Controls and compliance assessment.

Does Botium Toys currently have this control in place?

Case Study.
This 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 its main office, storefront, and warehouse for its products. However, Botium Toy's online presence has grown, attracting customers in the U.S. and abroad. As a result, its information technology (IT) department is under increasing pressure to support its online market worldwide.

The manager of the IT department has decided that an internal IT audit needs to be conducted. She expresses concerns about not having a solidified plan of action to ensure business continuity and compliance, as the business grows. 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 audit's goal is to provide an overview of the risks and/or fines that the company might experience due to the current state of its security posture.

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

Scenario

Botium Toys: Scope, goals, and risk assessment report.

Jefferson Joojo Yankson

Establishing The Scope of the Audit;

Scope refers to the specific criteria of an internal security audit. The audit will cover the entire security program at Botium Toys. This refers to individuals, assets, policies, and procedures that may affect the security posture of Botium Toys.

Goals;

- Ensuring business continuity by adhering to regulations such as the General Data Protection Regulation (GDPR) for EU citizens and the Payment Card Industry Data Security Standard (PCI DSS).
- Identifying and diminishing threats, risks, and vulnerabilities by implementing appropriate security controls.

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 are 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, e-commerce, and inventory management
- Internet access
- Internal network
- Data retention and storage
- Legacy system maintenance: end-of-life systems that require human monitoring

Risk Assessments.

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 the 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, storefront, and warehouse of products, has sufficient locks, up-to-date closed-circuit television (CCTV) surveillance, as well as functioning fire detection and prevention systems.*

Control categories

Controls within cybersecurity are grouped into three main categories:

- *Administrative/Managerial controls (address the human component of cybersecurity.)*
- *Technical controls(consist of solutions such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), antivirus (AV) products, encryption, etc.)*
- *Physical/Operational controls(They are used to limit physical access to physical assets by unauthorized personnel).*

Control types

Control types include, but are not limited to:
1. Preventative
2. Corrective
3. Detective
4. Deterrent

These controls work together to provide defense in depth and protect assets. Preventative controls are designed to prevent an incident from occurring in the first place. Corrective controls are used to restore an asset after an incident. Detective controls are implemented to determine whether an incident has occurred or is in progress. Deterrent controls are designed to discourage attacks.

Controls assessment checklist

Yes	No	Control	*Explanation*
☐	☑	Least Privilege	*Employees have access to abundant resources they need to perform their everyday tasks, these privileges can be exploited if not limited.*
☐	☑	Disaster recovery plans	*Currently, Botium Toys does not have any recovery plans in case of any disruptions which can lead to severe loss of data. They need to be implemented to enhance business continuity.*
☐	☑	Password policies	*There are no policies for setting up passwords. These vulnerabilities can be exploited by threat actors*

			authorizing themselves through the internal network of the company or employee accounts.
☐	☑	Separation of duties	*SoD is an essential internal control. An employee should not have permission to both authorize and execute tasks. These need to be implemented to ensure critical assets are secure.*
☑	☐	Firewall	*The existing firewall blocks all network traffic based on predefined security rules.*
☐	☑	Intrusion detection system (IDS)	*The IT department needs to set up an IDS to notify them in case of a threat.*
☐	☑	Backups	*The IT department must save copies of files and critical assets in a secure location in case of any disruptions or a breach to ensure business continuity.*
☑	☐	Antivirus software	*The current Antivirus Software has been set up to remediate any computer at risk. Monitored and updated regularly by the IT department.*
☐	☑	Manual monitoring, maintenance, and intervention for legacy systems	*The risk assessment implies that whilst legacy systems are in place, monitored, and maintained, there is no schedule in place for tasks and intervention. Without*

			regular maintenance, legacy systems may not receive recent updates and patches exposing the company to security risks.
☐	☑	Encryption	*Encryption is not implemented, hence all customer PII is visible to employees. Implementing this would improve the confidentiality of data.*
☐	☑	Password management system	*There's no password management system in place. Implementing this, passwords could be stored in a secure location and can be retrieved in case of any issues.*
☑	☐	Locks (offices, storefront, warehouse)	*There are physical security controls in place that protect physical critical assets from being tampered with.*
☑	☐	Closed-circuit television (CCTV) surveillance	*Surveillance footage is present 24/7*
☑	☐	Fire detection/prevention (fire alarm, sprinkler system, etc.)	*Some sensors would alert the cause of any fire outburst.*

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice	*Explanation*

☐	☑	Only authorized users have access to customers' credit card information.	*Currently, all employees have access to customer data stored in the company's internal database. (credit card info)*
☐	☑	Credit card information is accepted, processed, transmitted, and stored internally, in a secure environment.	*Credit card information is not encrypted which exposes sensitive financial information to unauthorized access.*
☐	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.	Encryption is not implemented to ensure the confidentiality of customers' financial data.
☐	☑	Adopt secure password management policies.	*Although password policy exists, they are nominal and do not meet the complex requirements as expected, leaving the company vulnerable to threat actors.*

General Data Protection Regulation (GDPR)

Yes	No	Best practice	***Explanation***
☐	☑	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.	*Yes, the IT department has established a plan to notify E.U. customers within 72 hours if there is a security breach.*
☐	☑	Ensure data is properly classified and inventoried.	*All employees have access to all data. Data is not classified and inventoried.*
☑	☐	Enforce privacy policies,	*Privacy policies, procedures, and*

		procedures, and processes to properly document and maintain data.	*processes have been developed and are enforced in the IT department*

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

Yes	No	Best practice	*Explanation*
☐	☑	User access policies are established.	*Employees have access to all kinds of data.*
☐	☑	Sensitive data (PII/SPII) is confidential/private.	*There are no pragmatic rules to ensure the confidentiality of data since encryption is not being implemented yet.*
☑	☐	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 accessible to all employees.*

Recommendations:

Several controls need to be implemented to ensure the confidentiality of customers' data SPII/PII, these principles could include

1. encryption to ensure that data is only accessible to authorized users.
2. Principle of least privilege, employees are strictly provided with the exact resources they need to perform a task.
3. Separation of duties to prevent employees from having multiple privileges in the organization.
4. IDS to alert any malicious behavior.
5. Password policies to outline guides for a robust password.

Jefferson Joojo Yankson

6. Password management systems to store passwords in case of any password issues.
7. Backups to ensure business continuity in case of any breach
8. Daily maintenance of legacy systems to receive regular updates and patches to prevent them from being vulnerable.

These practices will improve the security posture of the organization.

To address gaps in compliance, Botium Toys needs to adhere to international regulations and laws by keeping customer data safe through encryption. Other practices such as separation of duties, keeping E.U data secure, and making sure data is properly classified to identify controls needed to improve the security posture of the organization and protect its critical assets.