# 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: Suraj Khadka
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 following are the scope of Botium Toys Internal Audit:

- Evaluate current user permissions configured within the accounting, endpoint detection, firewalls, intrusion detection systems, and security information and event management (SIEM) tools.
- Analyze the currently implemented controls within the accounting, endpoint detection, firewall, intrusion detection system, and SIEM tool environments.
- Review and assess the present procedures and protocols established for the accounting, endpoint detection, firewall, intrusion detection system, and SIEM tool systems.

- Validate that the existing user permissions, controls, procedures, and protocols align with the requisite compliance standards.
- Verify the inclusion of current technology components, encompassing both hardware assets and system access rights.

**Goals:** The following are the goals of Botium Toys Internal Audit:

- Embrace the guidelines set forth by the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).
- Enhance and streamline system procedures to achieve and maintain compliance.
- Strengthen the control mechanisms within the system architecture.
- Adopt the principle of least permissions for effective user credential management.
- Develop comprehensive policies, procedures, and playbooks to govern operations.
- Strive to meet and exceed compliance requirements through diligent efforts.

**Critical findings** (must be addressed immediately):

- Polices needs to implement to meet GDPR, PCI DSS and SOC1/SOC2 compliance regulations and standards requirement.
- Separation of duties like accounting, database, security etc.
- Defense-in-depth like fence/wall around building, badge readers in gates and doors, and CCTV.
- Access permission depend on nature of works.
- Implement policies of using strong password and antivirus software.
- Need backup of information and secure network to prevent loss of data.
- Implement fire detection and prevention and systems like fire alarm, sprinkler system.
- Implement Business Continuity plans.
- Manual monitoring, maintenance, and intervention

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

- Signage indicating alarm service
- Locking cabinets especially for network gear
- Adequate lighting
- Time-controlled safe

**Summary/Recommendations:**

The Botium Toys Internal Audit has undertaken a comprehensive assessment of the organization's security infrastructure, controls, and procedures. The audit encompassed a thorough evaluation of user permissions, controls, protocols, and compliance standards across various domains including accounting, endpoint detection, firewalls, intrusion detection

systems, and security information and event management (SIEM) tools. The audit aimed to align the existing systems with the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) guidelines, enhance compliance procedures, bolster control mechanisms, and embrace the principle of least permissions.

Critical findings necessitating immediate attention include the implementation of policies to meet GDPR, PCI DSS, and SOC1/SOC2 compliance regulations, as well as the establishment of separation of duties, defense-in-depth strategies, access permissions based on job roles, and the enforcement of strong password policies and antivirus software. Urgent measures like data backup, secure network configurations, fire detection and prevention systems, and Business Continuity plans are recommended to safeguard against data loss and operational disruptions.

Less critical findings that should be addressed include the addition of signage indicating alarm services, locking cabinets for network gear, ensuring adequate lighting, and implementing time-controlled safes. While these findings may not require immediate action, addressing them would contribute to the overall security posture of the organization. Manual monitoring, maintenance, and intervention should also be integrated to ensure continuous oversight. The audit's comprehensive analysis and tailored recommendations provide a roadmap to enhance security measures, streamline procedures, and maintain compliance to industry standards.