INTERNAL SECURITY AUDIT



REPORT NUMBER: 007

AUDIT: BOTIUM TOYS

AUDIT DATE: 10-07-23 TO 16-07-23

AUDITOR: DURGESH SHAH

[www.durgeshaudit.com](http://www.durgeshaudit.com) Name of Company: Security Co.

Mob: 98XXXXXXXX Report Submission date: 17-07-23

Fax: 314XXXXXXX VERIFIED!

Table of Contents :-

[**Executive Report 4**](#_56uhwkfgvk16)

[Executive Summary 5](#_olrx5jwymvtb)

[Management Response 6](#_bgqe06d3tyla)

[Additional Procedures and Report Signatures 8](#_ao100kxy50xx)

[Procedures of audit 8](#_m55csofw7fb2)

[**Detailed Report 9**](#_6syvqtgjn8wy)

[Audit Scope and Goals 10](#_mgqp1yhcrmjp)

[Scope 10](#_5amnjv9mhbsx)

[Goals 10](#_7r1tjwtwsswm)

[Risk Assessment Results 11](#_plwjlriu9o5g)

[Current assets 11](#_jdudu6fs5rtm)

[Risk description 11](#_5i80k6dm51vy)

[Control best practices 11](#_pepjp18yvpjs)

[Risk score 11](#_ghnlzhum2uiy)

[Additional comments 12](#_kmpxjpzb7q2o)

[Internal Audit & Compliance Checklist 13](#_vri4met40jiv)

[Controls assessment 13](#_swls7m11ggfl)

[Compliance checklist 17](#_goe9xzxx0fid)

[Remediation Suggestions 19](#_hlkfqbb5s7r9)

[Control Best Practices - Identify (NIST CSF) 19](#_fctuix29dl31)

[Risk Score and Additional Comments 19](#_7nws7iykt6d9)

[Conclusion 20](#_lkkq58qm9l00)

# 

# Executive Report

## Executive Summary

Boltium Toys, a growing U.S. toy business, faces the challenge of expanding its online market presence while ensuring business continuity, compliance, and security in the face of increasing global demand. The Information Technology (IT) department recognizes the need to proactively address these concerns and has undertaken an internal IT audit to evaluate the company's security posture and identify potential risks, threats, and vulnerabilities. The audit, guided by the National Institute of Standards and Technology (NIST) Cybersecurity Framework, aims to enhance the company's security practices and position it for sustainable growth.

Context:

Boltium Toys operates both a physical location and a burgeoning online presence that serves customers across the United States and internationally. The IT department acknowledges the need to solidify a plan of action to support global online operations, ensure compliance with regulations, and mitigate potential risks to critical assets.

**Overall Facility Risk Impact: 8/10**

## Management Response

Dear [IT Manager's Name],

Thank you for your diligent efforts in conducting the internal IT audit for Boltium Toys. Your comprehensive assessment and the resulting action plan reflect your dedication to strengthening our company's security posture and ensuring compliance as we continue to expand our online operations.

We understand the significance of the audit findings and are fully committed to implementing the recommended action plan to address the identified risks and vulnerabilities. Your strategic approach in aligning with the NIST Cybersecurity Framework and industry best practices will undoubtedly fortify our defenses and enhance our ability to safeguard our assets and customer data.

Asset Management Enhancement:

We acknowledge the importance of robust asset management, and we will prioritize the implementation of effective tracking mechanisms. By meticulously cataloging and managing our assets, we can ensure that unauthorized access and potential vulnerabilities are minimized.

Controls and Policies Strengthening:

The proposal to develop and enforce enhanced controls and policies is well-received. Your emphasis on creating a structured framework to protect our infrastructure against potential threats is in line with our commitment to maintaining a secure environment for our operations.

Compliance Adherence:

Compliance with both U.S. and international regulations is paramount to our business success. We appreciate your attention to identifying the specific regulations that apply to our operations, particularly those concerning online payments and E.U. business. Ensuring compliance not only safeguards our legal standing but also builds trust with our customers.

Expanding the IT Department:

We acknowledge your goal of utilizing the audit findings to secure approval for expanding the IT department. The comprehensive assessment of risks and the well-defined action plan will undoubtedly provide the necessary evidence to demonstrate the department's crucial role in securing our company's future.

We value your leadership and expertise in driving this initiative. Your commitment to our security and compliance objectives is commendable and aligns perfectly with our company's vision of responsible growth.

Please let us know how we can best support you in executing this action plan effectively. We look forward to witnessing the positive impact of these measures on our overall security posture and future success.

Thank you once again for your dedication and hard work.

Sincerely,

[Management's Name]

[Management's Title]

Boltium Toys

## Additional Procedures and Report Signatures

### Procedures of audit

1. Discussing of the scope and goals
2. Conducting the risk assessment with help of risk management team
3. Conducting the Internal Audit and going through Compliance checklist
4. Remediation Plan Suggessions

**ACCEPTED:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_

Director of the company Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_

Manager of the company Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_

Leader of Risk Management Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_

Internal Auditor Date

# 

# 

# Detailed Report

## Audit Scope and Goals

### Scope

Botium Toys internal IT audit will assess the following:

* 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

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
* 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

## Risk Assessment Results

### 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.
* 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

### Risk description

Currently, there is inadequate management of assets. Additionally, Botium Toys does not have the proper controls in place and may not be 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 managing assets. Additionally, they will need to 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 necessary compliance regulations and standards.

### 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 lost. The likelihood of a lost asset or fines from governing bodies is high because Botium Toys does not have all of the necessary controls in place and is not adhering to required regulations and standards related to keeping customer data private.

## Internal Audit & Compliance Checklist

### Controls assessment

To review control categories, types, and the purposes of each, read the [control categories](https://docs.google.com/document/d/1HsIw5HNDbRXzW7pmhPLsK06B7HF-KMifENO_TlccbSU/template/preview) document provided by the company.

**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.
* 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 (internal network, wireless); applications (email, electronic data); data and restoration | X | Critical |
| 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 | Critical |
| 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 | Low |

| **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 | X | High |
| 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 | Critical |
| Backups | Corrective; supports ongoing productivity in the case of an event; aligns to the disaster recovery plan | X | Critical |
| Password management system | Corrective; password recovery, reset, lock out notifications | X | High |
| Antivirus (AV) software | Corrective; detect and quarantine known threats | X | Critical |
| 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 | Low |
| Adequate lighting | Deterrent; limit “hiding” places to deter threats |  |  |
| Closed-circuit television (CCTV) surveillance | Preventative/detective; can reduce risk of certain events; can be used after event for investigation |  |  |
| 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 |  |  |
| 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 |

### 

### Compliance checklist

To review compliance regulations and standards, read the controls, frameworks, and compliance documents.

* **The Federal Energy Regulatory Commission - North American Electric Reliability Corporation (FERC-NERC)**

The FERC-NERC regulation applies to organizations that work with electricity or that are involved with the U.S. and North American power grid. Organizations have an obligation to prepare for, mitigate, and report any potential security incident that can negatively affect the power grid. Organizations are legally required to adhere to the Critical Infrastructure Protection Reliability Standards (CIP) defined by the FERC.

* **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.

* **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.

* **The Health Insurance Portability and Accountability Act (HIPAA)**

HIPAA is a federal law established in 1996 to protect U.S. patients’ health information. This law prohibits patient information from being shared without their consent. Organizations have a legal obligation to inform patients of a breach.

* **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.

## Remediation Suggestions

### Control Best Practices - Identify (NIST CSF)

To address the risk of inadequate asset management and control deficiencies, Boltium Toys should focus on the "Identify" function of the NIST Cybersecurity Framework (CSF). The following control best practices are recommended:

**Asset Inventory and Management:**

* Establish a comprehensive inventory of all critical assets, including systems, applications, databases, and data stores.
* Implement asset management tools and practices to accurately track the lifecycle of assets, from procurement to retirement.
* Assign ownership and accountability for each asset to ensure proper maintenance and security.

**Impact Assessment:**

* Conduct a thorough impact assessment to determine the potential consequences of losing specific assets.
* Identify the criticality of assets to business operations, customer data, and overall business continuity.

**Control Implementation:**

* Implement access controls, authentication mechanisms, and encryption where applicable to protect assets from unauthorized access.
* Establish and enforce least privilege principles to limit access to assets based on job roles and responsibilities.
* Regularly review and update controls based on changes in asset status and emerging threats.

### Risk Score and Additional Comments

The current risk score of 8 out of 10 reflects the high level of risk posed by inadequate asset management and control deficiencies. The potential impact of asset loss is rated as medium due to the uncertainty surrounding which assets might be lost. However, the likelihood of asset loss or fines from regulatory bodies is high, given the absence of comprehensive controls and non-compliance with regulations pertaining to customer data privacy.

### Conclusion

To mitigate the identified risks, it is imperative for Boltium Toys to prioritize the implementation of robust asset management practices and effective controls. By adhering to the best practices outlined within the NIST CSF's "Identify" function, Boltium Toys can significantly enhance its security posture, reduce the risk of asset loss, and ensure compliance with relevant regulations and standards.

These remediation measures are essential for safeguarding the company's assets, ensuring business continuity, and maintaining customer trust. By taking proactive steps to address these concerns, Boltium Toys will be better equipped to navigate the challenges of its expanding online operations while upholding its commitment to security and compliance.