EMPIST

MANAGED IT | CYBERSECURITY | CLOUD | WEB DEV

Sample Report

Legal IT Health Assessment

Client: *Sample Law Firm — Chicago, IL*

Prepared By: *EMPIST Managed IT Provider*

Date: *December 10, 2025*

About This Assessment

This IT Health Assessment was conducted by **EMPIST**, a managed IT provider specializing in technology strategy, cybersecurity, and compliance for law firms. The goal of this report is to identify vulnerabilities, evaluate operational efficiency, and benchmark the firm's IT environment against best practices established by the **American Bar Association (ABA)** and the **National Institute of Standards and Technology (NIST).**

Each category has been assigned a score out of 10 based on technical findings, documentation maturity, and adherence to security and compliance frameworks.

Executive Summary

EMPIST performed a comprehensive review of [*Law Firm's*] IT systems, cybersecurity posture, and operational readiness. The assessment covered infrastructure, data protection, compliance & user practices across departments.

The firm maintains a **modern, stable technology foundation**, with cloud-based workloads, managed endpoints, and 24/7 monitoring. However, several weaknesses reduce overall security maturity — particularly incomplete multi-factor authentication (MFA), limited backup validation, and outdated governance documentation.

Overall IT Health Score: 7.2 / 10
Risk Level: *Moderate*

The technology stack is reliable, but the firm's governance and user-based controls need improvement to achieve full compliance and resilience.

Security & Compliance — Score: 6.5 / 10

Cybersecurity controls are implemented inconsistently across departments. MFA is active for most users but excluded from legacy email clients used by senior partners. This leaves critical accounts exposed to credential-theft attacks. Password policies require resets every 90 days but lack enforcement of modern complexity standards.

Endpoint protection is robust, using advanced EDR software on all firm devices, though several outdated agents need reinstallation. The firm currently lacks a **documented incident response plan** and has not performed a formal compliance audit in the past two years.

Recommendation: Expand MFA to all users, formalize an incident response plan, and align password and security policies with ABA and NIST guidelines.

Infrastructure Stability — Score: 8.0 / 10

The firm's infrastructure demonstrates maturity and reliability. Core workloads operate in Microsoft Azure with 99.9% uptime, supported by a redundant firewall configuration and proactive monitoring. Local Wi-Fi performance is excellent, though guest and internal networks share the same VLAN, creating a small but unnecessary exposure.

Recommendation: Segment the guest Wi-Fi, maintain quarterly performance reviews, and continue leveraging cloud redundancy for high availability.

Data Backup & Disaster Recovery — Score: 7.0 / 10

Daily cloud backups are automated and encrypted, but **no restore validation** has been performed since early 2024. Without validation testing, the firm cannot verify recovery reliability in case of ransomware or data loss.

Data retention is currently 30 days — below the threshold recommended for legal hold compliance. The firm has not defined Recovery Time (RTO) or Recovery Point Objectives (RPO), leaving downtime expectations undocumented.

Recommendation: Perform quarterly restore tests, extend retention to 90 days, and formalize RTO/RPO standards in a disaster recovery plan.

Software & Licensing — Score: 7.5 / 10

The software stack is functional and licensed properly. The firm uses iManage Cloud, Timeslips for billing, and Microsoft 365 for productivity. Integration gaps cause redundant data entry, and several users still operate outdated Timeslips versions nearing end-of-support.

Recommendation: Upgrade billing software, unify workflows across platforms, and implement automated version control to maintain consistency.

Endpoint & Mobile Device Management — Score: 8.5 / 10

Workstations are centrally managed through Microsoft Intune, maintaining 97% patch compliance and full disk encryption. Mobile devices, however, remain unmanaged under a Bring-Your-Own-Device policy, limiting the ability to enforce encryption or remote wipes.

Recommendation: Enroll all mobile devices in a Mobile Device Management (MDM) program and update the BYOD policy to enforce security compliance.

Email & Communication Systems — Score: 6.0 / 10

Email is hosted securely through Microsoft Exchange Online but lacks mandatory encryption policies for privileged correspondence. The firm has not conducted phishing simulation training, leaving staff vulnerable to social-engineering attacks.

Recommendation: Enforce automatic encryption for sensitive messages and deploy quarterly phishing awareness campaigns.

Governance, Policy & Training — Score: 6.5 / 10

Governance documentation lags behind current operations. The cybersecurity policy (dated 2021) does not reflect remote work standards or vendor risk management practices. Only 60% of staff completed cybersecurity training in the past year.

Recommendation: Update all IT and security policies, implement recurring quarterly training, and establish a vendor risk review process.

Cost Optimization — Score: 7.0 / 10

Licensing costs can be reduced immediately. Twelve unused Microsoft 365 licenses remain active, costing roughly $2,500 per year. Redundant software subscriptions such as Clio and PracticePanther add unnecessary expense.

Recommendation: Audit software licenses quarterly, consolidate redundant tools, and leverage Azure cold-tier storage for older case files.

Any Questions?

If you have questions on any of the items above, please do not hesitate to reach out for clarification. We are happy to assist you! *Next, we'll review your custom-tailored 12-Month Remediation Roadmap.*

12-Month Remediation Roadmap

Immediate (0-3 Months)

- Enforce MFA firmwide.
- Conduct full disaster recovery test and document results.

Short Term (3-6 Months)

- Implement MDM and update BYOD policy.
- Begin quarterly phishing simulations and training.
- Update all cybersecurity policies with employee acknowledgment.

Long Term (6-12 Months)

- Formalize vendor risk assessment.
- Optimize cloud storage and subscription tiers.
- Establish annual IT governance review.

If executed, these initiatives will raise the firm's IT Health Score from **7.2 to approximately 9.0**, representing a shift from *moderate* to *low risk*.

Conclusion

[*Sample Law Firm*] maintains a strong technology foundation and a clear commitment to cybersecurity. While its infrastructure and endpoint management rank above industry averages, gaps in authentication, governance, and training prevent full compliance. EMPIST recommends addressing these issues proactively to avoid exposure and ensure long-term data integrity.

Schedule Your Law Firm IT Health Check

Identify vulnerabilities before they become liabilities. **Scan the QR code** or visit www.empist.com/law-firm-assessment to schedule a free Law Firm IT Health Check with an EMPIST expert today.

EMPIST fuels businesses with the technology they need to succeed.