Controls and Compliance Checklist

Final Security Audit Report – Botium Toys

Date: 08/16/2025
Auditor: Victor Accioly
Audit Scope: The entire security program at Botium Toys, including employee equipment, IT devices, internal network, systems, software, services, physical store, and warehouse inventory.

1. Audit Objectives

1. Assess Botium Toys' existing assets.
2. Complete the controls and compliance checklist.
3. Determine which controls and compliance best practices need to be implemented to improve the company's security posture.

2. Asset Assessment

- **IT-managed equipment:** desktops, laptops, smartphones, headsets, cables, keyboards, mice, docking stations, surveillance cameras.
- **Store products:** available for in-store and online sale; stored in the warehouse.
- **Systems and software:** accounting, telecommunications, databases, security, e-commerce, inventory management.
- **Network and connectivity:** internet access, internal network.
- **Data retention and storage.**
- **Legacy systems:** manually monitored, no formal maintenance schedule.

3. Risk Assessment

- **Risk Description:** Inadequate asset management and missing some security controls, potentially causing non-compliance with national and international regulations.

- **Risk Score:** 8/10 (high).
- **Potential Impact:** Medium for asset loss, high for regulatory and financial risks.

Specific Findings:

- All employees have access to internal data, including potentially customers' PII/SPII.
- Credit card data is not encrypted.
- Least privilege and separation of duties controls are not implemented.
- Firewall and antivirus are active; data integrity is maintained.
- IDS is not installed; no disaster recovery plans or critical data backups.
- Password policy exists but is nominal; no centralized password management system.
- Legacy systems are monitored without a formal schedule.
- Physical security is adequate: locks, CCTV, and fire detection/prevention systems are functional.

Controls assessment checklist

Yes	No	Control	*Explanation*
☐	☑	Least Privilege	*Not currently enforced; all employees have unrestricted access to internal data.*
☐	☑	Disaster recovery plans	*No disaster recovery strategy is in place; establishing one is critical for ensuring business continuity.*
☐	☑	Password policies	*Existing password requirements are minimal and may allow unauthorized access via employee devices or internal network*

☐	☑	Separation of duties	*Not implemented; critical operations are concentrated, increasing the risk of errors or misuse.*
☑	☐	Firewall	*Firewall is active and configured with rules to appropriately manage network traffic.*
☐	☑	Intrusion detection system (IDS)	*IDS is not implemented; adding one would help detect and respond to potential threats.*
☐	☑	Backups	*Critical data is not regularly backed up; implementing backups is essential to maintain continuity after an incident.*
☑	☐	Antivirus software	*Antivirus solutions are installed and actively monitored by the IT team.*
☐	☑	Manual monitoring, maintenance, and intervention for legacy systems	*Legacy systems are monitored, but no formal schedule or procedures exist, increasing potential risk.*
☐	☑	Encryption	*Sensitive data is not encrypted; implementing encryption would enhance confidentiality and data protection.*
☐	☑	Password management system	*No centralized system exists; implementing one would improve security and reduce time spent on password recovery.*

☑	☐	Locks (offices, storefront, warehouse)	*Physical locks are in place and adequate for securing premises.*
☑	☐	Closed-circuit television (CCTV) surveillance	*Closed-circuit surveillance is installed and operational.*
☑	☐	Fire detection/prevention (fire alarm, sprinkler system, etc.)	*Fire alarms and sprinkler systems are installed and functioning properly.*

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice	***Explanation***
☐	☑	Only authorized users have access to customers' credit card information.	*Currently, all employees have access to the company's internal data.*
☐	☑	Credit card information is accepted, processed, transmitted, and stored internally, in a secure environment.	*Data is stored internally, but without encryption, posing confidentiality risks.*
☐	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.	Encryption is not implemented; securing transaction points and stored data is recommended.
☐	☑	Adopt secure password management policies.	*Password policies are basic, and no management system exists, increasing vulnerability.*

General Data Protection Regulation (GDPR)

Yes	No	Best practice	*Explanation*
☐	☑	E.U. customers' data is kept private/secured.	*Sensitive data is not encrypted, creating potential privacy risks.*
☑	☐	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.	*A notification plan exists and aligns with GDPR requirements.*
☐	☑	Ensure data is properly classified and inventoried.	*Assets are inventoried but not formally classified by sensitivity or risk.*
☑	☐	Enforce privacy policies, procedures, and processes to properly document and maintain data.	*Policies and procedures exist and are enforced among IT staff and employees as needed.*

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

Yes	No	Best practice	*Explanation*
☐	☑	User access policies are established.	*Least Privilege and separation of duties are not applied; all employees have full access to data.*
☐	☑	Sensitive data (PII/SPII) is confidential/private.	*Encryption is not in place to safeguard confidential information.*
☑	☐	Data integrity ensures the data is consistent, complete, accurate, and has been validated.	*Measures to maintain consistency, accuracy, and completeness of data are in place.*

☐	☑	Data is available to individuals authorized to access it.	*Data is accessible to all employees; access should be limited to those with a legitimate business need.*

---

6. Recommendations

1. Implement least privilege access controls and separate critical duties.
2. Develop disaster recovery plans and establish regular data backups.
3. Install an Intrusion Detection System (IDS).
4. Encrypt credit card and sensitive customer data.
5. Update password policies to meet modern complexity standards and implement a centralized password management system.
6. Formalize monitoring and maintenance schedules for legacy systems.
7. Classify and inventory all assets for better management and risk prioritization.
8. Regularly review PCI DSS, GDPR, and SOC compliance.

---

7. Conclusion

Botium Toys has basic physical security and IT measures (firewall, antivirus, data integrity).
However, there are **significant gaps** in critical IT controls, encryption, backups, privilege management, and compliance with PCI DSS, GDPR, and SOC standards.
Implementing the above recommendations will **significantly reduce risk, improve security posture, and ensure regulatory compliance**.