Stakeholder memorandum

TO: IT Manager, stakeholders
FROM: Destaalem
DATE: Sep 21, 2023
SUBJECT: Internal IT audit findings and recommendations

Dear Colleagues,

Please review the details regarding the Botium Toys internal audit concerning scope, goals, critical findings, and a summary with recommendations for improvement.

Scope:

- Evaluation of all IT systems including accounting, end point detection, firewalls, intrusion detection system, and SIEM tool.
- Assessment of user permissions, implemented controls, and operational procedures.
- Examination of compliance alignment with necessary regulations.
- Inventory of hardware and system access.

Goals:

- Compliance with the NIST Cybersecurity Framework (CSF).
- Enhancement of system processes for better compliance adherence.
- Strengthening of system controls.
- Implementation of a least privilege strategy for user access.

- Establishment and documentation of policies, procedures, and playbooks.
- Compliance with relevant regulatory requirements.

Critical findings (must be addressed immediately):

- Asset management is currently insufficient, posing significant risks.
- Critical system controls, especially around user access, are not in place.
- Disaster recovery plans are not established, which is vital for business continuity.
- Compliance gaps with GDPR and PCI DSS are present, needing urgent attention.
- Encryption for data in transit, particularly payment information, is not implemented.
- Intrusion detection systems are either outdated or missing, leaving us vulnerable to cyber-attacks.

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

- Physical security enhancements, including better lighting and secure storage for sensitive documents.
- Update and improve environmental controls like fire detection systems.
- Improve legacy system monitoring to prevent system failures and security breaches.
- Establish regular manual audits and checks for system vulnerabilities.

Summary/Recommendations: Summary/Recommendations:

- Immediate attention is recommended for findings related to PCI DSS and GDPR compliance due to the global nature of online payments processed by Botium Toys.

- Adoption of least privilege and user access policies as advised by SOC1 and SOC2 to formulate appropriate procedures.
- Disaster recovery and backup strategies are critical for maintaining operations during disruptions.
- Integration of IDS and AV software into systems to bolster threat identification and risk mitigation.
- Enhancement of physical security with locks and CCTV to protect Botium Toys' premises and assets.
- Long-term security posture will benefit from encryption, time-controlled safes, improved lighting, locking cabinets, fire detection and prevention, and clear alarm service signage.

Recommendations herein aim to reinforce the cybersecurity framework of Botium Toys, providing a secure and compliant environment for all stakeholders.