Controls and compliance checklist exemplar

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	Right now every employee can access customer information. Permissions need to be limited so only those who require access can view this data, which will help decrease the risk of a data breach.
☐	☑	Disaster recovery plans	*There is no documented plan for restoring operations after a major outage or cyber incident. A disaster recovery plan is needed to ensure the business can continue operating if systems fail.*
☐	☑	Password policies	*Current password standards are too weak. Stronger password requirements are needed to prevent unauthorized access to employee devices and internal systems.*
☐	☑	Separation of duties	*The CEO is managing both business operations and payroll, which concentrates too much control in one role. Separating responsibilities*

			would reduce the risk of fraud or misuse.
☑	☐	Firewall	*A firewall has been implemented and is configured with appropriate security rules to block unauthorized traffic from entering the network.*
☐	☑	Intrusion detection system (IDS)	*There is no IDS present to monitor the network for suspicious activity. Adding one would make it easier to detect potential intrusions.*
☐	☑	Backups	*Critical files are not currently backed up. The organization needs reliable backups to protect against data loss and support recovery after a security incident.*
☑	☐	Antivirus software	*Antivirus protection is installed and is being actively monitored by the IT department to detect and prevent malware.*
☐	☑	Manual monitoring, maintenance, and intervention for legacy systems	*Legacy systems are monitored, but only informally. There is no schedule or documented procedures for maintenance, which increases the risk of system compromise.*
☐	☑	Encryption	*Sensitive information is not encrypted. Adding encryption would increase confidentiality and protect customer and payment data.*
☐	☑	Password management system	*There is no password management tool in use.*

			Implementing one would reduce password-related IT issues and support stronger access security.
☑	☐	Locks (offices, storefront, warehouse)	*Physical security for the building appears sufficient. Doors at the office, storefront, and warehouse are properly secured.*
☑	☐	Closed-circuit television (CCTV) surveillance	*CCTV cameras are present at the physical location and functioning properly.*
☑	☐	Fire detection/prevention (fire alarm, sprinkler system, etc.)	*The building has working fire alarms and fire prevention systems, which protect both staff and assets.*

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 internal data, which means credit card information is not restricted to authorized personnel only.*
☐	☑	Credit card information is accepted, processed, transmitted, and stored	*Customer payment data is not encrypted and access is not limited to necessary employees,*

		internally, in a secure environment.	*meaning PCI DSS security requirements are not being met.*
☐	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.	*Encryption is not used, so financial information is not protected during storage or transmission.*
☐	☑	Adopt secure password management policies.	*There is no password management system in place and current password standards are weak, which increases the risk of unauthorized access.*

General Data Protection Regulation (GDPR)

Yes	No	Best practice	***Explanation***
☐	☑	E.U. customers' data is kept private/secured.	*The company does not currently use encryption to protect customer information, which places E.U. customer privacy at risk.*
☑	☐	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.	*The organization has an established procedure that aligns with GDPR requirements for breach notification within 72 hours.*
☐	☑	Ensure data is properly classified and inventoried.	*While assets have been recorded, there is no formal system to classify data based on sensitivity or business requirements.*
☑	☐	Enforce privacy policies, procedures, and processes to properly document and maintain data.	*The company has documented privacy policies and enforces them across 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.	*Least privilege and separation of duties are not applied, so all employees can access the company's internal stored data.*
☐	☑	Sensitive data (PII/SPII) is confidential/private.	*The organization does not use encryption to protect personal and sensitive personal information, leaving the data exposed.*
☑	☐	Data integrity ensures the data is consistent, complete, accurate, and has been validated.	*Current systems support the accuracy and consistency of organizational data.*
☐	☑	Data is available to individuals authorized to access it.	*Although data is available, access is not restricted based on job requirements — all employees can view customer information, including those who do not need it.*