# Stakeholder memorandum

TO: IT Manager, Stakeholders

FROM: Daniel Shneier   
DATE: 01/08/2023  
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:** A review of the security and data protection implementation of Botium Toys. Focusing on areas including, but not limited to:

* Identity Access Management 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 their policies and procedures, which includes their playbooks
* Ensure they are meeting compliance requirements

**Critical findings**: There are a number of critical findings that we discovered on the audit that Botium Toys needs to address and implement as a matter of urgency. These specifically relate to the issues within scope but there are a number that may fall out of scope that we suggest are implemented and corrected immediately. These issues relate to practices that need implementation such as the principle of least privilege within the organization, legal requirments such as PCI DSS 4 for payment encryption as well as data retention and policy ammendements using the European Union’s GDPR regulations. (More information can be found in the Assement Document attached.)

**Findings** A backup and password policy should be implemented to insure data protection and retention. Sign Posting and lighting should also be given attention to insure worker safety within the server rooms.

**Summary/Recommendations:** Although there are security challenges for Botium Toys to overcome, if these suggestions and recommendations are implemented effectively we believe that there will be a reduction in the company’s risk to reputational, legal and regulatory problems arising in the future.