Play It Safe: Manage Security Risks

Portfolio Activity: Conduct a security audit

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.

Scenario

Botium Toys: Scope, Goals, and Risk Assessment Report

Scope

The scope is defined as the entire security program at Botium Toys. This means all assets need to be assessed alongside internal processes and procedures related to the implementation of controls and compliance best practices.

Goals

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

Play It Safe: Manage Security Risks

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

Play It Safe: Manage Security Risks

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:

Additional Info

In Cybersecurity, control types can be classified in three ways:

1. Administrative/Managerial controls
2. Technical controls
3. Physical/Operational controls

Control types (providing defense and protecting assets) include, but are not limited to:

1. Preventative (preventing an incident from occurring in the first place)
2. Corrective (restoring an asset after an incident)
3. Detective (Determining whether an incident has occurred or is in progress)
4. Deterrent (Discouraging attacks)

Controls and compliance checklist

To complete the controls assessment checklist, refer to the information provided in the scope, goals, and risk assessment report. For more details about each control, including the type and purpose, refer to the control categories document.

Select "yes" or "no" to answer the question: *Does Botium Toys currently have this control in place?*

Controls assessment checklist

Yes	No	Control	Explanation
	●	Least Privilege	Currently, all employees have access to internally client data. These privileges need to be limited.

Play It Safe: Manage Security Risks

●	●	Disaster recovery plans	There are no disaster recovery plans currently in place. This needs to be implemented to provide business continuity.
●	●	Password policies	Although a password policy exists, its requirements are nominal and minimal. This increase the likelihood of account compromise through brute force or dictionary attack techniques.
●	●	Separation of duties	Separation of duties have not been implemented. It needs to be implemented to reduce the possibility of access to sensitive or critical data.
●	●	Firewall	The IT department has a firewall that blocks traffic based on an appropriately defined set of security rules.
●	●	Intrusion detection system (IDS)	The IT department has not installed an intrusion detection system (IDS). Its installation could identify possible attacks and intrusions.

●	●	Backups	The company does not have backups of critical data. In the case of a breach it could mean the loss of critical and personal data.
●	●	Antivirus software	Antivirus software is installed and monitored regularly by the IT department.
●	●	Manual monitoring, maintenance, and intervention for legacy systems	While legacy systems are monitored and maintained, there is no regular schedule in place for these tasks and intervention methods are unclear.
	●	Encryption	Encryption is not currently used to ensure confidentiality of customers' credit card information. Implementing it would improve confidentiality.
●	●	Password management system	There is no centralized password management system that enforces the password policy's minimum requirements. Implementing it would improve employee's productivity.
●	●	Locks (offices, storefront, warehouse)	The store's physical locations have sufficient locks.
●	●	Closed-circuit television (CCTV) surveillance	CCTV is installed/functioning at the store's physical

			location.
●	●	Fire detection/prevention (fire alarm, sprinkler system, etc.)	All the store's physical locations have as functioning fire detection and prevention systems.

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 the company's internal data.
●	●	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.	The environment is not secure due to the lack of encryption and access management.
●	●	Implement data encryption procedures to better secure credit card transaction touchpoints and data.	The company does not use encryption to ensure confidentiality.
●	●	Adopt secure password management policies.	Although a password policy exists, the requirements are minimum and there is not password management.

Play It Safe: Manage Security Risks

General Data Protection Regulation (GDPR)

Yes	No	Best practice	Explanation
	●	E.U. customers' data is kept private/secured.	It is not private/secured due to the lack of encryption.
●	●	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.	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.	The assets are inventoried but not classified.
●	●	Enforce privacy policies, procedures, and processes to properly document and maintain data.	Privacy policies, procedures, and processes have been developed and are enforced among IT department members/other employees.

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

Yes	No	Best practice	Explanation
	●	User access policies are established.	There isn't an implementation of the Least Privilege and Separation of Duties principles.
●	●	Sensitive data (PII/SPII) is	Encryption is not currently

		confidential/private.	used.
●	●	Data integrity ensures the data is consistent, complete, accurate, and has been validated.	Data integrity is implemented.
●	●	Data is available to individuals authorized to access it.	Data is available to all employees. The access to data needs to be limited by the individual’s job.