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	All employees have access to customer data. Privileges need to be limited to reduce the risk of a breach.
□	☑	Disaster recovery plans	There are no disaster recovery plans in place. These need to be implemented to ensure business continuity.
□	☑	Password policies	Employee password requirements are minimal, which could allow a threat actor to easily access secure data/other assets via employee work equipment/the internal network.
□	☑	Separation of duties	Needs to be implemented to reduce the possibility of fraud/access to critical data, since the company CEO currently runs day-to-day operations and manages the payroll.
☑	□	Firewall	The existing firewall blocks traffic based on an appropriately defined set of security rules.
□	☑	Intrusion detection system (IDS)	The IT department needs an IDS in place to help identify possible

			intrusions by threat actors.
□	☑	Backups	The IT department needs to have backups of critical data, in case a breach occurs to ensure business continuity.
☑	□	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 confirms the use of legacy systems. The risk assessment indicates that these systems are monitored and maintained, but there is no 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 is not used and implementing it would provide greater confidentiality of sensitive information.
□	☑	Password management system	There is no password management system in place. Implementing this control would improve IT department/other employee productivity in the case of password issues.
☑	□	Locks (offices, storefront, warehouse)	The store's physical location, which includes the company's main offices, store front, and warehouse of products, has sufficient locks.
☑	□	Closed-circuit television (CCTV) surveillance	CCTV is installed/functioning at the store's physical location.
☑	□	Fire detection/prevention (fire	Botium Toys' physical location has a

		alarm, sprinkler system, etc.)	functioning fire detection and prevention system.

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.	All employees 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 and all employees currently have access to internal data, including customers’ credit card information.
□	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.	The company does not currently use encryption to ensure the confidentiality of customers’ financial information.
□	☑	Adopt secure password management policies.	Password policies are nominal and no password management system is in place.

General Data Protection Regulation (GDPR)

Yes	No	Best practice	Explanation
□	☑	E.U. customers’ data is kept private/secured.	The company does not 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.	There is a plan to notify E.U. customers within 72 hours of a data breach.
□	☑	Ensure data is properly classified and inventoried.	Current assets have been inventoried/listed, but 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.

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

Yes	**No**	**Best practice**	**Explanation**
□	☑	User access policies are established.	Controls of Least Privilege and separation of duties are not in place and all of the employees have access to internally stored data.
□	☑	Sensitive data (PII/SPII) is confidential/private.	Encryption is not used to better ensure the confidentiality of PII/SPII.
☑	□	Data integrity ensures the data is consistent, complete, accurate, and has been validated.	Data integrity is in place.
□	☑	Data is available to individuals authorized to access it.	While data is available to all employees, authorization needs to be limited to only the individuals who need access to it to do their jobs.

Recommendation:

Botium Toys should immediately enforce the principle of least privilege to ensure confidentiality and integrity of its customers PII/SPII. Currently, all of your employees have unrestricted access to internal systems, which increases the likelihood of unauthorized data exposure.

Data encryption should be implemented for all of your customer credit card information to protect data at rest and in transit. This is essential for PCI DSS compliance and to mitigate risks tied to unencrypted financial data. Addressing both least privilege and encryption are necessary first steps that will address high risk control issues.

In order to strengthen Botium Toys' resilience, it would be prudent to establish a disaster recovery plan and deploy an intrusion detection system as soon as possible. Taking these steps will ensure rapid response and recovery should a system fail or a cyberattack occur.

The company should also revise its password policy to meet modern security standards (the minimum 8 characters, complexity requirement) and adopt a centralized password management system to improve enforcement and reduce support overhead.

Addressing these key issues, especially least privilege and encryption will significantly improve Botium Toys' security posture and ensure alignment with regulatory compliance standards such as PCI, DSS, GDPR, and SOC2.