

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 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 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.

- ☒ ☐ 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 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.

Controls and Compliance Needs	Recommendation
1. Currently, all Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers' PII/SPII.	Limit access to customer PII/SPII to only essential personnel. Use encryption and role-based access controls to protect sensitive data.

2. Encryption is not currently used to ensure confidentiality of customers' credit card information that is accepted, processed, transmitted, and stored locally in the company's internal database.	Implement strong encryption for all stored and transmitted credit card data. This reduces the risk of data breaches and ensures PCI compliance.
3. Access controls pertaining to least privilege and separation of duties have not been implemented.	Review job functions and apply least privilege principles. Implement role separation in IT to reduce risk and increase accountability.
4. The IT department has not installed an intrusion detection system (IDS).	Deploy an IDS to monitor network traffic and detect unauthorized activity. This will provide early warning of potential breaches.
5. There are no disaster recovery plans currently in place, and the company does not have backups of critical data.	Develop and regularly test a disaster recovery plan. Establish automated backups for all critical systems and data.
6. Although a password policy exists, its requirements are nominal and not in line with current minimum password complexity requirements (e.g., at least eight characters, a combination of letters and at least one number; special characters).	Update the password policy to meet current standards (e.g., length, complexity). Enforce the policy through technical controls.
7. There is no centralized password management system that enforces the password policy's minimum requirements, which sometimes affects productivity when employees/vendors submit a ticket to the IT department to recover or reset a password.	Implement a centralized password management system to enforce policies and reduce IT workload from reset requests.
8. While legacy systems are monitored and maintained, there is no regular schedule in place for	Create and follow a consistent maintenance schedule for legacy systems. Clearly define responsibilities

these tasks and intervention methods are unclear.	for monitoring and intervention.
---	----------------------------------