Stakeholder memorandum

TO: IT Manager, Stakeholders
FROM: Jose Narvaez Maldonado
DATE: 14/05/2025
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 audit evaluated the entirety of Botium Toys' cybersecurity program, including technical, administrative, and physical controls.

- Focus was placed on the accounting system, endpoint protection, firewalls, intrusion detection systems (IDS), and SIEM tools.

- The audit reviewed current user permissions, system access, and alignment with compliance standards.

- All IT-managed assets, both physical (e.g., desktops, mobile devices, surveillance equipment) and digital (e.g., databases, software systems), were included.

- Internal processes for access control, vendor management, and legacy systems were analyzed.

Goals:

- **Align the company's cybersecurity practices with the NIST Cybersecurity Framework (CSF).**

- **Enhance compliance with GDPR, PCI DSS, and SOC 2 regulations.**

- **Apply the principle of least privilege to reduce unnecessary access and associated risks.**

- **Improve business continuity through disaster recovery planning and regular data backups.**

- **Establish consistent security policies, procedures, and access control policies.**

Critical findings (must be addressed immediately):

- Inadequate asset management: Missing inventory and oversight for legacy and remote assets increases risk exposure.

- Lack of least privilege implementation: Overly broad user permissions across several systems create vulnerability to internal misuse or external compromise.

- Compliance gaps: Current practices do not fully meet GDPR or PCI DSS requirements, risking legal and financial consequences.

- Absence of disaster recovery plan: No documented or tested plan in place, increasing potential downtime during an incident.

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

- Weak password and access control policies: Current standards are not sufficiently robust to defend against brute-force attacks.

- Manual intervention for legacy systems: Resource-intensive and error-prone; automation should be explored.

- Inconsistent physical security controls: Locking mechanisms, surveillance, and alarm signage require improvement.

- Limited use of encryption: Encryption is not universally applied to sensitive data or backup systems.

Summary/Recommendations:

The audit revealed several high-risk issues that require immediate remediation, particularly in asset management, user access controls, and regulatory compliance. Implementing least privilege access, drafting and testing a disaster recovery plan, and enhancing encryption and password policies are essential first steps. In addition, Botium Toys should consider onboarding dedicated cybersecurity personnel to manage and monitor evolving risks. Long-term, the organization must align more closely with the NIST CSF and ensure all practices adhere to GDPR, PCI DSS, and SOC 2 standards. Proactively addressing these gaps will strengthen overall security posture, reduce regulatory risk, and improve business resilience.