# Stakeholder memorandum

TO: IT Manager, Stakeholders

FROM: Ethan Miller  
DATE: June 5th, 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:**

* Current user permissions set in the following systems: accounting, end point detection, firewalls, intrusion detection system, security information and event management (SIEM) tool.
* Current implemented controls in the following systems: accounting, end point detection, firewalls, intrusion detection system, Security Information and Event Management (SIEM) tool.
* Current procedures and protocols set for the following systems: accounting, end point detection, firewall, intrusion detection system, Security Information and Event Management (SIEM) tool.
* Ensure current user permissions, controls, procedures, and protocols in place align with necessary compliance requirements.
* Ensure current technology is accounted for. Both hardware and system access.

**Goals:**

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

* [Current policies](https://docs.google.com/document/u/0/d/17noq--B987ScxmJZfHl54VjvPSyKPu5IaQjm2Nfmx80/edit) fail to adhere to the following compliance regulations and standards:
  + **General Data Protection Regulation (GDPR)**
  + **Payment Card Industry Data Security Standard (PCI DSS)**
  + **System and Organizations Controls (SOC type 1, SOC type 2)**
* [Current controls](https://docs.google.com/document/u/0/d/1-CQT_kx8XVwak3SB3nSgk-9PFutRG1RNP1Ibhp8e7CY/edit) fail to meet most every goal set by the organization including:
  + Least privilege
  + asset access management
  + customer data security/integrity

Above is a list addressing the most volatile issues the audit discovered. Many of these items are an incredible threat to the organization both legally & financially. Correction of these issues (especially compliances) is critical for the continuation of the company.

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

After addressing online vulnerability listed above, it is important to remember that the greatest threats can still present themselves physically, and often come from within. Implementing physical security such as locks, cctv, and other common practices would go a long way in securing our operations offline.

**Summary/Recommendations:**

**Immediately implement proper online transaction security, data security, and vendor management strategies to safeguard the company while meeting the listed compliance regulation and standards requirements.**