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):

Based on the Botium Toys: Scope, Goals, and Risk Assessment Report, the company currently lacks critical security controls and does not fully comply with industry standards and regulatory frameworks. To mitigate the different risks and improve its security posture, the following recommendations have been made and should be prioritized:

1. Implement Access Controls by establishing least privilege access controls and enforce separation of duties. This will ensure that sensitive data is not exposed and it will reduce unauthorized access risks.

2. Increase Security Measures by deploying an IDS to detect potential security threats and implement a structured monitoring plan for legacy systems.

3. Strengthen Password Policies by updating its policy to require at least 12-character passwords with a mix of lowercase and uppercase letters, numbers, and special characters. Additionally, enabling multi-factor authentication and deploying a centralized password management system will increase account security.

4. Ensure Data Protection by encrypting all customer's credit card information and personally identifiable information or PII, both in transit and rest.

5. Develop a Disaster Recovery Plan by establishing a formal disaster recovery and data backup plan. Automated backup plans should be scheduled regularly and off-site storage should be considered.

6. Achieve PCI DSS Compliance by restricting access to credit card data, encrypting all payment transactions, and securing the payment processing environment.

7. Improve GDPR Compliance by conducting a full data inventory to classify and protect sensitive information. Also, privacy policies should be reinforced through regular employee training to ensure the compliance of GDPR.