Co-CIO

Fractional IT Leadership for Middle Tennessee

15-Point Infrastructure & Security Audit

Comprehensive IT Assessment Report

PREPARED FOR

_____

Audit Date: _____

Auditor: Jess Disney, Co-CIO

Report Version: 1.0

CONFIDENTIAL — This document contains proprietary information about the client's IT infrastructure. Distribution is limited to authorized personnel only.

Table of Contents

- Client Information & IT Environment Overview

01 Network Architecture Review

02 Firewall & Perimeter Security

03 Backup & Disaster Recovery

04 Endpoint Protection Assessment

05 Compliance Gap Analysis

06 Cloud Services Audit

07 Password & Access Policies

08 Email Security Check

09 Patch Management Review

10 Physical Security Assessment

11 Wi-Fi Security Scan

12 Vendor & License Audit

13 IT Budget Efficiency Score

14 AI Readiness Evaluation

15 Executive Summary & Roadmap

- Top Recommendations & Sign-Off

Client Information & IT Environment Overview

Company Information

COMPANY NAME

DBA / TRADE NAME

ADDRESS

CITY / STATE / ZIP

PRIMARY CONTACT

TITLE / ROLE

PHONE

EMAIL

INDUSTRY / VERTICAL

NUMBER OF EMPLOYEES

NUMBER OF LOCATIONS

COMPLIANCE REQUIREMENTS

Current IT Environment

CURRENT IT PROVIDER / STAFF

ANNUAL IT BUDGET (EST.)

NUMBER OF WORKSTATIONS

NUMBER OF SERVERS

DOMAIN / ACTIVE DIRECTORY

PRIMARY ISP / SPEED

BACKUP ISP

PHONE SYSTEM TYPE

EMAIL PLATFORM

LINE OF BUSINESS SOFTWARE

EHR / ERP SYSTEM

REMOTE WORKERS?

Known Pain Points / Concerns

01 Network Architecture Review

Assessment of network topology, segmentation, switching, and routing infrastructure

- [ ] Pass
- [ ] Needs Improvement
- [ ] Fail
- [ ] N/A

Risk Rating:

LOW	MEDIUM	HIGH	CRITICAL

Checklist

- [ ] Network diagram exists and is current
- [ ] VLANs implemented for network segmentation (guest, IoT, servers, workstations)
- [ ] Managed switches in use (not consumer-grade)
- [ ] Router/gateway firmware is current
- [ ] Bandwidth adequate for current and projected needs
- [ ] Redundant internet connection or failover configured
- [ ] DNS properly configured (internal and external)
- [ ] DHCP scopes documented and appropriate
- [ ] No single points of failure in core network path
- [ ] Network monitoring/alerting in place

Findings & Notes:

02 Firewall & Perimeter Security

Assessment of firewall rules, intrusion detection/prevention, and edge security

- [ ] Pass
- [ ] Needs Improvement
- [ ] Fail
- [ ] N/A

Risk Rating:

LOW	MEDIUM	HIGH	CRITICAL

Checklist

- [ ] Business-grade firewall in place (not ISP-provided router only)
- [ ] Firewall firmware/software is current
- [ ] Default credentials changed on all network devices
- [ ] Inbound rules follow least-privilege principle
- [ ] No unnecessary ports open to the internet
- [ ] VPN configured for remote access (no RDP exposed)
- [ ] IDS/IPS enabled and monitored
- [ ] Geo-blocking enabled for non-business countries
- [ ] Firewall logs reviewed regularly
- [ ] Content filtering / web filtering active

Findings & Notes:

03 Backup & Disaster Recovery

Assessment of backup strategy, offsite copies, RTO/RPO, and recovery testing

- [ ] Pass
- [ ] Needs Improvement
- [ ] Fail
- [ ] N/A

Risk Rating:

LOW	MEDIUM	HIGH	CRITICAL

Checklist

- [ ] All critical data backed up (servers, workstations, cloud services)
- [ ] 3-2-1 backup rule followed (3 copies, 2 media types, 1 offsite)
- [ ] Backups encrypted at rest and in transit
- [ ] Backup schedule is documented and appropriate
- [ ] Offsite/cloud backup in a different geographic location
- [ ] Backup success/failure alerts configured and monitored
- [ ] Test restore performed in the last 90 days
- [ ] Recovery Time Objective (RTO) defined and achievable
- [ ] Recovery Point Objective (RPO) defined and met
- [ ] Disaster recovery plan documented and staff trained

Findings & Notes:

04 Endpoint Protection Assessment

Assessment of antivirus, EDR, device encryption, and endpoint management

- [ ] Pass
- [ ] Needs Improvement
- [ ] Fail
- [ ] N/A

Risk Rating:

LOW	MEDIUM	HIGH	CRITICAL

Checklist

- [ ] Business-grade antivirus/EDR on all endpoints
- [ ] Real-time protection enabled and definitions current
- [ ] Full disk encryption enabled (BitLocker/FileVault)
- [ ] USB/removable media policy enforced
- [ ] Mobile device management (MDM) for company phones/tablets
- [ ] Local admin rights restricted to IT staff only
- [ ] Screen lock timeout configured (≤ 10 minutes)
- [ ] Asset inventory current (all devices documented)
- [ ] End-of-life devices identified and scheduled for replacement
- [ ] BYOD policy exists and enforced

Findings & Notes:

05 Compliance Gap Analysis

Assessment of regulatory compliance requirements and current adherence

- [ ] Pass
- [ ] Needs Improvement
- [ ] Fail
- [ ] N/A

Risk Rating:

LOW	MEDIUM	HIGH	CRITICAL

Checklist

- [ ] Applicable regulations identified (HIPAA, SOX, PCI-DSS, CMMC, etc.)
- [ ] Business Associate Agreements (BAAs) in place with all vendors
- [ ] Data classification policy exists (PHI, PII, financial, public)
- [ ] Access controls aligned with compliance requirements
- [ ] Audit logging enabled for compliance-relevant systems
- [ ] Employee security awareness training conducted annually
- [ ] Incident response plan documented and tested
- [ ] Data retention policies defined and enforced
- [ ] Risk assessment performed in the last 12 months
- [ ] Cyber insurance policy current and adequate

Findings & Notes:

06 Cloud Services Audit

Assessment of cloud platforms, SaaS usage, configuration, and shadow IT

- [ ] Pass
- [ ] Needs Improvement
- [ ] Fail
- [ ] N/A

Risk Rating:

LOW	MEDIUM	HIGH	CRITICAL

Checklist

- [ ] All cloud services inventoried (M365, Google, AWS, etc.)
- [ ] MFA enabled on all cloud admin accounts
- [ ] Conditional access policies configured
- [ ] Cloud backups in place (email, OneDrive/SharePoint, etc.)
- [ ] Offboarded employee accounts disabled/removed promptly
- [ ] Shadow IT assessment performed (unauthorized cloud services)
- [ ] Data sharing permissions reviewed (external sharing controls)
- [ ] Security defaults or security baselines applied

Findings & Notes:

07 Password & Access Policies

Assessment of authentication methods, password standards, and access management

- [ ] Pass
- [ ] Needs Improvement
- [ ] Fail
- [ ] N/A

Risk Rating:

LOW	MEDIUM	HIGH	CRITICAL

Checklist

- [ ] Multi-factor authentication (MFA) enabled for all users
- [ ] Password complexity requirements enforced (12+ chars)
- [ ] Business password manager in use
- [ ] No shared accounts or generic logins
- [ ] Privileged accounts separated from daily-use accounts
- [ ] Account lockout policy configured
- [ ] Offboarding process includes immediate credential revocation
- [ ] Principle of least privilege applied to all accounts
- [ ] Service account passwords unique and documented securely
- [ ] No passwords stored in plaintext (spreadsheets, sticky notes, etc.)

Findings & Notes:

08 Email Security Check

Assessment of email filtering, authentication, phishing protection, and encryption

- [ ] Pass
- [ ] Needs Improvement
- [ ] Fail
- [ ] N/A

Risk Rating:

LOW	MEDIUM	HIGH	CRITICAL

Checklist

- [ ] SPF, DKIM, and DMARC records configured correctly
- [ ] Advanced spam/phishing filter in place (beyond basic)
- [ ] External email banner/warning configured
- [ ] Attachment scanning and sandboxing enabled
- [ ] Link protection / Safe Links enabled
- [ ] Email encryption available for sensitive communications
- [ ] Phishing simulation/training conducted regularly
- [ ] Mail flow rules reviewed (no auto-forwarding to external)
- [ ] Email backup/archival solution in place
- [ ] Impersonation protection configured for executives

Findings & Notes:

09 Patch Management Review

Assessment of OS and application patching processes and currency

- [ ] Pass
- [ ] Needs Improvement
- [ ] Fail
- [ ] N/A

Risk Rating:

LOW	MEDIUM	HIGH	CRITICAL

Checklist

- [ ] All operating systems on supported versions (no EOL)
- [ ] Windows/macOS updates applied within 30 days of release
- [ ] Critical security patches applied within 14 days
- [ ] Third-party applications patched (Adobe, Java, Chrome, etc.)
- [ ] Server firmware and BIOS current
- [ ] Network device firmware current (switches, APs, firewalls)
- [ ] Patch management tool/process in place (WSUS, Intune, etc.)
- [ ] Patch compliance reporting available
- [ ] Test/staging process for critical patches
- [ ] Printer/copier firmware current

Findings & Notes:

10 Physical Security Assessment

Assessment of server room, access controls, surveillance, and environmental protections

☐ Pass ☐ Needs Improvement ☐ Fail ☐ N/A

Risk Rating:

LOW	MEDIUM	HIGH	CRITICAL

Checklist

- ☐ Server/network closet has locked access (key or badge)
- ☐ UPS/battery backup on servers and network equipment
- ☐ UPS batteries tested and within replacement date
- ☐ Dedicated cooling for server room/closet
- ☐ Temperature/humidity monitoring with alerts
- ☐ Fire suppression appropriate for electronics
- ☐ Security cameras covering entry points and server areas
- ☐ Visitor log/sign-in process
- ☐ Cable management clean and labeled
- ☐ Generator or extended runtime power plan for outages

Findings & Notes:

11 Wi-Fi Security Scan

Assessment of wireless network configuration, encryption, and segmentation

- [ ] Pass
- [ ] Needs Improvement
- [ ] Fail
- [ ] N/A

Risk Rating:

LOW	MEDIUM	HIGH	CRITICAL

Checklist

- [ ] WPA3 or WPA2-Enterprise in use (no WEP/WPA/open)
- [ ] Separate guest network isolated from corporate network
- [ ] Guest network has bandwidth limits and client isolation
- [ ] Corporate Wi-Fi uses 802.1X authentication (RADIUS)
- [ ] Access point firmware current
- [ ] Default AP admin credentials changed
- [ ] SSID broadcast appropriate (hidden for internal if needed)
- [ ] Rogue AP detection in place
- [ ] Wi-Fi coverage adequate (no dead zones in work areas)
- [ ] IoT devices on separate VLAN from corporate Wi-Fi

Findings & Notes:

12 Vendor & License Audit

Assessment of software licensing, vendor contracts, and third-party risk

- [ ] Pass
- [ ] Needs Improvement
- [ ] Fail
- [ ] N/A

Risk Rating:

LOW	MEDIUM	HIGH	CRITICAL

Checklist

- [ ] All software properly licensed (no pirated/unlicensed software)
- [ ] License inventory maintained and current
- [ ] Unused licenses identified (cost savings opportunity)
- [ ] Vendor contracts reviewed for auto-renewal traps
- [ ] All vendor admin credentials documented securely
- [ ] Critical vendor SLAs documented and adequate
- [ ] Vendor security practices evaluated (SOC 2, etc.)
- [ ] Business owns all domain registrations and DNS
- [ ] SSL certificates current and auto-renewing
- [ ] No vendor lock-in concerns identified

Findings & Notes:

13 IT Budget Efficiency Score

Assessment of technology spend vs. industry benchmarks and ROI

- [ ] Pass
- [ ] Needs Improvement
- [ ] Fail
- [ ] N/A

Risk Rating:

LOW	MEDIUM	HIGH	CRITICAL

Checklist

- [ ] IT budget defined and tracked
- [ ] Spend aligned with industry benchmarks (4-6% of revenue)
- [ ] Hardware lifecycle plan in place (3-5 year refresh)
- [ ] Duplicate/overlapping services identified
- [ ] Cost per user/endpoint calculated
- [ ] Technology debt quantified (deferred upgrades)
- [ ] Capital vs. operational expense balance appropriate
- [ ] ROI tracked for major technology investments

Findings & Notes:

14 AI Readiness Evaluation

Assessment of AI/automation opportunities and organizational readiness

☐ Pass ☐ Needs Improvement ☐ Fail ☐ N/A

Risk Rating:

LOW	MEDIUM	HIGH	CRITICAL

Checklist

- ☐ Repetitive manual processes identified (automation candidates)
- ☐ Data quality sufficient for AI/analytics use
- ☐ Customer communication could benefit from AI chatbot/routing
- ☐ Document processing/data entry ripe for automation
- ☐ Scheduling/resource allocation could be AI-optimized
- ☐ Staff open to AI-assisted workflows
- ☐ Existing tools have AI features not yet enabled
- ☐ Competitive advantage through AI identified
- ☐ AI governance/ethics policy needed
- ☐ Budget allocated for AI pilot projects

Findings & Notes:

15 Executive Summary & Roadmap

Overall assessment, priority findings, and recommended action plan

Section	Status	Risk	Priority Actions
01. Network Architecture			
02. Firewall & Perimeter			
03. Backup & DR			
04. Endpoint Protection			
05. Compliance			
06. Cloud Services			
07. Password & Access			
08. Email Security			
09. Patch Management			
10. Physical Security			
11. Wi-Fi Security			
12. Vendor & License			
13. IT Budget			
14. AI Readiness			

Top 5 Recommendations (Immediate Action)

1. _____
2. _____
3. _____
4. _____
5. _____

3-Year Technology Roadmap Notes:

Auditor Signature & Date

Client Representative & Date