TO: IT Manager, Stakeholders

FROM: Darius Amos  
DATE: May 26, 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:** Botium Toys internal IT audit will assess the following:

* Current user permissions are 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 are 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:** The goals for Botium Toys’ internal IT audit are:

* 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.
* Manual monitoring, maintenance, and intervention (Ensure they are meeting compliance requirements)
* Establish their policies and procedures, which includes their playbooks.

**Critical findings (**should be addressed immediately)**:**

Currently, there is inadequate management of assets and proper controls for several areas including: least privilege, disaster recovery plans, password, access control, and account management policies, separation of duties, an Intrusion Detection System, encryption, backups, a password management system, antivirus software, surveillance, locks, fire detection and prevention, manual monitoring, maintenance, and intervention. Additionally, Botium Toys may not be compliant with U.S. and international regulations and standards.

**Findings** (of concern but, can be implemented later):

* Time-controlled safe
* Adequate lighting
* Signage indicating alarm service provider

**Summary/Recommendations:** The company should focus on first and foremost becoming compliant with U.S. and international regulations. This would include securing company data and SPII for its customers as well as putting safeguards in place to secure this data, the infrastructure it runs on, and limiting who has access to only those who need to use it. Botium Toys can achieve this by referencing System and Organizations Controls (SOC type 1, SOC type 2) and or implementing least privilege, password policies, access control policies, account management policies, password management system, and separation of duties to monitor and control who has access. An Intrusion Detection System (IDS), encryption (especially for payment), manual monitoring (necessary for legacy systems), antivirus software, locks, Closed-circuit television (CCTV), maintenance and intervention should be implemented to prevent or to aid in the case of unwanted access and other security risks. Backups, disaster recovery plans, fire alarm systems, fire detection and prevention will aid with recovery time following a security incident, disaster, or system malfunction. All the above are high priority items intended to keep the organization in compliance as well as items that meet the goals set for this audit. Some other recommendations, that are not of immediate concern, are locking cabinets (for network gear), a time-controlled safe, adequate lighting and signage indicating an alarm service provider could be implemented to further secure the physical location and combat threats and threat actors.