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: Ulysses Bakolias
DATE: 2023-05-10
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:

1. Current user permissions set in the following systems: accounting, end point detection, firewalls, intrusion detection system, security information and event management (SIEM) tool.
2. Current implemented controls in the following systems: accounting, end point detection, firewalls, intrusion detection system, Security Information and Event Management (SIEM) tool.

3. Current procedures and protocols set for the following systems: accounting, end point detection, firewall, intrusion detection system, Security Information and Event Management (SIEM) tool.
4. Ensure current user permissions, controls, procedures, and protocols in place align with necessary compliance requirements.
5. Ensure current technology is accounted for. Both hardware and system access.

Goals:

1. To adhere to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
2. Establish a better process for their systems to ensure they are compliant
3. Fortify system controls
4. Implement the concept of least permissions when it comes to user credential management
5. Establish their policies and procedures, which includes their playbooks
6. Ensure they are meeting compliance requirements

Critical findings (must be addressed immediately):

1. Implement disaster recovery plan
2. Review and implement stronger password policies
3. Implement access control policies
4. Deploy firewalls
5. Maintain backups of all critical systems, infrastructure, and data
6. Deploy antivirus software
7. Implement physical security measures to secure network infrastructure gear (locking cabinets)
8. Implement physical security measures to secure any and all physical and digital assets (locks)
9. Implement fire detection and prevention systems

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

1. Implement account management policies
2. Review separation of duties and limitation of access to sensitive information
3. Implement intrusion detection systems
4. Review and implement encryption for all sensitive data and traffic

5. Implement password management system
6. Implement manual monitoring of legacy systems, and policies for maintenance and intervention in order to mitigate potential threats, risks, and vulnerabilities
7. Ensure adequate lighting in and around work areas
8. Deploy CCTV surveillance systems

Summary/Recommendations:

During the course of this internal security audit, we have identified a number of weak points in Botium Toys' security posture.

It is recommended that all the above findings be addressed as soon as possible in order to mitigate any risk of loss, damage, or legal liability to the company, its personnel and other stakeholders, and customers.

Critical findings should be addressed immediately, and other findings as soon as is appropriate given other restrictions - these findings have not been listed in any particular order of priority beyond the separation of *'critical findings*' and '*findings*.'

If necessary, personnel should be engaged and deployed to address the listed findings.