

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

- Enforce privacy policies, procedures, and processes to properly document and maintain data.

### System and Organizations Controls (SOC type 1, SOC type 2)

<b>Yes</b>	<b>No</b>	<b>Best practice</b>
<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.

---

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 FOR SECURITY CONTROLS / COMPLIANCES (BOTIUM TOYS)**

1. Implement the control of least privilege, a preventive control that reduces risk and overall impact of malicious insider or compromised accounts.
2. Implement disaster recovery plans,a corrective control that provide business continuity.

3. Implement separation of duties,a preventative control that reduces risk and overall impact of malicious insider or compromised accounts.
4. Implement IDS/IPS ,a detective control To detect and prevent anomalous traffic that matches a signature or rule.
5. Implement backups ,a corrective control that restore / recover from an event.
6. Implement Encryption,a deterrent control that provides confidentiality to sensitive information.
7. Implement password management system,a preventative control that reduces password fatigue.

## **RISK ASSESSMENT RECOMMENDATION**

1. There should be adequate management of assets and proper control,compliance and adherence of the five functions of the NIST/ CSF. compliance to best practices would drastically reduce the risk score.