

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, type an X in the “yes” or “no” column to answer the question: *Does Botium Toys currently have this control in place?*

Controls assessment checklist

Yes	No	Control
	X	Least Privilege
	X	Disaster recovery plans
	X	Password policies
	X	Separation of duties
X		Firewall
	X	Intrusion detection system (IDS)
	X	Backups
X		Antivirus software
X		Manual monitoring, maintenance, and intervention for legacy systems
	X	Encryption
	X	Password management system
X		Locks (offices, storefront, warehouse)
X		Closed-circuit television (CCTV) surveillance
X		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, type an X in the “yes” or “no” column 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
	X	Only authorized users have access to customers’ credit card information.
	X	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.
	X	Implement data encryption procedures to better secure credit card transaction touchpoints and data.
	X	Adopt secure password management policies.

General Data Protection Regulation (GDPR)

Yes	No	Best practice
	X	E.U. customers’ data is kept private/secured.
X		There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.
X		Ensure data is properly classified and inventoried.
X		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
X		User access policies are established.
	X	Sensitive data (PII/SPII) is confidential/private.
	X	Data integrity ensures the data is consistent, complete, accurate, and has been validated.
X		Data is available to individuals authorized to access it.

Recommendations (optional): Currently, the security of the business is low to medium. Here is a list of potential improvements:

- Only give access to passwords to the employees in charge of protecting them.
- Create backups of the important data.
- Configure an intrusion detection system to detect potential attacks. Also, in case a potential breach happens, shut down the system until we can find a solution.
- Apply encryption to passwords and other customer information. Also, increase the security by requiring passwords to be 8+ characters long, include an uppercase, lowercase, number, and symbol.