Controls and Compliance Checklist

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 employees have access to internally stored data. Access should be limited to employees that need it to perform their role.
☐	☑	Disaster recovery plans	There are no disaster recovery plans in place. These should be implemented to preserve business continuity in the event of a breach.
☐	☑	Password policies	While password policies exist, they are insufficient. Compliance with password requirements should be met.
☐	☑	Separation of duties	This should be implemented to prevent fraud.
☑	☐	Firewall	Firewall exists and is functioning appropriately.
☐	☑	Intrusion detection system (IDS)	There is no IDS, which could help detect when a threat actor is attempting to take sensitive information.
☐	☑	Backups	Backups are lacking and should be set up to preserve business continuity.

☑	☐	Antivirus software	AV software is in use and regularly monitored.
☐	☑	Manual monitoring, maintenance, and intervention for legacy systems	While legacy systems are monitored and maintained, there is not a clear intervention plan established.
☐	☑	Encryption	Encryption is not used, increasing the risk of a threat actor collecting sensitive information.
☐	☑	Password management system	There is no password management system in place to preserve business continuity in the event of a password issue.
☑	☐	Locks (offices, storefront, warehouse)	Locks are present and adequate.
☑	☐	Closed-circuit television (CCTV) surveillance	CCTV is present and adequate.
☑	☐	Fire detection/prevention (fire alarm, sprinkler system, etc.)	Fire detection and prevention is present and adequate.

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 internal data.

☐	☑	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.	Credit card information is not encrypted and employees may have access to credit card data.
☐	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.	Encryption is not in place.
☐	☑	Adopt secure password management policies.	Password policies are nominal and inadequate. There is no password management system in place.

General Data Protection Regulation (GDPR)

Yes	No	Best practice	Explanation
☐	☑	E.U. customers' data is kept private/secured.	Encryption is not in place.
☑	☐	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 the E.U. within 72 hours in the event of a breach.
☐	☑	Ensure data is properly classified and inventoried.	Data is inventoried but not classified.
☑	☐	Enforce privacy policies, procedures, and processes to properly document and maintain data.	Current policies, procedures, and processes exist and are enforced by the IT department.

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 in place.
☐	☑	Sensitive data (PII/SPII) is confidential/private.	Encryption is not in place.
☑	☐	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.	Data is available to all employees. There is no control of least privilege in place to determine access to sensitive information based on role.

Recommendations:

The findings from the internal security audit show significant cybersecurity risks to data security. In particular, there is a lack of administrative and technical controls to protect data from threat actors. The audit finds sufficient physical controls and does not recommend additional controls. While the company assets have been inventoried, they have not yet been classified. This should be done to help identify additional necessary controls. The below controls are recommended for implementation to reduce attack vectors of threat actors and increase the security posture of Botium Toys.

Administrative/Managerial Controls			
Control Name	**Control Type**	**Control Purpose**	**Priority**
Least Privilege	Preventative	Reduce risk and overall impact of malicious insider or compromised accounts	High
Disaster recovery plans	Corrective	Provide business continuity	Medium
Password policies	Preventative	Reduce likelihood of account compromise through brute force or dictionary attack techniques	Low
Access control policies	Preventative	Bolster confidentiality and integrity by defining which groups can access or modify data	High
Account management policies	Preventative	Managing account lifecycle, reducing attack surface, and limiting overall impact from disgruntled former employees and default account usage	Medium
Separation of duties	Preventative	Reduce risk and overall impact of malicious insider or compromised accounts	High

Technical Controls			
Control Name	**Control Type**	**Control Purpose**	**Priority**
IDS/IPS	Detective	To detect and prevent anomalous traffic that matches a signature or rule	High
Encryption	Deterrent	Provide confidentiality to sensitive information	High
Backups	Corrective	Restore/recover from an event	Medium
Password management	Preventative	Reduce password fatigue	High
Antivirus (AV) software	Corrective	Detect and quarantine known threats	High