Internal Security Audit Report: Botium Toys

March 27, 2025

Controls and Compliance Checklist

Controls Assessment Checklist

Control	Yes	No	Reason
Least Privilege	☐	✓	Botium Toys does not have access controls in place. Lack of least privilege and separation of duties.
Disaster Recovery Plans	☐	✓	There are no disaster recovery plans in place. Business continuity is at risk.
Password Policies	☐	✓	The password policy is not in line with current requirements. The policy does not meet modern complexity standards.
Separation of Duties	☐	✓	Separation of duties has not been implemented. Insider threats or compromised accounts could occur.
Firewall	✓	☐	A firewall is in place to block unauthorized traffic. Security is ensured with a defined set of rules.
Intrusion Detection System (IDS)	☐	✓	No IDS is currently installed. Lack of real-time detection for malicious activity.
Backups	☐	✓	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	✓	☐	Antivirus software is installed and monitored. Malware protection is actively managed.
Manual Monitoring, Maintenance, and Intervention for Legacy Systems	☐	✓	Legacy systems are monitored but without a regular schedule. Regular maintenance is required for legacy systems.
Encryption	☐	✓	No encryption is used for sensitive data. Sensitive data, including credit card information, is unprotected.
Password Management System	☐	✓	No centralized password management system. Password policy enforcement is difficult.
Locks (Offices, Storefront, Warehouse)	✓	☐	Adequate locks are in place for physical security. Physical security is in place for important areas.
Closed-Circuit Television (CCTV) Surveillance	✓	☐	CCTV is in place for physical security. Provides surveillance to detect unauthorized access.
Fire Detection/Prevention (Fire Alarm, Sprinkler System, etc.)	✓	☐	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.	☐	✓	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.	☐	✓	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.	☐	✓	No encryption is implemented for credit card data. Sensitive data is not encrypted during transmission or storage.
Adopt secure password management policies.	☐	✓	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.	✓	☐	Privacy policies and procedures are enforced. E.U. customer data is well protected.
There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.	✓	☐	A breach notification plan is in place. GDPR compliance ensures timely breach notification.
Ensure data is properly classified and inventoried.	☐	✓	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.	✓	☐	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.	☐	✓	Access control policies are not defined. Lack of least privilege and access controls for users.
Sensitive data (PII/SPII) is confidential/private.	☐	✓	Insufficient controls for sensitive data. Sensitive customer data is at risk of exposure.
Data integrity ensures the data is consistent, complete, accurate, and validated.	✓	☐	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.	✓	☐	Data access policies are in place for authorized individuals. Only authorized individuals can access sensitive data.

Recommendations

Given the identified risks and current lack of essential controls and compliance best practices, the following recommendations should be communicated to the IT manager:

- **Implement Least Privilege and Separation of Duties**: Introduce role-based access controls to ensure only authorized personnel have access to sensitive data.
- **Establish Disaster Recovery and Backup Plans**: Develop and implement disaster recovery plans, including regular backups of critical data to ensure business continuity in case of a disaster.
- **Strengthen Password Management**: Adopt a centralized password management system that enforces secure password policies and facilitates easier management.
- **Install Intrusion Detection Systems (IDS)**: Implement an IDS to detect and respond to potential malicious activity within the network.
- **Encrypt Sensitive Data**: Immediately implement encryption measures to secure sensitive customer data, including credit card information and personal data.
- **Adopt PCI DSS Compliance Practices**: Ensure that PCI DSS requirements, such as secure storage and encryption of credit card information, are fully implemented.
- **Ensure GDPR Compliance**: Formalize the classification and inventory process for customer data and ensure consistent enforcement of privacy practices.

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