

Botium-Toys-Security-Audit

Introduction

An internal security audit assessment done on Botium Toys, a fictitious toy company, completed as part of my cybersecurity portfolio and as part of Google's [Cybersecurity Professional Certificate](#) on Coursera in the [Play It Safe: Manage Security Risks](#) Course .

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 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 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.

Scope and Goal

The following systems are in scope: accounting, end point detection, firewalls, intrusion detection system, security information and event management (SIEM) tool. The systems will be evaluated for:

- Current user permissions
- Current implemented controls
- Current procedures and protocols
- Ensuring current user permissions, controls, procedures, and protocols in place align with GDPR, PCI DSS, compliance requirements
- Ensure current technology and assets are accounted for both hardware and system access.

The goals for Botium Toys' internal IT audit are:

- To adhere to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
- Establish a better process for their systems to ensure they are compliant
- Implement OWASP Security Principles
- Implement the concept of least permissions when it comes to user credential management
- Establish their policies and procedures, which includes their playbooks

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.

Compliance checklist

To review compliance regulations and standards, read the controls, frameworks, and compliance document. I found that Botium Toys will need to adhere to the following standards:

General Data Protection Regulation (GDPR)

GDPR is a European Union (E.U.) general data regulation that protects the processing of E.U. citizens' data and their right to privacy in and out of E.U. territory. Additionally, if a breach occurs and a E.U. citizen's data is compromised, they must be informed within 72 hours of the incident.

Botium Toys is expanding to offer services and handle the data of customers abroad, GDPR compliance is in scope for the handling of financial and personal information for customers in the European Union.

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is an international security standard meant to ensure that organizations storing, accepting, processing, and transmitting credit card information do so in a secure environment.

Botium Toys must adhere to PCI DSS as it accepts payments online and person and They also store and processes customer credit card on an international scale. It's requirements and compliance need to be taken seriously based on possible consequences. The consequences of not complying with this standard is more severe in impact: Monetary fines monthly (ranging from 5,000-100,000 USD), costs of forensic audits upon a data breach, payment brand restrictions, damage to brand reputation, and possibility of lawsuit costs in the event of data breaches.

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

The SOC1 and SOC2 are a series of reports that focus on an organization's user access policies at different organizational levels. They are used to assess an organization's financial compliance and levels of risk. They also cover confidentiality, privacy, integrity, availability, security, and overall data safety. Control failures in these areas can lead to fraud.

Botium Toys needs to establish and maintain appropriate user access for internal and external (third-party vendor) personnel to mitigate risk and ensure data safety.

Both of these standards evaluate the effectiveness of a company's internal controls. While SOC1 I focused on financial reporting controls, SOC2 is concerned with information security controls, including customer data safety.