Botium Toys

internal Risk Audit

Security Risk audit 07/10/2023

# Audit 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.

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

● Ensure they are meeting compliance requirements

# Risk Assement

**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 the necessary controls in place and is not adhering to required regulations and standards related to keeping customer data private.

# Control Assessment

| **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 | 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 / 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 |  | | N/A | |
| 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 | | 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 | 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 / Low |

# Assessing Compliance

**\_\_\_\_\_ 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.

**Explanation:**

**\_\_X\_\_\_ 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.

**Explanation:** To comply with EU sales standards Botium will need to be GDPR compliant

**\_\_X\_\_\_ 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.

**Explanation:** Botium Toys processess online and credit card payments and will need to compliant with the PCI DSS (Payment Card Industry Data and Security Standard)

**\_\_\_\_\_ 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.

**Explanation:**

**\_\_X\_\_\_ 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.

**Explanation:** Botium Toys needs to establish and enforce appropriate user access for internal and external (third-party vendor) personnel to mitigate risk and ensure data safety

# communication to stakeholders

TO: IT Manager, Stakeholders

FROM: J S Walley

DATE: 07/10/2023

SUBJECT: Internal IT Audit Findings and Recommendations

Dear Colleagues,

Please review the following information regarding the Botium Toys internal audit scope, goals, critical findings, summary and recommendations.

Scope:

● The following systems are in scope: accounting, end point detection, firewalls, intrusion detection system, SIEM tool. The systems will be evaluated for:

○ Current user permissions

○ Current implemented controls

○ Current procedures and protocols

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

align with PCI DSS and GDPR compliance requirements.

● Ensure current technology is 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.

● Adapt to 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.

Critical findings (must be addressed immediately):

● Multiple controls need to be developed and implemented to meet the audit

goals, including:

○ Control of Least Privilege and Separation of Duties

○ Disaster recovery plans

○ Password, access control, and account management policies, including

the implementation of a password management system

○ Encryption (for secure website transactions)

○ IDS

○ Backups

○ AV software

○ CCTV

○ Locks

○ Manual monitoring, maintenance, and intervention for legacy systems

○ Fire detection and prevention systems

● Policies need to be developed and implemented to meet PCI DSS and GDPR

compliance requirements.

● Policies need to be developed and implemented to align to SOC1 and SOC2

guidance related to user access policies and overall data safety.

Findings (should be addressed, but no immediate need):

● The following controls should be implemented when possible:

○ Time-controlled safe

○ Adequate lighting

○ Locking cabinets

○ Signage indicating alarm service provider

Summary/Recommendations: It is recommended that critical findings relating to

compliance with PCI DSS and GDPR be promptly addressed since Botium Toys accepts

online payments from customers worldwide, including the E.U. Additionally, since one

of the goals of the audit is to adapt to the concept of least permissions, SOC1 and

SOC2 guidance related to user access policies and overall data safety should be used

to develop appropriate policies and procedures. Having disaster recovery plans and

backups is also critical because they support business continuity in the event of an

incident. Integrating an IDS and AV software into the current systems will support our

ability to identify and mitigate potential risks, and could help with intrusion detection,

since existing legacy systems require manual monitoring and intervention. To further