Controls and compliance checklist exemplar

Problem Statement

You have been tasked with conducting a controls and compliance audit for Botium Toys. Your objective is to use the provided checklists to assess their existing security posture. Based on your analysis, you must identify gaps in their controls and compliance with standards such as PCI DSS, GDPR, and SOC, and then provide specific recommendations to address these vulnerabilities and improve their overall security.

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.*
	●	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.*
	●	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.*
	●	Backups	*The IT department needs to have backups of critical data, in the case of a breach, to ensure business continuity.*
●		Antivirus software	*Antivirus software is installed and monitored regularly by the IT department.*
	●	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.*
	●	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.*

●		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.*
●		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

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.	*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.*
	●	Implement data encryption procedures to better secure credit card transaction touchpoints and data.	*The company does not currently use encryption to better ensure the 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 currently 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 currently in place; all employees have access to internally stored data.*
	●	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):

To improve Botium Toys' security posture and reduce risks to assets, we recommend implementing the following controls and compliance measures:

1. Implement multiple controls: Least Privilege, disaster recovery plans, password policies, separation of duties, IDS, ongoing legacy system management, encryption, and password management system.
2. Address compliance gaps: Implement controls such as Least Privilege, separation of duties, and encryption to ensure compliance with regulations like PCI DSS and GDPR.
3. Properly classify assets: Identify and classify assets to determine additional controls needed to protect sensitive information.

By implementing these recommendations, Botium Toys can enhance their security posture, reduce the risk of data breaches and other security incidents, and ensure compliance with relevant regulations and standards.