Stakeholder memorandum

TO: IT Manager, stakeholders

FROM: Brianna Baird   
DATE: 1/18/2024  
SUBJECT: Internal IT audit findings and recommendations

Dear Colleagues,

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

**Scope:**

* The following systems are in scope: transaction processing systems, databases, financial applications, firewalls, intrusion detection systems, and encryption. The systems will be evaluated for:
  + Current user permissions
  + Access controls
  + Current procedures and protocols
  + Effectiveness of controls
* Evaluate compliance with financial regulations and alignment with GLBA and PCI DSS requirements.
* Assess technology assets; hardware and software, used in financial transactions.

**Goals:**

* Ensure compliance with GLBA and PCI DSS regulations.
* Strengthen data protection measures to safeguard customer financial records.
* Identify and address concerns that are a threat to financial operations.
* Develop business continuity strategy.
* Adhere to NIST CSF to enhance security.
* Provide recommendations for high-risk vulnerabilities.
* Develop and implement training programs.

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

* Multiple controls need to be developed and implemented to meet the audit goals, including:
  + Just-in Time privileged access management to limit access to systems
  + Principle of least privilege to access systems with customer financial data
  + Multifactor authentication password management for system access on employee devices
  + Data encryption to protect customer data in transit.
  + Intrusion Detection Systems (IDS)
  + Data Backups and recovery plans
  + Firewalls to
  + Biometric Locks at data centers
* Implement policies in alignment with SOC type 1 and SOC type 2 control standards to ensure data safety and integrity concerning user access.
* Policies must be implemented to remain in compliance with GDPR and PCI DSS regulations.

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

* The following controls should be implemented when possible:
  + Employee training on best cybersecurity to reduce the risk of error.
  + Surveillance cameras at office locations

**Summary/Recommendations:** It is recommended that XYZ Financial Services address the critical findings concerning compliance with financial regulations to protect customer information and reduce the risk of data breaches. The implementation of policies concerning systems access should be addressed to ensure our goals of data protection. Developing employee training programs to educate employees on the best cybersecurity practices is crucial to the protection of data. If not in compliance with GDPR and PCI DSS standards and regulations XYZ Financial Services may face ligation, financial loss, and damage to the brand. To ensure business continuity complete regular backups while developing a recovery plan. Implementation of IDS for quick identification and response to threats. The protection of physical assets is also a priority. The use of biometric locks and CCTV to monitor and control access to office buildings and data centers offers additional protection.

Sincerely,

Brianna Baird