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):

1) **Implement Least Privilege Access Controls**: Restrict employees' access to sensitive data based on their job responsibilities. This helps minimize the amount of unauthorized access. This includes separation of duties.

2) **Enhance Data Encryption Practices**: Implement encryption mechanisms, for sensitive information such as customer's credit/debit card data. Ensure that encryption is applied during data transmission, processing, and storage.

3) **Establish Disaster Recovery Plans and Regular Backups**: Develop disaster recovery plans to ensure business continuity in case of disruptions. Regularly back up critical data and systems to prevent data loss and expedite recovery in the event of a security incident.

4) **Install an Intrusion Detection System (IDS)**: Deploy an IDS to monitor network traffic for signs of suspicious activities or potential security threats.
5) **Improve Password Management Practices**: Create stronger password policies with minimum complexity requirements. Implement a centralized password management system to improve the speed of password-related processes and enhance overall security.

6) **Define User Access Policies**: Establish clear user access policies to govern the permissions and roles of individuals within the organization. This includes making access levels, regularly reviewing access rights, and promptly revoking access for employees who no longer require it.

7) **Enhance Privacy Policies and Procedures**: Strengthen privacy policies, procedures, and processes, especially the handling of sensitive data. To comply with privacy regulations make sure that data is properly classified, inventoried, and managed.

8) **Initiate Regular Security Training Programs**: Conduct regular security awareness and training programs for employees to educate them about

potential risks, security best practices, and the importance of following security policies.

9) **Implement Comprehensive Logging and Monitoring for Legacy Systems**: Improve logging mechanisms to watch for relevant security events and implement continuous monitoring practices. This will help with quick detection and response to security incidents.

10) **Regularly Update and Patch Systems**: Use a proactive approach to system maintenance by regularly updating and patching software and systems. This helps address vulnerabilities and ensures that the environment is strong against known security threats.