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	*Explanation*
□	☑	Least Privilege	*All employees have access to customer data, privileges should be limited to reduce the risk of breach.*
□	☑	Disaster recovery plans	*There are no disaster recovery plans. This should be implemented for business continuity.*
□	☑	Password policies	*Employee password policies are minimal, hence threat actors can easily access the secure data/assets via the employee work equipment/the internal network.*
□	☑	Separation of duties	*Need to be implemented to reduce the possibility of fraud, access to critical data.*
☑	□	Firewall	*The existing Firewall blocks traffic based on an appropriately defined set of security rules.*
□	☑	Intrusion detection system (IDS)	*IDS should be installed, to monitor the data packets, and can identify possible intrusions by threat actors.*
□	☑	Backups	*Backups of critical data is a must, to secure a company's reputation and business continuity,*

			if any threat occurs.
☑	□	Antivirus software	*Antivirus software is installed and monitored regularly by the IT department.*
□	☑	Manual monitoring, maintenance, and intervention for legacy systems	*The list of assets notes the use of legacy systems. The risk assessment indicates that these systems are monitored and maintained, but there is not a regular schedule in place for this task and procedures/ policies related to intervention are unclear, which could place these systems at risk of a breach.*
□	☑	Encryption	*Encryption of Critical data should be implemented, to maintain confidentiality of the data.*
□	☑	Password management system	*Implementing this control would help in password management for employees and users.*
☑	□	Locks (offices, storefront, warehouse)	*The store's physical location, which includes Botium Toys' main offices, store front, and warehouse of products, has sufficient locks.*
☑	□	Closed-circuit television (CCTV) surveillance	*Up-to-data Closed-circuit television(CCTV) surveillance is mantained.*
☑	□	Fire detection/prevention (fire alarm, sprinkler system, etc.)	*Botium Toys' has well functioning Fire detection and prevention systems.*

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**	***Explanation***
□	☑	Only authorized users have access to customers' credit card information.	*All employees has access to internally stored data, RBAC(role-based access control) should be implemented.*
□	☑	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.	*All employees may be able to access cardholder data and customers' PII/SPII data, which can lead to data loss, hence credit card information should be securely stored and can only be accessible to a particular group of employees or administrators.*
□	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.	*The company needs to use encryption, to maintain confidentiality.*
□	☑	Adopt secure password management policies.	*Password policies are nominal and no password management system has been implemented.*

General Data Protection Regulation (GDPR)

Yes	**No**	**Best practice**	***Explanation***
□	☑	E.U. customers' data is kept private/secured.	*No encryption process is maintained to secure*

			the confidentiality of the data.
☑	□	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.	*The IT department has established a plan to notify E.U. customers within 72 hours if there is a security breach.*
□	☑	Ensure data is properly classified and inventoried.	*Current assets have been listed/inventoried, not classified.*
☑	□	Enforce privacy policies, procedures, and processes to properly document and maintain data.	*Privacy policies, procedures, and processes have been developed and enforced among IT team members and other employees, as needed.*

<u>System and Organizations Controls (SOC type 1, SOC type 2)</u>

Yes	**No**	**Best practice**	***Explanation***
□	☑	User access policies are established.	*No control policies of Least privilege and separation of duties has been implemented. All employees have access to internal data.*
□	☑	Sensitive data (PII/SPII) is confidential/private.	*All employees have access to sensitive data, which is not at all a confidential way to store PII/SPII data.*
☑	□	Data integrity ensures the data is	*Data integrity is at place.*

		consistent, complete, accurate, and has been validated.	
□	☑	Data is available to individuals authorized to access it.	*Data is available to all the Botium Toys employees. Least privilege and separation of duty measures should be implemented.*

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.*
- *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.