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	*There is no least privilege, every employee has access to all customer data including PII, and SPII. There needs to be least privilege to reduce risk to a breach.*
□	☑	Disaster recovery plans	*No disaster recovery plans are in place. With no backups, so everything could be lost, and business may not be able to continue.*
□	☑	Password policies	*The password requirements are minimal, and don’t meet complexity safe requirements. A malicious actor could more easily access sensitive data.*
□	☑	Separation of duties	*The CEO operates all day-to-day operations and payroll. Separation of duties need to be implemented to reduce the possibility of fraud/access to critical data,*
☑	□	Firewall	*The company has a firewall that blocks traffic based on an appropriately defined set of security rules.*

□	☑	Intrusion detection system (IDS)	*The IT department doesn't use an IDS to identify possible intrusions by threat actors. This is needed for the IT department.*
□	☑	Backups	*Backups of critical data are not used, so significant risk for business continuity exists.*
☑	□	Antivirus software	*Antivirus software is installed and monitored regularly by the IT department.*
□	☑	Manual monitoring, maintenance, and intervention for legacy systems	*Legacy systems are monitored and maintained, but there is not a regular schedule in place for this task and procedures/ policies related to intervention are unclear, which could place these systems at risk of a breach.*
□	☑	Encryption	*No encryption is implemented, so confidentiality is compromised, there is a need for more confidentiality of all sensitive information.*
□	☑	Password management system	*No password management system is in place. so in the case of password recovery or lockout, it would be very difficult to improve productivity since the IT department would not know what steps to take.*
☑	□	Locks (offices, storefront, warehouse)	*There are sufficient locks for the physical locations.*

☑	□	Closed-circuit television (CCTV) surveillance	*A CCTV system is installed and actively monitoring the store's physical location.*
☑	□	Fire detection/prevention (fire alarm, sprinkler system, etc.)	*Botium Toys' does have a fire detection and prevention system in pl.ace.*

Compliance checklist

Select "yes" or "no" to answer the question: *Does Botium Toys currently adhere to this compliance best practice?*

<u>Payment Card Industry Data Security Standard (PCI DSS)</u>

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.*
□	☑	All Credit card information is in a secure environment and is accepted, processed, transmitted, and stored internally.	*No encryption exists with Credit card information additionally all employees have access to internal data, including customers' credit card information.*
□	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.	*The confidentiality of customer's financial information is not strong, since encryption is not implemented in the company.*
□	☑	Adopt secure password management policies.	*No password management system is in place, and the policy doesn't meet minimum complexity standards*

General Data Protection Regulation (GDPR)

Yes	No	Best practice	*Explanation*
□	☑	E.U. customers' data is kept private/secured.	*Data is not secure since there is no encryption 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.	*No classifications have been done, but assets have been inventoried.*
☑	□	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,*

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

Yes	No	Best practice	*Explanation*
□	☑	User access policies are established.	*All employees have access to the data, so access policies like Least Privilege and separation of duties are not implemented.*
□	☑	Sensitive data (PII/SPII) is confidential/private.	*Data that is sensitive is not encrypted so there is no protection, and confidential data is not protected.*
☑	□	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, yet because of least privilege and protection of data, this data should be limited to only those who need to access it to complete their assigned roles.*

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.

Multiple controls need to be implemented to improve Botium Toys' security posture and have confidentiality for sensitive information. This includes adding separation of duties and least privilege, password policies with more secure standards, encryption, Intrusion detection system (IDS) and management for security of the legacy system. Data must be classified to ensure ease of security and organizational management, including PII, and SPII, least privilege, recovery plans, and backup plans.