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.

Security Audit Recommendations for Botium Toys

1. Risk Description:

Current State: Botium Toys faces significant risk due to inadequate asset management, insufficient security controls, and lack of adherence to U.S. and international regulations.

Impact: Potential loss of assets or exposure to customer data, leading to fines and damage to business continuity.

Risk Score: 8/10 (high risk).

2. Recommendations:

Asset Management:

Issue: Botium Toys lacks proper identification and management of assets.

Recommendation: Implement a comprehensive asset management system to track hardware, software, and sensitive data. Use tools that automatically detect and classify assets, assigning risk levels based on their importance to the business.

NIST CSF Alignment: Focus on the Identifyfunction to prioritize assets and assess their value.

Data Access Controls:

Issue: All employees have unrestricted access to sensitive data, including cardholder information and PII.

Recommendation: Implement role-based access control (RBAC) and the principle of least privilege (PoLP). Ensure that employees can only access the data necessary for their role.

Action Steps:

1. *Define roles and responsibilities.*
2. *Restrict access to sensitive data (e.g., credit card details, customer PII).*
3. *Regularly review and audit access logs.*

Encryption & Data Protection:

Issue: Customer credit card data is not encrypted.

Recommendation: Implement encryption for data at rest and in transit. Ensure all sensitive data, such as credit card information, is encrypted using industry-standard algorithms (AES-256).

Compliance: Align with PCI DSS and GDPR requirements for data protection.

Password Management:

Issue: Password policy is outdated and not enforced.

*Recommendation: Strengthen the password policy by implementing minimum complexity requirements (e.g., length, special characters). Deploy a **centralized password management system** to enforce this policy and reduce password reset issues.*

Action Steps:

1. Update the password policy to require at least eight characters, including letters, numbers, and special characters.
2. Enforce password expiration and multi-factor authentication (MFA).
3. Implement a self-service password reset system.

Intrusion Detection System (IDS):

Issue: There is no IDS in place.

**Recommendation: Deploy an Intrusion Detection System (IDS) to monitor and detect suspicious activities in real time. This will allow the IT department to respond quickly to potential breaches.*

Action Steps:

1. Select and install an IDS solution.
2. Train the IT team to monitor alerts and respond to incidents.
3. Integrate IDS with existing firewalls and antivirus systems.

Disaster Recovery and Backup Plan:

Issue: No disaster recovery plan or backup of critical data.

Recommendation: Develop a Disaster Recovery (DR) plan and implement a regular backup schedule to ensure data availability in case of an incident.

Action Steps:

1. Conduct a business impact analysis (BIA) to identify critical systems.
2. Establish off-site or cloud-based backups.
3. Test the disaster recovery plan regularly.

Legacy System Maintenance:

Issue: Legacy systems are monitored, but no regular schedule is in place.

Recommendation: Implement a **regular maintenance schedule** for legacy systems, including updates, security patches, and decommissioning if necessary.

Action Steps:

1. Conduct risk assessments on legacy systems.
2. Schedule regular updates and define a process for intervention.
3. Consider virtualization or replacing legacy systems where feasible.

Compliance with Regulations:

Issue: Botium Toys may not be fully compliant with U.S. and international regulations, such as PCI DSS and GDPR.

Recommendation: Conduct a compliance audit to ensure that Botium Toys adheres to all relevant regulations. This includes securing customer data, limiting access to PII, and timely breach notification (e.g., 72-hour GDPR breach notification).

Action Steps:

1. Establish a compliance team to monitor regulations.
2. Create a compliance checklist for PCI DSS and GDPR.
3. Conduct annual reviews and updates to ensure ongoing compliance.

Physical Security:

Current State: Physical security is adequate with locks, CCTV, and fire detection systems in place.

Recommendation: Continue regular monitoring of physical security measures, and review CCTV and access logs periodically.

3. Control Best Practices:

Identify and Manage Assets: As per the NIST Cybersecurity Framework, focus on asset identification and classification to manage them efficiently and ensure business continuity.

Access Controls: Implement least privilege and separation of duties to protect sensitive data.

Encryption: Encrypt all sensitive data to ensure confidentiality.

Regular Audits: Conduct periodic audits to ensure compliance with security controls and regulatory requirements.

4. Conclusion:

Botium Toys needs to improve asset management, enhance security controls, and ensure compliance with international regulations. By following these recommendations, they can lower their risk score, strengthen security, and protect critical assets and customer data.