

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

#### General Data Protection Regulation (GDPR)

- | Yes | No | <b>Best practice</b>  |
|-----|----|---|
|     |    | 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  |
|-----|----|--|
|     | ●  | User access policies are established.  |
| ●   | ●  | Sensitive data (PII/SPII) is confidential/private.   |
| ●   | ●  | Data integrity ensures the data is consistent, complete, accurate, and has been validated. |
| ●   | ●  | 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.

## **Recommendations**

Based on the results of the controls and compliance assessment, Botium Toys should prioritize implementing several administrative, technical, and compliance-related controls to reduce overall risk and improve its security posture.

First, the company should implement least privilege access controls and separation of duties to ensure employees only have access to the data and systems necessary for their roles. This would significantly reduce the risk of unauthorized access to customer PII and credit card information.

Second, Botium Toys should encrypt all sensitive data, particularly customer credit card information that is stored, processed, or transmitted internally. Encryption is critical for meeting PCI DSS requirements and protecting data confidentiality in the event of a breach.

Third, the organization should establish regular data backups and a formal disaster recovery plan. Without backups or recovery procedures, Botium Toys faces a high risk of prolonged downtime and data loss following a cyber incident or system failure.

Additionally, deploying an intrusion detection system (IDS) and improving centralized password management would strengthen the company's ability to detect threats and reduce the likelihood of account compromise.

Finally, Botium Toys should improve data classification, inventory, and privacy enforcement processes to better align with GDPR and SOC compliance requirements, especially as the company continues to grow its international customer base.

Implementing these controls in a timely manner would reduce security risks, improve regulatory compliance, and support long-term business continuity.

