

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 - All employees have access to PII, so non-compliant.
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Disaster recovery plans - No backups of critical data. Business would find it difficult to return to baseline from an incident.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Password policies - BUT, the policy is currently below minimum standards. This should be updated and tested to ensure stronger passwords used throughout the business.
<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 - See comment relating to disaster recovery.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Antivirus software - monitored regularly by IT team.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Manual monitoring, maintenance, and intervention for legacy systems - but no regular system in place. Ideally set up a plan for these checks to ensure regularity.
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Encryption - not compliant with PCI DSS requirements. This is a huge risk to the business.

- | | | |
|-------------------------------------|-------------------------------------|---|
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Password management system - This is causing more work for IT teams when requests come through particularly for legacy systems. |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | Locks (offices, storefront, warehouse) - physical controls are generally good. |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | Closed-circuit television (CCTV) surveillance |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | 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 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 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 need to be implemented immediately to ensure compliance with PCI DSS and GDPR requirements. As failing to comply with these requirements can have significant financial and regulatory penalties, not to mention reputational issues, these should be prioritised.

Measures to be implemented in order to achieve the above are the following: Least Privilege, a disaster recovery plan, password policies, separation of duties, an IDS, ongoing legacy system management, encryption, and a password management system.