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	At present, every employee has access to customer data; however, access to this data should be limited to authorized personnel exclusively to mitigate the risk of potential data breaches.
□	☑	Disaster recovery plans	*There are no disaster recovery plans in place. To maintain operational resilience, the organization must develop and implement comprehensive disaster recovery strategies.*
□	☑	Password policies	*The organization's lax employee password requirements pose a significant risk, as they could enable threat actors to gain unauthorized access to sensitive data and critical assets through compromised employee devices or the internal network.*
□	☑	Separation of duties	*To mitigate the risk of fraud and unauthorized access to sensitive data, the company must implement segregation of duties, as the current*

			centralization of operational and financial responsibilities under the CEO poses a significant control weakness.
☑	□	Firewall	*The current firewall configuration effectively filters network traffic by enforcing a properly configured set of security policies.*
□	☑	Intrusion detection system (IDS)	*To enhance the organization's ability to detect potential cyber threats, the IT department should implement an Intrusion Detection System (IDS) that can identify and alert on suspicious activities indicative of attempted or successful intrusions.*
□	☑	Backups	*To safeguard against data loss and ensure operational continuity in the event of a security breach, the IT department must implement robust backup and recovery procedures for mission-critical data assets.*
☑	□	Antivirus software	*The IT department diligently maintains and monitors the organization's antivirus software installations, ensuring timely updates and effective protection against malware threats.*
□	☑	Manual monitoring, maintenance, and intervention for legacy	*While the asset inventory identifies the presence of legacy systems, and the risk*

		systems	*assessment acknowledges ongoing monitoring and maintenance efforts, the lack of a well-defined schedule and clear policies governing intervention procedures poses a potential vulnerability, leaving these outdated systems susceptible to security breaches.*
☐	☑	Encryption	*The absence of encryption measures within the current setup compromises the confidentiality of sensitive information. Implementing robust encryption protocols would significantly enhance the protection and privacy of critical data assets.*
☐	☑	Password management system	*The absence of a centralized password management system hinders productivity, as the implementation of such a solution would streamline the process of addressing password-related issues, thereby enhancing efficiency for both the IT department and other employees across the organization.*
☑	☐	Locks (offices, storefront, warehouse)	*The physical premises, encompassing the main offices, storefront, and product warehouse, are adequately secured with appropriate locking mechanisms.*
☑	☐	Closed-circuit television (CCTV) surveillance	*Comprehensive closed-circuit television (CCTV) surveillance is operational and monitoring*

			the store's physical premises.
☑	☐	Fire detection/prevention (fire alarm, sprinkler system, etc.)	*Botium Toys' physical facility is equipped with a functional fire detection and suppression system to mitigate fire-related risks.*

Compliance checklist

Select “yes” or “no” to answer the question: *Does Botium Toys currently adhere to this compliance best practice?*

<u>Payment Card Industry Data Security Standard (PCI DSS)</u>

Yes	No	Best practice	*Explanation*
☐	☑	Only authorized users have access to customers’ credit card information.	*The existing access control measures grant all employees unrestricted access to the company's internal data, posing a potential risk of unauthorized data exposure or misuse.*
☐	☑	Credit card information is accepted, processed, transmitted, and stored internally, in a secure environment.	*The lack of encryption for credit card information, coupled with the organization's current practice of granting all employees unrestricted access to internal data, including customers' sensitive financial details, poses a severe risk of data breaches and unauthorized exposure of confidential payment information.*
☐	☑	Implement data encryption procedures to better secure credit card transaction	The organization's failure to implement encryption protocols compromises the confidentiality

		touchpoints and data.	of customers' financial information, leaving sensitive data vulnerable to potential unauthorized access or interception.
☐	☑	Adopt secure password management policies.	*The organization's password security measures are inadequate, with minimal password policies and a lack of a centralized password management system, increasing the risk of compromised credentials and unauthorized access.*

General Data Protection Regulation (GDPR)

Yes	**No**	**Best practice**	***Explanation***
☐	☑	E.U. customers' data is kept private/secured.	*The organization currently fails to implement encryption mechanisms, thereby jeopardizing the confidentiality of customers' sensitive financial data, which remains susceptible to potential unauthorized access or disclosure.*
☑	☐	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 established protocols to promptly notify European Union customers within 72 hours in the event of a data breach incident, adhering to the mandated disclosure requirements.*
☐	☑	Ensure data is properly classified and inventoried.	*While an inventory of the organization's current assets has been compiled, the assets have yet to be categorized or classified*

			according to their criticality, value, or sensitivity.
☑	□	Enforce privacy policies, procedures, and processes to properly document and maintain data.	*Privacy policies, procedures, and processes have been formulated and implemented among IT team members and other relevant staff as required.*

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

Yes	**No**	**Best practice**	***Explanation***
□	☑	User access policies are established.	*The implementation of Least Privilege controls and separation of duties is absent; all employees currently possess access to internally stored data.*
□	☑	Sensitive data (PII/SPII) is confidential/private.	*Encryption is presently not employed to enhance the confidentiality of PII/SPII.*
☑	□	Data integrity ensures the data is consistent, complete, accurate, and has been validated.	*Data integrity measures have been established.*
□	☑	Data is available to individuals authorized to access it.	*Although data is accessible to all employees, authorization should be restricted to only those individuals who require access to perform their job duties.*

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.

Several measures must be implemented to enhance Botium Toys' security stance and reinforce the confidentiality of sensitive information, encompassing: Least Privilege, disaster recovery plans, password policies, separation of duties, an IDS, continuous management of legacy systems, encryption, and a password management system.

To rectify compliance deficiencies, Botium Toys should enact measures such as Least Privilege, separation of duties, and encryption. Additionally, the company must accurately classify assets to discern further controls necessary for enhancing their security posture and safeguarding sensitive information more effectively.