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 (*Employee password requirements are minimal, which could allow a threat actor to more easily access secure data/other assets via employee work equipment/the internal network.)*
	●	Separation of duties
●		Firewall
	●	Intrusion detection system (IDS)
	●	Backups
●		Antivirus software
	●	Manual monitoring, maintenance, and intervention for legacy systems. *(The list of assets notes the use of legacy systems. The risk assessment indicates that these systems are monitored and maintained, but there is not a regular schedule in place for this task and procedures/ policies related to intervention are unclear, which could place these systems at risk of a breach.)*
	●	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:

To ensure compliance to PCI DSS, controls such as least privilege, encryption and a strong password management policy must be enforced with a password management system. Encryption will also help meet compliance requirements of GDPR.

As a preventative measure, to maintain business continuity and create a strong posture, existing passwords need to be strengthened. Installing an IDS, logging

activities and using a SIEM tool to alert the security team will help add a higher layer of security to identify and respond to threats immediately. Adding a backup system will help maintain business continuity. As the company grows to reach the international market, these preventative measures must be put in place without fail to ensure no impact to the company's reputation.

Added physical controls such as locking cabinets for network gear and signage indicating alarm service provider are also great measures to reduce physical attack surface and prevent threats at Botium's office.