# Memo for stakeholders

To: IT Manager, Stakeholders

FROM: Lyncold Stephensky CHERY   
DATE: 04/21/2025   
SUBJECT: Results and Recommendations of the Internal IT Audit

Dear colleagues,

Please review the following information regarding the scope, objectives, key findings, summary and recommendations of the internal audit of Botium Toys.

**Scope :**

* The following systems are affected: accounting, endpoint detection, firewalls, intrusion detection system, SIEM tool. Systems will be evaluated based on the following criteria:
  + Current user permissions
  + Current controls implemented
  + Current procedures and protocols
* Ensure that user permissions, controls, procedures and protocols in place align with PCI DSS and GDPR compliance requirements.
* Ensure that current technology is considered, both for hardware and system access.

Goals :

* Join the NIST CSF.
* Implement a better process for their systems to ensure they are compliant.
* Strengthen system controls.
* Adapt to the concept of least permissions when it comes to managing user credentials.
* Establish their policies and procedures, including their playbooks.
* Ensure they meet compliance requirements.

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

* Multiple controls must be developed and implemented to achieve the audit objectives, including:
  + Least Privilege Control and Separation of Duties
  + Disaster recovery plans
  + Password, access control and account management policies, including the implementation of a password management system
  + Encryption (to secure transactions on websites)
  + IDS
  + Backups
  + Antivirus software
  + Video surveillance
  + Locks
  + Manual monitoring, maintenance and intervention for existing systems
  + Fire detection and prevention systems
* Policies must be developed and implemented to meet PCI DSS and GDPR compliance requirements.
* Policies should be developed and implemented to align with SOC1 and SOC2 guidelines for user access policies and general data security.

**Findings** (to be addressed, but there is no immediate need):

* The following controls should be implemented where possible:
  + Time-delayed safe
  + Adequate lighting
  + Lockable cabinets
  + Sign indicating the alarm service provider
  + Fire detection and prevention systems

**Summary/Recommendations:** It is recommended that critical findings related to PCI DSS and GDPR compliance be addressed promptly, as Botium Toys accepts online payments from customers worldwide, including the European Union. Furthermore, since one of the objectives of the audit is to adapt to the concept of least authorization, SOC1 and SOC2 guidance related to user access policies and overall data security should be used to develop appropriate policies and procedures. It is also essential to have disaster recovery plans and backups in place, as they help ensure business continuity in the event of an incident. Integrating IDS and AV software into current systems will enhance our ability to identify and mitigate potential risks and may assist in intrusion detection, as existing systems require manual monitoring and intervention. To further secure the IT resources hosted at Botium Toys's single physical location, locks and video surveillance systems should be used to secure physical resources (including equipment) and to monitor and investigate potential threats. While not immediately necessary, the use of encryption and the availability of a time-delay safe, adequate lighting, locked cabinets, fire detection and prevention systems, and signage indicating the alarm service provider will further enhance Botium Toys' security posture.