Security Audit Botium Toys

Contents

[Scenario 2](#_Toc144998128)

[Analyzing the audit scope, goals and risk assessment 3](#_Toc144998129)

[What are the biggest risks to the organization? 3](#_Toc144998130)

[Which controls are most essential to implement immediately versus in the future? 3](#_Toc144998131)

[Which compliance regulations does Botium Toys need to adhere to, to ensure the company keeps customer and vendor data safe, avoids fines, etc.? 4](#_Toc144998132)

[Controls Assessment 5](#_Toc144998133)

[Compliance checklist 9](#_Toc144998134)

[Analyzing audit results 12](#_Toc144998135)

[What were the audit scope and goals? 12](#_Toc144998136)

[What were the critical findings of the audit that need to be addressed immediately (i.e., What controls and/or policies need to be implemented immediately)? 12](#_Toc144998137)

[What were the findings (i.e., What controls and/or policies that need to be addressed in the future)? 13](#_Toc144998138)

[How can you summarize your recommendations clearly and concisely to stakeholders? 14](#_Toc144998139)



# 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. However, its online presence has grown, attracting customers in the U.S. and abroad. 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 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, and completing a risk assessment. The goal of the audit is to provide an overview of the risks the company might experience due to the current state of their security posture. The IT manager wants to use the audit findings as evidence to obtain approval to expand his department.

Our task is to review the IT manager’s scope, goals, and risk assessment. Then, perform an internal audit to complete a controls assessment and compliance checklist.

# Analyzing the audit scope, goals and risk assessment

**After reviewing the audit scope, goals and risk assessment, we consider the following questions:**

### What are the biggest risks to the organization?

The current situation involves inadequate management of assets and non-compliance with both U.S. and international regulations and standards. The IT department lacks clarity on potential asset losses in case of a compromise, resulting in a medium-rated impact. Consequently, the organization faces substantial fines from regulatory authorities due to the absence of essential controls required for customer data protection.

As a result of the insufficient controls and failure to meet compliance requirements, the current risk score stands at 8 out of 10.

### Which controls are most essential to implement immediately versus in the future?

*Inventory and Asset Management (immediately):*

* Maintain an up-to-date inventory of all hardware and software assets on the network.
* Implement asset tagging and tracking mechanisms.
* Determine the impact of the loss of existing assets.

*Security Governance and Compliance (future):*

* Establish a governance framework to ensure security policies align with business objectives.
* Regularly assess compliance with industry regulations and standards (e.g., GDPR, HIPAA, ISO 27001).

### Which compliance regulations does Botium Toys need to adhere to, to ensure the company keeps customer and vendor data safe, avoids fines, etc.?

***NIST Cybersecurity Framework:***

*Establish a better process for Botium Toys systems to ensure they are compliant:*

The NIST CSF provides a structured approach to cybersecurity risk management. It will help Botium Toys assess their current cybersecurity posture, set goals for improvement, and establish processes to achieve and maintain compliance.

*Fortify system controls:*

NIST provides a set of controls and best practices for enhancing the security of systems and networks. These controls cover areas such as access control, data protection, and incident response, helping the company strengthen its system controls.

*Implement the concept of least permissions when it comes to user credential management:*

The NIST framework emphasizes the importance of access control and the principle of least privilege. It provides guidance on managing user access and permissions effectively to minimize security risks.

*Establish policies and procedures, which includes playbooks:*

NIST includes guidance on developing cybersecurity policies and procedures. It encourages organizations to document and communicate their cybersecurity practices effectively. This can include creating incident response playbooks and other security-related documentation.

*Ensure Botium Toys are meeting compliance requirements:*

While the NIST CSF is not a specific compliance regulation, it is widely recognized and used as a foundation for achieving compliance with various regulations and standards. Botium Toys can map their existing compliance requirements to the NIST framework to ensure alignment.

# Controls Assessment

**Current assets**

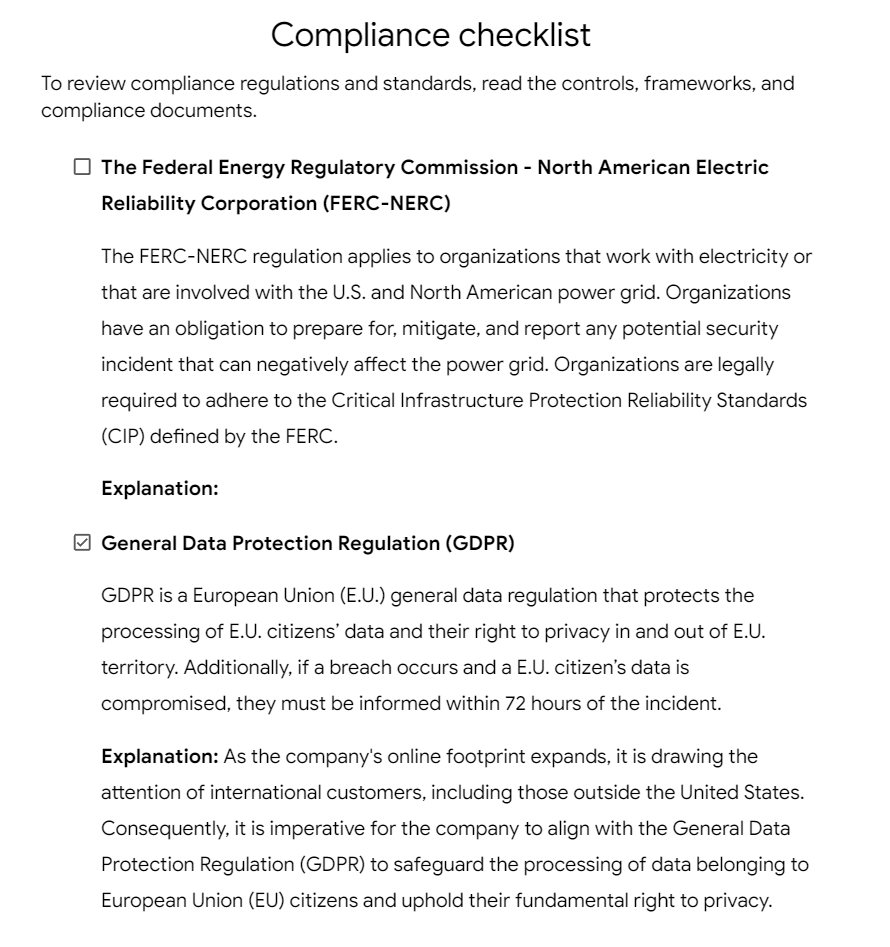
* On-premises equipment for in-office business needs
* Employee equipment: end-user devices (desktops/laptops, smartphones), remote workstations, headsets, cables, keyboards, mice, docking stations, surveillance cameras, etc.
* Management of systems, software, and services: accounting, telecommunication, database, security, ecommerce, and inventory management
* Internet access
* Internal network
* Vendor access management
* Data center hosting services
* Data retention and storage
* Badge readers
* Legacy system maintenance: end-of-life systems that require human monitoring

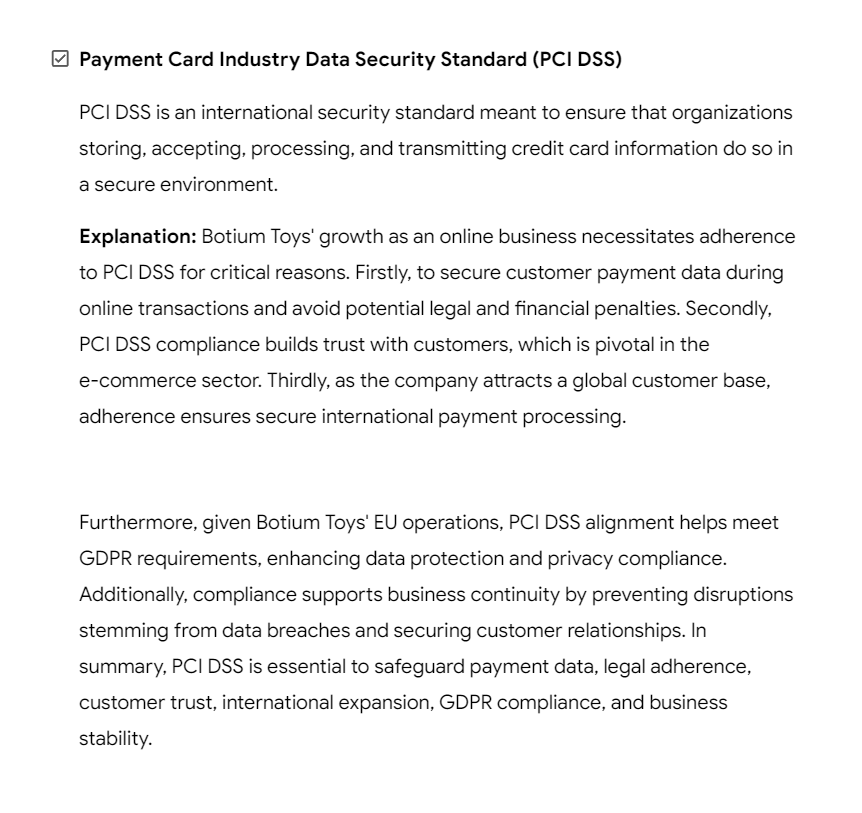
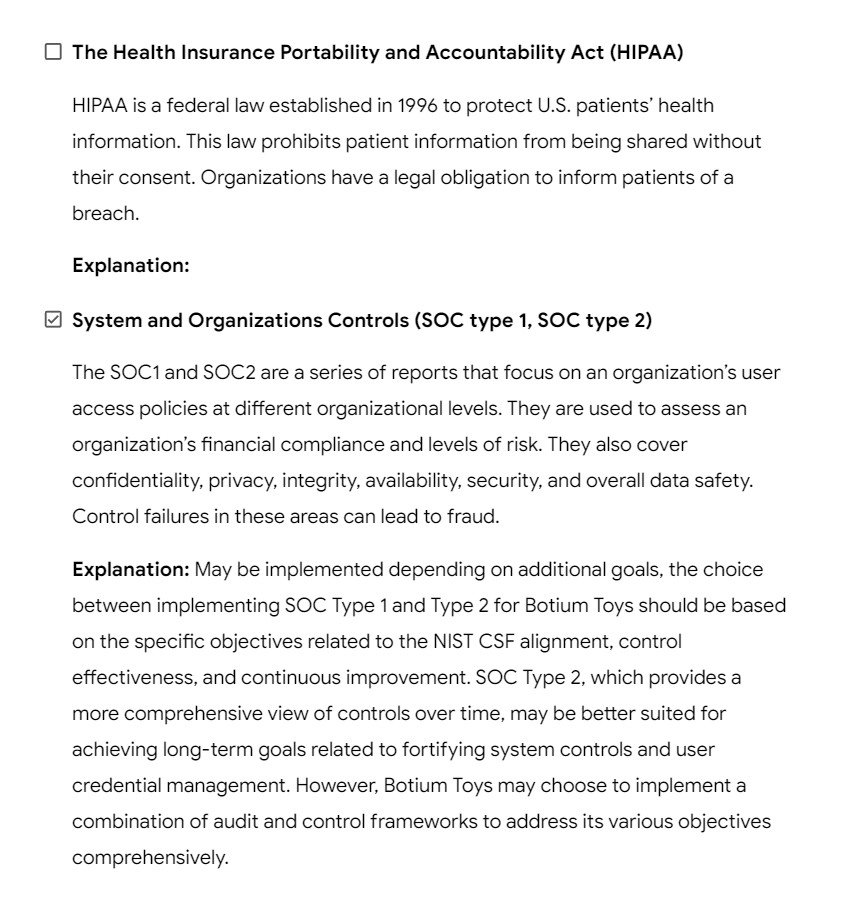
| **Administrative Controls** | | | |
| --- | --- | --- | --- |
| **Control Name** | **Control type and explanation** | **Needs to be implemented (X)** | **Priority** |
| Least Privilege | Preventative; reduces risk by making sure vendors and non-authorized staff only have access to the assets/data they 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 (int. network, wireless); applications (email, elec. data); data 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 | Medium |
| 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/Medium |
| 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 | Medium |
| 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 |
| Adequate lighting | Deterrent; limit “hiding” places to deter threats | X | Low |
| Closed-circuit television (CCTV) surveillance | Preventative/detective; can reduce risk of certain events; can be used after event for investigation | X | Medium |
| Locking cabinets (for network gear) | Preventative; increase integrity by preventing unauthorized personnel/individuals from physically accessing/modifying network infrastructure gear | X | 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 | Medium |
| 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/Low |

# Compliance checklist



# Analyzing audit results

## What were the audit scope and goals?

*Scope:*

* Current user permissions set in the following systems: accounting, end point

detection, firewalls, intrusion detection system, security information and event

management (SIEM) tool.

* Current implemented controls in the following systems: accounting, end point

detection, firewalls, intrusion detection system, Security Information and Event

Management (SIEM) tool.

* Current procedures and protocols set for the following systems: accounting,

end point detection, firewall, intrusion detection system, Security Information

and Event Management (SIEM) tool.

* Ensure current user permissions, controls, procedures, and protocols in place

align with necessary compliance requirements.

* Ensure current technology is accounted for. Both hardware and system access.

*Goals:*

* 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
* 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.
* Ensure they are meeting compliance requirements.

## What were the critical findings of the audit that need to be addressed immediately ?

*Administrative Controls to be implemented* ***immediately****:*

* Least Privilege – Reduce risks by making sure vendors and non-authorized staff only have access to the assets/data they need to do their jobs.
* Disaster Recovery Plans - 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.
* Password policies - Establish password strength rules.
* Access control policies - Increase confidentiality and integrity of data.
* Separation of duties - Ensure no one has so much access that they can abuse the system for personal gain.

*Technical Controls to be implemented* ***immediately****:*

* Intrusion Detection System (IDS) - Allow IT team to identify possible intrusions quickly (e.g. anomalous traffic).
* Encryption - Make confidential information/data more secure (e.g. website payment transactions).
* Backups - Supports ongoing productivity in the case of an event.
* Antivirus (AV) software - Detect and quarantine known threats.
* Manual monitoring, maintenance, and intervention - Required for legacy systems to identify and mitigate potential threats, risks, and vulnerabilities.

## What were the findings of the audit that need to be addressed in the future ?

*Administrative Controls to be implemented in the* ***future****:*

* Account management policies - Increase confidentiality and integrity of data.

*Technical Controls to be implemented in the* ***future****:*

* Password management system - Password recovery, reset, lock out notifications.

*Physical Controls to be implemented in the* ***future****:*

* Time-controlled safe - Reduce attack surface/impact of physical threats.
* Adequate lighting - Limit “hiding” places to deter threats.
* Closed-circuit television (CCTV) surveillance - Can reduce risk of certain events; can be used after event for investigation.
* Locking cabinets (for network gear) - increase integrity by preventing unauthorized personnel/individuals from physically accessing/modifying network infrastructure gear.
* Signage indicating alarm service provider - Makes the likelihood of a successful attack seem low.
* Locks - Physical and digital assets are more secure.
* Fire detection and prevention - Detect fire in the toy store’s physical location to prevent damage to inventory, servers, etc.

## How can you summarize your recommendations clearly and concisely to stakeholders?

***Immediate*** *Implementation (Administrative Controls):*

1. Least Privilege: Limit access to assets/data for vendors and non-authorized staff to only what's necessary for their roles, reducing security risks.
2. Disaster Recovery Plans: Ensure systems can continue running in incidents with minimal productivity downtime and system impact.
3. Password Policies: Establish rules for strong passwords to enhance security.
4. Access Control Policies: Increase data confidentiality and integrity by controlling who can access what.
5. Separation of Duties: Prevent individuals from having excessive access that could be misused for personal gain.

***Immediate*** *Implementation (Technical Controls):*

1. Intrusion Detection System (IDS): Quickly identify potential intrusions like unusual network traffic.
2. Encryption: Enhance the security of confidential data, especially in activities like website payment transactions.
3. Backups: Ensure ongoing productivity by having data backups in case of events.
4. Antivirus (AV) Software: Detect and isolate known threats.
5. Manual Monitoring and Maintenance: Necessary for legacy systems to identify and address potential threats and vulnerabilities.

***Future*** *Implementation (Administrative Controls):*

1. Account Management Policies: Further enhance data confidentiality and integrity.

***Future*** *Implementation (Technical Controls):*

1. Password Management System: Implement features like password recovery, reset, and lockout notifications.

***Future*** *Implementation (Physical Controls):*

1. Time-Controlled Safe: Reduce the impact of physical threats by limiting access to certain times.
2. Adequate Lighting: Deter threats by limiting hiding places.
3. Closed-Circuit Television (CCTV) Surveillance: Enhance security, investigate events, and deter potential incidents.
4. Locking Cabinets (for Network Gear): Prevent unauthorized access to network infrastructure, increasing data integrity.
5. Signage Indicating Alarm Service Provider: Create the perception of low risk, discouraging attacks.
6. Locks: Enhance security for physical and digital assets.
7. Fire Detection and Prevention: Detect and prevent fires in the toy store's location to protect inventory, servers, and assets.

*These recommendations aim to bolster the company's overall security posture, protect data, and minimize risks and vulnerabilities. Immediate implementation of selected controls is crucial, while future measures will further enhance security and resilience.*