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 HYPERLINK "https://docs.google.com/document/d/1DWmu8rVrIY\_vGR3nRCUl7sxekN2fGRYypcF6ej8YheA/template/preview"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: (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 scope of this audit is to assess current user permissions are set, to identify what controls are currently in place, and to identify what procedures and protocols are in place in case of a breach for the following departments: accounting, end point detection, firewall, intrusion detection system, Security Information and Event Management (SIEM) tool as well as ensure current technology is accounted for.

**Goals:** Ensure we are meeting compliance requirements. Ensure we are adhering to the NIST CSF and establish policies and procedures, which includes our playbooks. Implement the concept of least priviledges when it comes to user credential management. Fortify system controls and estalish a better process for our systems to ensure they are compliant.

**Critical findings** (must be addressed immediately): It seems that a majority of the administrative and technical controls are at high risk to be comprimised based on the current state of security with Botium. Password, access of control and account management policies are prioirty. Having a disaster recovery plan in place in the event of a worst case scenario is also highly advised. It is also recommended to implement software security measures like firewalls, encryption, IDS, and backups to make sure the CIA triad is upheld for customer data and information.

**Findings** (should be addressed, but no immediate need): The physical controls seem to need some implementation on better compliance as well but the priority is mainly customer data and online compliance due to the business aspect of the company growing rapidly. CCTV and better locks on-site need to be implemented right away.

**Summary/Recommendations:** It is recommended that critical findings being addressed since Botium Toys accepts online payments from customers worldwide. Having a disaster recovery plan and backups for data in place is also critical because they provide business continuity in teh event of an incident. Intergrating IDS and firewall software into the current systems will support our ability to identify and mitigate potential risks and could help with intrusion detection, since existing legacy systems require manual monitoring and intervention. CCTV should be installed and used around the physical location for Botium Toys to secure physical assets and monitor potential threats.