# Stakeholder memorandum

TO: IT Manager, Stakeholders

FROM: José Carlos T. Neto   
DATE: 15/01/2023  
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:** 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): Least Privilege; Disaster recovery plans; Password policies; Access control policies; Account management policies; Separation of duties; Intrusion Detection System (IDS); Encryption; Backups; Password management system; Antivirus (AV) software; Manual monitoring, maintenance, and intervention; Locks.

**Findings** (should be addressed, but no immediate need): Time-controlled safe; Adequate lighting; Signage indicating alarm service provider; Locking cabinets (for network gear); Fire detection and prevention (fire alarm, sprinkler system, etc.)

**Summary/Recommendations:**

Manage controls and access, adhere to PCI DSS, adhere to GDPR to conduct business in E.U; and enforce appropriate user access for internal and external (third-party vendor) personnel to mitigate risk and ensure data safety.