Checklist of controls and compliance

To complete the controls assessment checklist, refer to the information provided in the document.scope, objectives and risk assessment reportFor more details about each control, including type and purpose, see thecontrol categoriesdocument.

Next, select "yes" or "no" to answer the question:*Does Botium Toys currently have this control implemented?*

Controls assessment checklist

Yeah	No	Control
☐	☑	Minimum privilege
☐	☑	disaster recovery plans
☐	☑	Password policies
☐	☑	Separation of duties
☑	☐	Firewall
☐	☑	Intrusion detection system (IDS)
☐	☑	Backups
☑	☐	software antivirus
☐	☑	Manual supervision, maintenance and intervention for legacy systems
☐	☑	Encryption
☐	☑	Password management system
☑	☐	Locks (offices, shop windows, warehouses)
☑	☐	Closed-circuit television (CCTV) surveillance

☑	□	Fire detection and prevention (fire alarm, sprinkler system, etc.)

To complete the compliance checklist, refer to the information provided in the document.scope, objectives and risk assessment reportFor more details on each compliance regulation, please refer to thecontrols, frameworks and compliance reading.

Next, select “yes” or “no” to answer the question:*Does Botium Toys currently comply with these good compliance practices?*

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

Yeah	No	Best practices
□	☑	Only authorized users have access to customer credit card information.
□	☑	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.
□	☑	Implement data encryption procedures to improve the security of touchpoints and credit card transaction data.
□	☑	Adopt secure password management policies.

General Data Protection Regulation (GDPR)

Yeah	No	Best practices
□	☑	EU customer data is kept private/secure.
☑	□	There is a plan to notify EU customers within 72 hours if their data is compromised or a security breach occurs.

□	☑	Make sure the data is properly classified and inventoried.
☑	□	Apply privacy policies, procedures, and processes to properly document and maintain data.

<u>Systems and organizational controls (SOC type 1, SOC type 2)</u>

Yeah	**No**	**Best practices**
□	☑	User access policies are established.
□	☑	Sensitive data (PII/SPII) is confidential/private.
☑	□	Data integrity ensures that the data is consistent, complete, accurate, and has been validated.
□	☑	The data is available to those authorized to access it.

This section is*optional*and can be used to provide a summary of recommendations to the IT manager on what controls and/or compliance best practices Botium Toys should implement, based on the risk of not implementing them in a timely manner.

Recommendations (optional): It is necessary to implement multiple measures to guarantee confidentiality, integrity, and availability at Botium Toys. This must include implementing the principle of least privilege, separation of job roles, stronger password standards, the application of IDS/IPS, disaster recovery plans against events, and backups, as well as password management. Rigorous supervision of legacy systems is also needed, ideally isolating them in networks separate from sensitive information. Other matters include the protection of customer credit cards used to pay for the service/product; this must involve encryption so that unauthorized personnel cannot gain access to this information. Maintaining the integrity, confidentiality, and availability of this data reduces the risk of fines in the EU. An inventory of the organization's resources must also be implemented.