Project: Conduct a security audit

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	Currently, all employees have access to customer data; privileges need to be limited to reduce the risk of a breach.
	\square	Disaster recovery plans	There are no disaster recovery plans in place. These need to be implemented to ensure business continuity.
		Password policies	Employee password requirements are minimal, which could allow a threat actor to more easily access secure data/other assets via employee work equipment/the internal network.
	\checkmark	Separation of duties	Needs to be implemented to reduce the possibility of fraud/access to critical data, since 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)	The IT department needs an IDS in place to help identify possible intrusions by threat actors.
	\checkmark	Backups	The IT department needs to have backups of critical data, in the case of a breach, to ensure business continuity.
\checkmark		Antivirus software	Antivirus software is installed and monitored regularly by the IT department.
	\searrow	Manual monitoring, maintenance, and intervention for legacy systems	The list of assets notes the use of legacy systems. The risk assessment indicates that these 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.
	\checkmark	Encryption	Encryption is not currently used; implementing it would provide greater confidentiality of sensitive information.
	✓	Password management system	There is no password management system currently in place; implementing this control would improve IT

		department/other employee productivity in the case of password issues.
\square	Locks (offices, storefront, warehouse)	The store's physical location, which includes the company's main offices, store front, and warehouse of products, has sufficient locks.
\checkmark	Closed-circuit television (CCTV) surveillance	CCTV is installed/functioning at the store's physical location.
\square	Fire detection/prevention (fire alarm, sprinkler system, etc.)	Botium Toys' physical location has a functioning fire detection and prevention system.

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
	\checkmark	Only authorized users have access to customers' credit card information.	Currently, 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 currently have access to internal data, including customers' credit card information.
	\checkmark	Implement data encryption procedures to better secure	The company does not currently use encryption to better ensure

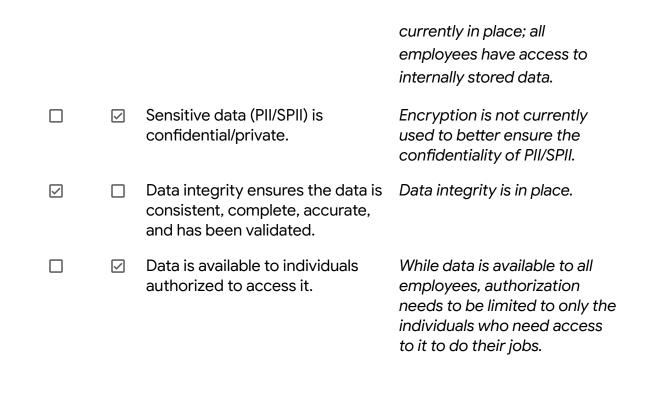
	credit card transaction touchpoints and data.	the confidentiality of customers' financial information.
\checkmark	Adopt secure password management policies.	Password policies are nominal and no password management system is currently in place.

General Data Protection Regulation (GDPR)

Yes	No	Best practice	Explanation
	abla	E.U. customers' data is kept private/secured.	The company does not currently use encryption to better ensure the confidentiality of customers' financial information.
abla		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.
	\checkmark	Ensure data is properly classified and inventoried.	Current assets have been inventoried/listed, but not classified.
abla		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
	\checkmark	User access policies are	Controls of Least Privilege and
		established.	separation of duties are not



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 better 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 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.