

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
	<input type="checkbox"/>	Least Privilege
	<input type="checkbox"/>	Disaster recovery plans
	<input type="checkbox"/>	Password policies
	<input type="checkbox"/>	Separation of duties
<input type="checkbox"/>	<input type="checkbox"/>	Firewall
	<input type="checkbox"/>	Intrusion detection system (IDS)
	<input type="checkbox"/>	Backups
<input type="checkbox"/>	<input type="checkbox"/>	Antivirus software
<input type="checkbox"/>	<input type="checkbox"/>	Manual monitoring, maintenance, and intervention for legacy systems
	<input type="checkbox"/>	Encryption
	<input type="checkbox"/>	Password management system
<input type="checkbox"/>	<input type="checkbox"/>	Locks (offices, storefront, warehouse)
<input type="checkbox"/>	<input type="checkbox"/>	Closed-circuit television (CCTV) surveillance
<input type="checkbox"/>	<input type="checkbox"/>	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
		<ul style="list-style-type: none">● 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
		<ul style="list-style-type: none">● 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): The company needs to focus on maintaining a secure environment in which the customers' PII/SPII are not accessible to all the employees by implementing OWASP's separation of duties. Antivirus software should be installed to ensure that the company is resistant to different malware attacks and data breaches. The company should have back plans and disaster recovery plans in case of any unfortunate attack on the company's assets and sensitive data that it holds. The customer data should be end to end encrypted when it is stored in the data base.