Controls and compliance checklist

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.)

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.

Recommendations (optional):

Botium Toys currently lacks a sufficient number of critical security controls. The existing systems fall short of meeting essential security objectives, particularly in the areas of **confidentiality** and **authorization**.

To enhance its security posture to an acceptable level, Botium should prioritize implementing the following:

- **Encryption** to protect sensitive customer and payment data
- **Least privilege** access policies to restrict data exposure
- **Disaster recovery plans** to ensure business continuity
- **Intrusion Detection System (IDS)** for real-time threat monitoring
- **Robust password policies and centralized management** to improve account security
- **Separation of duties** to reduce the risk of internal abuse or error

- **Consistent manual monitoring and maintenance of legacy systems** to prevent operational risks

Currently, the absence of these controls places Botium in **violation of key regulatory standards** such as **PCI DSS**, **GDPR**, and **SOC 2**, primarily due to the lack of data confidentiality and proper access controls.

To begin aligning with these regulations, **encryption**, **least privilege**, and **separation of duties** must be implemented as a minimum. This will help establish the basic foundation of **data protection** and **access control** required for regulatory compliance.