Stakeholder memorandum

TO: IT Manager, Stakeholders
FROM: Harsh Bali
DATE: 05/06/2023
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:

- For this audit following systems are in scope:
  - Accounting
  - End point detection
  - Firewalls
  - SIEM
  - These systems will be evaluated for:
    - Current user permission
    - Current implemented controls
    - Current procedures and protocols
- Ensure current user permissions, controls, procedures and protocols in place are aligned with PCI DSS & GDPR compliance requirements.
- Ensure current technology is accounted for both hardware and system access.

Goals:

- Adhere to NIST CSF.
- Establish better processes for Botium's systems to ensure they are compliant.
- Fortify system controls.
- Adapt to the concept of least permission 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):

- Control assessment findings states that these controls must be developed and implemented immediately to meet the audit goals:

    - Least Privilege
    - Disaster Recovery plans
    - Password policies
    - Access control policies
    - Account management policies
    - Separation of duties
    - IDS
    - Encryption
    - Backups
    - Antivirus software
    - Manual monitoring maintenance and intervention
    - CCTV
    - Locking cabinet
    - Locks
    - Fire detection and prevention system
- These policies must be developed and implemented immediately to meet the audit goals:
    - Policy to comply with PCI DSS.
    - Policy to comply with GDPR.
    - Policy to align with SOC1 and SOC2.

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

- Only when the critical controls/policies are addressed and implemented, then Botium should try to implement these controls to attain a strong security posture:
    - Adequate lighting
    - Time controlled safe
    - Signage indicating alarm service provider

Summary/Recommendations:
Firstly, Botium Toys should develop a disaster recovery plan as it will support business continuity in the event of an incident. After that, Botium Toys must develop policies/procedures that allow the company to be compliant with PCI DSS and GDPR. This is because the company conducts business worldwide, including the European Union. Failing to comply with PCI DSS and GDPR can restrict Botium's ability to conduct business worldwide. Then, the guidance available in SOC1 & SOC2 regarding user access policies and overall data safety should allow Botium Toys to develop and implement policies and procedures which will allow them to attain the goal of least privilege.

Then, implementing technological controls mentioned in critical findings can allow Botium to identify, contain and mitigate potential risks. Implementing physical controls such as CCTV will allow Botium Toys secure their physical assets.

Lastly, implementation of controls such as: Adequate lighting, Time controlled safe, Signage indicating alarm service provider could allow Botium Toys to implement defence in depth, thus, further improving their security posture.