To: IT Manager, IT Team

From: Paul Martin

Subject: Audit Findings Recommendations and Concerns

Current Systems Under Scope:

Accounting, End Point Detection, Firewalls, Intrusion Detection System, SIEM Tools

Crucial things to take care of asap:

Must Implement Policies to Meet Requirements of:

PCI, DSS, GDPR, SOC1, and SOC2

-Need to establish control of many systems

-Control Least Privilege and Separation of Duties

-Establish Secure Encryption of SPII and PII

-Establish Backup and Recovery Plans for Data

-Establish Security Protocols and keep up to date with threat detection software

Things we have to make sure to do:

We need to make sure we align with compliance requirements and have to account for our hardware and system access.

Adhere to NIST CSF

Establish systems to further facilitate compliance

Establish strong policies, procedures, and security playbooks

Fortify system controls, Data storage encryption, Security framework

Summary and Recommendations

To ensure compliance with PCI DSS and GDPR, Botium Toys must address critical security gaps, as it processes online payments globally, including in the EU. Additionally, aligning with SOC 1 and SOC 2 standards will help establish stronger user access policies and reinforce data security under the principle of least privilege. Implementing disaster recovery plans and regular backups is essential for business continuity. Upgrading legacy systems with an Intrusion Detection System (IDS) and antivirus (AV) software will improve threat detection and reduce reliance on manual monitoring. For physical security, installing locks and CCTV will help safeguard assets and monitor risks. While not urgent, adding encryption, a time-controlled safe, improved lighting, locking cabinets, fire protection systems, and security signage would further enhance overall protection.