

Stakeholder memorandum

TO: IT Manager and stakeholders

FROM:

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:

- Systems evaluated: accounting, endpoint detection, firewalls, IDS, SIEM
- Areas reviewed:
 - User permissions
 - Implemented controls
 - Current procedures
 - PCI DSS and GDPR compliance
 - Hardware and system access inventory

Goals:

- Follow NIST CSF
- Improve compliance processes
- Strengthen system controls
- Implement least permissions concept
- Create policies and procedures
- Meet compliance requirements

Critical Findings (Immediate Action):

- Needed controls:
 - Least Privilege and Duty Separation
 - Disaster recovery
 - Password/access management
 - Encryption for transactions
 - IDS and Backups

- Antivirus
 - Physical security (CCTV, locks)
 - Legacy system monitoring
 - Fire systems
- Develop policies for:
 - PCI DSS and GDPR compliance
 - SOC1/SOC2 alignment
 - User access and data safety

Non-Critical Findings:

- **Future recommendations/improvements needed:**
 - Time-controlled safe
 - Better lighting
 - Locking cabinets
 - Alarm service signage
 - Fire prevention systems