

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

1. Encrypt all sensitive data (e.g., cardholder information, PII/SPII) **in transit and at rest** using industry-standard encryption (AES-256, TLS 1.2+).

- Implement **tokenization or data masking** to minimize exposure of sensitive data.

2. Enforce the principle of least privilege: Grant employees access only to the data necessary for their roles.

- Apply **role-based access control (RBAC)** and implement **separation of duties** for critical functions (e.g., developers vs. auditors).

3. Deploy an Intrusion Detection System (IDS) and/or Intrusion Prevention System (IPS) to detect and respond to unauthorized access.

- Ensure **continuous monitoring** of logs and security events.

4. Password & Authentication Management

- Strengthen the **password policy** to enforce:
- Minimum 8 characters
- Combination of uppercase, lowercase, numbers, and symbols
- Implement a **centralized password management system** with self-service reset options to reduce help desk overhead.
- Consider **multi-factor authentication (MFA)** for sensitive systems and accounts.

5. Backup & Disaster Recovery

- Establish a **disaster recovery (DR) plan** with clear roles and communication channels.
- Set up **regular, automated backups** of critical systems and data.
- Test backups and **perform DR drills** periodically.

6. Legacy System Management

- Create a **scheduled maintenance plan** for legacy systems with clear documentation of interventions.
- Assess and consider **phasing out unsupported systems**.

7. Physical Security

- Maintain and routinely audit the existing **CCTV, locks, and fire detection systems**.
- Consider **access logs or badge entry systems** for sensitive areas.

8. Compliance & Policy

- Ensure compliance with **PCI-DSS** for cardholder data and **GDPR** for E.U. residents' privacy.
- Update and regularly review **privacy policies and data handling procedures**.
- Train all employees on **security awareness and data privacy responsibilities**.