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: Duncan Kromminga
DATE: 9/10/2023
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 for accounting
- Current implemented controls in accounting
- Current accounting procedures and protocols
- Compliance Requirements
- Ensure current technology is accounted for

Goals:

- Adhere to National Institute of Standards and Technology Cybersecurity Frameworks (NIST CSF)
- Establish better process for systems to ensure compliance
- Fortify System Controls
- Implement concept of least permissions when it comes to user credential management
- Establish playbooks
- Ensure compliance requirements

Critical findings (must be addressed immediately):
Botium Toys may not be in compliance with U.S and international regulations and standards due to inadequate management of assets.

Findings (should be addressed, but no immediate need):
Potential for loss of existing assets including systems and business continuity.

Summary/Recommendations:

Moving forward, Botium Toys needs to increase security around the management of assets. To do so, I recommend the implementation of the practices of least privilege and separation of duties to ensure that access to data and information is limited to only those who need to have it.
I also recommend the implementation of encryption on important information such as payment information to insure the safety of the information.
Both of these should be implemented immediately.
From there, the focus should be on the creation and implementation of a Disaster recovery plan in the event of a system failure. This plan should focus on ensuring the security of information and the continuity of operations in the event of a failure. The plans should also include implementation of backups for information and installation of antivirus software on all company computers.
Lastly, a focus should be placed on passwords and password security. Policy should be tightened on the requirements for company passwords. A password management system should also be implemented for password recovery and resets.