Stakeholder Memorandum

TO: IT Manager, Stakeholders

FROM: Riccardo Pradieu

DATE: January 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:

This involves looking over the whole cybersecurity program. This looks into all the assets, internal processes, and procedures related to information security in a company. The systems that will be looked over:

* Current user permissions
* Current implementation controls
* Current procedures and protocol

The systems will make sure that technology is up-to-date and will process technology for hardware and system. Also, the make sure that protocols and procedures are on the same track as the PCI DSS and GDPR meets the user agreement requirements

Goals:

There are many goals with this objective. Some include making a better process of the companies’ systems, implement rules and policies to ensure that everything is not a risk and follows the guidelines, rampart the system control to ensure that everything is going smoothly, embrace the rules in managing user credentials

Critical Findings (Must Be Addressed Immediately):

1. Many controls must be implemented and refined in order to meet audit goals such as: IDS, CCTV, Locks, fire detection, encryption, user passwords, and recovery plans.

2. Rules and procedures need to be put into place to reach the PCI DSS, GDPR user requirements and the SOC1 and SOC2 guidelines to protect data and user policies.

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

1. The following measures need to be implemented when feasible: time-controlled safe

sufficient lighting, locked cabinets, and signage indicating the alarm service provider.

Summary/Recommendations:

In summary, the audit revealed critical findings similar to the PCI DSS and GDPR agreement. If they agree to accept payments internationally from customers, it is recommended to use SOC1 and SOC2 as to helpful guide to help implement and develop a low risk for data safety and protect users accounts. While doing this it can implement disaster plans for businesses to help protect them. Making an IDS or AV software will strengthen the ability to identify risk and threat that may arise.

Sincerely,

Riccardo Pradieu

IT Security Auditor

XYZ Financial Services