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.

Currently, there are many issues around the confidentiality of user data. User access controls need to be implemented immediately, as any employee can access internally stored data, such as cardholder data and customers' PII/SPII. Employees should only have access to the data necessary for their job functions, which aligns with the principle of least privilege. There should be regular audits of access permissions to identify and revoke any unnecessary access rights.

This information also MUST be encrypted in case of a data breach; otherwise, this could cause severe damage to the reputation of Botium Toys, as well as many fines. The implementation of end-to-end encryption of sensitive data will protect customers' PII/SPII from unauthorized access.

On the note of data breaches, there are many internal security vulnerabilities, such as lacking password policies or separation of duties. While there are physical controls, such as CCTV and locks, there is a major threat of social engineering compromising our systems. Not only should a more secure password policy be put in place, there needs to be a password management system, as well as multi-factor authentication, as this would greatly improve the current security. I would suggest revising the current password policy to adhere to industry standards, such as requiring longer passwords with a mix of uppercase, lowercase, numbers, and special characters. As for the multi-factor authentication, this adds an additional layer of security beyond passwords.

Next, the company should look to implement an intrusion detection system (IDS), as while this will cost money, in the long run, it will save countless issues and headaches by potentially preventing costly data breaches due to unauthorized access attempts.

I also noticed a lack of disaster recovery and backup plans. There needs to be comprehensive disaster recovery plans and regular backups of critical data in order to ensure business continuity in case of a breach or system failure.

Finally, for legacy systems, there should be a regular maintenance schedule for legacy systems to ensure they are secure, as older devices can become vulnerability points. At some point, these systems should be phased out and replaced with newer, more secure systems.

With these changes, I'd also recommend instituting regular security awareness training for all employees in order to mitigate social engineering threats and ensure that they are aware of the best practices for data protection.

These changes will help Botium Toys align with relevant U.S and international compliance regulations, such as the GDPR.