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.

To enhance Botium Toys' security posture and address the identified issues, your IT manager can communicate the following recommendations:

Payment Card Industry Data Security Standard (PCI DSS):

Access Control:

- Implement strict access controls to ensure that only authorized users have access to customers' credit card information.

- Regularly review and update access privileges to minimize the risk of unauthorized access.

Data Encryption:

- Establish and enforce data encryption procedures for securing credit card transaction touchpoints and data.
- Ensure that encryption is applied during the storage, processing, and transmission of credit card information.

Password Management:

- Adopt secure password management policies, including regular password updates, strong password requirements, and multi-factor authentication.
- Educate employees on the importance of maintaining strong, unique passwords.

General Data Protection Regulation (GDPR):

Data Breach Response Plan:

- Ensure a comprehensive plan is in place to notify E.U. customers within the mandated 72 hours in the event of a data breach.
- Conduct regular drills and simulations to test the effectiveness of the response plan.

Data Classification and Inventory:

- Enhance the classification and inventory of data, including E.U. customer data, to better understand and manage privacy risks.
- Regularly review and update data classifications based on sensitivity and regulatory requirements.

Privacy Enforcement:

- Strengthen the enforcement of privacy policies, procedures, and processes to safeguard E.U. customers' data.
- Provide ongoing training to employees to ensure awareness of and adherence to privacy policies.

System and Organizations Controls (SOC Type 1, SOC Type 2):

User Access Policies:

- Establish and enforce user access policies to control and monitor access to sensitive data.
- Conduct regular audits to ensure compliance with access policies and promptly address any unauthorized access.

Confidentiality of Sensitive Data:

- Enhance measures to ensure the confidentiality and privacy of sensitive data, such as personally identifiable information (PII) and sensitive personal identifiable information (SPII).
- Implement encryption and access controls to protect sensitive data from unauthorized disclosure.