Table of Contents

[Overview 2](#_Toc190721504)

[Scenario 2](#_Toc190721505)

[The objectives of Botium Toys’ internal IT audit are to: 3](#_Toc190721506)

[Internal Security Audit 3](#_Toc190721507)

[The objectives for the internal IT audit at Botium Toys are as follows: 3](#_Toc190721508)

[Controls Assessment 3](#_Toc190721509)

[Current assets are as follows: 3](#_Toc190721510)

[Managerial Controls 4](#_Toc190721511)

[Technical Controls 5](#_Toc190721512)

[Physical Controls 6](#_Toc190721513)

[Compliance Checklist 7](#_Toc190721514)

[Stakeholder Report 8](#_Toc190721515)

[Scope: 8](#_Toc190721516)

[Goals: 8](#_Toc190721517)

[Must Fix: (High Risk) 8](#_Toc190721518)

[Must Fix (Medium Risk) 9](#_Toc190721519)

[Recommendations: 9](#_Toc190721520)

[Conclusion 10](#_Toc190721521)

[Reflections on My Mock Security Audit Experience 10](#_Toc190721522)

[Strengths: 10](#_Toc190721523)

[Areas for Improvement: 10](#_Toc190721524)

[Key Takeaways: 10](#_Toc190721525)

# Overview

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](https://www.coursera.org/google-certificates/cybersecurity-certificate) on Coursera in the  [Play It Safe: Manage Security Risks](https://www.coursera.org/learn/manage-security-risks?specialization=cybersecurity-certificate)Course .

The goal is to perform an audit of Botium Toys’ cybersecurity program. The audit needs to align current business practices with industry standards and best practices. It is meant to provide mitigation recommendations for vulnerabilities classified as “high risk” and present an overall strategy for improving the organization's security posture. The audit team must document their findings, provide remediation plans and efforts, and communicate with stakeholders.

# Scenario

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.

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.

## The objectives of Botium Toys’ internal IT audit are to:

1. Adhere to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).

2. Establish improved processes to ensure system compliance.

3. Strengthen system controls.

4. Implement the principle of least privilege in user credential management.

5. Develop comprehensive policies and procedures, including playbooks.

6. Ensure compliance with all relevant requirements.

# Internal Security Audit

## The objectives for the internal IT audit at Botium Toys are as follows:

1. Ensure compliance with the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).

2. Develop improved processes for their systems to guarantee compliance.

3. Strengthen system controls.

4. Apply the principle of least privilege in user credential management.

5. Establish comprehensive policies and procedures, including detailed playbooks.

6. Confirm adherence to all compliance requirements.

# Controls Assessment

## Current assets are as follows:

* 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

## Managerial Controls

| **Control Name** | **Control type and explanation** | **Needs to be implemented (X)** | **Priority** |
| --- | --- | --- | --- |
| Least Privilege | Preventative; reduces risk by making sure vendors and non-authorized staff only have access to the assets/data they need to do their jobs | X | High |
| Disaster recovery plans | Corrective; business continuity to ensure systems are able to run in the event of an incident/there is limited to no loss of productivity downtime/impact to system components, including: computer room environment (air conditioning, power supply, etc.); hardware (servers, employee equipment); connectivity (internal network, wireless); applications (email, electronic data); data and restoration | X | High |
| Password policies | Preventative; establish password strength rules to improve security/reduce likelihood of account compromise through brute force or dictionary attack techniques | X | High |
| Access control policies | Preventative; increase confidentiality and integrity of data | X | High |
| Account management policies | Preventative; reduce attack surface and limit overall impact from disgruntled/former employees | X | High |
| Separation of duties | Preventative; ensure no one has so much access that they can abuse the system for personal gain | X | High |

## Technical Controls

| **Control Name** | **Control type and explanation** | **Needs to be implemented (X)** | **Priority** |
| --- | --- | --- | --- |
| Firewall | Preventative; firewalls ***are already in place*** to filter unwanted/malicious traffic from entering internal network | NA | NA |
| Intrusion Detection System (IDS) | Detective; allows IT team to identify possible intrusions (e.g., anomalous traffic) quickly | X | High |
| Encryption | Deterrent; makes confidential information/data more secure (e.g., website payment transactions) | X | High |
| Backups | Corrective; supports ongoing productivity in the case of an event; aligns to the disaster recovery plan | X | High |
| Password management system | Corrective; password recovery, reset, lock out notifications | X | High |
| Antivirus (AV) software | Corrective; detect and quarantine known threats | X | High |
| Manual monitoring, maintenance, and intervention | Preventative/corrective; required for legacy systems to identify and mitigate potential threats, risks, and vulnerabilities | X | High |

## Physical Controls

| **Control Name** | **Control type and explanation** | **Needs to be implemented (X)** | **Priority** |
| --- | --- | --- | --- |
| Time-controlled safe | Deterrent; reduce attack surface/impact of physical threats | X | Medium/Low |
| Adequate lighting | Deterrent; limit “hiding” places to deter threats | X | Medium/Low |
| Closed-circuit television (CCTV) surveillance | Preventative/detective; can reduce risk of certain events; can be used after event for investigation | X | High/Medium |
| Locking cabinets (for network gear) | Preventative; increase integrity by preventing unauthorized personnel/individuals from physically accessing/modifying network infrastructure gear | X | High/Medium |
| Signage indicating alarm service provider | Deterrent; makes the likelihood of a successful attack seem low | X | Low |
| Locks | Preventative; physical and digital assets are more secure | X | High |
| Fire detection and prevention (fire alarm, sprinkler system, etc.) | Detective/Preventative; detect fire in the toy store’s physical location to prevent damage to inventory, servers, etc. | X | Medium |

# Compliance Checklist

To review compliance regulations and standards, read the [controls, frameworks, and compliance](https://www.coursera.org/learn/foundations-of-cybersecurity/supplement/xu4pr/controls-frameworks-and-compliance) documents.

* Botium Toys must follow the 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 an E.U. citizen's data is compromised, they must be informed within 72 hours of the incident.

* Botium Toys must follow the Payment Card Industry Data Security Standard (PCI DSS)

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

* Botium Toys must follow the System and Organizations Controls (SOC type 1, SOC type 2) The SOC1 and SOC2 are reports focusing on an organization's user access policies at different organizational levels. They are used to assess an organization's financial compliance and risk levels. They also cover confidentiality, privacy, integrity, availability, security, and data safety. Control failures in these areas can lead to fraud.

# Stakeholder Report

From: Triantaphyllos Georgatzis

Date: 17/02.2025

Subject: Internal Security Audit from the IT Department

Dear Colleagues,

Please review the following information carefully since it opposes a big threat towards Botium Toys Industries:

## **Scope:**

* 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:
* 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.

## **Goals:**

* Adhere to the NIST CSF.
* Establish a better process for their systems to ensure they are compliant
* Fortify system controls
* Implement the concept of least permissions when it comes to user credential management
* Establish their policies and procedures, which includes their playbooks

## Must Fix: (High Risk)

* Principle of Least Privilege and Separation of duties
* Disaster recovery plans
* Password, Access control, and Account management policies
* Intrusion Detection System (IDS)
* Encryption (secure website transactions wand disk drive(s) containing sensitive information)
* Backups
* Implementation of a Password management system
* Antivirus (AV) software
* Manual monitoring, maintenance, and intervention for legacy systems
* Closed-circuit television (CCTV) surveillance
* Locks
* Locking cabinets (for network gear)
* Fire detection and prevention (fire alarm, sprinkler system, etc.)
* Policies need to be developed and implemented for the following:

## **Must Fix (Medium Risk)**

* Time-controlled safe
* Adequate lighting
* Signage indicating alarm service provider for restricted areas

## Recommendations:

To ensure compliance with PCI and GDPR standards, it is crucial for Botium Toys to promptly address critical findings, especially as the company processes online payments and expands its services to handle customer data internationally, including within the European Union. User access policies should align with SOC1 and SOC2 guidelines, adopting the principle of least privilege to develop compliant policies and procedures.

Implementing disaster recovery plans and regular backups is essential to maintain business continuity in the event of incidents such as physical disasters (e.g., fires) or cyberattacks. As part of a comprehensive data and system resilience strategy, investing in fire detection and prevention systems is recommended to safeguard against physical threats.

Enhancing cybersecurity measures by integrating Intrusion Detection Systems (IDS) and antivirus (AV) software will help detect and mitigate potential risks. Additionally, legacy systems requiring manual monitoring and intervention should be evaluated and updated to reduce vulnerabilities.

To secure physical assets at Botium Toys' locations, the use of locks, CCTV surveillance, time-controlled safes, adequate lighting, and signage indicating alarm service providers is advised. These measures will strengthen the company's overall security posture and help monitor and deter potential threats.

# Conclusion

## Reflections on My Mock Security Audit Experience

It turned out to be a pretty eye-opening experience! It gave me a chance to put my knowledge and skills into practice. I felt good about identifying key controls and figuring out which risk mitigation strategies would work best for Botium Toys, but I also spotted some areas where I could improve.

## Strengths:

I was really happy with how I assessed the most urgent controls to reduce risk. Choosing the right regulations and standards that matched Botium Toys' needs felt good too—ensuring they stay compliant while tackling security issues. Overall, it was an awesome way to test my understanding and challenge myself with real-world problems.

## Areas for Improvement:

One challenge I faced was finding the right balance between detail and clarity in my stakeholder report. At first, I found it tough to keep my findings concise without overwhelming anyone with too much info. This process really taught me about structuring my thoughts better—like using bullet points, avoiding repetition, and sticking to the main points. It was a great reminder to prioritize clear and brief communication in a professional setting. I also had to put in extra effort to connect the System and Organizations Controls (SOC) standard with broader organizational policies and risks. While I got its value for financial compliance, making its impact clear on aspects like user access, data integrity, and confidentiality took some work. This experience helped me appreciate how compliance, security, and operational policies are all intertwined.

## Key Takeaways:

This assignment really reinforced how important it is to communicate clearly and tailor my technical knowledge for different audiences. It made me realize that security isn’t just about compliance; it’s about understanding the wider impact on an organization’s operations and overall risk posture. Moving forward, I’m eager to keep refining how I present complex ideas in a more straightforward and actionable way. If anyone has suggestions or other areas for me to explore to make this audit even better, I’m all ears! Overall, it was a rewarding experience, and I can’t wait to apply what I learned in future projects.