Security Audit Portfolio Project

Botium Toys Company (fictional company)

# Situation:

*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.

# Mission:

Review the [IT Manager’s scope, goals, and risk assessment report](#_Attachment). Then, perform an internal audit by completing a controls and compliance checklist.

# Execution:

## Controls and compliance checklist

To complete the controls assessment checklist, refer to the information provided in the [scope, goals, and risk assessment report](https://docs.google.com/document/d/1s2u_RuhRAI40JSh-eZHvaFsV1ZMxcNSWXifHDTOsgFc/template/preview#heading=h.evidx83t54sc). For more details about each control, including the type and purpose, refer to the [control categories](https://docs.google.com/document/d/1btezuy_bMKWoK8pd97ZuzdWB9y6au_zfkrpkfVf8ktI/template/preview) document.

Then, select “yes” or “no” to answer the question: *Does Botium Toys currently have this control in place?*

### Controls assessment checklist

|  |  |  |
| --- | --- | --- |
| **Yes** | **No** | **Control** |
| unchecked | unchecked | Least Privilege |
| unchecked | unchecked | Disaster recovery plans |
| unchecked | unchecked | Password policies |
| unchecked | unchecked | Separation of duties |
| unchecked | unchecked | Firewall |
| unchecked | unchecked | Intrusion detection system (IDS) |
| unchecked | unchecked | Backups |
| unchecked | unchecked | Antivirus software |
| unchecked | unchecked | Manual monitoring, maintenance, and intervention for legacy systems |
| unchecked | unchecked | Encryption |
| unchecked | unchecked | Password management system |
| unchecked | unchecked | Locks (offices, storefront, warehouse) |
| unchecked | unchecked | Closed-circuit television (CCTV) surveillance |
| unchecked | unchecked | Fire detection/prevention (fire alarm, sprinkler system, etc.) |

To complete the compliance checklist, refer to the information provided in the [scope, goals, and risk assessment report](https://docs.google.com/document/d/1s2u_RuhRAI40JSh-eZHvaFsV1ZMxcNSWXifHDTOsgFc/template/preview). For more details about each compliance regulation, review the [controls, frameworks, and compliance](https://www.coursera.org/learn/foundations-of-cybersecurity/supplement/xu4pr/controls-frameworks-and-compliance) reading.

Then, select “yes” or “no” to answer the question: *Does Botium Toys currently adhere to this compliance best practice?*

## Compliance checklist

### Payment Card Industry Data Security Standard (PCI DSS)

|  |  |  |
| --- | --- | --- |
| **Yes** | **No** | **Best practice** |
| unchecked | unchecked | Only authorized users have access to customers’ credit card information. |
| unchecked | unchecked | Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment. |
| unchecked | unchecked | Implement data encryption procedures to better secure credit card transaction touchpoints and data. |
| unchecked | unchecked | Adopt secure password management policies. |

### General Data Protection Regulation (GDPR)

|  |  |  |
| --- | --- | --- |
| **Yes** | **No** | **Best practice** |
| unchecked | unchecked | E.U. customers’ data is kept private/secured. |
| unchecked | unchecked | There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach. |
| unchecked | unchecked | Ensure data is properly classified and inventoried. |
| unchecked | unchecked | 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** |
| unchecked | unchecked | User access policies are established. |
| unchecked | unchecked | Sensitive data (PII/SPII) is confidential/private. |
| unchecked | unchecked | Data integrity ensures the data is consistent, complete, accurate, and has been validated. |
| unchecked | unchecked | Data is available to individuals authorized to access it. |

Recommendations:

In this section, provide recommendations related to controls and/or compliance needs, that my IT manager could communicate to stakeholders to reduce risks to assets and improve Botium Toys’ security posture.

## General Recommendations:

* Implement a policy of ‘least privilege’. Company employees should only have access to the minimum amount of data that they require to do their assigned duties (day to day tasks).
  + Configure data access controls to restrict access to encrypted data to authorized personnel only.
* Use MFA for access to sensitive systems.
* Prohibit group or shared accounts.
* Disable unnecessary services, ports, and protocols in the network.
* Schedule quarterly internal and external vulnerability scans.
  + Annual penetration tests.
* Monitor access to network resources:
  + Implement a SIEM system.
    - Maintain logs for no less than 12 months.
    - Review regularly for suspicious activity.
* Install IDS into the network.
* Establish a regular maintenance schedule for all systems including legacy systems.

## Password Policy:

* Improve current password policy. Suggest a few key points from the NIST CSF:
  + Minimum length of 8 characters.
  + Salt and hash stored passwords.
  + Use MFA for general account authentication.
  + Consider a password management system (follow best practices for their use).

## Disaster Recovery/Backups:

* Develop a Disaster Recovery Plan.
* Implement a data backup strategy:
  + Regularly make full backups.
    - Schedule incremental backups in between.
  + Determine frequency based on the data type.
* Consider offsite or cloud backups.
* Use redundant infrastructure:
  + Use real-time data replication between primary and secondary servers.
* Encrypt backups and regularly test to ensure data can be restored w/o corruption.

## PCI DSS Recommendation:

* Develop a PCI DSS Compliance program.
  + Schedule PCI DSS audits and employee training.
* Implement strong encryption for CC transactions.
  + Use TLS 1.2 or higher to encrypt all transmissions of cardholder data over public networks.
    - Enforce HTTPS for all communications.
    - Install a valid SSL/TLS certificate from a trusted authority (TA).
    - Disable older, insecure protocols if applicable.
* Use a PCI-compliant payment gateway (if not developing own).
* Secure storage of cardholder data
  + Use AES-256 encryption for stored data.
* Segment cardholder data with an additional firewall from the rest of the network.

# Attachment

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.