Stakeholder Memorandum

TO: IT Manager, Stakeholders  
FROM: Lily Schlossberg  
DATE: 01/18/2024  
SUBJECT: Internal IT Audit Findings and Recommendations

Dear Colleagues,

Please find below an overview of the recent internal IT audit conducted at XYZ Financial Services:  
Scope: The entire IT department with respect to

* customer financial data,
* employee devices data,
* as well as current assets.  
  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. Conduct a higher cybersecurity training for employees so that they can solve their own problems quickly  
2. Have a higher standard of law of the company for the employee devices so that the company has more control over employees  
Findings (Should Be Addressed, but No Immediate Need):  
1. Customer data backups need to be a higher priority  
2. Provide a higher physical security using cameras to ensure proper conduct

Summary/Recommendations:

In summary, the audit revealed critical findings requiring immediate action and additional findings  
for long-term improvements. We recommend addressing digital assets to minimize risks, financial assets to minimize unauthorized transactions so that it is more secure. I think that it is less necessary to get backups done and more necessary to get security cameras implemented, this will be sure that the physical location is better well-kept before we move onto the online backups. This is why it is important for employee’s phones to be well kept track of, so that information is not leaked out of the building.

Sincerely,  
Lily Schlossberg  
MIS Student  
XYZ Financial Services