Stakeholder memorandum

Complete each section of the stakeholder memorandum template to communicate your audit results and recommendations to stakeholders:

- Scope
- Goals
- Critical findings (must be addressed immediately)
- Findings (should be addressed, but no immediate need)
- Summary/Recommendations

Use information from the following documents:

- Botium Toys: Audit scope and goals
- Controls assessment (completed in “Conduct a security audit, part 1”)
- Compliance checklist (completed in “Conduct a security audit, part 1”)

[***Use the following template to create your memorandum]***

TO: IT Manager, Stakeholders
FROM: (Ryan Wong)
DATE: (06/30/2023)
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: Current user permissions, controls, procedures and protocols are to be assessed for the following systems: accounting, end point detection, firewalls, intrusion detection system, security information and event management tools. Ensure that these align with compliance requirements and controls. Also ensure that all current technology is accounted for hardware and system access.

Goals:

Adhere to the National Institute of Standards and Technology Cybersecurity Framework and create a better process for systems that is compliant and more efficient. Ensure that System Controls are fortified and user's have least permission privileges to do their job.

Critical findings (must be addressed immediately):
Least Privilege Controls
Disaster Recovery Plans
Password Policies
Access Control Policies
Separation of Duties
Firewall
Intrusion Detection System
Encryption
Backups
Locking Cabinets
Locks
Fire Detection and Prevention

Findings (should be addressed, but no immediate need):
Account Management Policies, Password Management System, Antivirus Software, Closed-Circuit Television, Signage indicating alarm service provider.

Summary/Recommendations:

It is recommended that we immediately focus on access and being compliant with NIST and the security controls we selected. We need to make sure that no one person has too much access to complete their job and only what they need. In addition we'll need to make sure that no one has unauthorized access to our equipment and assets by having physical controls in place. Since we have a strong online presence, it's recommended that we immediately implement online protection such as IDS, Encryption, and Firewalls to safeguard our data.