Controls and compliance checklist

For clarity, please refer to the information provided in the Scope, Goals, and Risk Assessment report. For more details about each control mentioned, refer to the Control Categories document.

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.

Recommendations :

There are multiple controls that are lacking and need to be implemented to improve Botium Toys’ security posture. By doing so, it will better ensure the confidentiality of sensitive information. I recommend the following areas in particular be implemented: Least Privilege, some form of disaster recovery planning, password policies including MFA, an IDS, and data encryption.

There are also gaps in compliance that must be addressed. Botium Toys’ needs to implement Least Privilege and separation of duties as well as encryption in order to reduce it’s current level of compliance related risk. The company also needs to properly classify assets to better identify any added controls that mya be required.