# 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 |

| Yes | No | |
|:---:|:---:|---|
| ☐ | ☑ | 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. |

| Yes | No | |
|:---:|:---:|---|
| ☑ | ☐ | Enforce privacy policies, procedures, and processes to properly document and maintain data. |

<u>System and Organizations Controls (SOC type 1, SOC type 2)</u>

| 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. |

---

Botium Toys should immediately encrypt sensitive data, implement access controls, and conduct a compliance review to mitigate high risks of unauthorized access and regulatory fines. In the short term, they need to install an IDS, develop a disaster recovery plan, and establish regular data backups to prevent data loss and undetected intrusions. Ongoing efforts should include maintaining physical security measures and conducting continuous security awareness training to reduce the risk of breaches.

**Recommendations:** To enhance Botium Toys' security posture, stakeholders should prioritize encrypting sensitive data, implementing strict access controls, and conducting a comprehensive compliance review to prevent unauthorized access and ensure regulatory adherence. Installing an intrusion detection system, developing a disaster recovery plan, and maintaining regular data backups will further safeguard against data loss and operational disruptions. Continuous physical security maintenance and employee security awareness training will mitigate physical and human-related security risks.