Index

[Botium Toys Integrated Compliance Checklist 2](#_Toc158022349)

[NIST Cybersecurity Framework (CSF) 2](#_Toc158022350)

[GDPR (General Data Protection Regulation) 2](#_Toc158022351)

[PCI DSS (Payment Card Industry Data Security Standard) 2](#_Toc158022352)

[HIPAA (Health Insurance Portability and Accountability Act) 3](#_Toc158022353)

[OWASP (Open Web Application Security Project) 3](#_Toc158022354)

[SOC 1 (Service Organization Control 1) 3](#_Toc158022355)

[SOC 2 (Service Organization Control 2) 3](#_Toc158022356)

# **Botium Toys Integrated Compliance Checklist**

## **NIST Cybersecurity Framework (CSF)**

Identify Function:

* **Asset Management:**
  + No comprehensive asset management system in place.

Protect Function:

* **Access Controls:**
  + Least privilege and separation of duties not enforced.

Respond Function:

* **Disaster Recovery and Backup:**
  + Inadequate disaster recovery plans and irregular backups.

Explanation:

Botium Toys is not fully compliant with the NIST CSF Identify Function as there is no comprehensive asset management system. Additionally, access controls lack the enforcement of least privilege and separation of duties.

## **GDPR (General Data Protection Regulation)**

* **Privacy Policies:**
  + Privacy policies need clearer enforcement and communication.

Explanation:

Botium Toys needs to enhance the enforcement and communication of privacy policies to align with GDPR requirements.

## **PCI DSS (Payment Card Industry Data Security Standard)**

* **Access Controls:**
  + Inadequate enforcement of least privilege and separation of duties.
* **Firewall:**
  + Firewall rules need improvement for better security.

Explanation:

Botium Toys is not fully compliant with PCI DSS access controls, which require the enforcement of least privilege and separation of duties. Additionally, firewall rules need enhancement for better security posture.

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

Administrative Safeguards:

* **Privacy Policies:**
  + Documentation and maintenance of data do not fully adhere to HIPAA privacy policies.

Physical Safeguards:

* **Physical Location Security:**
  + Lack of clarity on physical security controls.

Explanation:

Botium Toys needs to improve documentation and maintenance of data to fully adhere to HIPAA privacy policies. Additionally, there is a lack of clarity on physical security controls, which may impact compliance with HIPAA physical safeguards.

## **OWASP (Open Web Application Security Project)**

* **Security Awareness and Training:**
  + No specific emphasis on employee training and awareness programs for web application security.

Explain Non-Compliance:

Botium Toys needs to establish a specific security awareness and training program, focusing on web application security, to align with OWASP recommendations.

## **SOC 1 (Service Organization Control 1)**

* **Controls Relevant to Financial Reporting:**
  + Lack of clarity on controls relevant to financial reporting.

Explain Non-Compliance:

SOC 1 focuses on controls relevant to financial reporting. The non-compliance in this area indicates that Botium Toys hasn't provided sufficient clarity on controls specifically related to financial reporting processes. It's essential for the organization to clearly define and communicate these controls to meet SOC 1 criteria.

## **SOC 2 (Service Organization Control 2)**

* **Information Security Policies and Procedures:**
  + Policies and procedures need enhancement for better alignment with SOC 2 criteria.

Explain Non-Compliance:

SOC 2 emphasizes information security policies and procedures. The non-compliance suggests that Botium Toys' current policies and procedures may not align effectively with SOC 2 criteria. Enhancements are needed to ensure that the information security controls and practices meet the specific requirements of SOC 2.