Stakeholder memorandum

TO: IT Manager, Stakeholders
FROM: Areesha Aftab
DATE: 13 August 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: Assessment of the entire security posture of Botium Toys: including Physical and Digital assets, internal processes, and procedures.

Goals: Following NIST CSF

Strengthening overall security posture
Implement the concept of least privilege
Design a playbook based on improved policies and procedures.
Ensure the company meets legal compliance requirements

Critical findings (must be addressed immediately):

Adhere to GDPR and PCI DSS regulations

- To maintain customer security and privacy

Follow System and Organizations Controls (SOC type 1, SOC type 2)

- To help focus on an organization's user access policies at different organizational levels.

Controls required for

- Access Control
- Manual Managing of legacy systems
- Installation of Antivirus Software
- Encryption
- Data Backup

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

- Locks for Physical Assets
- Provider for alarm signage
- Proper lighting system

Summary/Recommendations:

The overall security posture of the company needs a lot of dedicated time and attention. Lack of data security and privacy will definitely hurt the company's finance and reputation in the long run.
Essential backup plans should be made to ensure business continuity. SOC2 should be used to develop appropriate policies and procedures.
The company should follow NIST CSF, to build a basic security structure, furthermore, additional steps should be taken to establish playbooks to overcome security incidents such as breaches, data theft, and disaster recovery plans.
After establishing a better security posture, the company can move on to findings that do not require immediate assistance, such as Locks for Physical Assets, Providers for alarm signage, lighting systems, etc.