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):

Here are some audit-friendly recommendations for Botium Toys based on the gaps I just covered.

1. Implement Role-Based Access Control (RBAC):
    - Lock it down. Access should be granted based on job function.
2. Establish and enforce password policies:
    - Set minimum complexity requirements, expiration cycles, and multi-factor authentication.
3. Create a data classification and inventory system:
    - Know what you have, where it lives, and how sensitive it is.

    - Label it.
4. Develop and document privacy policies:
    - GDPR doesn't care that you are new to this.
    - Get your data subject rights, consent practices, and breach notification protocols in writing.
5. Restrict access to PII/SPII:
    - Sensitive info should be accessible only to those who need it.
    - HR doesn't need to see the Dev teams private Slack messages.
6. Align with SOC 2 Trust Service Criteria:
    - Start with Security and Confidentiality. Use it to frame your policies for access, data retention, audit logging, and incident response.
7. Define breach response timelines:
    - Especially for GDPR, where that 72-hour rule isn't just a suggestion, it's the law.
8. Start internal audits and gap assessments:
    - SOC 2 and compliance frameworks are all about proving you're doing what you say you're doing. Documentation is your friend.