Stakeholder Memorandum

TO: IT Manager, Stakeholders
FROM: Kevin Ubilla
DATE: 5/14/23
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 entire security program at Botium Toys Inc., consisting of the following:

- 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 policies and procedures, including playbooks
- Ensure Botium Toys Inc. is meeting compliance requirements

Critical findings (must be addressed immediately):

The following control names which are **non-physical**: least privilege, password policies, access control policies, account management policies, separation of duties, firewall, Intrusion Detection System (IDS), Encryption, Backups, Password management system, Antivirus (AV) software, Manual monitoring, maintenance, and intervention,

The following control names which are **physical**: Adequate lighting, Closed-circuit television (CCTV) surveillance, Locking cabinets (for network gear), Signage indicating alarm service provider, Locks, Fire detection and prevention (fire alarm, sprinkler system, etc.)

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

The following control names which are **non-physical**: backups, disaster recovery plans

The following control names which are **physical**: time-controlled safe

Summary/Recommendations:

In order to comply with the **(1)** General Data Protection Regulation (GDPR), **(2)** Payment Card Industry Data Security Standard (PCI DSS), and the **(3)** System and Organizations Controls (SOC type 1, SOC type 2), the previous list of both critical and non critical findings should be adressed immediately. I recommend that your business prioritize the critical findings first, or those listed as ‘high priority’ in the Controls Assessment listed on the following page. Do not wait until these are completed to begin assigning personnel to take care of the rest of the findings. I highly recommend using this document as a template to create your company’s playbook for handling security risks. In this way, you will set your company up for long term success and reduce threat risks. If further assistance or recommendations are needed, please contact me at my direct line (747) 283-4373.