Stakeholder memorandum

TO: IT Manager, stakeholders
FROM: Mohammad Adil
DATE: 14 June 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:

- The following systems are in scope: accounting, end point detection, firewalls, intrusion detection system, and SIEM tool. The systems will be evaluated for:
    - ➔ Current user permissions
    - ➔ Current implemented controls
    - ➔ Current procedures and protocols
- Ensure current user permissions, procedures, controls, and protocols in place align with PCI DSS and GDPR compliance requirements.
- Ensure current technology is accounted for both system access and hardware.

Goals:

- Adhere to the NIST CSF.
- Establishing a better process for their systems to ensure they are compliant.
- Fortify system controls.
- Adapt to the concept of least privilege 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):

- Multiple controls need to be developed and implemented to meet the audit goals, including:
    - Control of Least Privilege and Separation of Duties
    - Disaster recovery plans
    - Password, access control, and account management policies, including the implementation of a password management system
    - Encryption (for secure online transactions)
    - Backups
    - IDS
    - Antivirus (AV) software
    - CCTV
    - Locks
    - Manual monitoring, maintenance, and intervention for legacy systems
    - Fire detection and prevention systems
- Policies need to be developed and implemented to meet PCI DSS and GDPR compliance requirements.
- Policies need to be developed and implemented to align to SOC1 and SOC2 guidance related to user access policies and overall data safety.

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

- The following controls should be implemented when possible:
    - Time-controlled safe
    - Adequate lighting
    - Locking cabinets
    - Signage indicating alarm service provider

Summary/Recommendations:

Prompt attention should be given to critical findings regarding compliance with PCI DSS and GDPR at Botium Toys, as they accept online transactions from worldwide, including the E.U. Additionally, in order to align with the principle of least privilege, it is advisable to refer to SOC1 & SOC2 guidelines pertaining to user access policies and overall data safety when formulating appropriate policies and procedures. Ensuring the existence of disaster recovery plans and backups is crucial as they facilitate uninterrupted business operations in the event of an incident. To enhance the ability to identify and mitigate potential risks, integrating an IDS and AV software into the current system is recommended, particularly since the existing

legacy systems necessitate manual monitoring and intervention. Furthermore, to bolster the security of assets housed at Botium Toy's physical location, it is advisable to employ locks and CCTV for physical security and threat monitoring and investigation. Although not immediately required, utilizing encryption, a time controlled safe, adequate lighting, locking cabinets, fire detection and prevention systems and displaying signage indicating the alarm service provider will further enhance Botium Toy's security posture.