# 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/1DWmu8rVrIY_vGR3nRCUl7sxekN2fGRYypcF6ej8YheA/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: (Your Name)  
DATE: (Today’s Date)  
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:**

* 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:**

* 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.

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

* Least privilege control must be implemented immediately as failure to adhere to this violates SOC type 1 and 2. These SOC covers confidentiality, privacy, integrity, availability, security and overall data safety. Failure in this regard can lead to fraud and reputational damage.
* Disaster recovery must also be implemented immediately in case data loss occurs. A recovery process must be clearly defined so business continuity is not impacted in case of data loss due to breaches or failures.
* Password policies should be strengthened by ensuring a minimum character of 12 that contains at least a capital letter, special character and number. This password should be changed every 90 days at a minimum.
* Access control mechanisms should be enforced so that only people who require specific data are configured to access it. This can be achieved by configuration of group policies with appropriate permissions for digital assets. For physical assets and locations key cards must be configured to give access to critical locations to required staff.
* Account management policy should also ensure MFA is a default setting for all user accounts. For exiting users there should be seamless communication between HR and the IT department so they are disabled once exit is confirmed.
* Separation of duties is implemented so there is a clear understanding of functions. This will assist in the design of group policies so appropriate permissions are granted to these groups for user access.
* Intrusion Detection System (IDS) should be implemented to monitor real time activities on the network so active attempts by threat actors to penetrate the network are identified and stopped.
* Backups- a clear backup policy is defined and implemented in compliance to global best practice. Backups should be separated by locations in case of issues so business continuity is not impacted.
* Password management system that is in charge and monitors password expiry dates, password recovery and lock out notifications in compliance to global best practices is implemented.
* Antivirus (AV) software that scans for malware and worms is implemented with regular updates to its definitions is implemented so individual user PC and servers are protected from the latest viruses that can impact data assets.
* Locks that can only be accessed with key cards. These cards are configured per group policy.
* Fire detection and prevention (fire alarm, sprinkler system, etc.) to quickly contain fires to limit destruction to assets if fire incident happens.

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

* Time -controlled safe implementation must be considered in the future to harden physical security on site.
* Adequate lighting should be provided in critical areas so there is no cover for potential threat actors trying to gain unauthorized access.
* Closed-circuit television (CCTV) surveillance should be implemented in common and critical infrastructure location to act as deterrent and source for data during investigation of possible breaches.
* Locking cabinets (for network gear) this is to prevent unauthorized access to threat actors that can impact network thus leading to down times.
* Signage indicating alarm service provider is implemented as deterrent so potential threat actors are aware that there are alarms on site.

**Summary/Recommendations:** These critical and non-too critical risks should be fixed in compliance to regulatory policies because non implementation will be in violation of some critical regulations like **System and Organizations Controls (SOC type 1, SOC type 2), Payment Card Industry Data Security Standard (PCI DSS) & General Data Protection Regulation (GDPR).**

if breach occurs as a result of any of these risks there will be regulatory fines, reputational damage and negative impact to business continuity.