

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
<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 checked="" type="checkbox"/>	<input 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

- ☒ ☐ 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 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 checked="" type="checkbox"/>	<input type="checkbox"/>	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: 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

1. Implement Access Controls (Least Privilege & Separation of Duties) Currently, all employees have access to internally stored data, including potential access to cardholder data and customer PII/SPII.

- **Recommendation:** Implement **Least Privilege** and **Separation of Duties** policies immediately. This ensures that only authorized users have access to sensitive data, which is a critical requirement for PCI DSS compliance.

2. Deploy Encryption for Sensitive Data Encryption is not currently utilized to ensure the confidentiality of customers' credit card information stored in the internal database.

- **Recommendation:** Implement encryption procedures for data at rest and in transit. This is necessary to better secure credit card transaction touchpoints and to comply with PCI DSS and GDPR privacy standards.

3. Establish Disaster Recovery Plans and Backups The company currently lacks disaster recovery plans and does not possess backups of critical data.

- **Recommendation:** Create and implement a **Disaster Recovery Plan** and regular **Backup** procedures. These are essential **Corrective Controls** to restore assets after an incident and ensure business continuity.

4. Strengthen Password Management The current password policy is nominal and does not meet minimum complexity requirements (e.g., character length and complexity). Furthermore, there is no centralized password management system.

- **Recommendation:** Adopt a secure password management system and enforce stricter password policies (Preventative Control) to reduce the likelihood of account compromise.

5. Install an Intrusion Detection System (IDS) The IT department has not installed an Intrusion Detection System.

- **Recommendation:** Implement an IDS as a **Detective Control** to identify anomalous traffic and potential ongoing attacks.

6. Formalize Asset Management There is inadequate management of assets, and the IT department does not know which assets would be at risk.

- **Recommendation:** Dedicate resources to identify and classify existing assets to determine the impact of their loss on business continuity.