Botium Toys 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	*Not implemented.*
□	☑	Disaster recovery plans	*No disaster recovery plans in place.*
□	☑	Password policies	*Policy is in place, but is not sufficient and needs to be improved.*
□	☑	Separation of duties	*Not implemented.*
☑	□	Firewall	*Botium Toys has an appropriate firewall in place.*
□	☑	Intrusion detection system (IDS)	*No intrusion detection system (IDS) in place.*
□	☑	Backups	*No backups of critical company data.*
☑	□	Antivirus software	*Software is installed and monitored regularly.*
□	☑	Manual monitoring, maintenance, and intervention for legacy systems	*Legacy systems are monitored and maintained, however there is no schedule for tasks and lack of intervention.*
□	☑	Encryption	*Customer credit card information is not being encrypted on the locally stored internal database.*

☐	☑	Password management system	*Current password management system does not enforce the password policy's minimum requirements.*
☑	☐	Locks (offices, storefront, warehouse)	*Locks are in compliance.*
☑	☐	Closed-circuit television (CCTV) surveillance	*CCTV is appropriate.*
☑	☐	Fire detection/prevention (fire alarm, sprinkler system, etc.)	*Systems are in place and functional.*

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 Botium Toys employees have access to customer credit card information and customers PII/SPII.*
☐	☑	Credit card information is accepted, processed, transmitted, and stored internally, in a secure environment.	*Not encrypted and employee's have access to internal data which includes customer credit card information.*
☐	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.	*Confidentiality is at risk due to lack of encryption.*

☐	☑	Adopt secure password management policies.	*Requirements do not meet current minimum password complexity requirements.*

General Data Protection Regulation (GDPR)

Yes	No	Best practice	*Explanation*
☐	☑	E.U. customers' data is kept private/secured.	*Encryption is currently not used to ensure customer credit card confidentiality.*
☑	☐	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 an establishing plan to notify E.U. customers within 72 hours if there is a security breach.*
☐	☑	Ensure data is properly classified and inventoried.	*Assets are inventoried and listed, but need to be classified.*
☑	☐	Enforce privacy policies, procedures, and processes to properly document and maintain data.	*Are implemented and enforced among the IT department members and other employees.*

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

Yes	No	Best practice	*Explanation*
☐	☑	User access policies are established.	*All Botium Toys employees have access to customer credit card information and customers PII/SPII.*
☐	☑	Sensitive data (PII/SPII) is confidential/private.	*Encryption is not implemented.*

☑	□	Data integrity ensures the data is consistent, complete, accurate, and has been validated.	*Data integrity is implemented.*
□	☑	Data is available to individuals authorized to access it.	*All Botium Toys employees have access to customer credit card information and customers PII/SPII. Only those with authorization should have access.*

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.

Currently Botium Toys' security posture and data confidentiality is insufficient. Current recommendations would be to implement: Least Privilege, disaster recovery plans, password policies, separation of duties, IDS, proper legacy system management, encryption, and a proper password management system.

In regards to compliance, Botium Toys does not meet any current regulatory standards. The company currently has control and compliance issues that could see implementation or improvement, such as: Least Privilege, separation of duties, encryption, and proper classification of assets. Changes to controls and compliance would allow Botium Toys to be in compliance and improve security posture.