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.

Yes	No	
☑	☐	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.

Based on the audit findings, it is crucial for Botium Toys to take immediate steps to enhance its security posture and compliance with U.S. and international regulations. To reduce the identified risks and improve overall security, the following recommendations can be communicated to stakeholders by the IT manager:

Implement Robust Access Controls and Encryption: Botium Toys should prioritize the implementation of access controls based on the principle of least privilege and separation of duties. This ensures that employees only have access to the data and systems necessary for their roles, reducing the risk of unauthorized access. Additionally, the company must implement strong encryption mechanisms, especially for customer

credit card information and sensitive personal data, both in transit and at rest. This will significantly improve the confidentiality of critical data.

Develop Comprehensive Disaster Recovery and Backup Plans: The absence of disaster recovery plans and critical data backups poses a substantial risk. Botium Toys should create well-documented and tested disaster recovery plans to ensure business continuity in the event of a security breach or data loss. Regularly scheduled backups of critical data should also be established to safeguard against data loss. This will enhance the company's ability to recover from incidents and minimize potential data breaches.

Enhance Password Management and Legacy System Maintenance: Botium Toys should update its password policy to meet current minimum complexity requirements and implement a centralized password management system to enforce these policies efficiently. Additionally, a clear and regular maintenance schedule for legacy systems should be established, ensuring that they are monitored, patched, and maintained to mitigate potential vulnerabilities. These measures will improve overall security and reduce the risk of unauthorized access.