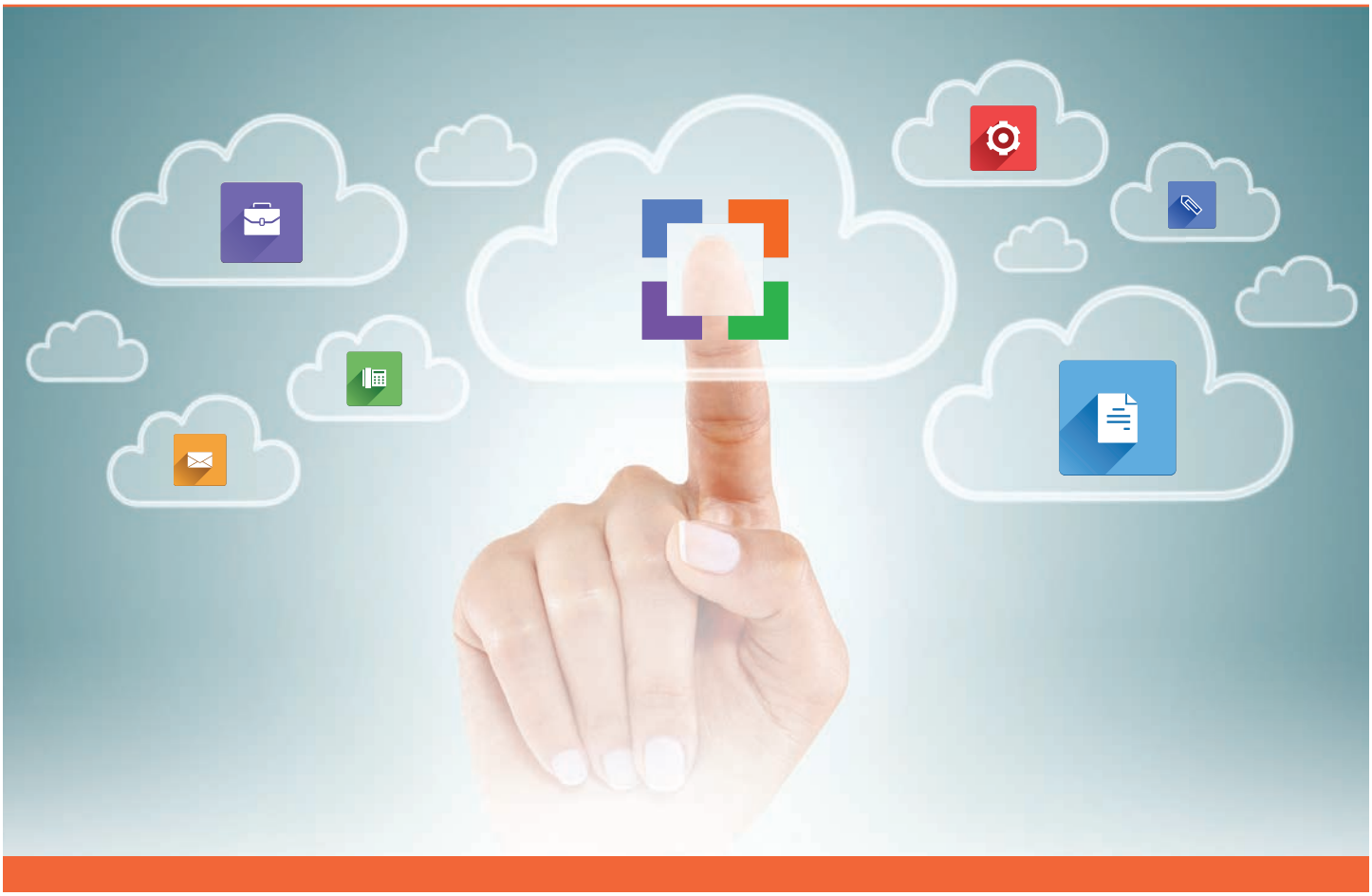

A CHECKLIST
FOR LAW FIRMS

CLOUD COMPUTING DUE DILIGENCE

Cloud service providers are springing up daily. Some are big, and some are small . . . making your decision to know where to start more difficult.

This is a must read—as a law firm, your stakes are high.

uptime
LEGAL SYSTEMS

EVERY DAY, FORWARD-THINKING LAW FIRMS

eliminate on-site servers and move their legal practice applications and data to the cloud. Those that remain have cloud computing on their radar, considering that it is hard to ignore. The benefits of cloud computing for law firms include:

- A Private Cloud is a proven, trusted, and secure solution for an internet connected practice
- The ability to work productively anywhere in the world, on any device
- Significant cost reduction through elimination of onsite servers and related IT expenses

In fact, there are numerous competitive business advantages cloud computing affords your practice, with little to no change to the way it now operates.

However, there are a number of serious issues to consider before selecting a cloud service provider. The legal profession has unique security, ethical, and compliance requirements to factor into the selection of a cloud provider. Law firms also have specialized software and mobility considerations that few cloud service providers are equipped to handle. Many cloud service providers—including otherwise capable and reputable providers—simply do not understand legal practice, issues surrounding privileged client information, nor do they have experience working with legal-specific software.

The consequences of choosing the wrong provider can be devastating to a law firm. Generally, the major risks a law firm assumes when moving to an ill-suited cloud service provider fall into these two categories:

SECURITY-RELATED RISKS:

- Exposure of confidential client data
- Violation of attorney-client privilege
- Breach of ethical obligations
- Damage to firm's reputation

PRODUCTIVITY-RELATED RISKS:

- Stability issues and downtime
- Workflow interruption
- Lack of support for legal software
- Lack of integration with peripherals

THIS CHECKLIST OUTLINES THE MOST

important requirements that your current (or prospective) cloud service provider must meet to minimize your risk when moving to the cloud. These requirements reduce the risk of both security breaches as well as downtime and system/workflow interruptions.

1. ESTABLISHED AND REPUTABLE PROVIDER

New cloud service providers are popping up every day. Small local IT firms are rebranding themselves as cloud providers to avoid losing clients. It is imperative you ensure that your selected provider is established and reputable: Make certain business and legal authorities such as the Inc. 5000 list, the American Bar Association, and one or more state bar associations have recognized them. A high-risk provider is one that is unknown to the larger legal technology community, or only known in a single city or region. Risks include slow response times, inexperienced technical support, system downtime, or worse, the provider simply going out of business.

2. EXCLUSIVE LEGAL FOCUS

Numerous Cloud Service Providers offer services to any business or industry. While they may be technically proficient, they typically do not have the experience to understand attorney's ethical obligations and compliance requirements, and likely will not have deep experience in legal software used by law firms. This means you should narrow your list to Cloud Service Providers that exclusively services the legal industry. Some generalist Cloud Service Providers may even claim to specialize in legal, though upon closer review, you will often find that legal is just one of many industries they serve.

3. CLOUD-FIRST COMPANY

In recent years, many companies not in the business of cloud computing have lost market share to the cloud, and often react by spinning up a cloud offering. This group includes software companies, local IT companies, and telecom/telephone companies.

These companies are desperately trying to stay relevant and/or stem the loss of business to the cloud. They almost certainly lack an independent perspective, the infrastructure, and software acumen to provide a reliable, dependable, and secure cloud platform.

A GOOD CLOUD SERVICE PROVIDER SHOULD BE ABLE TO POINT TO AT LEAST 100 LAW FIRM CLIENTS, AND ALSO OFFER YOU A RICH, DIVERSE LIST OF REFERENCES

4. DATA STORED IN THE US

Every bar association agrees that all client and confidential data should be stored within the continental United States.

Surprisingly, the locality of where your data is stored is ambiguous or simply not defined by many cloud service providers. Microsoft's own Office 365 states that your data may be stored or backed up to countries outside the US. This is one more reason to use a cloud service provider that is legal-centric, and only services the legal industry.

If your firm's data is stored or backed up to a country outside of the US, it can create a host of potential ethical issues.

5. DATA OWNERSHIP

Do not assume that data you store in the cloud belongs exclusively to you, even if the provider is well known and reputable. For example, in 2012, Google Drive came under fire for claiming the rights to anything a user uploaded, *in perpetuity*.

Once you decide to use a cloud provider, make certain that the fine print includes unambiguous, perpetual ownership of any data you store on their cloud.

6. LEGAL SOFTWARE SUPPORT

There are plenty of companies willing to host your legal software. But generalist Cloud Service Providers simply cannot be relied upon to provide best practices to support your practice management, document management, and billing/accounting software.

The Cloud Service Provider you select will not merely host the software your firm relies upon, it should also provide first-call support for your applications, and apply security and application patches and updates as necessary, so that you can focus on practicing law.

Ideally, your Cloud Service Provider will have a strong working relationship with major legal software publishers so they have rapid access to the software company's team when necessary.

7. BACKUPS AND DISASTER RECOVERY

Make certain you understand your Cloud Service Provider's backup and disaster recovery system. A dependable, robust provider will have at least two independent systems for backup and recovery.

The backup strategy should include a file-and-folder backup (so you and your staff can quickly recover deleted files) and a "bare-metal" recovery system (so the provider can perform a complete system restore in the event of a disaster).

Ideally, the Cloud Service Provider has an option to synchronize your data in the cloud back to a server or device at your site. This incremental layer of security gives you additional backup protection and a viable alternative should your Internet connectivity go offline for an extended period.

8. INFRASTRUCTURE AND DATA CENTER

Verify the provider has a best-in-class data center and server infrastructure. This ensures both data security and reliability. These considerations include:

- SSAE16 AUDITED
  Also called Statement on Standards for Attestation Engagements 16, SSAE16 is a regulation created by the Auditing Standards Board (ASB) for defining and updating how service companies report on compliance controls. Demand evidence that the data center is SSAE16 audited annually.

- EQUIPMENT OWNERSHIP
  Ensure the provider actually *owns* the server equipment. Some smaller Cloud Service Providers (especially local IT companies) simply rent servers or space from large public cloud providers such as Microsoft Azure or Amazon Web Services. This creates a significant problem as it complicates data ownership and seriously limits the cloud service provider's ability to control and support the infrastructure, making them essentially intermediaries.

- WORLD-CLASS DATA CENTER
  Ensure the data center has standard "top- tier" provisions including multiple upstream internet providers, redundant power sources including backup generators, fire and flood preventions systems, 24x7 closed-circuit video surveillance, and physical access restrictions. The ideal Cloud Service Provider will offer a tour of their data center facilities.

ADDITIONAL CONSIDERATIONS

Be Wary of Conflicts of Interest. Beware of a cloud provider whose core business is selling its own proprietary legal software, as there will likely be a conflict if you use and host other software applications.

Clearly understand what the provider will do if served a subpoena. Read the service contract carefully and question the process that occurs in the event of a subpoena of data and records.

Confirm that your service provider will notify you if your records have been requested, or if they receive any request for information pertaining to your firm.

Many cloud service providers, especially those without legal experience, are unprepared, and have no formal process for dealing with a subpoena.

SUMMARY

Cloud service providers are springing up daily. Some are big, and some are small... making your decision to know where to start more difficult. As a law firm, your stakes are high.

If you narrow your search to cloud-first, legal-first companies, and systematically analyze potential providers against this checklist, you can be confident you will find a solution with minimal risk, so you can add value to your firm . . . and practice better.

TO LEARN MORE

For more information on cloud computing for the legal industry and best practices when moving your law firm to the cloud, please contact us:

Uptime Legal Systems
7500 Flying Cloud Drive
Suite 640
Eden Prairie, MN 55344

888-878-4632
info@uptimeLEGAL.com
uptimeLEGAL.com

uptime LEGAL SYSTEMS
Practice Better®