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	*At present, every staff member has the ability to access customer data; it's imperative to restrict these privileges to mitigate the risk of a breach..*
☐	☑	Disaster recovery plans	*Currently, there are no established disaster recovery plans. It is essential to enact these plans to guarantee uninterrupted business operations.*
☐	☑	Password policies	*The employee password requirements are minimal, posing a risk that threat actors could potentially exploit to gain easier access to secure data or other assets through employee work equipment or the internal network.*
☐	☑	Separation of duties	*Implementation is necessary to diminish the risk of fraud or unauthorized access to critical data. This is especially crucial as the company CEO currently oversees day-to-day operations and manages payroll.*

☑	☐	Firewall	*The current firewall effectively blocks traffic according to a well-defined set of security rules.*
☐	☑	Intrusion detection system (IDS)	*The IT department needs an IDS to aid in the detection of potential intrusions by threat actors.*
☐	☑	Backups	*The IT department must establish backups of critical data to safeguard against breaches and ensure uninterrupted business operations.*
☑	☐	Antivirus software	*Antivirus software is installed and consistently monitored by the IT department.*
☐	☑	Manual monitoring, maintenance, and intervention for legacy systems	*The asset inventory identifies the utilization of legacy systems. The risk assessment highlights that while these systems are monitored and maintained, there is no established regular schedule for these tasks, and procedures/policies concerning intervention are unclear. This lack of clarity could potentially jeopardize the security of these systems and increase the risk of a breach.*
☐	☑	Encryption	*Encryption is presently not utilized. Its implementation would significantly enhance the confidentiality of sensitive information.*

☐	☑	Password management system	*A password management system is not currently in use. Introducing this control would enhance productivity for the IT department and other employees, particularly in addressing password-related issues.*
☑	☐	Locks (offices, storefront, warehouse)	*Adequate locks are installed throughout the store's physical location, encompassing the main offices, storefront, and product warehouse.*
☑	☐	Closed-circuit television (CCTV) surveillance	*CCTV is installed/functioning at the store's physical location.*
☑	☐	Fire detection/prevention (fire alarm, sprinkler system, etc.)	*Botium Toys' physical location has a 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.	*Currently, all employees have access to the company's internal data.*
☐	☑	Credit card information is	*Credit card information remains*

		accepted, processed, transmitted, and stored internally, in a secure environment.	*unencrypted, and all employees currently possess access to internal data, including customers' credit card details.*
☐	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.	*The company does not currently use encryption to better ensure the confidentiality of customers' financial information.*
☐	☑	Adopt secure password management policies.	*Password policies are basic, and there is no existing password management system implemented.*

General Data Protection Regulation (GDPR)

Yes	No	Best practice	***Explanation***
☐	☑	E.U. customers' data is kept private/secured.	*The company currently does not utilize encryption to enhance 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.	*The current assets have been inventoried and listed, but they have not been classified.*
☑	☐	Enforce privacy policies, procedures, and processes to properly document and maintain data.	*Privacy policies, procedures, and processes have been established and enforced among IT team members and other employees, as required..*

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

Yes	No	Best practice	*Explanation*
☐	☑	User access policies are established.	*The principles of Least Privilege and separation of duties are absent, as all employees currently possess access to internally stored data..*
☐	☑	Sensitive data (PII/SPII) is confidential/private.	*Encryption is not currently 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.*

Recommendations (optional):

To enhance Botium Toys' security posture and ensure the confidentiality of sensitive information, a comprehensive set of controls needs to be implemented. These include Least Privilege, disaster recovery plans, robust password policies, separation of duties, an Intrusion Detection System (IDS), ongoing management of legacy systems, encryption, and a password management system.

To bridge compliance gaps, Botium Toys should prioritize the implementation of controls such as Least Privilege, separation of duties, and encryption. Additionally, properly classifying assets will aid in identifying additional controls necessary to bolster their security posture and safeguard sensitive information.