# Botium Toys

Taylor Bryant
April 13th, 2025

## Frameworks Cited

| National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
| Payment Card Industry Data Security Standard (PCI DSS v.4.0)
| General Data Protection Regulation (GDPR)
| System and Organization Controls 1, System and Organization Controls 2 (SOC 1) (SOC2)

## Overview

The main purpose of this internal audit was to assess the stability of the security posture of Botium Toys, a steadily growing company. Increased consumer activity requires facilitating a stronger alignment with industry -standard cybersecurity frameworks. A detailed look within each framework is necessary.

The goal of this internal audit was to identify and review gaps that may threaten business continuity. By analyzing key IT and cybersecurity assets and controls, weaknesses were shown in disaster recovery planning, encryption, and access control practices. This is a summary of the contents outlining critical risks and a plan for industry -standard alignment for each framework cited.

## Focus

### Scope

This internal security audit for Botium toys will focus on the infrastructure that supports company IT assets and controls. A categorized evaluation will be provided for each asset and sorted within the control it influences. Areas measured for compliance include employee devices, data storage, and cybersecurity policies. This internal security audit will provide a bulleted plan for each area that requires improvement.

### Objectives

| Review the existing technical, administrative, and physical controls.
| Identify the risks within company IT systems and data.
| Provide an organized plan that aligns the company with standard compliance.

## Risk Summary

### Administrative Controls

- Lack of principle of least privilege.
  Sensitive data is accessible to everyone within the company.
  ***Frameworks | NIST CSF, PCI DSS***
- Lack of disaster recovery plans.
  Putting a plan in place will ensure business continuity in the case of an incident.
  ***Frameworks | NIST CSF, SOC 2***
- A stronger password policy is needed.
  Company assets could be compromised, this would lessen the risk.
  ***Frameworks | NIST CSF, PCI DSS***

## Risk Summary

### Administrative Controls

- Enforcing better division of responsibilities.
  This would lessen the risk of a single person having control over sensitive data.
  ***Frameworks | NIST CSF, SOC 2***

### Technical Controls

- Lack of Intrusion Detection System (IDS).
  Without an IDS, risks and suspicious behavior could go unnoticed by the company.
  ***Frameworks | NIST CSF, SOC 2***
- Lack of backups.
  Having backups of company-wide data would be beneficial in the case of a huge loss of assets.
  ***Frameworks | NIST CSF, PCI DSS***
- The legacy systems lack a process.
  Introducing a process would help close up any gaps in security during monitoring.
  ***Frameworks | NIST CSF, SOC 2***
- Lack of encryption.
  Introducing encryption to sensitive company and customer data would add an extra layer of security.
  ***Frameworks | PCI DSS, GDPR***
- Lack of Password Management System.
  A centralized system to secure passwords within the company would help introduce proper troubleshooting.
  ***Frameworks | NIST CSF, SOC 2***

### Physical Controls

**No further action needed.**

## Compliance Summary

NIST Cybersecurity Framework (NIST CSF)

| N/A | Low | Medium | High |
|---|---|---|---|

Payment Card Industry Data Security Standard (PCI DSS)

| N/A | Low | Medium | High |
|---|---|---|---|

General Data Protection Regulation (GDPR)

| N/A | Low | Medium | High |
|---|---|---|---|

System and Organization Controls (SOC 2)

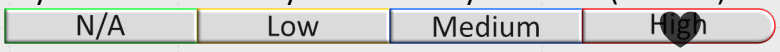
| N/A | Low | Medium | High |
|---|---|---|---|

## Plan

NIST Cybersecurity Framework (NIST CSF)

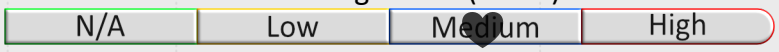

- Create a disaster recovery plan.
- Set up an Intrusion Detection System (IDS)
- Begin encrypting sensitive data.
- Implement a least privilege of responsibilities.
- Create a maintenance schedule for company legacy systems.

Payment Card Industry Data Security Standard (PCI DSS)



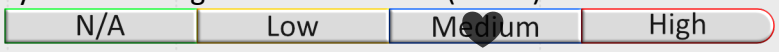

- Begin encrypting sensitive data.
- Set up restrictions for cardholder to be accessed by authorized personnel only.
- Implement stricter password requirements.
- Create backups of all sensitive cardholder data.

General Data Protection Regulation (GDPR)




- Begin encrypting sensitive data.
- Implement a data inventory system with categorization.
- Set up restrictions for sensitive data to be accessed by who needs it.
- Implement stricter password requirements.

System and Organization Controls (SOC 2)




- Create a disaster recovery plan.
- Set up an Intrusion Detection System (IDS)
- Implement a separation of duties.
- Implement a user access policy.
- Create a maintenance schedule for company legacy systems.

## Summary

This internal security audit for Botium Toys was completed in order to properly analyze the current state of the security posture. Starting with a list of referenced frameworks - a detailed overview and focus provided a foundation to build the risk assessment on. Producing a risk summary that highlights major flaws within satisfying the related framework helped structure a plan to meet proper compliance standards.

## Attachments