

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

#### General Data Protection Regulation (GDPR)

Yes	No	Best practice
	<input type="radio"/>	E.U. customers’ data is kept private/secured.
<input type="radio"/>		There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.
	<input type="radio"/>	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
		<ul style="list-style-type: none"> <li>● User access policies are established.</li> <li>● Sensitive data (PII/SPII) is confidential/private.</li> <li>● Data integrity ensures the data is consistent, complete, accurate, and has been validated.</li> </ul>
		<ul style="list-style-type: none"> <li>● Data is available to individuals authorized to access it.</li> </ul>

---

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.

Botium Toys should implement a strategy of role-based access control to safeguard client information. Only authorized personnel should have access to sensitive data, such as addresses, credit card details, and birthdates, while others must be restricted from viewing it. Encrypting all credit card information is crucial to prevent identity theft and comply with the Payment Card Industry Data Security Standard (PCI DSS).

Despite having a notification plan for European clients, Botium Toys currently lacks adequate security measures for their data. Implementing encryption will address this issue and ensure compliance with the General Data Protection Regulation (GDPR) by properly classifying and inventorying data.

While the IT department has established controls for data integrity and availability, user access policies are currently absent. Enhancing confidentiality of sensitive information will align Botium Toys with System and Organizations Controls (SOC type 1, SOC type 2) requirements.