

# 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
	<input checked="" type="checkbox"/>	Only authorized users have access to customers’ credit card information.
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Implement data encryption procedures to better secure credit card transaction touchpoints and data.
<input type="checkbox"/>	<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.

- 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
	<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.

### Recommendations

→ Multiple control needs to be implemented for Botium Toy's Security posture to improve it, and to ensure confidentiality. Integrity.