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.

<u>System and Organizations Controls (SOC type 1, SOC type 2)</u>

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 on time.

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.

Recommendations:

Control Name	**Control Type**	**Recommendation**
Password policies	Preventative	**1.** In terms of user authentication, it is necessary to define a password manager, such as Cognito,

		Keycloak or another where it is allowed to establish a password policy that meets the minimum security (at least 8 characters, combinations of upper and lower case letters, numbers and at least one special character) to increase the complexity of the same, likewise adopting the idea that the user is the one who must change his password when necessary, thus allowing a normal flow of the system without generating unproductivity.
Least Privilege	Preventative	**2.** Keeping privileges to a minimum ensures a lesser impact from a malicious attack or human error caused by an employee. It is necessary to define profiles to ensure that only that group of people can perform those actions.
Encryption	Deterrent	**3.** It is necessary to protect the sensitive data of PII/SPII users, through information encryption techniques, making use of symmetric

		keys, tokens, data encryption through different types of encryption, and encryption at rest and in transit. Encryption at Rest refers to the encryption applied to the stored data. Encryption in Transit refers to encrypting data that is transferred between two nodes of the network.
Access control policies	Preventative	**4.** About privileges, it is necessary to design a model of roles and permissions to define and restrict the actions that one or a group of users can perform on the systems. It is also necessary to define employee access to data and internal systems and infrastructure, and to maintain minimum privilege control, only for authorized personnel.