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 improve the security of Botium Toys, it is strongly recommended to begin by creating a complete inventory of all IT assets and classifying them based on their risks and vulnerabilities. This will help the team understand what needs the most protection. Access to sensitive data should be restricted using the principle of least privilege, so employees only have access to what they truly need. In addition, the company should start using encryption to protect customer credit card information and personal data both when it is stored and when it is being sent.

It’s also important to install an intrusion detection system (IDS) to monitor for suspicious activity and strengthen defenses against cyberattacks. Currently, there are no backups or disaster recovery plans in place, which puts the company at serious risk if data is lost. A reliable backup system and a disaster recovery plan should be created and tested regularly. The existing password policy should be updated to meet current security standards, and a centralized password management system should be used to make password control easier and more secure.

Lastly, legacy systems should be checked and maintained on a clear schedule, and physical security should continue to be maintained. Regular reviews of compliance with data protection laws like GDPR and PCI DSS should also be conducted to avoid legal or financial consequences. These simple steps will greatly improve Botium Toys security and reduce the risk of data breaches or system failures.