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 currently have access to customer data. Access privileges should be restricted to minimize the risk of a breach.*
☐	☑	Disaster recovery plans	*There are no disaster recovery plans in place. These plans need to be developed to ensure business continuity in the event of a disruption.*
☐	☑	Password policies	*Employee password policies are minimal, potentially allowing a threat actor easier access to secure data or other assets through employee devices or the internal network.*
☐	☑	Separation of duties	*The company’s CEO currently manages daily operations and payroll. Implementing additional measures is necessary to mitigate the risk of fraud and unauthorized access to critical data.*
☑	☐	Firewall	*The current firewall blocks traffic based on a well-defined set of security rules.*
☐	☑	Intrusion detection system (IDS)	*The IT department needs an Intrusion Detection System (IDS) to detect potential intrusions by threat actors.*
☐	☑	Backups	*The IT department must maintain backups of critical data to ensure business continuity in the event of a breach.*

☑	☐	Antivirus software	*Antivirus software is installed and regularly monitored by the IT department.*
☐	☑	Manual monitoring, maintenance, and intervention for legacy systems	*The asset inventory notes the use of legacy systems. These these systems are monitored and maintained, but there is no established maintenance schedule. The intervention procedures and policies are unclear, potentially exposing these systems to security risks.*
☐	☑	Encryption	*Encryption is not currently in use. Implementing encryption would enhance the confidentiality of sensitive information.*
☐	☑	Password management system	*There is no password management system in place. Implementing this control would improve productivity for the IT department and employees in managing password-related issues.*
☑	☐	Locks (offices, storefront, warehouse)	*The physical location of the store, including the main offices, storefront, and warehouse, is secured with adequate locks. CCTV is installed and operational at this location. Botium Toys' physical premises are equipped with a functioning fire detection and prevention system.*
☑	☐	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.	*All employees currently have access to the company’s internal data.*
☐	☑	Credit card information is accepted, processed, transmitted, and stored internally, in a secure environment.	*No encryption is currently used and employees 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 better ensure the confidentiality of customers’ financial information.*
☐	☑	Adopt secure password management policies.	*Password policies are nominal with no central password management system 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 use encryption and have not established separation of duties to ensure 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 IT department has established a pllan 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 are enforced among IT department members/other employees.*

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 currently in place; all employees have access to internally stored data.*
☐	☑	Sensitive data (PII/SPII) is confidential/private.	*Currently there is no use of encryption to 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.	*Internal data is currently available to all employees, posing a security risk. Authorization needs to be limited to only the individuals who need access to it to do their jobs.*

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.

To enhance Botium Toys' security posture and better safeguard sensitive information, several controls need to be implemented, 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 compliance gaps, Botium Toys should implement controls such as Least Privilege, separation of duties, and encryption. The company must also ensure proper asset classification to identify any additional controls that may be required to strengthen its security posture and better protect sensitive data.