**Botium Toys Security Audit**

**Table of Contents**

[Audit Scope And Goals 3](#_Toc142490898)

[Controls assessment 4](#_Toc142490899)

[Compliance Checklist 6](#_Toc142490900)

# Audit Scope And Goals

The biggest risks to Botium Toys are:

* Inadequate management of assets, which could lead to asset misplacement or theft and potential data breaches.
* The absence of proper controls leaves the organization vulnerable to cyber threats and unauthorized access.
* Non-compliance with U.S. and international regulations and guidelines, posing legal and reputational risks.

**The controls that are most essential to implement immediately are:**

**Least Privilege:** Ensure that vendors and non-authorized staff have access only to the assets and data required for their roles, reducing the risk of unauthorized access and data breaches.

**Disaster Recovery:** Develop and implement a plan to ensure system functionality during incidents, minimizing downtime and ensuring business continuity.

**Password Policies:** Establish password strength rules to enhance security and reduce the likelihood of account compromises.

**Access Control Policies:** Implement policies that enhance data confidentiality and integrity by controlling access to sensitive information.

**Compliance regulations for customer and vendor data safety:**

To ensure customer and vendor data safety, avoid fines, and maintain compliance, Botium Toys must adhere to relevant data protection and privacy regulations. This includes:

* General Data Protection Regulation (GDPR) if conducting business with EU citizens.
* Payment Card Industry Data Security Standard (PCI DSS) if accepting payments through credit cards.

# Controls assessment

|  |  |  |  |
| --- | --- | --- | --- |
| **Administrative Controls** | **Control Type and Explanation** | **Needs to be Implemented (X)** | **Priority** |
| Least Privilege | Preventative; Ensure vendors and unauthorized staff access only necessary data | Yes | High |
| Disaster Recovery | Corrective; Plan to maintain system functionality during incidents | Yes | High |
| Password Policies | Preventative; Establish password strength rules for improved security | Yes | Medium |
| Access Control Policies | Preventative; Enhance data confidentiality and integrity | Yes | High |
| Account Management Policies | Preventative; Limit potential impact from disgruntled/former employees | Yes | Low |
| Separation of Duties | Preventative; Prevent abuse of the system for personal gain | No | NA |

|  |  |  |  |
| --- | --- | --- | --- |
| **Technical Controls** | **Control Type and Explanation** | **Needs to be Implemented (X)** | **Priority** |
| Firewall | Preventative; Filters unwanted/malicious traffic | NA | NA |
| Intrusion Detection System (IDS) | Detective; Identify possible intrusions quickly | Yes | High |
| Encryption | Deterrent; Enhances security of confidential information | No | NA |
| Backups | Corrective; Supports ongoing productivity in case of an event | Yes | Medium |
| Password Management System | Corrective; Password recovery, reset, and lockout notifications | No | NA |
| Antivirus (AV) Software | Corrective; Detect and quarantine known threats | Yes | Low |
| Manual Monitoring, Maintenance | Preventative/Corrective; Required for legacy system threats | Yes | Medium |

|  |  |  |  |
| --- | --- | --- | --- |
| **Physical Controls** | **Control Type and Explanation** | **Needs to be Implemented (X)** | **Priority** |
| Time-Controlled Safe | Deterrent; Reduces the impact of physical threats | Yes | Medium |
| Adequate Lighting | Deterrent; Limits hiding places for potential threats | Yes | Low |
| CCTV Surveillance | Preventative/  Detective; Reduces risk and aids in investigations | Yes | High |
| Locking Cabinets | Preventative; Restricts access to authorized personnel | Yes | Medium |
| Signage Indicating Alarm | Deterrent; Creates an impression of low likelihood of a successful attack | Yes | Low |
| Locks | Preventative; Enhances security for physical and digital assets | Yes | High |
| Fire Detection and Prevention | Detective/Preventative; Detect and prevent fire damage | No | NA |

# Compliance Checklist

|  |  |  |
| --- | --- | --- |
| **Compliance Regulation/Standard** | **Applicability to Botium Toys** | **Explanation** |
| Federal Energy Regulatory Commission - NERC (FERC-NERC) | Applicable if Botium Toys works with electricity or is involved in the U.S. and North American power grid. | Organizations must prepare for, mitigate, and report potential security incidents affecting the power grid and adhere to Critical Infrastructure Protection Reliability Standards (CIP) defined by FERC. |
| General Data Protection Regulation (GDPR) | is Applicable if Botium Toys handles the personal data of EU citizens. | GDPR protects the processing of EU citizens' data and their right to privacy, mandating notification within 72 hours in case of a data breach. |
| Payment Card Industry Data Security Standard (PCI DSS) | Applicable if Botium Toys stores, accepts, processes, or transmits credit card information | PCI DSS ensures secure handling of credit card data internationally. |
| Health Insurance Portability and Accountability Act (HIPAA) | Applicable if Botium Toys deals with U.S. patients' health information. | HIPAA protects patients' health information and requires organizations to inform patients of any breaches. |
| System and Organizations Controls (SOC Type 1, SOC Type 2) | Applicable to assess Botium Toys' user access policies, financial compliance, and risk levels. | SOC reports assess confidentiality, privacy, integrity, availability, security, and data safety, helping prevent fraud and ensure compliance. |