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”)

TO: IT Manager, Stakeholders
FROM: Connor England
DATE: 07/15/2023
SUBJECT: Botium Toys IT Audit: Enhanced Security and Compliance

Dear Colleagues,

Below is a comprehensive overview of our internal audit for Botium Toys, detailing our scope, goals, crucial findings, and strategic recommendations.

Scope:

The audit was conducted to assess and enhance Botium Toys' IT infrastructure and policies. We focused on:

- User permissions and control mechanisms across critical systems including accounting, endpoint detection, firewalls, Intrusion Detection Systems (IDSs), and Security Information and Event Management (SIEM) tools.
- Compliance alignment with required standards.

- Comprehensive evaluation of Botium Toys' technology assets, including hardware and system access.

Goals:

The objectives of this audit included:

- Aligning with the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).
- Ensuring adherence to critical compliance standards and improving systemic compliance processes.
- Identifying key assets and evaluating existing and necessary control implementations.
- Developing robust policies and procedures, including incident response playbooks.
- Instituting the principle of least privilege for user account management.

Critical Findings (Immediate Action Required):

Immediate implementation of the following compliance standards is essential:

- System and Organizations Controls (SOC types 1 and 2): Vital for safeguarding personally identifiable information (PII) of employees and customers.
- Payment Card Industry Data Security Standard (PCI DSS): Crucial for secure handling of payment data.
- General Data Protection Regulation (GDPR): Applicable for future EU market expansions.

High-priority controls requiring urgent implementation predominantly involve administrative and technical aspects, such as the principle of least privilege, disaster recovery planning, firewall setup, and the utilization of IDS and SIEM tools.

Refer to the comprehensive controls assessment for detailed priority ratings.

Findings (Future Considerations):

While immediate alignment with the NIST CSF addresses numerous security objectives and compliance requirements, the adoption of additional security frameworks can be deferred during Botium Toys' growth phase.

Some physical security measures, including safes, enhanced lighting, and security signage, are important but not as urgent as other controls.

Summary/Recommendations:

This audit underscores the need for immediate action in critical areas to strengthen Botium Toys' security posture in line with its rapid expansion. Focal points should include compliance with GDPR, PCI DSS, SOC types 1 and 2, thorough asset identification and categorization, and the implementation of vital security controls.

Leveraging the NIST CSF will facilitate many security initiatives. As the company grows, the refinement of disaster recovery and business continuity plans will become increasingly crucial. We recommend reviewing the complete controls assessment and compliance checklist for specific security enhancements. Additionally, early adoption of the NIST Risk Management Framework is advised for comprehensive security goal achievement.

Best Regards,

Connor England