**Stakeholder Memorandum**

**TO:** IT Manager, Stakeholders

**FROM:** Andrew Allen

**DATE:** January 19, 2024

**SUBJECT:** Internal Audit Findings and Recommendations

Dear Colleagues,

Please find below an overview of the recent internal IT audit conducted at XYZ Financial Services:

**Scope:** Our internal IT audit assessed the organization's information technology systems, assets, controls, and compliance with relevant regulations and standards.

**Goals:** The primary objectives of this audit were to evaluate controls, assess compliance, identify vulnerabilities, and provide recommendations for enhancing security and risk management.

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

1. **Data Encryption Implementation:** The audit identified the urgent need to implement data encryption to protect customers' financial data in transit and at rest. Data Encryption is crucial for maintaining the confidentiality and integrity of sensitive information.
2. **Access Controls for Employee Devices:** Strong access controls must be implemented immediately to restrict unauthorized access to employee devices (computers, phones). This is essential for preventing potential security breaches and safeguarding sensitive information.

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

1. **Employee Training on Cybersecurity:** While employee training on cybersecurity best practices has been initiated, continuous efforts are needed to reinforce a culture of security awareness and reduce the risk of human errors in data handling.
2. **Regular Data Backups for Business Continuity:** Although regular data backups are in place, improvements can be made to enhance the frequency and efficiency of backup processes, ensuring better business continuity in the event of data loss.

**Summary/Recommendations:** In summary, the audit revealed critical findings requiring immediate action and additional findings for long-term improvements. We recommend addressing the identified issues promptly to enhance security and compliance measures. Specifically:

* Swift implementation of data encryption measures to protect customer financial data.
* Urgent establishment of strong access controls for employee devices.
* Ongoing and reinforced employee training on cybersecurity best practices.
* Optimization of regular data backup processes for improved business continuity.

Sincerely,

[Andrew Allen]

 []

 XYZ Financial Services