# Stakeholder memorandum

TO: IT Manager, Stakeholders
FROM: Samuel Sulewski
DATE: 7/20/2023
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 entirety Botium Toys security program (accounting, end point detection, firewalls, intrusion detection system, Security Information and Event Management (SIEM) tools). Ensuring that current user permissions, policies and procedures are congruent with PCI DSS and GDPR compliance requirements.**

**Goals: Improve the security posture of the organization, which includes adhering to the NIST framework, establish processes, policies and procedures for security playbook, fortify security controls, implement concept of least permissions for credential management, and meet compliance requirements.**

**Critical findings** The following requires immediate implementation.

Compliance Regulations and standards

-General Data Protection Regulation (GDPR): general data regulation that protects the processing of E.U. citizens' data and their right to privacy in and out of E.U. territory. Botium needs to comply with regulations relating to conducting online business in the EU.

- Payment Card Industry Data Security Standard (PCI DSS): international security standard meant to ensure that organizations storing, accepting, processing, and transmitting credit card information do so in a secure environment. Botium is expanding their online business abroad and will be handling credit card payment processing.

-System and Organizations Controls (SOC type 1, SOC type 2): Reports that focus on an organization's user access policies at different organizational levels, which are used to assess an organization's financial compliance and levels of risk. Botium needs to establish appropriate internal and external user excess for organization personnel and 3rd party vendors in order to secure data and mitigate risks.

Administrative controls

-Least privilege: vendors and non-authorized staff only have access to the assets/data they need to do their jobs.

-Disaster recovery plans: Ensures business continuity for our systems in the event of an incident so there is limited to no loss of productivity downtime/impact to system components.

-Password policies: Establish password strength rules that improve security/reduce likelihood of account compromise through brute force/dictionary techniques.

-Access control policies: Increase confidentiality and integrity of data.

-Account management policies: Reduce attack surface and limit overall impact from disgruntled/former employees.

-Separation of duties: Ensure no one has so much access that they can abuse the system for personal gain.

Technical Controls

-Encryption: Makes confidential information/data more secure, such as website payment transactions.

-Backups: Supports ongoing productivity in the case of an event.

-Antivirus (AV) software: Detect and quarantine known threats.

-Manual monitoring, maintenance, and intervention: Required for legacy systems to identify and mitigate potential threats, risks, and vulnerabilities.

Physical Controls

-Locks: Physical and digital assets are more secure.
-Manual monitoring, maintenance, and intervention for legacy systems

**Findings** The following need to be addressed in the future, but are not immediate.

Technical Controls

-Intrusion Detection System (IDS): Allows IT team to quickly identify possible intrusions.
-Password management system: Password recovery, reset, lock out notifications.

Physical Controls

-Time-controlled safe:  Reduce attack surface/impact of physical threats.
-Closed-circuit television (CCTV) surveillance: Can reduce risk of certain events and be used after the event for investigation.
-Locking cabinets (for network gear):  Increase integrity by preventing unauthorized personnel/individuals from physically accessing/modifying gear.

**Summary/Recommendations:**

With Botium Toys growing its online ecommerce footprint domestically and internationally, It is imperative that the organization immediately enforces sweeping administrative controls and compliance to applicable regulatory standards. The scope of the security audit ecompasses all of Botium's security program. The goals of the audit encompass implementation of the least permissions concept, adherence to compliance requirements, establishing better processes for our systems that ensure compliance, and applying the NIST framework to establish policies and procedures and fortified security controls. The compliance standards that require immediate adherence relate to the handling of sensitive customer payment information, both domestic and in international territories that our business is growing into, and establishing appropriate/secure internal and external user access for organization personnel and outside vendors. The security controls that need implementation first are predominantly administrative controls, as these pertain to data access to authorized users that is appropriate to business continuity. Recommendations include separation of duties and least privileges, so that no authorized user has too much access that it prevents a major security risk. Policies regarding disaster recovery plans, account management, and password strength are also recommended to keep business continuity in the event of an incident.