Controls and compliance checklist

Project Description:

This scenario is based on a fictional company:
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.

Controls assessment checklist

Yes	No	Control	*Explanation*
☐	☑	Least Privilege	*Everyone at work can see customer info; we should cut back who can do that to lower the chance of a data leak.*
☐	☑	Disaster recovery plans	*There are no disaster recovery plans in place.*
☐	☑	Password policies	*Employee passwords are too simple, making it easier for hackers to access sensitive data, work devices, or the internal network.*
☐	☑	Separation of duties	*We need this to stop fraud and protect important data because right now, the CEO is doing daily stuff and handling payroll too.*
☑	☐	Firewall	*The current firewall stops traffic using a set of well-made security rules.*
☐	☑	Intrusion detection system (IDS)	*The IT team needs an IDS to spot when threat actors might be trying to break in.*
☐	☑	Backups	*The IT department should maintain backups of critical data to ensure the business can continue operating in case of a security breach.*

☑	☐	Antivirus software	*The IT team puts antivirus on and checks it often.*
☐	☑	Manual monitoring, maintenance, and intervention for legacy systems	*The asset list shows that old systems are still in use. While they are monitored and maintained, there's no set schedule for this, and the procedures or policies for handling them are unclear, which could make them vulnerable to a breach.*
☐	☑	Encryption	*Encryption isn't used. Adding it would keep sensitive info more private.*
☐	☑	Password management system	*There's no system for managing passwords right now. Setting one up would help the IT team and employees deal with password problems faster.*
☑	☐	Locks (offices, storefront, warehouse)	*The store's building, including the offices, shop, and warehouse, has enough locks for security.*
☑	☐	Closed-circuit television (CCTV) surveillance	*The store has working CCTV cameras installed.*
☑	☐	Fire detection/prevention (fire alarm, sprinkler system, etc.)	*Botium Toys' building has a working fire alarm 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*
☐	☑	Only authorized users have access to customers' credit card information.	*All employees can access the company's internal data.*
☐	☑	Credit card information is accepted, processed, transmitted, and stored internally, in a secure environment.	*Credit card info isn't encrypted, and all employees can access internal data, including customer credit card details.*
☐	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.	*The company doesn't use encryption to keep customer financial info more private.*
☐	☑	Adopt secure password management policies.	*Password rules are basic, and there's no system to manage passwords right now.*

General Data Protection Regulation (GDPR)

Yes	No	Best practice	*Explanation*
☐	☑	E.U. customers' data is kept private/secured.	*The company doesn't use encryption to keep customers' financial info more secure..*
☑	☐	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.	*There's a plan to tell E.U. customers within 72 hours if there's a data breach.*
☐	☑	Ensure data is properly classified and inventoried.	*The current assets have been listed, but not sorted into categories.*

☑	☐	Enforce privacy policies, procedures, and processes to properly document and maintain data.	*Privacy rules and processes have been made and followed by the IT team and other employees when needed.*

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

Yes	No	Best practice	*Explanation*
☐	☑	User access policies are established.	*There are no controls for Least Privilege or separating duties right now; all employees can access internal data.*
☐	☑	Sensitive data (PII/SPII) is confidential/private.	*Encryption isn't used right now to keep PII/SPII more private..*
☑	☐	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, but access should be limited to just the people who need it for their work.*

Recommendations:

Botium Toys needs to put in place several security measures to protect sensitive info, like Least Privilege, disaster recovery plans, password rules, separating duties, an IDS, managing old systems, encryption, and a password manager.

To fix compliance issues, Botium Toys should use controls like Least Privilege, separating duties, and encryption. The company also needs to properly sort their

assets to figure out other controls that could help improve security and protect sensitive information.