Controls and compliance checklist

Select “yes” or “no” to answer the question: *Does Botium Toys currently have this control in place?*

Controls assessment checklist

Yes	No	Control	*Explanation*
☐	☑	Least Privilege	*Currently, this control is not in place, which means all the users may have more access privileges than necessary, increasing the risk of unauthorized access and potential security breaches.*
☐	☑	Disaster recovery plans	*There are no disaster recovery controls in place to recover critical systems and data in the event of a disaster or system failure.*
☐	☑	Password policies	*Organization’s password policies lack comprehensive password policies. This could increase the risk of unauthorized access through weak or compromised passwords.*
☐	☑	Separation of duties	*Needs to be implemented to prevent fraud and errors by ensuring that no single individual has complete control over all aspects of a critical process.*
☑	☐	Firewall	*The existing firewall allows or*

			blocks traffic based on an appropriately defined set of security rules.
□	☑	Intrusion detection system (IDS)	*Needs to be implemented to monitor network traffic for suspicious activity or potential security threats.*
□	☑	Backups	*Needs to have backups of critical data to protect against data loss due to accidental deletion, hardware failure, or cyberattacks.*
☑	□	Antivirus software	*Antivirus software is installed which helps detect and remove malware from the company's computer systems.*
□	☑	Manual monitoring, maintenance, and intervention for legacy systems	*There is no regular schedule in place for performing manual monitoring and maintenance for legacy systems. This increases the risk of overlooking critical updates or vulnerabilities, potentially leading to system failures or security breaches.*
□	☑	Encryption	*Encryption procedures are not in place; it is essential for protecting sensitive data from unauthorized access during transmission or storage.*
□	☑	Password management system	*There is no password management system currently in place; this can help enforce strong password policies, facilitate password storage and retrieval, and ensure that users adhere to best practices*

			for password security.
☑	□	Locks (offices, storefront, warehouse)	*The company has locks installed at its offices, storefront, and warehouse, which help restrict physical access to these premises.*
☑	□	Closed-circuit television (CCTV) surveillance	*The company has CCTV surveillance installed, providing visual monitoring and recording of activities.*
☑	□	Fire detection/prevention (fire alarm, sprinkler system, etc.)	*The company has fire detection and prevention systems in place.*

Compliance checklist

Select "yes" or "no" to answer the question: *Does Botium Toys currently adhere to this compliance best practice?*

Payment Card Industry Data Security Standard (PCI DSS)

Yes	**No**	**Best practice**	***Explanation***
□	☑	Only authorized users have access to customers' credit card information.	*Currently, all users have access to the company's internal data.*
□	☑	Credit card information is accepted, processed, transmitted, and stored internally, in a secure environment.	*Credit card information is not encrypted currently.*
□	☑	Implement data encryption procedures to better secure credit card transaction	*The company does not have data encryption procedures in place which can be used to provide*

		touchpoints and data.	*confidentiality to user data.*
☐	☑	Adopt secure password management policies.	*Password policies are nominal, and no password management system is currently in place.*

General Data Protection Regulation (GDPR)

Yes	**No**	**Best practice**	***Explanation***
☐	☑	E.U. customers' data is kept private/secured.	*The company does not currently use encryption to ensure the confidentiality of customers' financial information.*
☑	☐	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.	*The company has a plan to notify E.U. customers within 72 hours of a security breach.*
☐	☑	Ensure data is properly classified and inventoried.	*The company needs to classify the assets.*
☑	☐	Enforce privacy policies, procedures, and processes to properly document and maintain data.	*Privacy policies, procedures, and processes have been developed and enforced among IT department members.*

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

Yes	**No**	**Best practice**	***Explanation***
☐	☑	User access policies are established.	*The company needs to establish user access policies.*
☐	☑	Sensitive data (PII/SPII) is confidential/private.	*The company needs to implement encryption procedures to better ensure*

			the confidentiality of sensitive data (PII/SPII).
☑	□	Data integrity ensures the data is consistent, complete, accurate, and has been validated.	*The company has implemented measures to ensure data integrity.*
□	☑	Data is available to individuals authorized to access it.	*The company needs to implement access controls and authentication mechanisms to restrict data access to authorized users based on their roles and permissions.*

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.