

# 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
		<ul style="list-style-type: none"><li>Least Privilege</li><li>Disaster recovery plans</li><li>Password policies</li><li>Separation of duties</li></ul>
		<ul style="list-style-type: none"><li>Firewall</li><li>Intrusion detection system (IDS)</li><li>Backups</li></ul>
		<ul style="list-style-type: none"><li>Antivirus software</li><li>Manual monitoring, maintenance, and intervention for legacy systems</li><li>Encryption</li><li>Password management system</li></ul>
		<ul style="list-style-type: none"><li>Locks (offices, storefront, warehouse)</li><li>Closed-circuit television (CCTV) surveillance</li></ul>

- 
- 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"> <li>Only authorized users have access to customers’ credit card information.</li> <li>Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.</li> <li>Implement data encryption procedures to better secure credit card transaction touchpoints and data.</li> <li>Adopt secure password management policies.</li> </ul>

#### General Data Protection Regulation (GDPR)

Yes	No	Best practice
		<ul style="list-style-type: none"> <li>E.U. customers’ data is kept private/secured.</li> <li>There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.</li> <li>Ensure data is properly classified and inventoried.</li> <li>Enforce privacy policies, procedures, and processes to properly document and maintain data.</li> </ul>

## 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></ul>
		<ul style="list-style-type: none"><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.