

# 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 checked="" type="checkbox"/>	Least Privilege
	<input checked="" type="checkbox"/>	Disaster recovery plans
	<input checked="" type="checkbox"/>	Password policies
	<input checked="" type="checkbox"/>	Separation of duties
<input checked="" type="checkbox"/>		Firewall
	<input checked="" type="checkbox"/>	Intrusion detection system (IDS)
	<input checked="" type="checkbox"/>	Backups
<input checked="" type="checkbox"/>		Antivirus software
	<input checked="" type="checkbox"/>	Manual monitoring, maintenance, and intervention for legacy systems
	<input checked="" type="checkbox"/>	Encryption
	<input checked="" type="checkbox"/>	Password management system
<input checked="" type="checkbox"/>		Locks (offices, storefront, warehouse)
<input checked="" type="checkbox"/>		Closed-circuit television (CCTV) surveillance
<input checked="" 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
	<input checked="" type="checkbox"/>	Only authorized users have access to customers’ credit card information.
	<input checked="" type="checkbox"/>	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.
	<input checked="" type="checkbox"/>	Implement data encryption procedures to better secure credit card transaction touchpoints and data.
	<input checked="" type="checkbox"/>	Adopt secure password management policies.

### General Data Protection Regulation (GDPR)

Yes	No	Best practice
	<input checked="" type="checkbox"/>	E.U. customers’ data is kept private/secured.
<input checked="" type="checkbox"/>		There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.
	<input checked="" type="checkbox"/>	Ensure data is properly classified and inventoried.
<input checked="" type="checkbox"/>		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
	<input checked="" type="checkbox"/>	User access policies are established.
	<input checked="" type="checkbox"/>	Sensitive data (PII/SPII) is confidential/private.
<input checked="" type="checkbox"/>		Data integrity ensures the data is consistent, complete, accurate, and has been validated.
	<input checked="" type="checkbox"/>	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 this section, provide recommendations, related to controls and/or compliance needs, that your IT manager could communicate to stakeholders to reduce risks to assets and improve Botium Toys' security posture.

**Answer:** 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 properly classify assets, to identify additional controls that may need to be implemented to improve their security posture and better protect sensitive information.