Controls and compliance checklist

To complete the controls assessment checklist, refer to the information provided in the scope, goals, and risk assessment report. For more details about each control, including the type and purpose, refer to the control categories document.

Then, select “yes” or “no” to answer the question: *Does Botium Toys currently have this control in place?*

Controls assessment checklist

Yes	No	Control
☐	☑	Least Privilege
☐	☑	Disaster recovery plans
☐	☑	Password policies
☐	☑	Separation of duties
☑	☐	Firewall
☐	☑	Intrusion detection system (IDS)
☐	☑	Backups
☑	☐	Antivirus software
☐	☑	Manual monitoring, maintenance, and intervention for legacy systems
☐	☑	Encryption
☐	☑	Password management system
☑	☐	Locks (offices, storefront, warehouse)
☑	☐	Closed-circuit television (CCTV) surveillance

☑	☐	Fire detection/prevention (fire alarm, sprinkler system, etc.)

To complete the compliance checklist, refer to the information provided in the scope, goals, and risk assessment report. For more details about each compliance regulation, review the controls, frameworks, and compliance reading.

Then, select "yes" or "no" to answer the question: *Does Botium Toys currently adhere to this compliance best practice?*

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice
☐	☑	Only authorized users have access to customers' credit card information.
☐	☑	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.
☐	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.
☐	☑	Adopt secure password management policies.

General Data Protection Regulation (GDPR)

Yes	No	Best practice
☐	☑	E.U. customers' data is kept private/secured.
☑	☐	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.
☐	☑	Ensure data is properly classified and inventoried.

☑	☐	Enforce privacy policies, procedures, and processes to properly document and maintain data.

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

Yes	No	Best practice
☐	☑	User access policies are established.
☐	☑	Sensitive data (PII/SPII) is confidential/private.
☑	☐	Data integrity ensures the data is consistent, complete, accurate, and has been validated.
☐	☑	Data is available to individuals authorized to access it.

This section is *optional* and can be used to provide a summary of recommendations to the IT manager regarding which controls and/or compliance best practices Botium Toys needs to implement, based on the risk posed if not implemented in a timely manner.

Recommendations (optional): In this section, provide recommendations, related to controls and/or compliance needs, that your IT manager could communicate to stakeholders to reduce risks to assets and improve Botium Toys' security posture.

Overview

Botium Toys faces significant security and compliance risks due to inadequate asset management, insufficient controls, and non compliance with critical regulatory requirements. To strengthen its security posture and mitigate risks, the IT manager should communicate the following key recommendations to stakeholders.

1. Implement Robust Access Controls

Current Issue: All employees have access to internally stored data, including cardholder data and customers' Personally Identifiable Information (PII)/Sensitive PII (SPII).

Recommendation:

- Enforce **least privilege access** to restrict data access to only those who require it for their job functions.
- Implement **role based access control (RBAC)** to separate duties and reduce the risk of unauthorized access.
- Enable **multi factor authentication (MFA)** for all employees accessing sensitive systems and data.

Compliance Impact: Aligns with PCI DSS and General Data Protection Regulation (GDPR) requirements.

2. Strengthen Data Encryption Measures

Current Issue: Customer credit card information is not encrypted during processing, transmission, or storage.

Recommendation:

- Deploy **end to end encryption (E2EE)** to protect customer payment data during transactions.
- Utilize **encryption** for storing sensitive customer information within databases.
- Enforce **Transport Layer Security (TLS) 1.2+** for secure data transmission.

Compliance Impact: Achieves compliance with PCI DSS and GDPR data protection standards.

3. Deploy an Intrusion Detection System (IDS)

Current Issue: No IDS is in place to monitor potential security breaches.

Recommendation:

- Implement an **intrusion detection and prevention system (IDPS)** to monitor and respond to suspicious activity.
- Conduct **regular penetration testing** to identify and address vulnerabilities proactively.

Compliance Impact: Enhances compliance with NIST CSF's Detect and Respond functions.

4. Develop a Comprehensive Disaster Recovery and Backup Plan

Current Issue: No disaster recovery plan or data backup strategy is currently in place.

Recommendation:

- Establish an **automated backup system** for critical data with offsite and cloud redundancy.
- Develop and document a **disaster recovery plan (DRP)** that includes roles, responsibilities, and recovery time objectives (RTOs).
- Conduct **regular disaster recovery drills** to ensure preparedness.

Compliance Impact: Aligns with industry best practices and reduces business continuity risks.

5. Strengthen Password Policies and Management

Current Issue: The current password policy is weak, and there is no centralized password management system.

Recommendation:

- Enforce **complex password policies** (minimum 8 characters, mix of uppercase/lowercase letters, numbers, and symbols).
- Implement a **centralized password management system** to reduce password recovery requests.
- Encourage the use of **password managers** to enhance security without affecting productivity.

Compliance Impact: Aligns with NIST password guidelines and improves overall security hygiene.

6. Establish a Regular Legacy System Maintenance Schedule

Current Issue: Legacy systems are maintained but without a defined schedule or clear intervention methods.

Recommendation:

- Implement a **structured maintenance schedule** to update and patch legacy systems.
- Evaluate the feasibility of **system modernization or migration** to newer, more secure platforms.

Compliance Impact: Reduces security risks associated with outdated systems and aligns with NIST best practices.

7. Improve Compliance with E.U. Data Protection Regulations

Current Issue: Compliance efforts for E.U. customers exist but may be insufficient for GDPR.

Recommendation:

- Appoint a **Data Protection Officer (DPO)** to oversee GDPR compliance.
- Ensure **data processing agreements (DPAs)** are in place with third-party vendors handling E.U. customer data.
- Conduct **regular GDPR compliance audits** to verify adherence.

Compliance Impact: Ensures full compliance with GDPR, reducing the risk of penalties.

8. Enhance Physical Security Measures

Current Issue: While locks, CCTV, and fire detection systems are in place, additional security layers can be added.

Recommendation:

- Implement **access control systems** (badge or biometric-based) to secure sensitive areas.
- Conduct **periodic security audits** of the physical location to identify vulnerabilities.
- Ensure **security awareness training** for employees to prevent insider threats.

Compliance Impact: Strengthens overall security and aligns with best practices in physical security management.