Controls and compliance checklist

Scenario

Review the following scenario. Then complete the step-by-step instructions.

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
	●	Least Privilege
	●	Disaster recovery plans
	●	Password policies
	●	Separation of duties
●		Firewall
	●	Intrusion detection system (IDS)
	●	Backups
●		Antivirus software
	●	Manual monitoring, maintenance, and intervention for legacy systems
	●	Encryption
	●	Password management system
●		Locks (offices, storefront, warehouse)
●		Closed-circuit television (CCTV) surveillance
●		Fire detection/prevention (fire alarm, sprinkler system, etc.)

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice
	●	Only authorized users have access to customers' credit card information.

- Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.
- Implement data encryption procedures to better secure credit card transaction touchpoints and data.
- Adopt secure password management policies.

General Data Protection Regulation (GDPR)

Yes	No	Best practice
	●	E.U. customers' data is kept private/secured.
●		There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.
	●	Ensure data is properly classified and inventoried.
●		Enforce privacy policies, procedures, and processes to properly document and maintain data.

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

Yes	No	Best practice
	●	User access policies are established.
	●	Sensitive data (PII/SPII) is confidential/private.
●		Data integrity ensures the data is consistent, complete, accurate, and has been validated.
	●	Data is available to individuals authorized to access it.

Recommendations :

Control assessment recommendations:

- Create a Disaster Recovery Plan
- Set up regular Backups
- Enforce Password Policies + Use a Password Manager
- Implement Least Privilege + Role Separation
- Introduce Encryption for Sensitive Data

Compliance assessment recommendations:

- PCI DSS compliance is legally required
- Document user access policies and train staff on handling sensitive data
- Inventory and classify personal data (especially EU customer info)
- Implement data encryption and regular audits to ensure integrity and confidentiality
- Implement user access controls, encrypt sensitive data, and ensure regular backups with uptime monitoring.
- Establish clear security policies to protect data integrity, confidentiality, and availability.