Security audit results and recommendations to stakeholders

AUDIT SCOPE

- The audit scope encompasses Botium Toys' entire security program.
- It includes an assessment of user permissions in critical systems like accounting, endpoint detection, firewalls, intrusion detection, and SIEM tools.
- The scope also involves evaluating existing controls within these systems to enhance security.
- Additionally, it covers the examination of procedures and protocols related to these systems.
- The audit ensures that current technology, both hardware and system access, is thoroughly documented and secured.
- Compliance requirements are a key aspect of the audit scope, ensuring alignment with industry standards and best practices.

AUDIT GOAL

- Adherence to the National Institute of Standards and Technology (NIST) Cybersecurity Framework is a primary goal.
- Establishing more robust compliance processes to ensure the organization meets regulatory requirements.
- Strengthening system controls to enhance the overall security posture.
- Implementation of the principle of least privilege for user credential management, minimizing access to only necessary functions.
- Development and enforcement of clear policies and procedures, including playbooks, to guide security practices.
- Ensuring alignment with compliance requirements and industry best practices to bolster security measures and protect sensitive data.

High-Level Summary of Audit Scope:

- The audit scope covered the entire security program at Botium Toys, including user permissions, controls, procedures, and compliance requirements.

High-Level Summary of Audit Goals:

- The audit goals included adhering to the NIST Cybersecurity Framework, establishing better compliance processes, fortifying system controls, implementing least privilege principles for user credential management, and establishing policies and procedures.

Critical Findings:

- Inadequate user permissions in various systems, posing security risks.
- Lack of sufficient controls in critical systems.
- Unclear or missing procedures and protocols for system management.
- Uncertainty about the security of current technology assets.
- Potential compliance gaps.

Other Findings:

- Other findings may include recommendations for continuous monitoring, updating policies, conducting regular audits, and enhancing security training and awareness programs.

Summary/Recommendations:

- Prioritize addressing critical findings immediately to mitigate high-risk vulnerabilities.
- Develop a comprehensive security roadmap that outlines ongoing improvements and regular audits.
- Allocate necessary resources and personnel to support security initiatives effectively.
- Establish clear communication channels to update stakeholders on progress and security posture.
- Emphasize the importance of continuous security awareness and training for all employees to strengthen the organization's overall security culture.