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	*All staff members currently have access to customer data; therefore, privileges must be restricted to lower the possibility of a breach.*
☐	☑	Disaster recovery plans	*Plans for disaster recovery are nonexistent. Implementing these is necessary to guarantee business continuity.*
☐	☑	Password policies	*The lack of strict password requirements for employees may make it easier for a threat actor to gain access to confidential information or other assets through employee work equipment or the internal network.*
☐	☑	Separation of duties	*Implementation is necessary to lessen the likelihood of fraud or unauthorized access to vital data, as the CEO of the company currently oversees daily operations and payroll.*
☑	☐	Firewall	*Traffic is blocked by the current firewall according to a suitably defined set of security*

			rules.
☐	☑	Intrusion detection system (IDS)	*IDS must be implemented by the IT department in order to assist in locating potential threat actor intrusions.*
☐	☑	Backups	*In the event of a breach, the IT department must keep backups of vital information to guarantee company continuity.*
☑	☐	Antivirus software	*The IT department routinely installs and maintains antivirus software.*
☐	☑	Manual monitoring, maintenance, and intervention for legacy systems	*The utilization of old systems is mentioned in the list of assets. The risk assessment shows that these systems are kept up to date and monitored, but there isn't a set timetable for this work and there are ambiguous intervention-related regulations and procedures, which could put these systems at danger of being compromised.*
☐	☑	Encryption	*Since encryption is not currently in use, putting it into practice would increase the secrecy of sensitive data.*
☐	☑	Password management system	*Currently, there is no password management system in place; adding this control will increase the productivity of the IT department and other staff*

			members in the event that password problems arise.
☑	☐	Locks (offices, storefront, warehouse)	*The company's main offices, retail space, and goods warehouse are all physically secured with enough locks.*
☑	☐	Closed-circuit television (CCTV) surveillance	*The actual site of the store has CCTV installed and operational.*
☑	☐	Fire detection/prevention (fire alarm, sprinkler system, etc.)	*There is a working fire detection and prevention system at the physical location of Botium Toys.*

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 staff members currently have access to internal corporate data.*
☐	☑	Credit card information is accepted, processed, transmitted, and stored internally, in a secure environment.	*Currently, internal data, including credit card information from clients, is accessible to all staff and is not encrypted.*
☐	☑	Implement data encryption procedures to better secure credit card transaction	At the moment, the business does not employ encryption to further protect the privacy of its clients'

		touchpoints and data.	financial information.
☐	☑	Adopt secure password management policies.	*There isn't a password management system in place at the moment, and password policies are minimal.*

General Data Protection Regulation (GDPR)

Yes	No	Best practice	*Explanation*
☐	☑	E.U. customers' data is kept private/secured.	*To further protect the privacy of its customers' financial information, the company does not currently use encryption.*
☑	☐	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.	*When a data breach occurs, clients in the EU are supposed to be notified within 72 hours.*
☐	☑	Ensure data is properly classified and inventoried.	*While listed and inventoried, current assets have not yet been classified.*
☑	☐	Enforce privacy policies, procedures, and processes to properly document and maintain data.	*When necessary, the IT team and other staff members have created and implemented privacy policies, procedures, and processes.*

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

Yes	No	Best practice	*Explanation*
☐	☑	User access policies are established.	*Limitations of the Least There are currently no privileges or divisions of responsibilities,*

			and all employees have access to data that is kept internally.
☐	☑	Sensitive data (PII/SPII) is confidential/private.	*PII/SPII confidentiality is not currently improved by the use of encryption.*
☑	☐	Data integrity ensures the data is consistent, complete, accurate, and has been validated.	*There is data integrity.*
☐	☑	Data is available to individuals authorized to access it.	*Although all employees have access to the data, authorization should only be granted to those who require it in order to perform their tasks.*

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.

Multiple controls need to be implemented to improve Botium Toys' security posture and better ensure the confidentiality of sensitive information, 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 gaps in compliance, Botium Toys needs to implement controls such as Least Privilege, separation of duties, and encryption. The company also needs to properly classify assets, to identify additional controls that may need to be implemented to improve their security posture and better protect sensitive information.