

# Internal Security Audit Report: Botium Toys

April 5, 2025

## Controls and Compliance Checklist

### Controls Assessment Checklist

Control	Yes	No	Reason
Least Privilege	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Botium Toys does not have access controls in place. Lack of least privilege and separation of duties.
Disaster Recovery Plans	<input type="checkbox"/>	<input checked="" type="checkbox"/>	There are no disaster recovery plans in place. Business continuity is at risk.
Password Policies	<input type="checkbox"/>	<input checked="" type="checkbox"/>	The password policy is not in line with current requirements. The policy does not meet modern complexity standards.
Separation of Duties	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Separation of duties has not been implemented. Insider threats or compromised accounts could occur.
Firewall	<input checked="" type="checkbox"/>	<input type="checkbox"/>	A firewall is in place to block unauthorized traffic. Security is ensured with a defined set of rules.
Intrusion Detection System (IDS)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	No IDS is currently installed. Lack of real-time detection for malicious activity.
Backups	<input type="checkbox"/>	<input checked="" type="checkbox"/>	No backup system is currently in place. Critical data is at risk of being lost.

(Continued from previous page)			
Control	Yes	No	Reason
Antivirus Software	✓	<input type="checkbox"/>	Antivirus software is installed and monitored. Malware protection is actively managed.
Manual Monitoring, Maintenance, and Intervention for Legacy Systems	<input type="checkbox"/>	✓	Legacy systems are monitored but without a regular schedule. Regular maintenance is required for legacy systems.
Encryption	<input type="checkbox"/>	✓	No encryption is used for sensitive data. Sensitive data, including credit card information, is unprotected.
Password Management System	<input type="checkbox"/>	✓	No centralized password management system. Password policy enforcement is difficult.
Locks (Offices, Storefront, Warehouse)	✓	<input type="checkbox"/>	Adequate locks are in place for physical security. Physical security is in place for important areas.
Closed-Circuit Television (CCTV) Surveillance	✓	<input type="checkbox"/>	CCTV is in place for physical security. Provides surveillance to detect unauthorized access.
Fire Detection/Prevention (Fire Alarm, Sprinkler System, etc.)	✓	<input type="checkbox"/>	Fire detection and prevention systems are functional. Prevents fire damage through alarms and sprinklers.

## Compliance Checklist

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

Best Practice	Yes	No	Reason
Only authorized users have access to customers' credit card information.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	All employees have access to sensitive data. Access to credit card data is not restricted.
Credit card information is stored, accepted, processed, and transmitted in a secure environment.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	No encryption is used to secure credit card information. Cardholder data is stored without proper security measures.
Implement data encryption procedures to secure credit card transaction touchpoints and data.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	No encryption is implemented for credit card data. Sensitive data is not encrypted during transmission or storage.
Adopt secure password management policies.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	The password policy does not meet the necessary standards. Weak password policies make it easier for attackers to compromise accounts.

### General Data Protection Regulation (GDPR)

Best Practice	Yes	No	Reason
E.U. customers' data is kept private/secured.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	The company does not currently use encryption to better ensure the confidentiality of customers' financial information.
There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	A breach notification plan is in place. GDPR compliance ensures timely breach notification.
Ensure data is properly classified and inventoried.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	No formal classification or inventory process is in place. Data classification and inventory need formal procedures.

(Continued from previous page)			
Best Practice	Yes	No	Reason
Enforce privacy policies, procedures, and processes to properly document and maintain data.	✓	<input type="checkbox"/>	Privacy policies and processes are enforced. Data handling complies with privacy requirements.

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

Best Practice	Yes	No	Reason
User access policies are established.	<input type="checkbox"/>	✓	Access control policies are not defined. Lack of least privilege and access controls for users.
Sensitive data (PII/SPII) is confidential/private.	<input type="checkbox"/>	✓	Insufficient controls for sensitive data. Sensitive customer data is at risk of exposure.
Data integrity ensures the data is consistent, complete, accurate, and validated.	✓	<input type="checkbox"/>	Data integrity is actively managed by the IT department. IT department ensures that data is accurate and complete.
Data is available to individuals authorized to access it.	<input type="checkbox"/>	✓	While data is available to all employees, authorization needs to be limited to only the individuals who need access to it to do their jobs.

## Recommendations

Multiple controls need to be implemented to improve Botium Toys' security posture and better ensure the confidentiality of sensitive information, including: Least Privilege, disaster recovery plans, password policies, separation of duties, an IDS, ongoing legacy system management, encryption, and a password management system.

To address gaps in compliance, Botium Toys needs to implement controls such as Least Privilege, separation of duties, and encryption. The company also needs to properly classify assets, to identify additional controls that may need to be implemented to improve their security posture and better protect sensitive information.

By addressing these issues promptly, Botium Toys can improve its security posture and meet necessary regulatory requirements.