**Table of Contents**

[Cybersecurity Audit for Botium Toys](#__RefHeading___Toc2171_2067123913)  [2](#__RefHeading___Toc2171_2067123913)

[Summary, scope and objectives of audit](#__RefHeading___Toc2201_2067123913)  [2](#__RefHeading___Toc2201_2067123913)

[Range](#__RefHeading___Toc2193_2067123913)  [2](#__RefHeading___Toc2193_2067123913)

[Objective](#__RefHeading___Toc2191_2067123913)  [2](#__RefHeading___Toc2191_2067123913)

[Risk Assessment](#__RefHeading___Toc2207_2067123913)  [3](#__RefHeading___Toc2207_2067123913)

[Current digital resources](#__RefHeading___Toc2185_2067123913)  [3](#__RefHeading___Toc2185_2067123913)

[Risk Description](#__RefHeading___Toc2199_2067123913)  [3](#__RefHeading___Toc2199_2067123913)

[Good practices in control](#__RefHeading___Toc2189_2067123913)  [3](#__RefHeading___Toc2189_2067123913)

[Risk scores](#__RefHeading___Toc2187_2067123913)  [4](#__RefHeading___Toc2187_2067123913)

[Additional comments](#__RefHeading___Toc2197_2067123913)  [4](#__RefHeading___Toc2197_2067123913)

[Assessment of controls](#__RefHeading___Toc2205_2067123913)  [4](#__RefHeading___Toc2205_2067123913)

[Current digital resources](#__RefHeading___Toc2195_2067123913)  [4](#__RefHeading___Toc2195_2067123913)

[Compliance Checklist](#__RefHeading___Toc2203_2067123913)  [7](#__RefHeading___Toc2203_2067123913)

[\_\_\_\_\_ The Federal Energy Regulatory Commission - North American Electric](#__RefHeading___Toc2173_2067123913)  [7](#__RefHeading___Toc2173_2067123913)

[Reliability Corporation (FERC-NERC)](#__RefHeading___Toc2183_2067123913)  [7](#__RefHeading___Toc2183_2067123913)

[\_\_X\_\_ General Data Protection Regulation (GDPR)](#__RefHeading___Toc2181_2067123913)  [8](#__RefHeading___Toc2181_2067123913)

[\_\_X\_\_ Payment Card Industry Data Security Standard (PCI DSS)](#__RefHeading___Toc2179_2067123913)  [8](#__RefHeading___Toc2179_2067123913)

[\_\_\_\_\_ The Health Insurance Portability and Accountability Act (HIPAA)](#__RefHeading___Toc2177_2067123913)  [8](#__RefHeading___Toc2177_2067123913)

[\_\_X\_\_ System and Organization Controls (SOC type 1, SOC type 2)](#__RefHeading___Toc2175_2067123913)  [8](#__RefHeading___Toc2175_2067123913)

****Cybersecurity Audit for Botium Toys****

# **Summary, scope and objectives of the audit**

****Summary****   
Botium Toys is experiencing remarkable growth in the online market, exposing its systems to new risks. This internal audit was conducted to assess the company's cybersecurity posture, identify vulnerabilities, and verify compliance with regulatory requirements (PCI DSS, GDPR, etc.).

The assessment revealed several weaknesses, including the absence of a business continuity plan, insufficient access controls, and incomplete compliance procedures. Immediate recommendations were made.

## **Scope**

**Botium Toys' internal IT audit will assess the following:**

* **Current user permissions in the following systems: accounting, endpoint detection, firewall, intrusion detection system, security information and event management (SIEM) tools**
* **Controls currently implemented in the following systems: accounting, endpoint detection, firewall, intrusion detection system, security information and event management (SIEM) tools**
* **Procedures and protocols in place for the following systems: accounting, endpoint detection, firewall, intrusion detection system, security information and event management (SIEM) tools**
* **Ensure that user authorizations, controls, procedures and protocols in place meet necessary compliance requirements.**
* **Ensure current technologies are considered. Access to hardware and system.**

## **Objective**

**The objectives of Botium Toys' internal IT audit are as follows:**

* **Adhere to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)**
* **Implement a better process for their systems to ensure they are compliant**
* **Strengthen system controls**
* **Implement the concept of least privilege in user credential management**
* **Establish their policies and procedures, including their playbooks**
* **Ensure they meet regulatory compliance requirements**

# **Risk assessment**

## **Current digital resources**

**The digital resources managed by the IT department are as follows:**

* **On-site equipment for business needs**
* **Employee equipment: user devices (desktops/laptops, smartphones), remote workstations, headsets, cables, keyboards, mice, docking stations, surveillance cameras, etc.**
* **Systems, software and services management: accounting, telecommunications, database, security, e-commerce and inventory management**
* **Internet access**
* **Internal network**
* **Data center hosting management**
* **Data retention and storage**
* **Badge readers**
* **Maintenance of legacy systems: end-of-life systems that require human monitoring**

## **Description of risks**

Currently, resource management is inadequate. Furthermore, Botium Toys does not have appropriate controls in place and cannot comply with U.S. and international regulations and standards.

## **Good practices in control**

The first of the five functions of the NIST CSF is to identify . Botium Toys will need to focus on resource management. In addition, they will need to determine the impact of the loss of existing resources, including systems, on business continuity.

## **Risk scores**

**On a scale of 1 to 10, the risk score is 8, which is quite high. This is due to a lack of controls and adherence to necessary regulations and compliance standards.**

## **Additional comments**

The potential impact of a resource loss is rated as medium because the IT department does not know which resources would be lost. The likelihood of resource loss or fines from government agencies is high because Botium Toys has not implemented all necessary controls and does not adhere to required regulations and standards regarding customer data privacy.

# **Evaluation of controls**

## **Current digital resources**

The digital resources managed by the IT department are as follows:

* On-site equipment for business needs
* Employee Equipment: User devices (desktops/laptops, smartphones), remote workstations, headsets, cables, keyboards, mice, docking stations, surveillance cameras, etc.
* Systems, software and services management: accounting, telecommunications, databases, security, e-commerce and inventory management
* Internet access
* Internal network
* Supplier Access Management
* Data center hosting services
* Data retention and storage
* Badge readers
* **Maintenance of legacy systems: end-of-life systems that require human monitoring**

| Administrative controls | | | |
| --- | --- | --- | --- |
| Name of the control | Type of control and explanation | Must be implemented (X) | Priority |
| Least privilege | Preventative; reduces risk by ensuring vendors and unauthorized personnel only have access to the IT resources/data they need to do their jobs | X | Pupil |
| Disaster recovery plans | Corrective; business continuity to ensure systems can operate in the event of an incident/there is limited or no loss of productivity due to downtime/low impact on 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 recovery | X | Pupil |
| Password Policies | Preventative; establish password strength rules to improve security/reduce the likelihood of accounts being compromised by brute force or dictionary attack techniques | X | Pupil |
| Access control policies | Preventive; strengthen data confidentiality and integrity | X | Pupil |
| Account Management Policies | Preventative; reduce the attack surface and limit the overall impact of disgruntled/former employees | X | Pupil/  AVERAGE |
| Separation of duties | Preventative; ensuring that no one has access that could allow them to abuse the system for personal gain | X | Pupil |

|  |  |  |  |
| --- | --- | --- | --- |
| Technical controls | | | |
| Name of the control | Type of control and explanation | Must be implemented  (X) | Priority |
| Firewall | Preventative, firewalls are already in place to filter unwanted/malicious traffic that enters the internal network | SO | SO |
| Intrusion Detection System (IDS) | Detective; allows the IT team to quickly identify possible intrusions (e.g., abnormal traffic) | X | Pupil |
| Encryption | Deterrent; makes confidential information/data more secure (e.g., payment transactions on websites) | X | Pupil/  AVERAGE |
| Backups | Corrective; helps maintain productivity in the event of an event; aligns with the disaster recovery plan | X | Pupil |
| Password management system | Fix; Password recovery, reset, lock notifications | X | Pupil/  AVERAGE |
| Antivirus (AV) software | Patch; detect and quarantine known threats | X | Pupil |
| Manual monitoring, maintenance and intervention | Preventative/corrective; required for existing systems to identify and mitigate potential threats, risks, and vulnerabilities | X | Pupil |

|  |  |  |  |
| --- | --- | --- | --- |
| Physical checks | | | |
| Name of the control | Type of control and explanation | Must be implemented  (X) | Priority |
| Time-delayed safe | Deterrent; reduction of attack surface/impact of physical threats | X | AVERAGE/  Weak |
| Adequate lighting | Deterrent; limit hiding places to deter threats | X | AVERAGE/  Weak |
| Closed-circuit television (CCTV) surveillance | Preventive/detective; can reduce the risk of certain events; can be used after the event for investigative purposes | X | Pupil/  AVERAGE |
| Lockable cabinets (for network equipment) | Preventive; increase integrity by preventing unauthorized personnel/individuals from physically accessing or modifying network infrastructure equipment | X | AVERAGE |
| Sign indicating the alarm service provider | Deterrent; reduces the likelihood of a successful attack | X | Weak |
| Locks | Preventive; physical and digital resources are more secure | X | Pupil |
| Fire detection and prevention (fire alarm, sprinkler system, etc.) | Detective/Preventative: Detect a fire at the physical toy store location to prevent damage to inventory, servers, etc. | X | AVERAGE/  Weak |

# **Compliance Checklist**

#### \_\_\_\_\_ The Federal Energy Regulatory Commission - North American Electric

#### Reliability Corporation (FERC-NERC)

FERC-NERC regulations apply to companies operating in the electric power sector or involved in the electric grid in the United States and North America. Companies are required to prepare for, mitigate, and report any potential security incidents that could negatively impact the electric grid. Companies are legally required to adhere to the FERC's Critical Infrastructure Protection (CIP) reliability standards.

**Explanation:** SO

#### \_\_ X \_\_ General Data Protection Regulation (GDPR)

The GDPR is a European General Data Regulation that governs the processing of data of European Union (EU) citizens and their right to privacy within and outside the EU. Furthermore, if a breach occurs and an EU citizen's data is compromised, they must be notified within 72 hours of the incident.

Explanation: Botium Toys must adhere to the GDPR because it conducts business and collects personal information from people around the world, including the European Union.

#### \_\_ X \_\_ Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is an international security standard designed to ensure that companies that store, accept, process, and transmit credit card information do so within a secure environment.

**Explanation:** Botium Toys must adhere to PCI DSS because it stores, accepts, processes, and transmits credit card information in person and online.

#### \_\_\_\_\_ The Health Insurance Portability and Accountability Act (HIPAA)

HIPAA is a federal law established in 1996 to protect the health information of American patients. This law prohibits the sharing of patient information without their consent. Companies have a legal obligation to notify patients of a breach.

**Explanation:** SO

#### \_\_ X \_\_ System and Organization Controls (SOC type 1, SOC type 2)

SOC1 and SOC2 reports cover user access policies at various levels of the organization. They are used to assess financial compliance and risk levels. They also cover the confidentiality, privacy, integrity, availability, security, and safety of all data. Control failures in these areas can lead to fraud.

**Explanation:** Botium Toys must establish and enforce appropriate user access for internal and external (third-party vendor) personnel to mitigate risks and ensure data security.

## **Recommendations**

1. **Implement a business continuity plan (BCP/BCP)**
2. **Apply least privilege policy** on all systems
3. **Strengthen access controls** , monitoring and account management
4. **Update and formalize internal policies**
5. **Perform regular backups**
6. **Ensure that encryption is properly applied to sensitive data**
7. **Raise awareness and train staff on cybersecurity** (phishing, passwords, etc.)
8. **Perform regular monitoring of security incidents and system logs**