Botium Toys: Controls and compliance checklist

Control assessment checklist

Yes	No	Control Name	Control Explaination
□	☑	Least Privilege	Employees have access to customer data; privileges need to limited to reduce risk of a breach
□	☑	Disaster Recovery Plan	Company does not have any Data Recovery plans. It needs to be implement.
□	☑	Password Policies	Password policy in place is not in line with current minimum password complexity requirements;
□	☑	Separartion of Duties	Needs to be implemented; Ceo runs day to day operations
☑	□	Firewall	IT department has a firewall that blocks traffic based on an appropriately defined set of security rules
□	☑	IDS/PS	Currently no IDS/PS is installed exposing business to intrusions
□	☑	Encryption	IT should use encryption to store confidential customers' data
□	☑	Backups	IT needs to set up a plan for freqeuent backups of critical data
□	☑	Password management	No password management in place;
☑	□	Antivirus (AV) software	Antivirus is installed and monitored regularly
□	☑	Manual monitoring, maintenance, and intervention	Regular schedule needs to be implemented to monitor legacy sytems
☑	□	Locks	Company's physical location have sufficient locks to prevent physical access
☑	□	Closed-circuit television (CCTV)	An up to date CCTV monitoring is in place
☑	□	Fire detection and prevention	The physical store has functioning Fire detection and prevention

Compliance checklist

GDPR Compliance			
Yes	**No**	**Best Practice**	**Explaination**
☐	☑	Store customer's data in a secure place	Data is not securely stored
☑	☐	Data breach notification	Company has a plan to notify E.U. customers within 72 hours if there is a security breach
☐	☑	Ensure privacy	Currently employees can easily access customers' data

Payment Card Industry Data Security Standard (PCI DSS)			
Yes	**No**	**Best Practice**	**Explaination**
☐	☑	Encryption of Customer's data	Customers' credit card information is not encrypted
☐	☑	Credit card information is accepted, processed, transmitted, and stored internally, in a secure environment	Data is not securely stored
☐	☑	Limited Access to customer's data	All the employees have access to internally stored data

System and Organizations Controls (SOC type 1, SOC type 2)				
□	☑	User access policy	Currently, controls of least privilage is not in place	No
□	☑	PII/SPII data is confidential	Customers' PII/SPII is easily available	No
☑	□	Data Integrity	IT has integrated controls to ensure data integrity	Yes
□	☑	Authorization	Currently, all the employees have access to internally stored data	No