Controls and Compliance Checklist

Controls assessment checklist

Yes	No	Control	*Explanation*
☐	☑	Least Privilege	*At present, all employees possess access to customer data; it's necessary to restrict privileges to minimize the risk of a breach.*
☐	☑	Disaster recovery plans	*There are currently no existing disaster recovery plans. It is imperative to establish these plans to guarantee business continuity.*
☐	☑	Password policies	*The current employee password requirements are minimal, potentially facilitating easier access for threat actors to secure data or other assets through employee work equipment or the internal network.*
☐	☑	Separation of duties	*Implementation is necessary to lower the risk of fraud and unauthorized access to critical data, as the company CEO currently oversees daily operations and manages payroll.*
☑	☐	Firewall	*The current firewall blocks traffic according to a well-defined set of security rules.*

☐	☑	Intrusion detection system (IDS)	*The IT department requires an Intrusion Detection System (IDS) to assist in detecting potential intrusions by malicious actors.*
☐	☑	Backups	*It's essential for the IT department to maintain backups of critical data to secure business continuity in the event of a breach.*
☑	☐	Antivirus software	*The IT department installs antivirus software and conducts regular monitoring.*
☐	☑	Manual monitoring, maintenance, and intervention for legacy systems	*The asset inventory includes legacy systems, which are monitored and maintained according to risk assessment findings. However, there is currently no established regular schedule for these tasks, and the procedures and policies for intervention are unclear. This lack of clarity could potentially expose these systems to security breaches.*
☐	☑	Encryption	*Encryption is not currently employed; its implementation would enhance the confidentiality of sensitive information.*
☐	☑	Password management system	*Currently, there is no password management system in place. Implementing such a system would enhance productivity for both the IT department and other*

			employees when dealing with password-related issues.
☑	☐	Locks (offices, storefront, warehouse)	*The store's physical premises, encompassing the company's main offices, storefront, and product warehouse, are equipped with adequate locks.*
☑	☐	Closed-circuit television (CCTV) surveillance	*Closed-circuit television (CCTV) is operational at the store's physical location.*
☑	☐	Fire detection/prevention (fire alarm, sprinkler system, etc.)	*Botium Toys' physical premises are equipped with a functional fire detection and prevention system.*

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.	*At present, all employees can access the company's internal data.*
☐	☑	Credit card information is accepted, processed, transmitted, and stored internally, in a secure environment.	*Credit card information lacks encryption, and all employees currently possess access to internal data, including customer credit card details.*
☐	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.	*The company currently does not employ encryption to enhance the confidentiality of customers' financial information.*

☐	☑	Adopt secure password management policies.	*Password policies are basic, and there is currently no password management system implemented.*

General Data Protection Regulation (GDPR)

Yes	No	Best practice	***Explanation***
☐	☑	E.U. customers' data is kept private/secured.	*Currently, the company 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 strategy in place to inform EU customers within 72 hours of a data breach.*
☐	☑	Ensure data is properly classified and inventoried.	*The existing assets have been inventoried and listed, but not categorized.*
☑	☐	Enforce privacy policies, procedures, and processes to properly document and maintain data.	*Privacy policies, procedures, and processes have been created and implemented within the IT team and other relevant employees.*

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

Yes	No	Best practice	***Explanation***
☐	☑	User access policies are established.	*Currently, there are no controls for Least Privilege and separation of duties in place; all employees have*

			access to internally stored data.
☐	☑	Sensitive data (PII/SPII) is confidential/private.	*Encryption is currently not implemented to enhance the confidentiality of Personally Identifiable Information (PII) or Sensitive Personally Identifiable Information (SPII).*
☑	☐	Data integrity ensures the data is consistent, complete, accurate, and has been validated.	*Data integrity measures are implemented.*
☐	☑	Data is available to individuals authorized to access it.	*Although data is accessible to all employees, authorization should be restricted to individuals who specifically require access to perform their job duties.*

Recommendations: *Botium Toys should implement several measures to enhance security and safeguard sensitive information. These include adopting Least Privilege, establishing disaster recovery plans, enforcing robust password policies, implementing separation of duties, deploying an Intrusion Detection System (IDS), maintaining legacy systems, employing encryption, and setting up a password management system.*

To ensure compliance and strengthen security, Botium Toys must prioritize implementing controls such as Least Privilege, separation of duties, and encryption. Additionally, the company should classify assets accurately to identify further necessary controls that can enhance security posture and protect sensitive information effectively.