

# Controls and compliance checklist

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"/>	<input checked="" type="checkbox"/>	Least Privilege
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Disaster recovery plans
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Password policies
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Separation of duties
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Firewall
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Intrusion detection system (IDS)
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Backups
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Antivirus software
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Manual monitoring, maintenance, and intervention for legacy systems
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Encryption
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Password management system
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Locks (offices, storefront, warehouse)
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Closed-circuit television (CCTV) surveillance
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Fire detection/prevention (fire alarm, sprinkler system, etc.)

---

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="checkbox"/>	<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 type="checkbox"/>	<input checked="" type="checkbox"/>	E.U. customers’ data is kept private/secured.
<input checked="" type="checkbox"/>	<input 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 type="checkbox"/>	<input checked="" type="checkbox"/>	Ensure data is properly classified and inventoried.
<input checked="" type="checkbox"/>	<input 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 type="checkbox"/>            | <input checked="" type="checkbox"/> | User access policies are established.  |
| <input type="checkbox"/>            | <input checked="" type="checkbox"/> | Sensitive data (PII/SPII) is confidential/private.   |
| <input checked="" type="checkbox"/> | <input type="checkbox"/>            | Data integrity ensures the data is consistent, complete, accurate, and has been validated. |
| <input type="checkbox"/>            | <input checked="" type="checkbox"/> | Data is available to individuals authorized to access it.                                  |

---

**Recommendations (optional):** There are significant risks and vulnerabilities identified within Botium Toys' current security posture. To address these issues and strengthen the company's overall security framework, the following controls need to be implemented: least privilege access policies, disaster recovery plans, updated password policies, separation of duties, an intrusion detection system (IDS), data backups, manual monitoring and maintenance for legacy systems, encryption for sensitive data, and a centralized password management system.

These measures mitigate risks such as unauthorized access, data breaches, and data loss while ensuring compliance with industry standards like PCI DSS, GDPR, and SOC frameworks. Collectively, these actions uphold the principles of the CIA Triad (Confidentiality, Integrity, and Availability) by protecting sensitive data, ensuring its reliability, and maintaining availability for authorized users.