# Stakeholder memorandum

TO: IT Manager, Stakeholders

FROM: Dhruv Prajapati

DATE: 21/10/2024

SUBJECT: Internal IT Audit Findings and Recommendations

Dear Colleagues,

I hope this memo finds you well. I would like to bring to your attention the results of the recent internal audit conducted on Botium Toys' IT assets and management systems. The audit aimed to evaluate the current state of our IT infrastructure and identify areas that require attention and improvement.

**Scope:**

The audit encompassed a comprehensive assessment of the company's IT assets and services, including but not limited to:

* On-premises equipment catering to in-office business requirements.
* Employee equipment, consisting of end-user devices such as desktops, laptops, smartphones, along with accessories like headsets, cables, keyboards, mice, and docking stations.
* Management of various systems, software, and services encompassing accounting, telecommunication, database, security, ecommerce, and inventory management.
* Oversight of internet access and the internal network.
* Vendor access management to ensure secure collaborations.
* Data center hosting services for critical applications and services.
* Data retention and storage solutions to manage information effectively.
* Badge readers for access control.
* Maintenance of legacy systems that are nearing end-of-life and necessitate human supervision.

**Goals:**

The primary objectives of the audit were to assess the efficiency, security, and reliability of our IT assets and services. By doing so, we aimed to identify vulnerabilities, streamline operations, and enhance overall system performance.

**Critical Findings (Must be addressed immediately):**

During the audit, we identified several critical findings that demand immediate attention to ensure the security and stability of our IT environment:

1. **Security Vulnerabilities in Legacy Systems**: Our end-of-life legacy systems have shown significant security vulnerabilities that expose our network to potential breaches. Immediate action is required to secure these systems or plan for their replacement.
2. **Access Control Weaknesses:** Inconsistent badge reader implementation and vendor access management could lead to unauthorized access. It is crucial to strengthen access controls to safeguard sensitive areas and data.

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

While the following findings do not pose an immediate threat, addressing them will contribute to overall operational improvement:

1. **Software Update Management:** Some systems and software require more regular updates to ensure optimal performance and security. A more structured approach to update management is recommended.
2. **End-User Equipment Monitoring:** Monitoring and managing end-user devices more proactively can prolong their lifespan and prevent unexpected downtime.

**Summary/Recommendations:**

In summary, this audit has provided valuable insights into the state of our IT assets and management systems. To address the critical findings, I recommend the following actions:

1. **Legacy System Mitigation:** Engage a team to assess and apply security patches to the end-of-life legacy systems or expedite plans for their replacement.
2. **Access Control Enhancement:** Review and enhance our badge reader implementation and vendor access management protocols to prevent unauthorized entry.
3. **Update Management Protocol:** Develop a comprehensive software update management protocol to ensure all systems and software are regularly updated to minimize security risks.
4. **End-User Device Management:** Implement a proactive device monitoring strategy to extend the lifespan of end-user equipment and reduce unexpected disruptions.

Your commitment to addressing these issues promptly will reinforce the security and efficiency of our IT operations. Kindly review these recommendations and collaborate with the relevant teams to implement the necessary actions.