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
	●	Least Privilege
	●	Disaster recovery plans
●		Password policies
	●	Separation of duties
●		Firewall
	●	Intrusion detection system (IDS)
	●	Backups
●		Antivirus software
	●	Manual monitoring, maintenance, and intervention for legacy systems
	●	Encryption
	●	Password management system
●		Locks (offices, storefront, warehouse)
●		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
	●	Only authorized users have access to customers' credit card information.
●		Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.
	●	Implement data encryption procedures to better secure credit card transaction touchpoints and data.
	●	Adopt secure password management policies.

General Data Protection Regulation (GDPR)

Yes	No	Best practice
	●	E.U. customers' data is kept private/secured.
●		There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.
	●	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
	●	User access policies are established.
	●	Sensitive data (PII/SPII) is confidential/private.
●		Data integrity ensures the data is consistent, complete, accurate, and has been validated.
●		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.

- Improve upon password strength policy to ensure that it is in line with current recommendations
- Passwords should contain a mixture of alphanumeric characters, both upper case and lower case, as well as at least one symbol or special character.
- While data is available to those who need to access it, it has been noted that all customer data, including PII/SPII is available to all members of staff, *including* those who are not authorised to access such information.
- Although customers located in the EU will be notified of a breach within 72 hours, the risk assessment report suggests that such data has not been properly secured. It is recommended to secure EU customer data in a manner complying with GDPR before the next audit
- In order to comply with PCI DSS, Botium Toys should ensure that only employees who are authorised to access customers' credit card information should be able to do so. It is not recommended that all employees have access to this data as this violates the principle of least privilege
- Encryption should also be implemented so that any transactions made to and from the company are able to be made securely and safely. Currently, no encryption measures have been implemented within the environment

- At present, there is no disaster recovery strategy in place, and it is recommended that one be put into place to protect customer data in the event that a breach occurs
- To reduce the likelihood of a breahc occurring, it is also important to ensure that no employees are responsible for too many things. Each employee should be responsible for one activity within the company, as per separation of duties,
- As there is no current IDS system in place to monitor breaches, it is strongly recommended that once be deployed to detect and manage any potential security issues. Additionally, important customer data should be securely backed up such that it is able to be restored in a timely manner in the event that it becomes compromised or lost.