Stakeholders 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 Manger, Security Team Head, Stakeholders

FROM: Rahul Shrivastava

DATE: 19/02/2026

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 will assess Botium Toys current user permissions, implemented controls, procedures, and protocols in the following systems:

- Accounting
- End point detection
- Firewalls
- Intrusion Detection Systems (IDSs)
- Security Information and Event Management (SIEM) tools

The audit will also ensure that these elements align with any compliances that are required of Botium Toys. Additionally, all of Botium Toys' current technology will be accounted for during this audit – both hardware and system access.

Goals:

- Implement the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
- Ensure that Botium Toys adheres to any required compliances and establish a better process for their systems to ensure compliance
- Identify assets and the current controls that are protecting them, as well as required controls to be implemented
- Establish policies and procedures such as playbooks
- Implement the principle of least privilege for user credential management

Critical findings (must be addressed immediately):

The following compliances will need to be implemented:

- System and Organizations Controls (SOC type 1, SOC type 2)
    - Required to protect PII of personnel and customers

- Payment Card Industry Data Security Standard (PCI DSS)
    - Required when handling payment data
- General Data Protection Regulation (GDPR)
    - This only applies to when Botium Toys begins to do business in E.U. countries

There are many high priority security controls that will need to be implemented in order to ensure good security posture, business continuity, and safety. Most of the controls that need to be addressed immediately are admin and technology related, such as implementing the principle of least privilege, creating a disaster recovery plan, setting up firewalls, and using Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) tools.

Please see the full controls assessment for individual priority scores of the controls.

Findings (should be addressed in the future):

Adhering to the NIST CSF will help in completing many of the desired security goals and compliances, so implementing further security frameworks can likely be addressed later on in Botium Toys' growth.

Since Botium Toys is a quickly scaling small business, most security controls need to be implemented immediately. However, some physical controls such as safes, lighting, and signage aren't as timely as the others.

Summary/Recommendations:

This audit has highlighted many crucial security controls and compliances that Botium Toys will need to implement immediately so that the organization's security goals can

be met alongside their rapid growth. The key areas of focus for improving security posture are aligning with the required compliances (GDPR, PCI DSS, SOC type 1 and SOC type 2), identifying/categorizing all current assets, and implement crucial security controls.

Completing many of these tasks will be made easier through adherence to the NIST CSF, which has been identified as one of the security goals. As Botium Toys continues to grow as a business, disaster recovery plans and controls related to business continuity will become increasingly important to refine. Please see the full controls assessment and compliance checklist for detailed items to improve security posture. For additional recommendations, please consider implementing the NIST Risk Management Framework as doing so in the early stages of the business can be extremely beneficial in completing security goals.

Thanks & Regards