enforcement.
* Automate monitoring and maintenance for legacy systems to reduce risk and increase efficiency.
* Create a GDPR-compliant breach notification process to notify EU customers within 72 hours.
* Improve data classification and inventory practices to enhance visibility and accountability.
* Promote the adoption of secure password management practices aligned with PCI DSS.