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): In order to mitigate the risks caused by security incidents as well as to adhere, the PII and SPII and data at rest and in transit shall be encrypted in order to ensure the confidentiality of customers' credit card information.

The principle of minimum privilege shall be employed in order to reduce the attack surface.

Passwords shall be securely stored and respect minimum complexity requirements. A password management system shall be used to ensure the effective time management of the IT team when resetting the passwords.

Implementing an Intrusion Detection System represents a preemptive measure to detect and treat potential incidents.

Prioritizing the legacy system security shall be implemented, because they hold personal data that could be involved in a security incident. Without a regular monitoring schedule, security incidents on legacy systems might go unnoticed for extended periods, This delay can lead to more significant damage and data breaches.

Adhering to Payment Card Industry Data Security Standard (PCI DSS) requirements ensures that the company processing data is trustworthy.

Failing to comply with General Data Protection Regulation (GDPR) can lead to significant financial penalties.