RIZE™ TECHNOLOGIES

AI Readiness for Law Firms:
A Five-Part Series for IT Leaders

PART 3 – NETWORK AND COMPUTING INFRASTRUCTURE

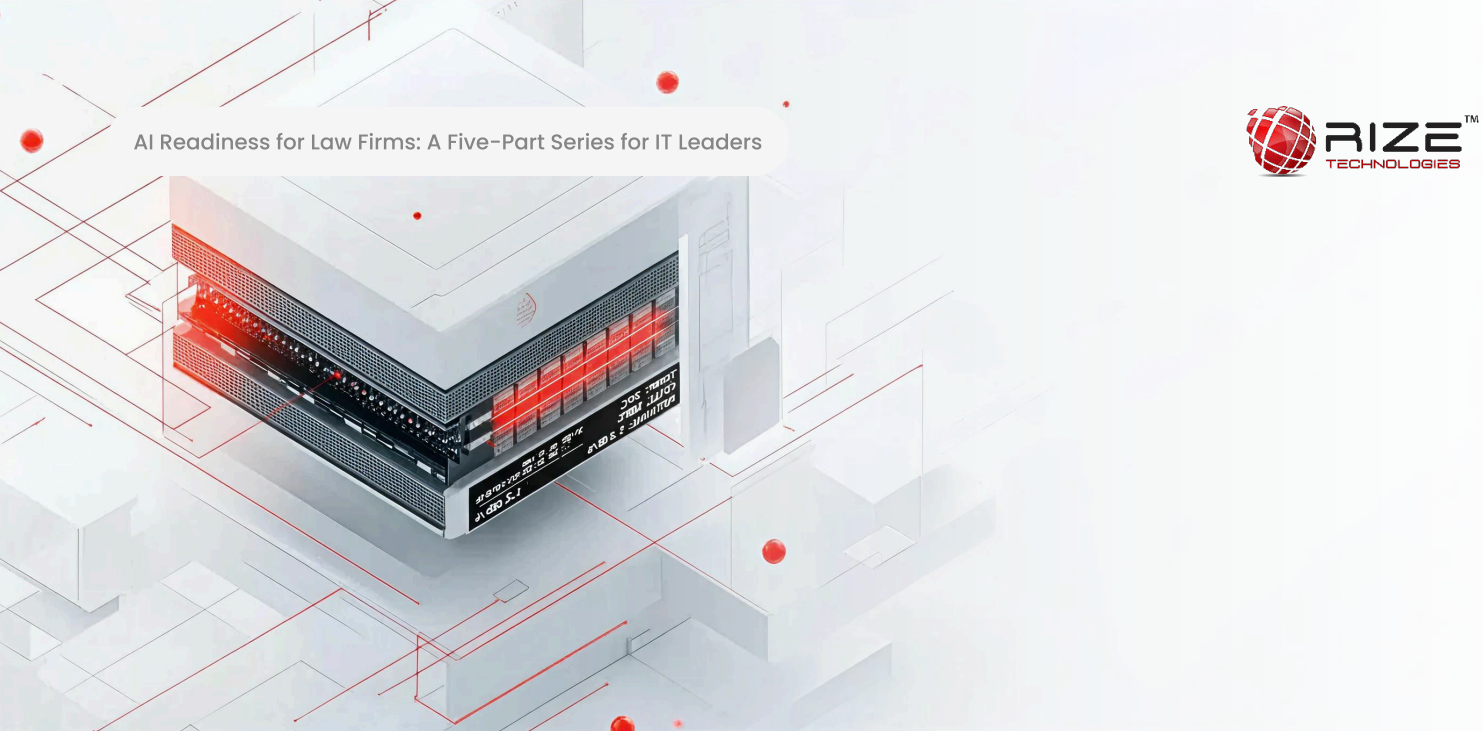
www.rizetechnologies.com

Introduction to Ebook Series

The legal industry stands at an inflection point. Artificial intelligence has moved from theoretical promise to practical reality, with tools that can draft contracts, conduct legal research, analyze discovery documents, and predict case outcomes. For mid-size law firms, the question is no longer whether to adopt AI, but how to do so responsibly, securely, and in compliance with ethical obligations.

While firm leadership focuses on strategic AI adoption and attorneys explore use cases, IT teams face a critical challenge: building the technical foundation that makes safe, effective AI deployment possible. Without proper preparation, firms risk data breaches, ethical violations, regulatory non-compliance, and malpractice exposure.

This five-part series provides IT leaders at mid-size law firms with a practical roadmap for AI readiness, covering the technical, security, and operational considerations essential for successful AI integration. If law firms lack the appropriate IT resources on their staffs, the professional services team at Rize Technologies is available to help them plan and implement a customized roadmap for AI readiness.



Network and Computing Infrastructure

AI tools place different demands on IT infrastructure than traditional legal technology. The document management system that served you well for years might not support the data flows AI requires, and the network capacity that handles daily operations might buckle under AI workloads.

Before you can deploy AI effectively, you need to assess whether your existing infrastructure can handle these new demands—not just technically, but economically. AI workloads often involve different cost structures than traditional software, with cloud computing expenses that scale with usage, bandwidth requirements that may necessitate circuit upgrades, and integration needs that could require middleware or API management platforms you don't currently have.

The infrastructure decisions you make now will either enable or constrain your AI capabilities for years to come, affecting everything – from which AI tools you can realistically deploy, to how quickly they perform, to what your ongoing operational costs will be. Getting infrastructure right requires understanding the specific technical requirements AI imposes, honestly assessing your current capabilities against those requirements, and planning investments that balance performance, security, and cost-effectiveness.

Evaluate Network Capacity

Cloud-based AI platforms require robust internet connectivity. When an attorney uploads a hundred-page contract for AI analysis, that document needs to reach the AI service quickly. When the AI processes thousands of discovery documents, the results need to flow back without delays. Consider the cumulative bandwidth requirements when multiple users access AI tools simultaneously—what works fine for one attorney might overwhelm your connection when twenty attorneys adopt the same tool.

Network latency matters too, particularly for real-time AI applications like transcription services or chatbot interfaces. A two-second delay is barely noticeable for email but creates a terrible user experience for conversational AI. You might need to evaluate whether home internet connections and VPN capacity can support AI tool usage for remote and hybrid workers without performance degradation.

Many firms find they need to increase bandwidth capacity significantly to support AI adoption. This is a good problem to have—**it means attorneys are using the tools**—and planning for high usage prevents frustrating bottlenecks that could undermine adoption. Consider redundant internet connections to ensure AI tool availability even if your primary connection fails.

Plan Computing Resource Requirements

Some AI applications may require significant computing power. You need to determine early on whether you'll host any AI workloads on-premises or rely entirely on cloud services. On-premises AI might require a server infrastructure that can handle computational demands, potentially including GPU-accelerated hardware that could represent a substantial capital investment.

Even if you use cloud-based AI exclusively, local computing resources matter. Some AI features involve client-side processing that requires modern workstations with adequate memory and processing power. That five-year-old laptop might handle traditional legal work fine, but it could struggle with AI-enhanced document review.

Be sure to budget for increased cloud computing costs if using third-party AI platforms, which typically charge based on usage volume. Those costs can escalate quickly as adoption grows. A tool that costs a few hundred dollars during pilot testing might generate thousands in monthly charges when deployed across the firm. Consider hybrid approaches that balance cost, performance, and security requirements—keeping highly sensitive workloads on-premises while leveraging cloud services for general-purpose AI.

Design Integration Architecture

AI tools rarely function in isolation. They need to integrate with your document management system, billing platform, case management software, and other core applications. The technical challenge is making these connections work securely and reliably.

Start by evaluating the API capabilities of your existing systems. Can your document management system export documents to an AI platform, then re-import the enhanced versions? Can AI tools authenticate against your existing identity providers using SAML, OAuth, or similar protocols? Many legacy systems lack modern API capabilities, forcing you to choose between manual workflows that eliminate much of AI's efficiency benefit or expensive system upgrades.

Consider middleware or integration platforms that facilitate connections between AI tools and legacy systems. These platforms can bridge technical gaps, but they also represent another potential point of failure and additional security concerns to manage. Establish API security standards covering authentication, encryption, rate limiting, and monitoring to ensure integrations don't create vulnerabilities.

Document all integration points and data flows meticulously. You'll need this documentation for compliance purposes, but it's equally valuable for troubleshooting when something breaks and for onboarding new IT staff who need to understand how all the pieces fit together.

In Part 4 of this 5-part series, we will look at specific compliance and risk management issues as they relate to AI-readiness. Be sure to download the entire series by visiting the Resources section on **rizetechnologies.com**

About This Guide

This guide was developed based on emerging best practices in legal technology, cybersecurity, and professional responsibility for AI adoption in law firms, but it does not constitute legal, technical, or professional advice. While we always strive to provide accurate information, we make no warranties regarding completeness or accuracy, and we assume no liability for any damages, losses, or consequences arising from your use of or reliance on this information. Each firm is solely responsible for evaluating the applicability of this guidance to their situation and for all decisions and actions taken.

About Rize Technologies

Rize Technologies helps law firms thrive in today's fast-moving, AI-powered world. With more than a decade of experience serving the legal industry, we deliver end-to-end IT solutions that keep firms secure, productive, and ready for what's next. From 24/7 managed IT and cloud services to advanced cybersecurity, data protection, disaster recovery, and AI readiness, every solution is built around the unique needs of each firm. Our white-glove support and proactive approach to IT helps minimize downtime and maximize confidence. Discover how your firm can rise higher at

rizetechnologies.com