# Stakeholder memorandum

Complete each section of the stakeholder memorandum template to communicate your audit results and recommendations to stakeholders:

* Scope
* Goals
* Critical findings (must be addressed immediately)
* Findings (should be addressed, but no immediate need)
* Summary/Recommendations

Use information from the following documents:

* [Botium Toys: Audit scope and goals](https://docs.google.com/document/d/1bA-J96jzDVFi9XjNOKd4w2bCR7X7ZTs3_szPElOkyFM/template/preview)
* Controls assessment (completed in “Conduct a security audit, part 1”)
* Compliance checklist (completed in “Conduct a security audit, part 1”)

[***Use the following template to create your memorandum]***

TO: IT Manager, Stakeholders

FROM: Alex David Usuga  
DATE: 05/07/2024  
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:**

**Botium Toys internal IT audit will assess the following:**

**Current user permissions set in the following systems: accounting, end point detection, firewalls, intrusion detection system, security information and event management (SIEM) tool.**

**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:**

**The goals for Botium Toys’ internal IT audit 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**:

| **Administrative Controls** | | | |
| --- | --- | --- | --- |
| **Control Name** | **Control type and explanation** | **Needs to be implemented (X)** | **Priority** |
| Least Privilege | Preventative; reduces risk by making sure vendors and non-authorized staff only have access to the assets/data they need to do their jobs | X | High |
| Disaster recovery plans | Corrective; business continuity to ensure systems are able to run in the event of an incident/there is limited to no loss of productivity downtime/impact to system components, including: computer room environment (air conditioning, power supply, etc.); hardware (servers, employee equipment); connectivity (internal network, wireless); applications (email, electronic data); data and restoration | X | High |
| Password policies | Preventative; establish password strength rules to improve security/reduce likelihood of account compromise through brute force or dictionary attack techniques | X | High |
| Access control policies | Preventative; increase confidentiality and integrity of data | X | High |
| Account management policies | Preventative; reduce attack surface and limit overall impact from disgruntled/former employees | X | High/  Medium |
| Separation of duties | Preventative; ensure no one has so much access that they can abuse the system for personal gain | X | High |

| **Technical Controls** | | | |
| --- | --- | --- | --- |
| **Control Name** | **Control type and explanation** | **Needs to be implemented**  **(X)** | **Priority** |
| Intrusion Detection System (IDS) | Detective; allows IT team to identify possible intrusions (e.g., anomalous traffic) quickly | X | High |
| Encryption | Deterrent; makes confidential information/data more secure (e.g., website payment transactions) | X | High/  Medium |
| Backups | Corrective; supports ongoing productivity in the case of an event; aligns to the disaster recovery plan | X | High |
| Password management system | Corrective; password recovery, reset, lock out notifications | X | High/  Medium |
| Antivirus (AV) software | Corrective; detect and quarantine known threats | X | High |
| Manual monitoring, maintenance, and intervention | Preventative/corrective; required for legacy systems to identify and mitigate potential threats, risks, and vulnerabilities | X | High |

| **Physical Controls** | | | |
| --- | --- | --- | --- |
| **Control Name** | **Control type and explanation** | **Needs to be implemented**  **(X)** | **Priority** |
| Closed-circuit television (CCTV) surveillance | Preventative/detective; can reduce risk of certain events; can be used after event for investigation | X | High/  Medium |
| Locks | Preventative; physical and digital assets are more secure | X | High |

These are regulations necessary to do business other countries and too to management users and data private.

* **General Data Protection Regulation (GDPR)**

GDPR is a European Union (E.U.) general data regulation that protects the processing of E.U. citizens’ data and their right to privacy in and out of E.U. territory. Additionally, if a breach occurs and a E.U. citizen’s data is compromised, they must be informed within 72 hours of the incident.

* **Payment Card Industry Data Security Standard (PCI DSS)**

PCI DSS is an international security standard meant to ensure that organizations storing, accepting, processing, and transmitting credit card information do so in a secure environment.

* **System and Organizations Controls (SOC type 1, SOC type 2)**

The SOC1 and SOC2 are a series of reports that focus on an organization’s user access policies at different organizational levels. They are used to assess an organization’s financial compliance and levels of risk. They also cover confidentiality, privacy, integrity, availability, security, and overall data safety. Control failures in these areas can lead to fraud.

**Findings**

| **Physical Controls** | | | |
| --- | --- | --- | --- |
| **Control Name** | **Control type and explanation** | **Needs to be implemented**  **(X)** | **Priority** |
| Time-controlled safe | Deterrent; reduce attack surface/impact of physical threats | X | Medium/  Low |
| Adequate lighting | Deterrent; limit “hiding” places to deter threats | X | Medium/  Low |
| Locking cabinets (for network gear) | Preventative; increase integrity by preventing unauthorized personnel/individuals from physically accessing/modifying network infrastructure gear | X | Medium |
| Signage indicating alarm service provider | Deterrent; makes the likelihood of a successful attack seem low | X | Low |
| Fire detection and prevention (fire alarm, sprinkler system, etc.) | Detective/Preventative; detect fire in the toy store’s physical location to prevent damage to inventory, servers, etc. | X | Medium/  Low |

**Summary/Recommendations:**

It's necessary the company achieve the critical findings because of this deppend that organization has a better practices, all critical Is obligatory is complience.

Beyond there are regulations o standars are achieve, then for that a campana must cervicales.