Conduct An Audit

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.

Botium Toys: Scope, Goals, and Risk assessment report

Scope and goals of the audit

Scope: The scope of this audit is defined as the entire security program at Botium Toys. This includes their assets like employee equipment and devices, their internal network, and their systems. You will need to review the assets Botium Toys has and the controls and compliance practices they have in place.

Goals: Assess existing assets and complete the controls and compliance checklist to determine which controls and compliance best practices that need to be implemented to improve Botium Toys' security posture.

Current Assets

Assets managed by the IT department include:

- On-premises equipment for in-office business needs.

- Employee equipment: end-user devices (desktops/laptops, smartphones), remote workstations, headsets, cables, keyboards, mice, docking stations, surveillance cameras, etc.
- Storefront products available for retail sale on site and online; stored in the company's adjoining warehouse.
- Management of systems, software, and services: accounting, telecommunication, database, security, ecommerce, and inventory management.
- Internet access.
- Internal network.
- Data retention and storage.
- Legacy system maintenance: end-of-life systems that require human monitoring.

Risk Assessment

Risk description: Currently, there is inadequate management of assets. Additionally, Botium Toys does not have all of the proper controls in place and may not be fully compliant with U.S. and international regulations and standards.

Control best practices: The first of the five functions of the NIST CSF is Identify. Botium Toys will need to dedicate resources to identify assets so they can appropriately manage them. Additionally, they will need to classify existing assets and determine the impact of the loss of existing assets, including systems, on business continuity.

Risk score: On a scale of 1 to 10, the risk score is 8, which is fairly high. This is due to a lack of controls and adherence to compliance best practices.

Additional comments: The potential impact from the loss of an asset is rated as medium, because the IT department does not know which assets would be at risk. The risk to assets or fines from governing bodies is high because Botium Toys does not have all of the necessary controls in place and is not fully adhering to best practices related to compliance regulations that keep critical data private/secure. Review the following bullet points for specific details:

- Currently, all Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers' PII/SPII.
- Encryption is not currently used to ensure confidentiality of customers' credit card information that is accepted, processed, transmitted, and stored locally in the company's internal database.
- Access controls pertaining to least privilege and separation of duties have not been implemented.
- The IT department has ensured availability and integrated controls to ensure data integrity.
- The IT department has a firewall that blocks traffic based on an appropriately defined set of security rules.
- Antivirus software is installed and monitored regularly by the IT department.
- The IT department has not installed an intrusion detection system (IDS).
- There are no disaster recovery plans currently in place, and the company does not have backups of critical data.

- The IT department has established a plan to notify E.U. customers within 72 hours if there is a security breach. Additionally, privacy policies, procedures, and processes have been developed and are enforced among IT department members/other employees, to properly document and maintain data.
- Although a password policy exists, its requirements are nominal and not in line with current minimum password complexity requirements (e.g., at least eight characters, a combination of letters and at least one number; special characters).
- There is no centralized password management system that enforces the password policy's minimum requirements, which sometimes affects productivity when employees/vendors submit a ticket to the IT department to recover or reset a password.
- While legacy systems are monitored and maintained, there is no regular schedule in place for these tasks and intervention methods are unclear.
- The store's physical location, which includes Botium Toys' main offices, store front, and warehouse of products, has sufficient locks, up-to-date closed-circuit television (CCTV) surveillance, as well as functioning fire detection and prevention systems.

Controls and Compliance Checklist

Controls assessment checklist

Control	Yes/No/?	Explanation
Least Privilege	No	All employees have access to internally stored customer data.
Disaster recovery plans	No	The company has no disaster recovery plans and no backups of critical data.
Password policies	?	A password policy is in place, but its requirements do not align with the minimum password complexity requirements.
Separation of duties	?	It is not indicated whether the decisions that are made are made as a group or an individual.
Firewall	Yes	A firewall is in use and effective.
Intrusion detection system (IDS)	No	There is no intrusion detection system installed.
Backups	No	The organisation does not keep backups of critical data.
Antivirus software	Yes	The IT department has installed antivirus software and regularly monitors it.

Manual monitoring, maintenance, and intervention for legacy systems	?	Legacy systems are in use and monitored but there is not a regular schedule to the monitoring and maintenance.
Encryption	No	Encryption is not used to encrypt centrally stored data.
Password management system	No	There is no password management system in use.
Locks	Yes	The physical location uses locks.
Closed-circuit television (CCTV) surveillance	Yes	CCTV is in use at the physical location.
Fire detection/prevention	Yes	There is an operational fire detection and prevention system installed at the physical location.