# Stakeholder memorandum By Ziad Ayman

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](https://docs.google.com/document/d/1DWmu8rVrIY_vGR3nRCUl7sxekN2fGRYypcF6ej8YheA/template/preview)
* Controls assessment (completed in “Conduct a security audit, Part 1”)
* Compliance checklist (completed in “Conduct a security audit, Part 1”)

[***Use the following template to create your memorandum]***

TO: IT Manager, Stakeholders

FROM: (Ziad Ayman)  
DATE: (7/14/2023)  
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:**

**Goals:**

**Critical findings** (must be addressed immediately):

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

**Summary/Recommendations:**

To ensure the utmost security and compliance, here are some essential recommendations for the orgnization:

1. Promptly address critical findings regarding compliance with PCI DSS and GDPR. This is crucial as Botium Toys accepts online payments from customers worldwide, including the European Union (E.U.).

2. Embrace the concept of least permissions by utilizing guidance from SOC1 and SOC2. This will help establish robust user access policies and enhance overall data safety.

3. Establish disaster recovery plans and backups to support business continuity in the face of unforeseen incidents.

4. Enhance risk identification and mitigation capabilities by integrating Intrusion Detection Systems (IDS) and Anti-Virus (AV) software into the current systems. This will aid in identifying potential threats and enable more efficient intrusion detection, addressing the limitations of existing manual monitoring in legacy systems.

5. Safeguard physical assets and bolster security at Botium Toys' physical location by implementing locks, Closed-Circuit Television (CCTV) surveillance, and proactive monitoring to identify and investigate potential threats.

6. Consider additional security measures, such as encryption, time-controlled safes, adequate lighting, locking cabinets, fire detection and prevention systems, and signage indicating the alarm service provider. While not immediately necessary, these measures can further enhance Botium Toys' security posture.

By following these recommendations, Botium Toys can fortify its security, ensure compliance, and protect valuable assets for sustained success.