Controls and compliance checklist

Type an X “yes” or “no” column 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 unrestricted access to customer data. Access privileges should be restricted to minimize the potential risk of a security breach.
☐	☑	Disaster recovery plans	Currently, there are no disaster recovery plans in place. These need to be implemented to ensure business continuity.
☐	☑	Password policies	Employee password requirements are minimal, which could allow a threat actor to more easily access secure data/other assets via employee work equipment/the internal network.
☐	☑	Separation of duties	Needs to be implemented to reduce the possibility of fraud/access to critical data, since the company CEO currently runs day-to-day operations and manages the payroll.
☑	☐	Firewall	The existing firewall blocks traffic based on an appropriately defined set of security rules.

Yes	No	Control	Explanation
☐	☑	Intrusion detection system (IDS)	The IT department has not yet implemented an IDS, which would help identify possible intrusions by threat actors.
☐	☑	Backups	The IT department needs to have backups of critical data, in the case of a breach, to ensure business continuity.
☑	☐	Antivirus software	Antivirus software is installed and monitored regularly by the IT department.
☐	☑	Manual monitoring, maintenance, and intervention for legacy systems	The list of assets notes the use of legacy systems. The risk assessment indicates that these systems are monitored and maintained, but there is no defined schedule for regular maintenance and the procedures for intervention are unclear, leaving these systems vulnerable to potential security risks.
☐	☑	Encryption	Encryption is not currently used, implementing it would provide greater confidentiality of sensitive information.
☐	☑	Password management system	There is no password management system currently in place, implementing this control would improve IT department/other employee productivity in the case of password issues.
☑	☐	Locks (offices, storefront, warehouse)	Botium Toys physical premises, which include the main office, store front, and warehouse, are secured with sufficient locks.
☑	☐	Closed-circuit television (CCTV) surveillance	CCTV is installed/functioning at the store’s physical location.

Yes	No	Control	Explanation
☑	☐	Fire detection/prevention (fire alarm, sprinkler system, etc.)	Botium Toys physical location has a functioning fire detection and prevention system.

Compliance checklist

Type an X in the "yes" or "no" column 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 stored, accepted, processed, and transmitted internally, in a secure environment.	Credit card information is not encrypted and all employees currently have access to internal data, including customer's 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 and no password management system is 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 currently employ encryption to better ensure 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 plan 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 according to their importance or sensitivity.
☑	☐	Enforce privacy policies, procedures, and processes to properly document and maintain data.	Privacy policies, procedures, and processes have been established and enforced among IT team members and other employees, as needed.

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.	The company does not currently utilize encryption to protect PII/SPII, which could put customer data at greater risk in the event of a breach.
☑	☐	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.	While data is available to all employees, access should be restricted to only those who require it to perform their job duties, to reduce the likelihood of unauthorized access to sensitive information.

Recommendations: To enhance Botium Toys security posture and better safeguard sensitive information, several critical controls need to be put in place. These include enforcing the principle of Least Privilege, implementing disaster recovery plans, establishing stronger password policies, applying separation of duties, deploying an Intrusion Detection System (IDS), maintaining legacy systems on a regular schedule, using encryption, and introducing a password management system.

To address existing compliance gaps, Botium Toys should prioritize the implementation of controls such as Least Privilege, separation of duties, and encryption. Additionally, the company should classify its assets properly, which will help identify further controls needed to strengthen security measures and protect sensitive data.