Controls and compliance checklist

Then, 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	Currently, all employees have access to customer data; privileges must be limited to reduce risk and overall impact of malicious insider or compromised accounts.
□	☑	Disaster recovery plans	There are no disaster recovery plans currently in place, this affects the business continuity.
□	☑	Password policies	Password requirements are minimal, which can lead a threat actor to have easier access to the assets.
□	☑	Separation of duties	Need to be implemented to reduce risk and overall impact of malicious insider or compromised accounts. Critical actions should rely on multiple people.
☑	□	Firewall	Firewall is blocking traffic based on an appropriately defined set of security rules.
□	☑	Intrusion detection system (IDS)	The IT department needs an IDS to help in the detection of possible intrusions from threat actors.

☐	☑	Backups	There are no backups of critical data, in 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	Needs to implement a regular schedule in the monitoring, maintenance and intervention in those systems. This is necessary to identify and manage threats, risks or vulnerabilities.
☐	☑	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 and other employee productivity in the case of password issues.
☑	☐	Locks (offices, storefront, warehouse)	The company building has sufficient locks.
☑	☐	Closed-circuit television (CCTV) surveillance	The CCTV surveillance is up-to-date.
☑	☐	Fire detection/prevention (fire alarm, sprinkler system, etc.)	Fire detection/prevention is functioning.

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

Compliance checklist

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 have access to internally stored data and may be able to access cardholder data and customers’ PII/SPII.
□	☑	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.	Credit card information is stored locally in the company’s internal database.
□	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.	Encryption is not currently used to ensure confidentiality of customers’ credit card information
□	☑	Adopt secure password management policies.	Password requirements are minimal and no password management.

General Data Protection Regulation (GDPR)

Yes	No	Best practice	Explanation
□	☑	E.U. customers’ data is kept private/secured.	Encryption is not currently used 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 plan to notify E.U. customers within 72 hours if there is a security breach.
□	☑	Ensure data is properly classified and inventoried.	Current assets have been inventoried but not classified. Classifying is important to determine the impact of the loss of existing assets.
☑	□	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 and other employees,

<u>System and Organizations Controls (SOC type 1, SOC type 2)</u>

Yes	**No**	**Best practice**	**Explanation**
□	☑	User access policies are established.	Control of least privilege and separation of duties have not been implemented. All employee have access to internally stored data.
□	☑	Sensitive data (PII/SPII) is confidential/private.	Encryption is not currently used to ensure confidentiality of customers
☑	□	Data integrity ensures the data is consistent, complete, accurate, and has been validated.	The IT department has ensured availability and integrated controls to ensure data integrity.

□	☑	Data is available to individuals authorized to access it.	Since data is available to all employees, authorization needs to be limited to only the individuals who need access to it to do their job.

Recommendations: 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 controls need to be implemented to improve the company's overall security that include: Least of privilege, separation of duties, disaster recovery plans, password policies, IDS (intrusion detection system), legacy system schedule, encryption, and password management.

To achieve gaps in compliance, the company needs to implement controls such as Least of privilege, separation of duties and encryption. The company needs to properly classify assets to improve its security posture and better protect sensitive information.