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
	\checkmark	Least Privilege
	\checkmark	Disaster recovery plans
	\checkmark	Password policies
	\checkmark	Separation of duties
\checkmark		Firewall
	\checkmark	Intrusion detection system (IDS)
	\checkmark	Backups
\checkmark		Antivirus software
	\checkmark	Manual monitoring, maintenance, and intervention for legacy systems
	\checkmark	Encryption
	\checkmark	Password management system
\checkmark		Locks (offices, storefront, warehouse)
\checkmark		Closed-circuit television (CCTV) surveillance

V		Fire detection/prevention (fire alarm, sprinkler system, etc.)				
goals, and	l risk as	compliance checklist, refer to the information provided in the scope. ssessment report. For more details about each compliance regulation, ols, frameworks, and compliance reading.				
	-	or "no" to answer the question: Does Botium Toys currently adhere see best practice?				
Complian	ce che	ecklist				
Payment Card Industry Data Security Standard (PCI DSS)						
Yes	No	Best practice				
		Only authorized users have access to customers' credit card information.				
	\checkmark	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.				
	\checkmark	Implement data encryption procedures to better secure credit card transaction touchpoints and data.				
	\checkmark	Adopt secure password management policies.				
General Data Protection Regulation (GDPR)						
Yes	No	Best practice				
	\checkmark	E.U. customers' data is kept private/secured.				
\checkmark		There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.				
	\checkmark	Ensure data is properly classified and inventoried.				

\checkmark	Enforce privacy policies, procedures, and processes to properly
	document and maintain data.

System and Organizations Controls (SOC type 1, SOC type 2)

No	Best practice
\checkmark	User access policies are established.
\checkmark	Sensitive data (PII/SPII) is confidential/private.
	Data integrity ensures the data is consistent, complete, accurate, and has been validated.
\checkmark	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.

Multiple controls need to be implemented to improve Botium Toys' security posture and better ensure the confidentiality of sensitive information, including: Least Privilege, disaster recovery plans, password policies, separation of duties, an IDS, ongoing legacy

system management, encryption, and a password management system.

To address gaps in compliance, Botium Toys needs to implement controls such as Least

Privilege, separation of duties, and encryption. The company also needs to properly classify assets, to identify additional controls that may need to be implemented to improve their security posture and better protect sensitive information.