**To: IT Manager, Stakeholders**

**From: Debayan Das**

**Date: 09/08/2023]**

**Subject: Internal IT Audit Findings and Recommendations**

Dear Colleagues,

I would like to inform you of the outcomes of the recent internal IT audit conducted for Botium Toys. The purpose of this communication is to provide an overview of the audit scope, goals, critical findings, and recommendations for your consideration.

**Scope:**

The audit encompassed various aspects of our IT infrastructure, including on-premises equipment, network access, data management, and compliance with industry standards.

**Goals:**

The primary objectives of the audit were to:

* Enhance our security posture by aligning with industry best practices, such as adhering to the NIST CSF and implementing the concept of least privilege.
* Provide recommendations for mitigating identified risks through controls, policies, and documentation.
* Determine the compliance regulations that Botium Toys must adhere to based on our business operations and payment processes.

**Critical Findings (Must be Addressed Immediately):**

During the audit, several critical findings were identified that require immediate attention:

* Inadequate management of assets, posing a risk to asset security and potential data breaches.
* The absence of proper controls leaves our organization vulnerable to cyber threats and unauthorized access.
* Potential non-compliance with U.S. and international regulations and guidelines could lead to legal and reputational consequences.

**Findings (Should be Addressed, but No Immediate Need):**

The audit uncovered findings that should be addressed in due course to ensure our IT environment's robustness and compliance. These include access control policies, disaster recovery planning, and password management.

**Summary/Recommendations:**

The audit has provided valuable insights into our IT landscape. To address the critical findings and mitigate associated risks, we recommend the following immediate actions:

* Implement the principle of least privilege to limit unauthorized access and data exposure.
* Develop and execute a comprehensive disaster recovery plan to ensure business continuity during incidents.
* Strengthen access control policies to enhance data confidentiality and integrity.
* Initiate compliance assessments to ensure adherence to relevant regulations, such as GDPR and PCI DSS.

For the findings that require attention but do not demand immediate action, we propose a comprehensive plan to enhance our IT infrastructure's overall security and compliance posture.

Your collaboration and support are essential to ensure the successful implementation of these recommendations and the ongoing improvement of our IT security. Please feel free to reach out if you have any questions or require further clarification.

Thank you for your time and commitment to maintaining the security and integrity of our IT systems.

Best regards,

Debayan Das