Controls and compliance checklist

Botium Toys: Scope, goals, and risk assessment report

Controls assessment checklist

Yes	No	Control	*Explanation*
☐	☑	Least Privilege	*All employees have access to customer data.*
☐	☑	Disaster recovery plans	*There are no disaster recovery plans in place.*
☐	☑	Password policies	*Employee password requirements are minimal and need to be more demanding*
☐	☑	Separation of duties	*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.*
☐	☑	Intrusion detection system (IDS)	*There is no IDS in place to help identify possible intrusions by threat actors.*
☐	☑	Backups	*There are no backups of critical data.*
☑	☐	Antivirus software	*Antivirus software is installed and monitored regularly by the IT department.*
☐	☑	Manual monitoring,	*There is not a regular schedule*

		maintenance, and intervention for legacy systems	*in place for this task and procedures/ policies related to intervention are unclear.*
☐	☑	Encryption	*Encryption is not currently used.*
☐	☑	Password management system	*There is no password management system currently in place.*
☑	☐	Locks (offices, storefront, warehouse)	*The store's physical locations have sufficient locks.*
☑	☐	Closed-circuit television (CCTV) surveillance	*CCTV is installed/functioning at the store's physical location.*
☑	☐	Fire detection/prevention (fire alarm, sprinkler system, etc.)	*Botium Toys' physical location has a functioning fire detection and prevention system.*

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 the company's internal data.*
☐	☑	Credit card information is accepted, processed, transmitted, and stored internally, in a secure environment.	*Credit card information is not encrypted and all employees have access to internal data, including customers' credit card information.*
☐	☑	Implement data encryption procedures to better secure	*The company does not use encryption to better ensure the*

		credit card transaction touchpoints and data.	*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 use 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.*
☑	☐	Enforce privacy policies, procedures, and processes to properly document and maintain data.	*Privacy policies, procedures, and processes have been developed 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 in place.*
☐	☑	Sensitive data (PII/SPII) is confidential/private.	*Encryption is not currently used to better ensure the confidentiality of PII/SPII.*
☑	☐	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, authorization needs to be limited to only the individuals who need access to it to do their jobs.*

Recommendations (optional):

Multiple controls need to be implemented to improve Botium Toys' security posture and ensure the confidentiality of sensitive information, including Least Privilege, disaster recovery plans, password policies, separation of duties, an IDS, ongoing legacy system management, encryption, and a password management system.

To address these gaps in compliance, Botium Toys needs to implement controls such as Least Privilege, separation of duties, and encryption. The company also needs to properly classify assets, to identify additional controls that may need to be implemented to improve their security posture and better protect sensitive information.