Stakeholder Memorandum

TO: IT Manager, Stakeholders
FROM: (Armando Martell)
DATE: (4/21/22)
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 systems covered include accounting, endpoint detection, firewalls, intrusion detection systems, and Security Information and Event Management (SIEM) tools. The assessment aims to ensure that the existing user permissions align with necessary compliance requirements and that the implemented controls, procedures, and protocols are in line with industry standards. Additionally, the audit evaluates the inclusion of current technology, encompassing both hardware and system access, to ensure comprehensive coverage. The goal is to identify any gaps or areas of improvement in these aspects and take necessary actions to enhance security and compliance within the organization.

Goals:
The organization aims to:
- Adhere to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), which provides a comprehensive set of guidelines and best practices for cybersecurity.
- Establish an improved process for their systems to ensure compliance with relevant regulations and standards.
- Strengthen system controls to enhance the security and resilience of their infrastructure and data.
- Implement the concept of least permissions, which involves granting users the minimum privileges necessary for their roles, in order to enhance user credential management and reduce the risk of unauthorized access.

- Establish policies and procedures, including playbooks, to define clear guidelines and protocols for managing cybersecurity incidents and ensuring consistent responses.
- Ensure ongoing compliance with applicable requirements, such as legal and regulatory frameworks, industry standards, and internal policies.

By focusing on these objectives, the organization aims to enhance its cybersecurity posture, minimize vulnerabilities, and maintain a robust and compliant security framework.

Critical findings;
Our top priority is achieving compliance with industry regulations. This includes adhering to the General Data Protection Regulation (GDPR) to safeguard our clients' personally identifiable information. To meet these requirements, we will adopt the System and Organizations Controls (SOC type 1, SOC type 2) framework, tailored to our specific needs. Implementing the principles of least privilege, robust password policies, and proactive monitoring of privileged users will enable us to ensure data protection both at rest and in transit.

Findings:
After conducting an assessment, it has been identified that enhancing the physical security measures is essential. Strengthening the locks on doors and cabinets within the server rooms, improving the lighting conditions, and implementing a comprehensive CCTV system are crucial steps in mitigating the risk of successful attacks.

Summary/Recommendations:
The Botium Toys internal audit covers various systems, including accounting, endpoint detection, firewalls, intrusion detection systems, and SIEM tools. The audit aims to ensure compliance, improve processes, strengthen controls, implement least privilege, establish policies and procedures, and meet legal requirements. Critical findings emphasize the importance of GDPR compliance and recommend adopting the SOC framework. Additional findings highlight the need to enhance physical security through reinforced locks, improved lighting, and a comprehensive CCTV system. By addressing these findings, Botium Toys aims to enhance cybersecurity, protect data, and maintain a robust security framework.