iManage
Making knowledge work

TECHNICAL CONSIDERATIONS OF CLOUD ADOPTION

CONTENTS

We instinctively view the transition to the cloud as similar to moving from one house to another. But it's more like migrating from an isolated cabin in the woods to a luxurious penthouse suite in the heart of a thriving metropolis. Your firm gains access to new transportation models, greater interconnectivity, and a multitude of advanced capabilities that increase client satisfaction and profitability.

Building a cloud ecosystem is an ongoing circuitous journey, not a one-time, linear trip to a single destination. Researchers have found that companies that meet their projected timelines when migrating to the cloud are 9 percent more likely to have developed an end-to-end implementation roadmap up front, including the security and compliance framework, rather than funding a series of one-off initiatives.

(**Source:** mckinsey.com)

In this report, legal industry peers and experts share their hard-won advice for successfully transitioning to the cloud. Explore cost and process optimization tips across IT infrastructure, maintenance, data management, security, and other functions, and see how the cloud vendor you partner with can significantly affect the value you receive.

This information will help you:

Create an implementation roadmap to take full advantage of the opportunities that come with cloud migration.

Articulate cloud benefits and set realistic expectations with key decision-makers to gain support and funding for switching to the cloud.

Ensure a holistic transition that supports your firm's short- and long-term business objectives.

KNOW YOUR WHY: TECHNICAL SOURCES OF VALUE

PEER ADVICE

"First understand the foundational reasons for moving to the cloud, then you can justify the move. The question isn't 'should we move?' it's 'when' and 'how' — and how will we manage the risk."

Cloud computing helps law firms meet growing expectations and thrive amid economic uncertainty with a more stable and nimble business model.

When laying out your plan, link your explanations to how cloud adoption can help the firm achieve IT-related business goals such as:

Simplify continuity

Improve network availability

Reduce downtime risk

Enhance data resiliency

Improve disaster recovery

Get user training & support

Get troubleshooting assistance

Get state-of-the-art security

Shift risk to a third party

Secure your firm with advanced protocols

Monitor threats 24/7

Benefit from a predictive maintenance model

Get a dedicated, proactive expert security team

Increase agility

Adapt to ongoing regulatory change

Meet evolving client demands

Support hybrid work

Control compliance with auditable trails

IT decision-makers say their top drivers for cloud investment are to:

Enable disaster recovery and business continuity:
40%

Replace on-premises legacy systems:
39%

Lower the total cost of ownership:
34%

Improve employee productivity:
33%

Increase flexibility to react to changing market conditions:
32%

(**Source:** foundryco.com)

IDENTIFY FIRM IT FOOTPRINT

PEER ADVICE

"Without cloud, you won't be able to use the leading technologies or have the most innovative capabilities."

Include costs and impact stories related to the firm's entire IT landscape in your discussions with executive leaders, not just one area or application. That means you'll need to identify your firm's full IT footprint, including all hardware, software, devices, and users. Then you can create a comprehensive picture of how your firm currently uses technology and where data may be located.

Self-assessment: Overcome firm data challenges

To estimate the potential costs and complexities of your cloud transition, you'll also need to get a handle on your firm's data.

Existing data

- Identify the data in your firm's information ecosystem. (emails, Word and Excel documents, employee data, client data, third-party data, etc.)

- Where is it located? (shared drives, hard drives, data centers, cloud storage, etc.)

- What are the various format types? (PDFs, text, video and audio files, etc.)

Current integrations

- Identify the applications and services integrated with firm data. (Practice management software, document management software, CRM, etc.)

- Do lawyers or staff use any other applications or services you're unaware of? (instant messaging, transcription software, data storage, etc.)

Existing information governance and security practices

- Identify the firm's current data security and privacy procedures.

- What systems are in place to ensure regulatory compliance?

- What measures have been taken to ensure data integrity?

- How consistently have people followed current data governance policies?

A thorough self-assessment will solidify your footing to help you manage stakeholders' expectations as you lay out your migration roadmap.

Many firms have governance-related policies like records retention, email management, and litigation hold policies, yet only 45 percent have a formal information governance policy or strategy, according to the ILTA 2022 Technology Survey. Seventeen percent identify information governance as one of their firms' top three technology issues. (**Source:** .iltanet.org)

Security and privacy measures are increasingly important, as 30 percent of law firms said that a client or potential client asked them to fill out a security questionnaire, according to the 2022 ABA Legal Technology Survey. Larger law firms are more likely to receive this request, with 40 percent of firms with more than 100 lawyers answering in the affirmative, followed by 20 percent of firms with 50-99 lawyers. (**Source:** americanbar.org)

This could be because law firm clients battle the same issues in their businesses. Six hundred CIOs across 18 countries and 14 industries said improving data security is their top investment priority, according to an MIT Technology Review survey. A subset of

"leaders" will increase their data security spending by an average of 101 percent over the next three years and will invest 85 percent more in data governance. (**Source:** databricks.com)
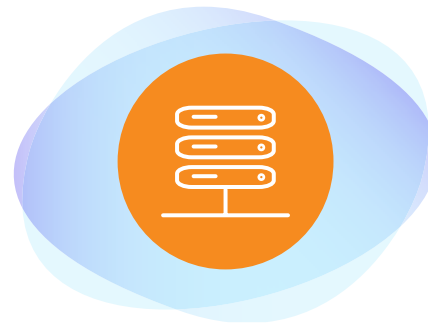
Sizing your data pipeline

Implementing cloud services will likely increase your internet bandwidth needs. Deciding which applications and IP addresses to connect to the cloud (versus a local database) often boils down to which route offers the lowest latency. High latencies can create communication problems among systems that could lead to data loss and performance issues.

Evaluate the status of the cloud-enabled application integrations that must be migrated. Healthy integrations are vital for business continuity and providing a seamless experience for users.

Your cloud transition is also an opportunity for your firm to cull useless and redundant data. You wouldn't need to bring the lawn mower from your country home to a modern city apartment. The same is true of firm data.

PREPARE FOR CLOUD CONVERSATIONS

PEER ADVICE

"Look at the total business impact, then re-rationalize your entire tech landscape and services potential to tell the whole cost management story."

When critical systems are due for upgrades, firm leaders must decide whether to invest in on-premises technology and data centers or transition to cloud solutions. Let's go over some factors to consider in preparing for this moment.

Challenges of maintaining on-premises systems

Explore the investments in hardware, physical space, ongoing maintenance, and troubleshooting required to maintain on-premises solutions.

Busy firms struggle to arrange downtime for maintenance and upgrades. IT teams face the time-consuming daily demands of applying the latest security safeguards, checking for vulnerabilities, patching security bugs, and ensuring only the right people can access secure information.

Cloud providers perform these responsibilities for you, keeping your networks, servers, and systems running securely and at optimum efficiency. Cloud adoption also eliminates the cost of physical server space. Firms have regained entire floors previously dedicated to server farms, greatly reducing their carbon footprint.

Your IT team remains in control, able to quickly add and manage users and increase storage capacity without purchasing additional hardware. Various cloud models offer different levels of customer control.

CLOUD MODELS AND CUSTOMER CONTROL

	Software-as a-Service (SaaS)	Platform-as-a Service (PaaS)	Infrastructure-as-a-Service (IaaS)
Definition	Cloud provider installs and operates the application software in the cloud where users can access the software from cloud clients.	Cloud provider offers a computing platform including OS, programming language execution environment, database, and web server where developers develop and run software.	Cloud provider offers the physical infrastructure including virtual machines, servers, storage, load balancers, network, and datacenter space with power and cooling.
Control	• Provider controls underlying infrastructure • Provider controls the configuration of their application	• Provider controls underlying infrastructure • Customer controls the configuration of their application	• Provider controls the physical assets • Customer controls all other aspects of infrastructure
Examples	• Salesforce • Google Apps • Microsoft Office 365 • Workday	• Microsoft Azure • Google App Engine • Heroku • Force.com	• Amazon Web Services (AWS) • Rackspace • Go-Grid • OpenStack

(**Source:** michaelskenny.com)

The cost of doing nothing: technical debt

Technical debt is the ongoing cost of supporting increasingly obsolete hardware and software. The longer a law firm waits to move to the cloud, the more technical debt it accumulates.

Outdated software is not designed to work with newer hardware and software versions. This can create unpredictable conflicts that lead to system slowdowns and crashes. Older technology also lacks the latest security features, leaving your system vulnerable to attack.

The IT "costs of doing nothing" discussed here are in addition to the substantial failed innovation and lost productivity "costs of doing nothing."

Proactive predictive maintenance

Compare the benefit of the predictive maintenance approach that modern vendors take to the traditional break/fix model seen when IT teams manage on-premises technology.
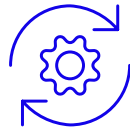
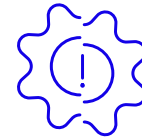### Predictive Maintenance Model

Dedicated professional team

24/7 monitoring of system health and performance

Catch issues before impact

Reduce downtime and frustration

Increase productivity

Traditional Break/ Fix Support Model

Unexpected outages and downtime

Reduced productivity

Frustrated staff

Higher risk of data loss

Limited security and compliance

Inefficiencies due to manual processes

IT time and training investments

Consider that vendor-managed services can include ongoing training for your IT team, lawyers, and staff with additional learning resources.

As cloud adoption progresses, IT teams spend less time sourcing, maintaining, and updating on-premises technologies. Yet, some members may need training to master new cloud deployment models, including integrating data and applications and automating workflows.

IT teams may also be tasked with teaching lawyers and staff to use new features and functions and, especially, awareness training, to prevent data breaches. In 2022, 82 percent of data breaches involved a human element (**Source:** verizon.com), such as skill-based errors and phishing scams, with an average data breach cost of $4.35 million. (**Source:** ibm.com)

CONSIDER YOUR IT BUDGET

PEER ADVICE
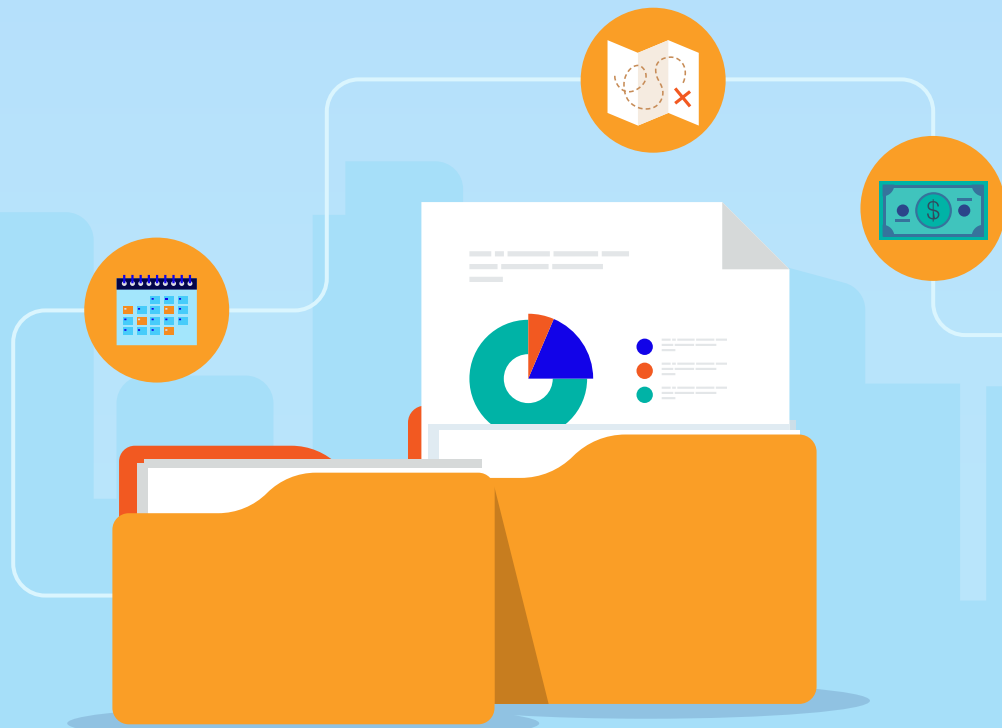
"Timing is critical. Consider your tech roadmap. And don't move to the cloud only for cost savings. Additional value is in the innovation premium."

Moving too quickly can lead to missed opportunities. Take time to reap all the benefits of the latest cloud features and functions.

Develop a multiyear cloud adoption strategy

There is no single strategy when it comes to making the move to the cloud. Every firm works with their provider to agree on a schedule that meets their needs. Am Law 50 firm Baker Botts migrated several key applications, including document and email management, for more than 1,500 legal professionals in just 90 days, but the move was only one part of its larger cloud strategy. Netflix spent seven years moving all of its IT systems to the cloud (**Source:** ciodive.com).

IT costs will decrease over time as your firm:

- Accommodates changing business needs without buying additional hardware or software
- Deprecates on-premises technologies as they are slowly phased out

- Eases the IT team's maintenance burdens for on-premises technology
- Starts seeing savings from pay-as-you-go pricing

What will you migrate first?

"In 2023 and 2024, firms will continue to focus on upgrading their financial management, document management, knowledge management and client relationship management systems and implementing Microsoft 365. We can expect to see cloud-based technology being the top priority, along with continued investment in information security/cybersecurity and data centers." (**Source:** 2023 Citi Hildebrandt Client Advisory)

Nearly 74 percent of law firms have already or will transfer their email security solutions to the cloud in the next 12 months, according to ILTA's 2022 Technology

EXPERT TIP

Migrating your email systems to Microsoft Exchange first can be beneficial as lawyers and staff won't need to learn a new system from scratch and can take advantage of an existing knowledge base that includes tutorials, forums, and support services.

Survey, up from 67 percent in 2021. Solutions that firms increasingly migrated to the cloud in 2022, in addition to email, included payroll (67 percent), document management systems (59 percent), and human resources (56 percent). Time and billing cloud use for larger firms is at 38 percent, and two-thirds of firms surveyed indicated they will move time and billing to the cloud in the next 12 months. (**Source:** iltanet.org)

CapEx and OpEx cloud computing

When transitioning to the cloud, it is important to understand the financial implications of CapEx and OpEx expenses. The impact of each will overlap as your cloud migration progresses through different phases.
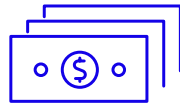
CapEx (capital expenditure)

Large upfront cash outlays

Typically longer-term investments

Includes recurring lifetime costs

Examples: servers, software licenses, network equipment, security tools

The annual cost to own and manage software applications can be up to four times the cost of initial purchase.
(**Source:** forbes.com)

OpEx (operating expenditure)

Lower upfront cash outlays

Typically shorter-term investments

Recurring cost structure

Examples: pay-as-you-go software subscriptions, managed services

Spread your IT budget over more applications and free up cash to contribute to other areas.

Remember the future

Forecast for growth to ensure your IT purchases can support firm operations long term.

For example, if a firm purchases a large number of servers upfront, then discovers they need fewer than initially anticipated, it may be stuck paying for unneeded servers. On the other hand, firms that purchase cloud services on an as-needed basis can easily scale up or down as circumstances dictate.

Failing to account for future growth can lead to:

- An insufficient budget for future needs
- Costly upgrades or replacements
- A flat CapEx that does not reflect the firm's actual state

LEVERAGE VENDOR SOURCES OF VALUE

PEER ADVICE

"Vendor transparency is critical. Ask questions and make sure your vendor can demonstrate security and scalability."

Help stakeholders understand how heavily the firm's cloud partner influences the success of your cloud transition.

The shared responsibility matrix

Be able to explain the shared responsibility matrix, which ensures both parties know their roles and responsibilities, particularly regarding security and compliance efforts.

Generally, the higher the service level you sign up for, the more responsibility you can expect the vendor to take on, including:

- Managing and maintaining the physical infrastructure, including servers, storage, networking, and virtualization

- Ensuring infrastructure is secure and compliant with applicable laws and regulations

- Ensuring data and applications are secure and compliant with applicable laws and regulations, including:
  - configuring access controls
  - encrypting data at rest and in transit
  - 24/7 monitoring for suspicious activity

- Data backup and recovery, disaster recovery planning, and incident response

- Regularly maintaining and patching systems and applications

- Following best practices for application development and integrations

When discussing the shared responsibility matrix, you can ensure your firm takes all necessary steps to protect its data and applications in the cloud.

Regulatory and compliance services

Factor in the potential ROI of meeting regulatory, compliance, and privacy requirements with a cloud system.

On-premises efforts can never match the capabilities of cloud vendors that invest millions of dollars in security every year. Cloud computing also makes it easy to store data in multiple locations to meet data residency, disaster recovery, and data segregation requirements. Twelve organizations using Azure regulatory and compliance services experienced:

- 465 percent return on investment
- 35 percent reduction in costs of compliance-related penalties
- Easier regulatory and IT compliance environment audits
- Built-in compliance with industry standards like HIPAA, HITECH, and SEC regulations

(**Source:** microsoft.com)

Contractual value

Account for how SLAs and contract clauses that dictate indemnifications, data breach notifications, and liability limitations can affect the long-term value of your vendor relationship.

Contracts often represent significant investments for both parties. Service level agreements (SLAs) in contracts typically include details such as uptime guarantees, response times, availability of support personnel, and other performance metrics. They ensure you receive the quality of service you pay for and may include penalties for not meeting the agreed-upon terms.

Insurance and liability

Consider how the vendor's enhanced cloud security can reduce other costs and risks such as:

- **Insurance.** Insurance companies may charge higher premiums for on-premises technology due to the increased risk of a data breach or other security incident. The same risk exists in the cloud, but insurance costs may be less because cloud vendors provide higher levels of more advanced security measures.
  - In the US, cyber insurance costs rose more than 100 percent year-on-year by late 2021 and increased around 48 percent year-on-year by the third quarter of 2022. (**Source:** tech.co)
- **Liability.** Without the vendor protections of your cloud system, your law firm may be held liable for damages caused by a data breach or other security incident. This can bring serious negative financial and reputational consequences.

Demand full transparency from vendors

Since 2020, cyberattacks on law firms have multiplied, exposing the personal data of hundreds of thousands of Americans and costing law firms thousands of dollars. (**Source:** law.com) Top cloud providers can provide a security policy detailing comprehensive security measures that include:

Security certifications

Certifications prove that a vendor adheres to a set of standards and best practices that ensure measures are up-to-date and effective. Your cloud vendor must hold specific security certifications for your law firm to comply with various regulations and industry standards, potentially including but not limited to:

- ISO 27001
- SOC 2
- CSA STAR
- PCI-DSS

Zero Trust architecture for controlled access

Zero Trust architecture assumes that all users, devices, and networks are untrusted and must be verified before they can access data. Controlled access is necessary to protect client and firm data. Look for:

- Military-grade authentication that requires users to prove their identity before they can access the data
- Two-factor authentication that adds an extra layer of security by requiring users to provide two pieces of evidence that they are who they say they are
- Authorizations that determine levels of access for each user
- Advanced encryption that ensures only authorized users can view the data
- Restricted access to the vendor's facility with surveillance and alarms

Disaster prevention

Even vendors with Zero Trust architecture must still monitor, detect, and respond to malicious threats and intrusion attempts. Further disaster prevention involves best practices such as:

- Penetration testing
- Methods to prevent data co-mingling in a multi-tenant environment
- Virtualization or containerization for additional security layers
- Regular data backup and recovery procedures to protect against data loss and accidental deletion.

EXPERT TIP

Vendors should also list sub-servicers and whether they are committed to the same standards.

MODERNIZE YOUR NETWORK

PEER ADVICE

" Upgrading to the cloud offers a unique opportunity to modernize the firm's network architecture to better serve practice needs."

Upgrading frees your firm from legacy systems that don't work well together or are duplicative and difficult to manage. Real-time visibility aids in spotting and solving issues before impact. These and other benefits improve network availability and reduce downtime risk — a critical advantage when **more than 60 percent of outages result in at least $100,000 in total losses.** (**Source:** businesswire.com)

The cloud is a powerful tool for law firms looking to optimize their IT infrastructure and data management. By partnering with the right cloud vendor, you can save time and money while gaining access to the latest technologies and best practices in the industry.

Developing a comprehensive cloud strategy will help you show firm leaders how they'll reap the rewards of cloud migration and enjoy greater overall efficiency, scalability, and cost savings.

Get started expanding your opportunities by making the cloud the new home for your firm's data. **Visit the Migrating to the Cloud page on our website** today for next steps or to learn more about the technical considerations of cloud adoption.

LEARN MORE ❯

iManage

Making knowledge work

twitter.com/imageinc

youtube.com/imanage

linkedin.com/company/imanage

www.imanage.com