Stakeholder memorandum

TO: IT Manager, Stakeholders

FROM: Carlos Ernesto Alzaga Ledezma  
DATE: 05/29/2023  
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:** Establish all the best practices and norms set by the industry and goverment to enssure a better management of assets and data in the company and avoid any breaches or loss of vital information and productivity.

* The following systems are in scope: accounting, end point detection, firewalls,

intrusion detection system, SIEM tool.

The systems will be evaluated for:

1. Current user permissions
2. Current implemented controls
3. 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:**

* 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

**Critical findings** (must be addressed immediately):

1. Least Privilege
2. Disaster recovery plans:
3. Password policies:
4. Intrusion Detection System (IDS)
5. Encryption:
6. Backups:
7. Password management system
8. Antivirus (AV) software
9. Closed-circuit television (CCTV) surveillance
10. Locks
11. Fire Detection and prevention system

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

1. Time-controlled safe
2. Adequate lighting
3. Signage indicating alarm service provider

**Summary/Recommendations:**

Given that Botium Toys accepts online payments from clients all over the world, including those in the EU, it is advised that serious concerns about compliance with PCI DSS and GDPR be addressed right away. Additionally, SOC1 and SOC2 recommendations about user access policies and overall data safety should be used to build suitable policies and processes, as one of the audit's objectives is to adapt to the notion of least permissions. Backups and disaster recovery plans are essential for ensuring business continuity in the case of an occurrence. Since the current old systems need manual monitoring and intervention, integrating an IDS and AV software will boost our ability to recognize and reduce potential hazards and could assist with intrusion detection. Locks and CCTV should be utilized to secure physical assets (including equipment) as well as to monitor and analyze potential threats in order to better secure assets located within Botium Toys' sole physical location. Encryption, a time-controlled safe, proper lighting, fire detection and prevention systems, and signage identifying the alarm service provider will all help to further strengthen Botium Toys' security posture, albeit they are not immediately necessary.