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.

Internal Security Audit Report for Botium Toys

Scope

The internal IT audit covers Botium Toys' current IT infrastructure, policies, procedures, and controls. The audit aims to identify potential risks, vulnerabilities, and non-compliance with relevant regulations, such as PCI DSS and GDPR.

Goals

1. Assess the effectiveness of existing security controls.
2. Identify and prioritize security risks.
3. Ensure compliance with PCI DSS and GDPR.
4. Provide recommendations for improving the company's security posture.

Risk Assessment

The following table summarizes the identified risks, their potential impact, and the likelihood of occurrence.

Risk	Impact	Likelihood
Unauthorized access to sensitive data (customer PII, credit card information)	Financial loss, reputational damage, regulatory fines (PCI DSS, GDPR)	High
Data breaches	Financial loss, reputational damage, loss of customer trust, regulatory fines (PCI DSS, GDPR)	Medium
System outages and downtime	Disruption of business operations, loss of revenue, damage to reputation	Medium
Non-compliance with PCI DSS and GDPR	Regulatory fines, legal action, loss of business	High
Inadequate incident response capabilities	Increased damage from security incidents, prolonged downtime, loss of customer trust	Medium
Lack of disaster recovery plan	Inability to recover from a disaster, significant business disruption, potential loss of data and assets	Medium

Controls Assessment Checklist	Yes	No
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	Yes	No
Payment Card Industry Data Security Standard (PCI DSS)		
Only authorized users have access to customers\u2019 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)		
E.U. customers\u2019 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)		
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

Based on the audit findings, Botium Toys needs to implement several security controls and compliance measures to mitigate the identified risks. The following recommendations are prioritized based on their potential impact and the likelihood of occurrence:

1. **Implement least privilege and separation of duties:** Restrict access to sensitive data and systems to only authorized personnel and ensure that no single individual has complete control over critical processes.
2. **Encrypt sensitive data:** Implement encryption for cardholder data, PII/SPII, and other sensitive information at rest and in transit to protect it from unauthorized access.

3. **Develop and implement an incident response plan:** Establish procedures for detecting, responding to, and recovering from security incidents to minimize damage and downtime.
4. **Create and test a disaster recovery plan:** Develop a comprehensive plan for recovering critical systems and data in the event of a disaster, ensuring business continuity.
5. **Strengthen password policies and implement a password manager:** Enforce strong password policies and provide employees with a password manager to help them create and manage complex passwords.
6. **Deploy an intrusion detection system (IDS):** Implement an IDS to monitor network traffic for suspicious activity and alert security personnel to potential threats.
7. **Implement regular backups:** Establish a regular backup schedule for critical data and test the restoration process to ensure that data can be recovered in case of loss or corruption.
8. **Establish a comprehensive asset inventory and classification process:** Identify and classify all IT assets to understand their value and prioritize their protection.
9. **Ensure compliance with PCI DSS, GDPR, and SOC 2:** Implement the necessary controls and best practices to meet the requirements of these regulations and standards.

By addressing these recommendations, Botium Toys can significantly improve its security posture and reduce the risk of financial loss, reputational damage, and regulatory fines.