Stakeholder memorandum

TO: IT Manager, Stakeholders
FROM:Javon
DATE:7/17/2023
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:

- Assessing security controls for the protection of sensitive data and information systems.
- Evaluating network security, data protection, user access management, and endpoint security measures.
- Reviewing incident response, security awareness training, and third-party risk management practices.

Goals:

- **Adhere to NIST CSF**
- **Establish better access controls**
- **Establish clear policies that fall into compliance along with playbooks**
- **Ensure technical controls are updated regularly and have the staff be well trained.**
- **Ensure password policies are enforced and require password changes every three months**

Critical findings (must be addressed immediately): Multiple controls need to be developed and implemented to meet the audit
goals, including:

- Least Privilege
- Disaster Recovery Plan

- Password Policies
- Access Control Policies
- Separation of duties
- IDS System
- Encryption (web transactions and system files)
- Backups
- Antivirus software
- CCTV (Closed-circuit television surveillance)
- Locks

Findings (should be addressed, but no immediate need):
The following controls should be implemented when possible:

- Fire detection and prevention (fire alarm, sprinkler system, etc.)
- Locking cabinets (for network gear)
- Time-controlled safe
- Manual monitoring, maintenance, and intervention
- Password management system
- Account management policies

Summary/Recommendations:
The cybersecurity audit for Botium Toys' has revealed commendable efforts towards data protection and information security. The company demonstrates a strong commitment to cybersecurity, with various measures in place to safeguard sensitive data and information systems. However, several critical findings require immediate attention to enhance the organization's security posture significantly. Urgent actions are recommended, such as implementing least privilege access controls, developing a comprehensive disaster recovery plan, enforcing strong password policies, and establishing clear access control policies. Additionally, Botium Toys' should consider implementing an Intrusion Detection System (IDS), encryption for web transactions and sensitive files, and regular data backups. Antivirus software must be kept up-to-date on all systems, and CCTV surveillance should be implemented in critical areas to enhance physical security. Addressing these critical issues promptly will ensure better protection against potential cyber threats and position Botium Toys' to meet industry best practices and compliance standards.