Audit Stakeholder Memorandum

TO: IT Manager, stakeholders

FROM: Kyle Johnson

DATE: 7/18/23

SUBJECT: Internal IT audit findings and recommendations

Dear Colleagues,

Please review the following information regarding the Graphix Collab LLC internal audit scope,goals, critical findings, summary and recommendations.

Audit Scope

Current user permissions, implemented controls, procedures, and protocols set in the following systems:

- accounting,
- end point detection,
- firewalls,
- intrusion detection system,
- security information and
- Event management (SIEM) tool.

● Ensure current user permissions, controls, procedures, and protocols in place align with necessary compliance requirements.

● Ensure current technology is accounted for. Both hardware and system access.

Audit Goals

To adhere to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF):

- Establish a better process for their systems to ensure they are compliant
- Fortify system controls

- Implement the concept of least permissions when it comes to user credential management
- Establish their policies and procedures, which includes their playbooks
- Ensure they are meeting compliance requirements

Critical Findings (must be addressed immediately)

Administrative controls recommended for immediate implementation (high-priority):

- Least Privilege, Disaster recovery plans, Account management policies, and Separation of duties.

Technical Controls recommended for immediate implementation (high-priority):

- Intrusion Detection System (IDS), Encryption, Backups, Antivirus (AV) software, Manual monitoring, maintenance, and intervention

Physical controls recommended for immediate implementation (high-priority):

- Closed-circuit television (CCTV) surveillance, Locking cabinets (for network gear), Fire detection and prevention (fire alarm, sprinkler system, etc.)

Other Findings

General Data Protection Regulation (GDPR):

- Graphix Collab LLC needs to adhere to GDPR because they conduct business and collect personal information from people worldwide, including the E.U.

Payment Card Industry Data Security Standard (PCI DSS):

- Graphix Collab LLC needs to adhere to PCI DSS because they store, accept, process, and transmit credit card information in person and online.

System and Organizations Controls (SOC type 1, SOC type 2):

- Graphix Collab LLC needs to establish and enforce appropriate user access for internal and external (third-party vendor) personnel to mitigate risk and ensure data safety.

Summary/Recommendations

The IT team assessed current user permissions, implemented controls, procedures, and protocols set across various systems at Graphix Collab LLC. The goal of this audit is to adhere to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). We found that there are several administrative, technical, and physical controls that need to be implemented immediately to adhere to the voluntary NIST CSF framework, which is considered best-practice.

Having disaster recovery plans and backups is also critical because they support business continuity in the event of an incident. Integrating an IDS and AV software into the current systems will support our ability to identify and mitigate potential risks, and could help with intrusion detection, since existing legacy systems require manual monitoring and intervention. To further secure assets housed at Graphix Collab LLC single physical location, locks and CCTV should be used to secure physical assets (including equipment) and to monitor and
investigate potential threats.

Compliance findings include urgent need for adhering to the GDPR regulations,PCI DSS requirements, and SOC1 and SOC2 controls which will directly mitigate fraud risk, and ensure data safety. Implementing these recommendations will further improve Graphix Collab LLC security posture.