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 :

Multiple controls need to be implemented to improve Botium Toys' security posture and better ensure the confidentiality of sensitive information, including: Least Privilege, disaster recovery plans, password policies, separation of duties, an IDS, ongoing legacy system management, encryption, and a password management system.

To address gaps in compliance, Botium Toys needs to implement controls such as Least Privilege, separation of duties, and encryption. The company also needs to be properly classify assets, to identify additional controls that may need to be implemented to improve their security posture and better protect sensitive information.