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: (Your Name)
DATE: (Today’s Date)
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 in the organizations’ systems.
- Currently implemented controls in the organizations’ systems.
- Current procedures and protocols set for the organizations’ systems.
- Ensuring alignment with necessary compliance requirements.
- Ensure accountability for both hardware and system access.

Goals:

- To adhere to the NIST CSF Framework
- Fortify system controls
- Implement the system of least privilege
- Establish policies and procedures, and their playbooks
- Ensure they are meeting compliance requirements

Critical findings (must be addressed immediately):

- Data and disaster recovery plans need to be implemented immediately.
- Principle of least privilege needs to be implemented
- Password and Access Control Policies need to be updated.
- Detection, monitoring and prevention systems such as IDS, Anti viruses, CCTV needs to be implemented.
- Encryption of data needs to be implemented
- Hardware needs to be physically protected using locks and locking cabinets
- Must comply with GDPR, PCI DSS and Systems and Organizations Controls

Findings (should be addressed, but no immediate need):

- Adequate lighting needs to be there
- Fire detection systems need to be installed
- Alarm service provide needs to be installed

Summary/Recommendations:

It is recommended that findings related to GDPR and PCI DSS should be addressed immediately as the company operates worldwide. Administrative policies need to be updated to comply with SOC1 and SOC2. Disaster recovery plans and backups are absolutely critical for the long term growth of the company. IDS and Antivirus software needs to be installed on systems. Locks and CCTVs need to be installed to secure the physical assets.