FREE SYSTEMS AUDIT DELIVERABLE

Systems Architecture & Vulnerability Review

A prioritized, evidence-led review of technology risks, operational dependencies, and practical next steps.

PREPARED FOR

Sarasota Coastal Law Group, PA
[FICTITIOUS ORGANIZATION]

REPORT DATE

September 4, 2026
Illustrative Version 1.0

PREPARED BY

Gregory Mathews
Systems Architect & Owner

ASSESSMENT TYPE

Complimentary, non-invasive on-site Systems Audit

ILLUSTRATIVE SAMPLE – NOT A REAL CLIENT REPORT

Every organization, observation, addressable risk, price, and remediation example in this document is fictitious. A real report is customized to evidence observed during an authorized visit.

1. EXECUTIVE SUMMARY

What this illustrative audit found

The fictitious firm relies on Microsoft 365, a local file server, remote laptops, VoIP phones, and transaction-sensitive email. The sample review identifies five conditions that deserve prioritized follow-up. Ratings describe operational exposure observed in this scenario; they are not predictions that an incident will occur.

Highest priorities

- Separate guest and internal network access.
- Remove routine local-administrator rights and verify laptop encryption.
- Require MFA and named accounts for email and remote access.
- Protect backup administration and test restoration.
- Lock and document core network equipment.

Overall sample rating

CRITICAL

This rating reflects the combination of flat network access, shared credentials, unverified recovery, and privileged endpoint use in the fictitious environment.

Business workflows at risk

- Client and matter-file availability
- Court and calendar deadlines
- Email-based payment or wire instructions
- Remote work and deposition readiness
- Communications during local power or carrier outages

Important boundary

This is a technical and operational assessment, not a legal determination or certification. Counsel, insurers, auditors, and regulated entities determine applicable duties.

Authorized review scope

- ✓ Physical walkthrough
- ✓ Network and Wi-Fi architecture
- ✓ Endpoint and identity controls
- ✓ Backup and recovery evidence
- ✓ Microsoft 365 configuration review
- ✓ Operational dependency interview
- ✓ Policy and ownership inventory
- ✓ Prioritized roadmap

Not performed in this sample: destructive testing, exploit attempts, password collection, credential export, production changes, legal interpretation, formal penetration testing, or a guarantee that every vulnerability would be discovered.

2. METHOD AND CONTEXT

Evidence first; obligations confirmed separately

The sample method combines an authorized walkthrough, staff interview, read-only configuration views displayed by an authorized representative, and review of available records. Conclusions are tied to what was actually observed or could not be verified.

> Regulatory context: lawyers have confidentiality and technology-competence duties under applicable rules and ABA guidance, but safeguards are fact-specific. ALTA Best Practices are voluntary unless made binding by an applicable contract or authority. FTC, HIPAA, SEC, insurance, and client requirements apply only when their definitions and scope are met. See sources on page 8.

3. OPERATIONAL WORKFLOW & MOBILITY READINESS

WORKFLOW DOMAIN	ILLUSTRATIVE OBSERVATION	POTENTIAL IMPACT	RECOMMENDED VERIFICATION
Power continuity	Core switch and file server appear connected without a managed UPS.	Unclean shutdown, equipment interruption, uncertain restart sequence.	Document load, runtime need, graceful shutdown, and quarterly test owner.
Field devices	Two remote laptops lack a documented charging, patching, and readiness process.	Delayed deposition or remote-work setup; inconsistent control state.	Confirm inventory, encryption, update status, spare power, and support path.
Authentication	Shared generic sign-in is used for a workflow; MFA coverage was not demonstrated.	Weak accountability, broader credential exposure, incomplete audit trail.	Move to named identities; verify MFA method, recovery path, and privileged roles.
File transmission	Sensitive attachments may be exchanged through ordinary email or an unmanaged sharing account.	Misdelivery, access that outlives the matter, and incomplete revocation evidence.	Map data flows and approve a protected sharing method with access expiry.
Change control	Endpoint updates occur without an agreed maintenance window or owner.	Poorly timed reboot or postponed security update.	Define rings, deadlines, exceptions, rollback, and maintenance communication.
Network expansion	An undocumented desktop switch was added outside the network diagram.	Unknown path, weak physical control, and harder troubleshooting.	Trace ports, update diagram, confirm capacity, and remove unsupported equipment.

Interpretation rule: “Not verified” is not the same as “absent.” The real engagement requests evidence, records the owner, and separates a confirmed configuration from a missing artifact.

4. RISK AND CONTROL MATRIX

Priorities tied to observable conditions

SECURITY DOMAIN	OBSERVED OR UNVERIFIED CONDITION	RATING	NEXT EVIDENCE / ACTION
Network segmentation	Guest test device can reach services in the same address space as internal systems.	CRITICAL	Validate routing and firewall rules; isolate guest and IoT zones; retest from each segment.
Endpoint privilege & encryption	Standard workflow uses local administrator rights; laptop encryption status is not centrally evidenced.	CRITICAL	Inventory privilege; deploy least privilege; escrow recovery keys; verify encryption reporting.
Identity & access	Shared identity exists and MFA coverage for Microsoft 365 was not demonstrated.	HIGH	Create named accounts; verify MFA and recovery; review administrators and stale sessions.
Backup & recovery	Backup job is reported as active, but an independent protected copy and recent restore evidence were not produced.	CRITICAL	Separate administration; verify retention; perform a measured restore; record RPO/RTO assumptions.
Physical infrastructure	Carrier equipment and network switch are accessible in a shared supply area.	HIGH	Restrict access; label power and ports; record ownership; protect with monitored power.
Policies & records	Current incident, access-review, disposal, and recovery records were not produced during the sample visit.	MODERATE	Confirm which documents apply; assign owners and review triggers; retain evidence of execution.

How the sample ratings work

CRITICAL
Material exposure with a plausible path to broad operational or data impact. Prioritize containment and verification.

HIGH
Significant weakness that can increase incident likelihood or impact. Assign near-term owner and due date.

MODERATE
Control or evidence gap that deserves planned correction and verification.

OBSERVED CONTROL
Evidence was reviewed for this sample snapshot. This is not a certification or guarantee of future effectiveness.

Ratings are triage tools. A real report records confidence, evidence, scope, dependencies, compensating controls, business tolerance, and the organization's decision—not a universal legal conclusion.

5. KEY VULNERABILITY FINDINGS

Evidence, consequence, and a testable next step

01 Guest and internal network reachability — CRITICAL

Condition: From the fictitious lobby guest network, a read-only reachability check indicated internal services in the same routing space. No exploit or credential test was performed.

ILLUSTRATIVE EVIDENCE
Authorized test-device network details, redacted reachability output, current network diagram marked “incomplete,” and photograph of the guest access point label.

Business relevance: A flat path can increase the systems reachable from a compromised or untrusted device. Actual impact depends on firewall rules, service exposure, credentials, endpoint controls, and monitoring.

Verify closure: Place guest and IoT devices in separate zones, allow only required egress, and document retest results from guest, staff, server, voice, and management networks.

02 Routine local-administrator rights and encryption evidence — CRITICAL

Condition: A standard user demonstrated local-administrator capability on one sample workstation. Central evidence of laptop encryption and recovery-key escrow was not available during the visit.

ILLUSTRATIVE EVIDENCE
Redacted account-membership view, device inventory entry, and encryption-status screen displayed by an authorized representative. No passwords or recovery keys are copied into the report.

Business relevance: Excess privilege can expand the effect of malicious or accidental execution. Missing encryption evidence makes lost-device response slower; reportability still depends on the facts and applicable law.

Verify closure: Remove routine privilege, document elevation workflow, confirm encryption for every portable device, escrow keys securely, and test recovery.

03 Named identities and MFA coverage — HIGH

Condition: A shared account supports one workflow, and complete MFA evidence for users, administrators, remote access, and recovery paths was not produced.

ILLUSTRATIVE EVIDENCE
Redacted identity inventory, administrator-role export, and authentication-method summary. Tokens, phone numbers, passwords, codes, and secrets are excluded.

Business relevance: Shared access weakens accountability. Password-only access increases exposure to credential theft and makes session and offboarding response harder.

Verify closure: Replace shared sign-in with named access, enforce appropriate MFA, reduce privileged roles, document emergency access, and review stale sessions.

6. RECOVERY AND PHYSICAL RESILIENCE

04 Backup administration and restoration proof — CRITICAL

Condition: Management reports that scheduled backups run, but the review did not receive evidence of a separately protected copy, administrator separation, or a recent measured restoration.

ILLUSTRATIVE EVIDENCE
Redacted job-status summary and retention view. The sample contains no repository credentials, secret links, recovery keys, client filenames, or backup contents.

Business relevance: A successful job is not proof that required data can be restored within an acceptable time. Credentials shared with production can also expose accessible copies to the same incident.

Verify closure: Define critical data, RPO and RTO assumptions; separate backup administration; protect an independent copy; restore a representative workload; record duration, integrity, owner, and lessons learned.

05 Network equipment, power, and lifecycle records — HIGH

Condition: Core carrier and network equipment is located in a shared supply area, connected without documented power-runtime calculations. A complete asset lifecycle and media-disposition record was not produced.

ILLUSTRATIVE EVIDENCE
Equipment photograph with serial numbers masked, redacted asset list, power-path sketch, and document-request checklist.

Business relevance: Physical access, unplanned power loss, undocumented ownership, and unsupported equipment can lengthen outages and complicate containment. Media sanitization method should match data sensitivity and the selected disposition process.

Verify closure: Restrict and log access, label devices and power, size managed UPS capacity, test graceful shutdown, update inventory, and document sanitization or destruction evidence using the organization's approved standard.

Decision register

DECISION	OWNER	TARGET	CLOSURE EVIDENCE
Isolate guest/IoT access	Technology owner	0–14 days	Approved diagram, rule export, segmented reachability retest
Remove routine admin rights	Technology + practice	0–30 days	Inventory, exception approval, sampled endpoint verification
Enforce named access and MFA	Identity owner	0–30 days	Coverage report, privileged-role review, recovery test
Prove restoration	Data owner	0–30 days	Signed test record with actual duration and integrity checks
Secure network equipment	Facilities + technology	31–60 days	Access control, labels, UPS test, updated asset record

7. STRATEGIC ARCHITECTURE ROADMAP

A phased plan with measurable closure

0–30 DAYS · CONTAIN

Reduce immediate exposure

- Isolate guest and IoT access.
- Remove routine local-administrator rights.
- Verify portable-device encryption and key recovery.
- Enforce named identities and appropriate MFA.
- Protect backup administration and run a measured restore.
- Name incident, insurer, counsel, and communications contacts.

Exit evidence: retest results, identity report, sampled endpoint checks, and restore record.

31–60 DAYS · STABILIZE

Build repeatable operations

- Approve network and data-flow diagrams.
- Define patch rings, deadlines, exceptions, and rollback.
- Document onboarding and offboarding.
- Restrict core-equipment access and test power continuity.
- Review vendor access and required agreements.
- Establish access, backup, and incident review cadence.

Exit evidence: approved records, sampled tickets, owner sign-off, and exception log.

61–90 DAYS · EXERCISE

Test recovery and decisions

- Run a ransomware and BEC tabletop.
- Exercise callback and dual-control workflow.
- Restore a representative system and Microsoft 365 item.
- Review privileged roles and dormant accounts.
- Confirm lifecycle and media-disposition records.
- Reassess residual risk and accepted exceptions.

Exit evidence: after-action record, measured recovery, updated plan, and decision register.

Architecture principles—not product guarantees

Segmentation, least privilege, managed detection, protected backups, identity controls, and documented response provide layers. No architecture, vendor, or monitoring service can promise complete prevention, continuous availability, or regulatory compliance.

Ongoing managed-services scope

A real proposal would define covered users and devices, service hours, alert and response responsibilities, escalation, on-site allowance, patching, backup responsibilities, third-party licensing, exclusions, project work, hardware, data retention, and termination assistance. The MSA and SOW—not this sample—govern service commitments.

Client decision owner · illustrative

Gregory Mathews · Systems Architect · illustrative

8. ILLUSTRATIVE FINANCIAL EXAMPLE

Planning numbers—not a quote

ILLUSTRATIVE INVESTMENT PHASE	EXAMPLE AMOUNT
Phase 1: Remediation & Deployment Example eight-user hardware and labor scope	$4,850.00
Complimentary Systems Audit Free on-site review and customized report	$0.00
Phase 2: Concierge Management & Security (All-Inclusive) Example recurring per-user amount shown in the prior public sample	$225.00 / User / Mo.

Pricing and scope disclaimer

These figures are fictitious, illustrative planning examples only and are not an offer or quote. Final pricing and scope require a written proposal, MSA, and SOW. Hardware, taxes, onboarding, projects, after-hours or on-site work, third-party licenses, device or usage limits, and other exclusions may be priced separately. “All-Inclusive” applies only to the services expressly listed in the signed agreement.

PRIMARY SOURCES USED FOR THE REPORT FRAMEWORK

1. Florida Bar, Rules of Professional Conduct, Rule 4-1.6. floridabar.org · Rules Chapter 4 PDF
2. American Bar Association, Formal Opinion 477R (2017). americanbar.org · Formal Opinion 477R PDF
3. American Land Title Association, Best Practices Framework and Assessment Procedures v4.2. alta.org · Best Practices v4.2 PDF
4. FTC, Safeguards Rule guidance. ftc.gov · Safeguards Rule guidance
5. NIST SP 800-88 Rev. 1, Guidelines for Media Sanitization. csrc.nist.gov · SP 800-88 Rev. 1
6. NIST SP 800-207, Zero Trust Architecture. csrc.nist.gov · SP 800-207
7. FBI Internet Crime Complaint Center, 2025 IC3 Annual Report. ic3.gov · 2025 IC3 Report PDF
8. U.S. Treasury OFAC, Ransomware Advisory. ofac.treasury.gov · Ransomware Advisory PDF

Illustrative / no-advice statement

This document is a marketing sample, not a real assessment, certification, warranty, legal opinion, compliance determination, insurance recommendation, penetration test, or incident-response instruction. Sources are provided for readers to review with qualified advisors. Laws, rules, contracts, insurer requirements, technologies, threats, and source URLs change. Verify current applicability before acting.