# Stakeholder 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:**

● 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):

Administrative controls must be put in place which include:

* putting restrictions on data for non-employees
* creating a disaster recovery plan for physical and digital assets
* establishing a stronger password policy
* better separation of duties

Operational/Technical controls:

* installing an intrusion detection system
* creating backups as part of disaster recovery
* installing antivirus software
* manual monitoring of legacy systems

Physical Controls:

* using locks for physical and digital assets

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

Additionally, the following areas need controls put in place at a later time:

* strict account management
* data encryption
* password management system
* installation of additional physical controls including lighting, CCTV, locking cabinets, alarm signage, and fire control and prevention

**Summary/Recommendations:**

Without proper implementation of the security controls listed above, the company is at significant risk to business continuity and asset loss. The company is also at risk to incur penalties due the discovery of non-compliance of GDPR in the case of personal data loss of E.U. customers. We recommend the immediate implementation of all the controls listed in our critical findings to ensure a strong security posture.