Stakeholder memorandum

TO: IT Manager, Stakeholders
FROM: Leonel Ramirez
DATE: 25/06/2023
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: The scope managed in this audit included

- **User permissions set in the next systems: accounting, end point detection, firewalls, intrusion detection system, security information and event management tool**
- **Implemented controls set in the next systems: accounting, end point detection, firewalls, intrusion detection system, security information and event management tool**
- **Current procedures and protocols set in the next systems: accounting, end point detection, firewalls, intrusion detection system, security information and event management 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 Toy's internal IT audits 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**

- **Establish their policies and procedures, which includes their playbooks**
- **Ensure they are meeting compliance requirements**

Critical findings (must be addressed immediately):
The next list has high priority items to solve quickly in order to compliment the audit goals.

- Least privilege measure
- Password and access control policies
- Separation of duties
- Firewall configuration
- Implement Intrusion detection system (IDS)
- Encryption of important information
- Create Backups in case of a event
- Manual monitoring, maintenance and intervention
- Adress to GDPR, PCI DSS and SOC1 and SOC2 compliance.

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

- Make a disaster recovery plan
- Use a password management system
- Install an antivirus software in the office's devices
- Time-controlled safe
- Adequate lighting
- Closed-circuit television surveillance
- Locking cabinets
- Signage indicating alarm service provider
- Locks
- Fire detection and prevention

Summary/Recommendations:

As a result of the audit, we found some critical points to work on in order to accomplish the audit goals. As a growing company, it's essential to maintain the organization, its employees and its customers' private information confidential, complete and available. Therefore, it is recommended to start implementing the compliance of the next guidelines, such as GDPR, PCI DSS due to the worldwide online sales that Botium Toys does. In the same line, the SOC1 and SOC2 will empower the privacy and security of the general data in the organization.

Besides the mentioned before, the office's devices and network have a poor security architecture. In this way, it is urgent to put in action the critical findings, such as implementing a password and access policies, a least privilege measure, an Intrusion Detection System, firewall and antivirus, blocking a potential data breach by an internal or external threat. Other options are creating a data backup and a disaster recovery plan to avoid critical losses in case a security incident occurs.

Also, some steps should be implemented in the security of the office, related to the physical controls such as a closed circuit television surveillance, locks, and a fire detection and prevention system, making a physical data breach easy to handle.

Having this in mind, now the organization will have a fortified system control, a user credential management, established policies and procedures, and a compliance to the guidelines mentioned before. All these actions will make the corporation have a great security posture that will allow it to maintain a safe space to work in, and develop its normal business continuity regardless of the possible security incidents.