# Stakeholder memorandum

TO: IT Manager, stakeholders

FROM: Himanshu Gidwani  
DATE: 21-05-2023  
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 following systems are in scope: accounting, end point detection, firewalls, intrusion detection system, SIEM tool. The systems will be evaluated for:
  + Current user permissions
  + Current implemented controls
  + Current procedures and protocols
* Ensure current user permissions, controls, procedures, and protocols in place align with PCI DSS and GDPR compliance requirements.
* Ensure current technology is accounted for both hardware and system access.

**Goals:**

* Adhere to the NIST CSF.
* Establish a better process for their systems to ensure they are compliant.
* Fortify system controls.
* Adapt to 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):

* Multiple controls need to be developed and implemented to meet the audit goals, including:
  + Control of Least Privilege and Separation of Duties
  + Disaster recovery plans
  + Password, access control, and account management policies, including the implementation of a password management system
  + Encryption (for secure website transactions)
  + IDS
  + Backups
  + AV software
  + CCTV
  + Locks
  + Manual monitoring, maintenance, and intervention for legacy systems
  + Fire detection and prevention systems
  + Time-controlled safe
* Policies need to be developed and implemented to meet PCI DSS and GDPR compliance requirements.
* Policies need to be developed and implemented to align to SOC1 and SOC2 guidance related to user access policies and overall data safety.

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

* The following controls should be implemented when possible:
  + Adequate lighting
  + Locking cabinets
  + Signage indicating alarm service provider

**Summary/Recommendations:** It is recommended that critical findings relating to compliance with PCI DSS and GDPR be promptly addressed since Botium Toys accepts online payments from customers worldwide, including the E.U

Based on the report findings, I recommend taking immediate action to address critical issues and prioritize the implementation of controls and policies necessary to ensure compliance and fortify system controls. Here are the key recommendations:

Develop and Implement Controls:

Control of Least Privilege and Separation of Duties: Review and adjust user permissions to grant the minimum necessary privileges for their roles. Ensure proper segregation of duties to minimize the risk of unauthorized access.

Disaster Recovery Plans: Create comprehensive disaster recovery plans to effectively recover from system failures or disasters and minimize downtime.

Password, Access Control, and Account Management Policies: Develop and implement strong password policies, including regular password changes. Consider implementing a password management system to enhance control and security. Review and update access control measures to prevent unauthorized access.

Encryption: Implement encryption protocols for secure website transactions to protect sensitive data from unauthorized access and interception.

Intrusion Detection System (IDS): Deploy an IDS to monitor network traffic and detect potential security breaches promptly.

Backups: Establish regular backup procedures for critical data to ensure data integrity and enable efficient recovery in case of data loss.

Antivirus (AV) Software: Deploy and maintain up-to-date AV software across systems to detect and prevent malware infections.

Closed-Circuit Television (CCTV): Install CCTV systems to monitor and record activities in sensitive areas, enhancing physical security.

Locks: Implement robust locking mechanisms to control access to physical areas containing sensitive assets or systems.

Manual Monitoring, Maintenance, and Intervention for Legacy Systems: Develop procedures for manual monitoring, maintenance, and intervention to ensure the security and functionality of legacy systems that may not have automated controls.

Fire Detection and Prevention Systems: Install fire detection and prevention systems to minimize the risk of fire-related incidents and protect critical infrastructure.

Time-Controlled Safe: Utilize time-controlled safes to secure valuable assets.

Develop and Implement Policies:

PCI DSS and GDPR Compliance: Develop and implement policies that align with PCI DSS and GDPR requirements to protect customer data, ensure privacy, and maintain compliance.

SOC1 and SOC2 Guidance: Align policies with SOC1 and SOC2 guidance to establish robust user access policies and ensure overall data safety and security.

Adhere to NIST CSF:

Follow the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) guidelines to establish a risk-based approach to cybersecurity and improve the organization's security posture.

Establish Better Processes:

Enhance existing processes to ensure ongoing compliance with regulatory requirements and industry standards.

Regularly review and update processes to adapt to changing compliance requirements and emerging threats.

While addressing the critical findings is essential, it is also important to gradually implement the recommended controls and policies identified in the non-critical findings. These include implementing adequate lighting, locking cabinets, and displaying signage indicating the alarm service provider to enhance physical security.

By implementing these recommendations, the organization will enhance its overall security posture, establish robust compliance measures, and fortify system controls. Taking immediate action will help mitigate risks and ensure the protection of sensitive data and assets.