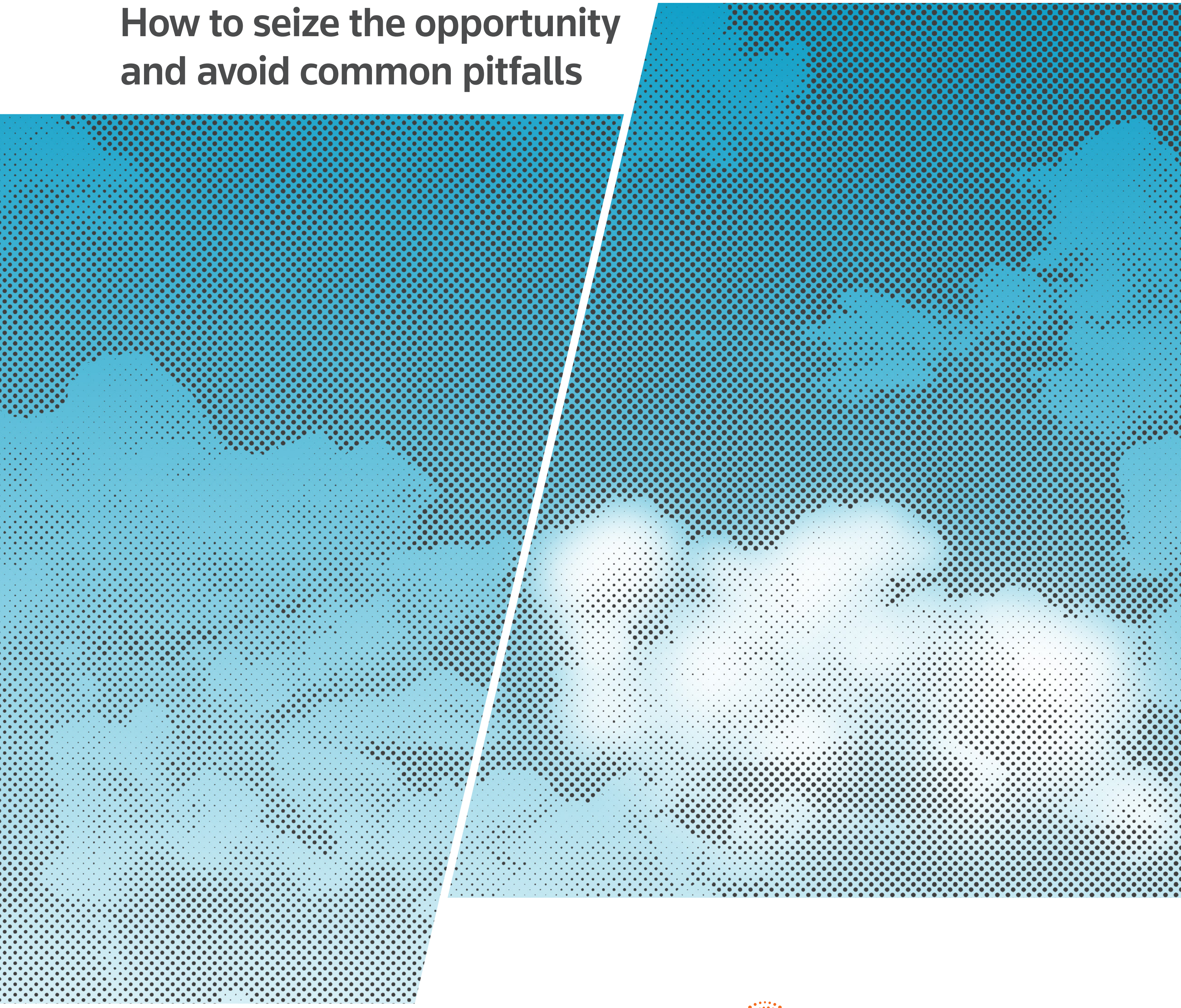
Navigating the cloud with confidence:

How to seize the opportunity and avoid common pitfalls



THOMSON REUTERS®

Introduction

When it comes to law firms thinking about moving into the cloud, it's now a question of when and not if. Embracing the cloud is a logical and important step on the journey of technological advancement: something that few firms can ignore as they seek to deliver the best service to clients and facilitate modern ways of working for their staff.

Clients who are accustomed to conducting their business online and working remotely with colleagues expect their external legal advisers to deploy collaborative and transparent solutions that provide real-time access to information and insights. They are impressed when their lawyers have immediate, accurate answers to questions thanks to having data at their fingertips rather than having to go away and check before responding. When firms demonstrate this kind of proactive as well as responsive approach, they are likely to deliver more high-quality work and greater client value, which should ultimately enable them to win more work.

In order to do all this, law firms need enabling technologies, and that means adopting smart solutions that are hosted in the cloud. It's time for large and mid-sized law firms to start or accelerate the process of modernizing the way they deliver legal services to keep up with the pace of change.

Choosing a cloud-based enterprise financial and practice management system such as Thomson Reuters® 3E brings many benefits in terms of improved business performance, greater agility and scalability, and enhanced security. However, many misconceptions remain around the best approach, and there are several pitfalls to watch out for.

In this guide, we delve into four key questions that explore several important issues and areas of opportunity for cloud migration. Armed with this know-how, firms will be well-placed to make informed decisions; navigate a sensible, smooth, and secure transition with confidence; and ensure they stay at the forefront of technological developments, both now and going forward.

1. How secure is public cloud versus private cloud?

For growing numbers of large and mid-sized law firms, data security concerns are one of the major drivers of the shift into the cloud. With this in mind, the next critical question is whether to invest in a public or a private cloud solution.

With public cloud, a third-party provider allows businesses to use their cloud infrastructure. The data hosted for each business is kept separate and secure, and only your users are able to access your data and services. The cloud services provider is responsible for data security and system maintenance.

In a private cloud solution, a standalone internal or corporate cloud is created specifically for your firm, connected over the internet or via a private network. Private clouds can be hosted on your own premises or in a third-party data center. However, as the infrastructure is not shared, you are responsible for data security and system maintenance.

While the latter may sound attractive from a control perspective, the word "private" should not be confused with "secure." In fact, 3E is deployed in the Microsoft® Azure public cloud platform and provides a handful of security advantages.

Microsoft spends $5 billion a year on cybersecurity — a level of investment no law firm could dream to match for a standalone system. Public providers have the economies of scale to invest in the best and to test, test, test their software's resilience. Given the scale, complexity, and rapidly changing nature of the potential threats out there, and the types of sensitive and confidential data law firms hold, that's a critical consideration when looking at the cloud.

Together with Microsoft, Thomson Reuters has developed a multi-layered security approach for 3E to maximize how financial, practice, and client data is safeguarded in the public cloud:

i. **Physical security**
Microsoft's data centers around the world are designed to withstand direct physical attacks and natural disasters. They are reinforced with measures such as fortified perimeters, biometric identification tools, and multi-factor authentication access requirements.

ii. **Infrastructure security**
Microsoft deploys AI technology plus thousands of analysts to detect and neutralize potential threats. Secure communication with application modules is assured via the use of best-in-class standards-based identity and access management.

iii. **Application security**
Controlling who can access a firm's software applications and validating their identities are core factors in a secure cloud platform. 3E supports verification components like multi-factor authentication to make it harder for hackers to gain entry and Single Sign On (SSO) so that staff can access multiple applications with a single user identity, bolstering security while making access more seamless. On top, Thomson Reuters has built robust privileged access management capabilities for the needs of law firms into the architecture of 3E.

iv. **Data security**
3E uses a single-tenant data strategy to protect business-critical information and confidential client data. This isolates individual firm data, storing it separately from the data of other law firms in a way which complies with national and international data protection and privacy regulations. End-to-end encryption, verified by appropriate certificates and keys, adds another layer of defense.

2. What is the difference between a "lift and shift" approach and going "cloud native," and why does it matter?

Beyond choosing whether to go public or private with your cloud, it's also important to decide whether to take a "lift and shift" approach to adoption, or to take the fully "cloud native" option. Here we explain what the difference is, and the pros and cons of each.

What is lift and shift?

A lift and shift approach requires minimal effort to move existing on-premise applications to the cloud — something which benefits the vendor more than the end user: you. The software provider literally just picks it up and drops it into the cloud, where it runs unchanged. This is the quickest way to move the application to the cloud because no modernization, no new technology, no updating of identity standards or security practices, and no code changes or training on new technology are involved.

What is cloud native?

A cloud native approach means implementing new and specially-designed architecture, tools, and technologies that are built to operate in the cloud and therefore take full advantage of the cloud computing model. They are intended to be agile, reliable, and scalable, delivering highly resilient and flexible applications that adapt to meet law firms' — and clients' — needs. And because they are constantly being updated and upgraded by the vendor, the burden of maintenance and security on law firms is eliminated.

A lift and shift approach may seem like the easiest option short-term, and it will deliver some cloud benefits in the form of reduced infrastructure and hardware costs. However, because everything continues just as it did before, this approach fails to deliver all the advantages of a true cloud platform and may not offer a fit-for-purpose solution long-term. With lift and shift:

- Agility and scalability are diminished because systems have not been modernized and they lack flexibility to grow with your firm.
- The burden of software maintenance and security remains with you, the customer, rather than being borne by the provider, incurring continued costs.
- Resilience and performance are undermined because solutions are not automatically updated with the latest upgrades — which can also make them slower, more inefficient, and less easy to use.
- Migration failures can occur if the application's requirements are not accurately translated to the corresponding features on the cloud. Any inherent problems in the system design will also be carried across, creating potential for ongoing, recurring problems.

A cloud native approach takes longer and is more labor intensive for law firms to implement, but the payoff comes later with the lower total cost of ownership and more flexible, responsive infrastructure. By embracing modern cloud architecture, you get faster and easier integration of new technologies, safer upgrades, and better security practices with no delay or disruption to firm operations.

Ultimately, law firms that opt to lift and shift their financial management systems into the cloud may find themselves going cloud native in the end in order to achieve the full benefits.

One way to manage the transition is to take a modular approach, migrating some of your software solutions to the cloud before others. A gradual approach allows firms to control costs while balancing the process against internal appetite for change. Moving practice and financial management systems to the cloud is a good place to start.

3. What's wrong with building modern security on legacy technology?

Modern security practices, especially those in the cloud, are radically different than in the past. You can no longer just turn on Windows Authentication in your web server and be done. There's a widely held belief that it's possible to simply bolt modern security methods onto legacy systems and that's good enough. However, this is neither advisable nor practical.

On-premises legacy systems are typically built on a "trust but verify" model, which gives users widespread access to files and data once they are on the network, relying on their physical location or their IP address as proof they are allowed to be in the system. But this approach does not afford the best protection, because once a user (or a hacker) is in, there are no boundaries on what they can do. Using VPNs (virtual private networks) for remote workers does not solve the problem, either.

Best practice today dictates that Zero Trust principles should apply. This means that system designers should assume that a breach will take place and seek to minimize the fallout. Building a Zero Trust architecture in the cloud should include granting "least privilege" to users — effectively restricting access to what a user needs and no more. Data should also be modularized so users will need specific permissions to access particular types of data. In this way, if a data breach occurs, the damage is contained, protecting confidential information and limiting firms' liability.

Unfortunately, these modern security measures cannot simply be added into existing systems. Instead, they must be re-architected and integrated across the entire application environment. Exhaustive testing, analysis, and verification will then be required. There's no easy fix, but it's far better to implement a full cloud system with Zero Trust built in.

In the ABA 2021 Legal Technology Survey Report, 25% of respondents reported that their firms had experienced a data breach at some time. In the following year's 2022 survey, respondents were asked if their firms ever experienced a security breach and 27% answered in the affirmative[1].

[1] ABA 2022 Survey: americanbar.org/groups/law_practice/publications/techreport/2022/cybersecurity/

4. Is the cloud secure enough for legal data specifically?

The arguments outlined above around cloud security are compelling. But given the nature of their work and the types of confidential, sensitive, and privileged information they hold, it's natural to wonder whether the cloud is really an appropriate place for law firms to house their data.

As we have seen, hosting data in the public cloud and using a cloud native approach with Zero Trust principles baked in are key ways to enhance security for businesses in general. But for law firms specifically, there are a number of additional considerations.

First and foremost, it's important to use vendors whose services are specially designed for the legal market. As such, they should comply with all the relevant legal and regulatory data protection requirements that apply to law firms. They must have robust privacy practices in place and the terms of the contract must state that the law firm retains ownership and control of the data.

Providers also need to offer suitable archive and backup services, so that you can retrieve documents and data whenever you need to, whatever happens. Cloud-hosting services must be able to support and integrate with the tech solutions your firm is using for seamless data transfer.

It's worth asking questions of potential vendors to check all these issues, as well as analyzing exactly what security provisions they provide to make sure they deliver the level of service and security you need and expect. For instance, providers may vary in the level of Zero Trust principles they have built into their cloud services, and as a result, some may be more robust than others.

3E is backed by Thomson Reuters, the standard for best-in-class solutions for the legal industry for more than 150 years. By investing heavily in its own expertise, working closely with law firms the world over, and partnering over many years with Microsoft, you can be sure that 3E has been designed with the legal and security needs and obligations of your law firm in mind.

Privacy and the regulatory landscape

It's a myth that there are certain instances in the legal profession in which putting information into the cloud breaches privacy laws and regulations. In fact, law firms can store any type of data in the cloud, as long as it is being held securely in accordance with regulatory requirements.

But given that regulations are changing all the time and can vary around the world, this is no small task. So it's vital to carry out thorough due diligence on potential providers, including looking at their track record on breaches, investigations, and any regulatory sanctions. Trust, experience, and reputation matter when choosing a cloud provider.

The transformative power of 3E in the cloud: A case study

The world's most innovative large and mid-sized law firms trust 3E to run their mission-critical financial and practice management operations. Dallas-based law firm Shearman & Sterling chose 3E Cloud to provide better client service, according to Meredith Williams-Range, Chief Knowledge and Client Value Officer.

"[3E] allows our people not to focus on maintaining multiple systems of record, but instead lets our people focus on how we bring the best value to both the partnership and clients."

When choosing a vendor, it was important for Shearman & Sterling firm leadership to make sure the system architecture worked with their current structure and could scale up or down. Also critical in their decision to purchase 3E was the security and integration of internal and external data in order to make informed decisions.

"3E data, blended with other systems' data, helps us understand how much it costs us to generate a document, for example," said Glenn LaForce, Global Director of Knowledge and Research. "Then we can more accurately price alternative fee arrangements — that will lead to greater profitability."

Jeff Saper, Global Director of Enterprise Architecture and Delivery Services, added, "The fact that 3E is built on Azure and Microsoft spends billions of dollars on security alone means I don't have to worry about the updates, the upgrades, or the security patching. We can focus on productivity."

> *□□For us, 3E is the smart choice. It's the right time, the right system, and the right partnership.□□*
>
> **-Meredith Williams-Range, Chief Knowledge and Client Value Officer**

Conclusion

The legal industry is ripe with opportunity for innovators, and there's huge pressure to go above and beyond client expectations. Firms must be poised to deliver.

There's no doubt that law firms today recognize that cloud technology can help them sharpen their competitive edge, enabling them to enhance service delivery to their clients while increasing the efficiency and robustness of their operations.

It's about being more agile, leveraging new technologies, boosting data security, increasing resilience, and lowering operating costs. No wonder 93% of law firms see cloud technology as part of their future, according to ILTA's 2021 Technology Survey.

Moving to the cloud is a big step and there is a lot to bear in mind to make the transition smooth and successful, meeting the firm's and users' needs, client expectations, and regulatory requirements. Issues such as security, reliability, adaptability, compliance, and ROI loom large.

Not all cloud solutions are created equal. So it's vital to understand and evaluate the different options to find the one that is right for your firm. 3E delivers performance you can see and value clients will feel, and it's trusted by law firms everywhere.

Learn more about 3E and why so many firms have chosen it as their cloud-based financial management solution, or request a demo today.

2023

THOMSON REUTERS®