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 and compliance checklist

TO: IT Manager, Stakeholders
FROM: Nguyen Tran Binh Nhu
DATE: 04/10/2023
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 systems: accounting, end point detection, firewall, intrusion detection system, Security Information and Event Management (SIEM) tool. The system will be assessed for:
    - Current user permissions.
    - Current implemented controls
    - Current procedures and protocols.
- Align current internal processes and procedures, protocols with U.S. and international regulation and standards.
- Hardware assets of the company.

Goals:

- To adhere to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
- Establish a better process for company's systems to ensure they are compliant
- Fortify system controls
- Ensure they are meeting compliance requirements

Critical findings (must be addressed immediately):

- Implement the concept of least permissions and separation of duties to all Botium Toys employees, only authorized users can access certain data. This will reduce risk and overall impact of compromised accounts.
- Implement encryption to ensure confidentiality of customers' credit card information. This type of data needs to be protected immediately.
- Backup critical data.
- Implement stricter password policy to minimize surface attack.
- Implement intrusion detection system, enable IT teams to identify possible intrusions quickly.
- Create a disaster recovery plan.

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

- Establish a centralized password management system to improve employees' productivity.
- Establish intervention methods for legacy systems.

Summary/Recommendations:

Given that Botium Toys accepts online payments from clients all over the world, including those in the EU, it is recommended that critical findings about compliance with PCI DSS and GDPR need to be addressed promptly. Backups and disaster recovery plans, implementing intrusion detection system are essential for ensuring business continuity in the case of an incident.