# Stakeholder Memorandum

TO: IT Manager, stakeholders

FROM: Christina Canady  
DATE: 1/19/24  
SUBJECT: Internal IT audit findings and recommendations

Dear Colleagues,

Please review the following information regarding the XYZ Financials internal audit scope, goals, critical findings, summary and recommendations.

**Scope:**

* This evaluation encompasses the entire cybersecurity program. The assessment includes all assets, internal processes, and procedures related to information security. Specifically, it will assess:
  + Current user permissions
  + Current implemented security controls
  + Current cybersecurity procedures and protocols
* Evaluation of compliance with financial regulations, including GLBA and PCI DSS.
* Assessment of technology assets, including hardware and software used for financial transactions.

**Goals:**

* Ensure compliance with financial regulations such as GLBA and PCI DSS to protect customer financial data and maintain regulatory trust.
* Strengthen data protection measures, including encryption and access control, to safeguard customer financial records.
* Identify and address vulnerabilities that could disrupt financial operations and develop a business continuity strategy.
* Enhance the overall security posture of the organization by aligning with the industry best practices and standards
* Provide recommendations for mitigating high-risk vulnerabilities and improving overall cybersecurity
* Develop and implement training programs to educate employees about cybersecurity best practices

**Critical findings** (must be addressed immediately):

* Multiple controls need to be developed and implemented to meet the audit goals, including:
  + Limiting who can access and modify customer records
  + Employee cyber security training
  + Password management system; 2FA
  + Encryption (for secure website transactions)
  + Backups
  + AV software
  + IDS
  + Fire detection and prevention systems
* Policies need to be developed and implemented to meet PCI DSS and GDPR compliance requirements.
* Policies need to be developed and implemented to align to SOC1 and SOC2 guidance related to user access policies and overall data safety.

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

* The following controls should be implemented when possible:
  + Time-controlled safe
  + Adequate lighting
  + Locking cabinets

**Summary/Recommendations:**

It is recommended that critical findings relating to compliance with PCI DSS and GDPR be promptly addressed since XYZ financials does business with customers outside of the US, specifically the EU. XYZ financials also needs to be brought into compliance with SOC1 and SOC2. This will ensure secure user access policies, data integrity, and overall data safety with respect to employee devices. The implementation of a disaster recovery plan is critical to support business continuity in the event of an incident. This means XYZ must begin making backups of customer financial data. All employees should be trained in cybersecurity best practices as well as integrating IDS and AV software into the current system. There is no immediate need (but should be addressed) for better protection of XYZ’s physical assets including office locations and server equipment. A time-controlled safe should be used, adequate lighting should be installed outside as well as locking cabinets. There should also be fire protection and prevention systems installed throughout the XYZ office buildings.