# 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: Davin Paige  
DATE: May 17, 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:**

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** (must be addressed immediately):

**Compliance Issues**

General Data Protection Regulation (GDPR) is a compliance issue that Botium Toys needs to address when providing ecommerce services in the E.U. This regulation is considered high risk because it protects the data and privacy rights of E.U. citizens. Failure to comply with GDPR can result in significant penalties and fines. Additionally, the requirement to notify individuals within 72 hours of a data breach adds urgency and pressure to effectively manage and protect personal data.

Payment Card Industry Data Security Standard (PCI DSS) is another compliance issue that Botium Toys needs to adhere to due to its handling of credit card information. PCI DSS is considered high risk because it sets international security standards to ensure the secure storage, processing, and transmission of credit card data. Non-compliance can lead to compromised customer payment information, financial losses, and damage to the reputation of Botium Toys.

System and Organizations Controls (SOC) Type 1 and SOC Type 2 reports are important for assessing an organization's financial compliance and levels of risk. These reports focus on user access policies, confidentiality, privacy, integrity, availability, security, and data safety. Failure to maintain adequate controls in these areas can increase the risk of fraud and compromise sensitive information. Botium Toys needs to enhance its access control mechanisms for third parties to mitigate risk and ensure the overall protection of data, making SOC compliance crucial.

**High Priority Controls**

High priority controls that need to be implemented include:

1. Least Privilege: Limiting access to assets/data for vendors and non-authorized staff to reduce risk.

2. Disaster Recovery Plans: Ensuring business continuity and minimizing productivity downtime/impact to system components in the event of an incident.

3. Password Policies: Establishing password strength rules to improve security and reduce the likelihood of account compromise.

4. Access Control Policies: Increasing the confidentiality and integrity of data.

5. Account Management Policies: Reducing the attack surface and limiting the overall impact from disgruntled or former employees.

6. Separation of Duties: Preventing individuals from having excessive access that could be abused for personal gain.

7. Intrusion Detection System (IDS): Identifying possible intrusions quickly.

8. Encryption: Enhancing the security of confidential information and data.

9. Backups: Supporting ongoing productivity and aligning with the disaster recovery plan.

10. Antivirus (AV) Software: Detecting and quarantining known threats.

11. Manual Monitoring, Maintenance, and Intervention: Required for legacy systems to identify and mitigate potential threats, risks, and vulnerabilities.

12. Closed-Circuit Television (CCTV) Surveillance: Acting as a preventive and detective measure, reducing certain risks and aiding investigation after an event.

13. Locking Cabinets (for network gear): Increasing integrity by preventing unauthorized physical access to network infrastructure gear.

14. Locks: Enhancing the security of physical and digital assets.

15. Fire Detection and Prevention: Detecting fire to prevent damage to inventory, servers, and other components.

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

Low priority controls that need to be implemented include:

1. Password Management System: Providing features for password recovery, reset, and lockout notifications.

2. Time-Controlled Safe: Reducing the attack surface and impact of physical threats through controlled access to sensitive areas.

3. Adequate Lighting: Limiting hiding places and deterring physical threats.

4. Signage Indicating Alarm Service Provider: Creating the perception of low likelihood of a successful attack.

Medium priority controls that need to be implemented include:

1. Locking Cabinets (for Network Gear): Increasing integrity by preventing unauthorized physical access or modification of network infrastructure gear.

2. Fire Detection and Prevention (Fire Alarm, Sprinkler System, etc.): Combining detective and preventive measures to detect and prevent fire damage to inventory, servers, and other components.

**Summary/Recommendations:**

The recent suggestions and goals align to provide comprehensive solutions for Botium Toys by focusing on adherence to the NIST CSF and compliance requirements, establishing better processes, fortifying system controls, implementing least permissions in user credential management, and establishing policies and procedures. This includes measures such as disaster recovery plans, backups, intrusion detection systems, encryption, antivirus software, and manual monitoring. The emphasis on access control policies, account management policies, and separation of duties further enhances security and reduces the risk of insider threats. Overall, these efforts aim to ensure a secure and compliant IT environment for Botium Toys.