Controls and compliance checklist

Scenario

Botium Toys is a small U.S. business that develops and sells toys. The business has a single physical location, which serves as their main office, a storefront, and warehouse for their products. However, Botium Toy's online presence has grown, attracting customers in the U.S. and abroad. As a result, their information technology (IT) department is under increasing pressure to support their online market worldwide.

The manager of the IT department has decided that an internal IT audit needs to be conducted. She's worried about maintaining compliance and business operations as the company grows without a clear plan. She believes an internal audit can help better secure the company's infrastructure and help them identify and mitigate potential risks, threats, or vulnerabilities to critical assets. The manager is also interested in ensuring that they comply with regulations related to internally processing and accepting online payments and conducting business in the European Union (E.U.).

The IT manager starts by implementing the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), establishing an audit scope and goals, listing assets currently managed by the IT department, and completing a risk assessment. The goal of the audit is to provide an overview of the risks and/or fines that the company might experience due to the current state of their security posture.

Your task is to review the IT manager's scope, goals, and risk assessment report. Then, perform an internal audit by completing a controls and compliance checklist.

Risk Assessment Report –
https://drive.google.com/file/d/1ZX3ZXCV0ogqbNBXbPhZ7beL3p-svYfnM/view?usp=drive_link

Controls assessment checklist

Yes	No	Control	*Explanation*
	X	Least Privilege	*Currently, all employees have access to customer data; privileges need to be limited to reduce the risk of a breach.*

	X	Disaster recovery plans	*There are no disaster recovery plans in place. These need to be implemented to ensure business continuity.*
	X	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.*
	X	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.*
X		Firewall	*The existing firewall blocks traffic based on an appropriately defined set of security rules.*
	X	Intrusion detection system (IDS)	*The IT department needs an IDS in place to help identify possible intrusions by threat actors.*
	X	Backups	*The IT department needs to have backups of critical data, in the case of a breach, to ensure business continuity.*
X		Antivirus software	*Antivirus software is installed and monitored regularly by the IT department.*
	X	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.
	X	Encryption	*Encryption is not currently used; implementing it would provide greater confidentiality of sensitive information.*
	X	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.*
X		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.*
X		Closed-circuit television (CCTV) surveillance	*CCTV is installed/functioning at the store's physical location.*
X		Fire detection/prevention (fire alarm, sprinkler system, etc.)	*Botium Toys' physical location has a functioning fire detection and prevention system.*

Compliance checklist

Type an X in the "yes" or "no" column 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*

	X	Only authorized users have access to customers' credit card information.	*Currently, all employees have access to the company's internal data.*
	X	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.*
	X	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.*
	X	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***
	X	E.U. customers' data is kept private/secured.	*The company does not currently use encryption to better ensure the confidentiality of customers' financial information.*
X		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.*
	X	Ensure data is properly classified and inventoried.	*Current assets have been inventoried/listed, but not classified.*
X		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*
	X	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.*
	X	Sensitive data (PII/SPII) is confidential/private.	*Encryption is not currently used to better ensure the confidentiality of PII/SPII.*
X		Data integrity ensures the data is consistent, complete, accurate, and has been validated.	*Data integrity is in place.*
	X	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 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.