Stakeholder memorandum

TO: IT Manager, Stakeholders
FROM: (Your Name)
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 entire Botium Toys IT/Security system

Goals: To adhere to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) by:

- Establishing a better process for their systems to ensure they are compliant
- Fortify system controls
- Implement the concept of least permissions when it comes to user credential management
- Establish their policies and procedures, which includes their playbooks
- Ensure they are meeting compliance requirements

Critical findings (must be addressed immediately):

Immediate controls to implement are within Administrative and Technical categories. The company will need to have both employee access from least privilege and password policies enforced as preventative measures. Within the Technical category, IDS, backups, and Firewall are some of the detective and preventive measures required to set up. Least priority are Physical controls, which don't need to be immediately implemented in order to be compliant in accepting orders worldwide.

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

The company does not currently meet System and Organizations Controls (SOC type 1, SOC type 2) standards in order to properly handle physical inventory.

Summary/Recommendations:

In order to meet Botium Toys goal of adhering to the NIST guidelines for their entire IT/Security department, the company must first become immediately compliant with GDPR, PCI DSS. If not compliant, there is a risk as the company will face financial loss due to governing fines worldwide. For SOC 1 & 2, Botium Toys need to utilize least

privilege as they enforce Access & Account policies at various levels, especially with the financial risk they hold in their current posture. Botium Toys also need to establish and enforce appropriate user access for internal and external (third-party vendor) personnel to mitigate risk and ensure data safety. This can be done by implementing Technical and Administrative controls immediately, while developing Physical controls over time as the security of the business grows.