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: The scope of this audit is defined as the entire security program at Botium Toys. This means all assets need to be assessed alongside internal processes and procedures.
Following assets managed by the IT Department were considered for audit:
● On-premises equipment for in-office business needs

● Employee equipment: end-user devices (desktops/laptops, smartphones), remote workstations, headsets, cables, keyboards, mice, docking stations, surveillance cameras, etc.
● Management of systems, software, and services: accounting, telecommunication, database, security, ecommerce, and inventory management
● Internet access
● Internal network
● Vendor access management
● Data center hosting services
● Data retention and storage
● Badge readers
● Legacy system maintenance: end-of-life systems that require human monitoring

Goals: The goals for Botium Toys' internal IT audit are:
● 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): Following findings must be addressed immediately:
● Application of least privilege and separation of duties principle
● Ensuring password, access control policies are in place
● Ensuring safety of physical assets and network gear
● Compliance to Payment Card Industry Data Security Standard (PCI DSS) for storing any credit/debit card related information.
● Compliance to General Data Protection Regulation (GDPR) for storing customer, vendor or/and employee data as the company wants to expand its operations to European Union(EU).

Findings (should be addressed, but no immediate need): Following findings need to be addressed:
● Ensuring disaster recovery plan and creating backups in case of loss of data

- Using a strong firewall and encryption
- Ensuring proper intrusion detection system, locks and CCTV for surveillance.

Summary/Recommendations: Botium Toys Company needs to strengthen its security systems for safeguarding its assets. It also needs to follow the NIST CSF guidelines for the same. It also needs to comply to the above mentioned regulations and standards for a smooth business operation and also for expanding it.