# 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 |
|---|---|---|
| | ● | 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 | Best practice |
|---|---|---|
| | ● | 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. |

---

**Recommendations (optional):** Botium Toys must adopt multiple security controls to strengthen its overall security posture and safeguard the confidentiality of sensitive information. These controls include implementing the principle of Least Privilege, establishing disaster recovery plans, enforcing password policies, ensuring separation of duties, deploying an intrusion detection system (IDS), maintaining legacy systems on an ongoing basis, applying encryption, and utilizing a password management system.

To remediate compliance gaps, the organization should focus on specific measures such as enforcing Least Privilege, separation of duties, and encryption. In addition, Botium Toys must conduct proper asset classification to identify where further controls are required. This will help the company enhance its security posture and provide stronger protection for sensitive data.