TO: IT Manager, Stakeholders
FROM: Mark Lysaght
DATE: 13th June 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:

- Within scope of this audit are the following:
    - Accounting
    - End point detection
    - Firewalls
    - Intrusion detection system
    - Security information and event management (SIEM) tool.
- These systems will be investigated in order to evaluate:
    - Current user permissions
    - Current implemented controls
    - Current procedures and protocols
- Ensure current user permissions, controls, procedures, and protocols in place align with GDPR and PCI DSS compliance requirements.
- Ensure current technology is accounted for. Both hardware and system access.

Goals:

- Adhere to NIST CSF
- Establish a better process for systems to ensure they are compliant
- Fortify system controls
- Implement the concept of least permissions when it comes to user credential management
- Establish policies and procedures, which includes their playbooks
- Ensure compliance requirements are being met

Critical findings (must be addressed immediately):

- Multiple controls need to be developed and implemented to meet the audit goals, including:
    - Control of Least Privilege
    - Disaster recovery plans
    - Password policies
    - Access control policies
    - Account management policies
    - Separation of Duties
    - IDS
    - Encryption (for secure website transactions)
    - Backups
    - Password management system
    - Antivirus software

    - Manual monitoring, maintenance, and intervention for legacy systems

- Policies for compliance requirements with GDPR and PCI DSS need to be developed and implemented.
- Policies need to be developed and implemented to align with SOC1 and SOC2 guidance related to user access policies and overall data safety.

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

- Several controls take less priority but should not be forgotten about:
    - Time-controlled safe
    - Adequate lighting
    - CCTV
    - Locking cabinets (for network gear)
    - Signage indicating alarm service provider
    - Locks
    - Fire detection and prevention

Summary/Recommendations:
It is recommended that critical findings relating to compliance with PCI DSS and GDPR be addressed with the highest priority since Botium Toys accepts online payments from customers internationally. One of the goals of this audit is to implement the concept of least permissions, SOC1 and SOC2 guidance related to user access policies and overall data safety should be used to develop appropriate policies and procedures. Having disaster recovery plans and backups is also critical because they support business continuity in the event of an incident. Integrating an IDS and AV software into the current systems will support the ability to identify and mitigate potential risks, and could help with intrusion detection, since existing legacy systems require manual monitoring and intervention. To secure assets housed at Botium Toys' single physical location, locks and CCTV should be used to secure physical assets (including equipment) and to monitor and investigate potential threats. Less urgent security controls that are worth addressing (not necessarily immediately but in the near future) such as having a time-controlled safe, adequate lighting, locking cabinets, fire detection and prevention systems, and signage indicating the alarm service provider are all ways in which Botium Toys' security posture can be improved.