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?*
Yes

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?*
Yes

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 :

- Asset Management- Clearly define and implement asset management practices to identify, classify, and manage all assets within Botium Toys, including on-premises equipment, employee devices, storefront products, management systems, and data storage.
- Controls and Compliance: Develop and implement controls and compliance measures to ensure adherence to U.S. and international regulations and standards, particularly regarding data security and privacy. This should include measures such

as encryption of sensitive data, access controls, and regular audits to assess compliance.

- Compliance with EU Regulations: Ensure compliance with EU regulations, particularly regarding data privacy and breach notification requirements. Develop and enforce privacy policies and procedures, establish clear protocols for breach notification within 72 hours, and provide training to employees on their responsibilities in maintaining data privacy.
- Risk Mitigation: Develop a comprehensive risk mitigation strategy to address the identified risks, focusing on reducing the risk score from its current level of 8. This may involve implementing additional controls, enhancing existing security measures, and ensuring alignment with best practices such as the NIST Cybersecurity Framework.
- Data Security: Strengthen data security measures, including access controls, encryption, and the implementation of a centralized password management system to enforce stronger password policies and improve productivity.
- Disaster Recovery and Business Continuity: Develop and implement disaster recovery plans and procedures to ensure business continuity in the event of a security breach or other disruptive incident. This should include regular backups of critical data and the establishment of clear protocols for incident response and notification.
- Legacy System Management: Establish a structured approach to monitoring and maintaining legacy systems, including the implementation of regular maintenance schedules and clear intervention methods to address issues as they arise.
- Physical Security: Maintain and enhance physical security measures at Botium Toys' physical location, including locks, surveillance systems, and fire detection/prevention systems, to protect both physical assets and sensitive data stored on-site.