Stakeholder memorandum

TO: IT Manager, Stakeholders
FROM: Cyber Analyst
DATE: 5/12/23
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:
- **Current user permissions set in the following systems: accounting, end point detection, firewalls, intrusion detection system, security information and event management (SIEM) tool.**

- **Current implemented controls in the following systems: accounting, end point detection, firewalls, intrusion detection system, Security Information and Event Management (SIEM) tool.**

- **Current procedures and protocols set for the following systems: accounting, end point detection, firewall, intrusion detection system, Security Information and Event Management (SIEM) tool.**

- **Ensure current user permissions, controls, procedures, and protocols in place align with necessary compliance requirements.**

- **Ensure current technology is accounted for. Both hardware and system access.**

Goals:
- **To adhere to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)**

- **Establish a better process for their systems to ensure they are compliant**
- **Fortify system controls**
- **Implement the concept of least permissions 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): Disaster Recovery Plan/Business Continuity Plan must be implemented. AntiVirus Software must be installed in all devices, Account management policies need updates, Absolutely need to make backups on all data.

Findings (should be addressed, but no immediate need): Fire suppression system needs an overhaul, needs more adequate lighting, need locks, install a CCTV system

Summary/Recommendations:
It is highly recommended to implement a disaster recovery plan as the top priority, along with improving and upgrading security systems that will align with the NIST framework. Demonstrating a high level of security and protection to employees and customers will bring trust and confidence to handle and protect sensitive information.