Table of contents

3  Momentum toward cloud computing
4  What is the cloud?
5  Why move to the cloud?
6    Business and IT agility
6    Risk reduction
7    Collaboration and client service
7  Business risks, technical limitations, and other considerations
7    Connectivity
7    Latency and network bandwidth
8  Security
8    Data sovereignty
9  HP Autonomy cloud content management solutions for law firms and corporate legal departments
10 Key advantages of WorkSite in the Cloud
11    Architecture
11  Conclusion
11  About HP Autonomy
12  WorkSite in the Cloud: Technical Supplement
Managing legal content in the cloud

Without a doubt, the cloud is transforming the way people access and use computing resources. Organizations of all sizes are seeking to upgrade their application capabilities and the agility of their IT infrastructure without the capital expense and overhead of on-premise data centers. For law firms and corporate legal departments, the dynamics of a cloud delivery approach can be especially attractive—making it possible to increase staff productivity, deliver better client service, and improve business agility while reducing expense.

Momentum toward cloud computing

Gartner estimates that the global market for public cloud services will reach $131 billion in 2013—including nearly $20 billion for Software as a Service (SaaS), a model often used for cloud-based enterprise applications—and will continue to grow at a compound annual growth rate (CAGR) of 17.7% through 2016.¹ From small businesses looking for high-end IT capabilities without the capital expense and overhead, to large enterprises motivated by greater agility and cost efficiency, organizations are moving quickly to embrace on-demand, pay-as-you-go cloud computing.

While the cost savings for a cloud approach can be substantial, it’s the benefits of productivity, agility, and risk reduction that law firms and corporate legal departments find most compelling. Facilitating collaboration beyond the firewall, a cloud solution can also improve attorney productivity and client service. More broadly, the cloud can help address an all-too-familiar challenge for legal IT: solving pressing IT needs in law firms with limited IT resources, or in the legal departments of organizations whose IT departments are focused elsewhere, as is so often the case. For example, the firm or corporate legal department can use a cloud solution to support a disaster recovery environment without the high hardware costs of a traditional business continuity implementation—a common initial use case.

Many in the legal field already see cloud computing as the inevitable future of legal IT. In a recent survey by Legal IT Professionals, 57% of respondents expected cloud computing to overtake on-premise computing within five years, and 81% expected it to happen within a decade. Only 16% did not expect it to happen at all.²

A new survey of 28 large law firms CIOs shows an even more dramatic shift in specific application areas that are acknowledged to have cloud advantages:

<table>
<thead>
<tr>
<th></th>
<th>Email spam</th>
<th>Email DR</th>
<th>Email archive</th>
<th>Archive</th>
<th>Time &amp; bill</th>
<th>DMS primary</th>
<th>DMS (DR)</th>
<th>File sync</th>
</tr>
</thead>
<tbody>
<tr>
<td>Today</td>
<td>82%</td>
<td>50%</td>
<td>21%</td>
<td>11%</td>
<td>4%</td>
<td>7%</td>
<td>7%</td>
<td>36%</td>
</tr>
<tr>
<td>In 3 years</td>
<td>75%</td>
<td>64%</td>
<td>54%</td>
<td>57%</td>
<td>45%</td>
<td>50%</td>
<td>86%</td>
<td>68%</td>
</tr>
</tbody>
</table>

Rapid adoption expected

Source: 2013 LegalIT Leadership Summit sponsored by HP Autonomy, June 2013

² Legal IT Professionals, Global Cloud Survey Report 2012.
Still, many firms and corporate legal departments have concerns about adopting cloud services:
• How will the security of client data be assured?
• How can availability and reliability be assured for mission-critical applications?
• What legal liabilities might the firm be exposed to?

Issues like these trigger mixed feelings about moving key applications to the cloud. Respondents to the Legal IT Professionals survey were split on the question, with 44.5% in favor and 46.3% opposed. Given the potential benefits, gaining insight into the substance of these concerns is a top priority for law firms and corporate legal departments.¹

This paper aims to help legal IT professionals clarify what cloud computing can mean for their organizations. Following a definition of the cloud, we explore the benefits and limitations of cloud technologies, and then address the concerns of firms and corporate legal departments. Our intention is to help you make your own decision about whether, and how, the cloud can make sense for your organization. We also introduce HP Autonomy’s cloud solutions for legal and discuss the advantages and trade-offs of deploying Autonomy WorkSite and other solution components in the cloud.

What is the cloud?

While “the cloud” can mean a variety of different things, in strict IT terms it refers to resources such as networks, services, storage, applications, and services that are delivered over the Internet and are:
• On-demand – Always available and delivered whenever and wherever they are needed
• Metered – Service providers can bill customers based on actual usage, instead of the flat-rate approach of licensed on-premise software
• Elastic – Rapid, seamless, and cost-efficient scalability is available to support large numbers of users as the customer’s needs grow

---

¹ Legal IT Professionals, Global Cloud Survey Report 2012.
Cloud deployments come in several varieties. These include:

- **Public cloud** – Cloud services are delivered to the consumer on shared IT infrastructure by a third-party service provider. To ensure security, most public cloud solutions offer secure multi-tenancy to isolate access to client data and configurations from each other.

- **Private cloud** – Cloud services are delivered to a single organization on dedicated IT infrastructure. Private cloud deployments can have many of the same elastic and service capabilities as a public cloud.

- **Hybrid cloud** – Both corporate and third-party infrastructure work in tandem to deliver services. Organizations can move specific types of workloads from an internal data center to a public cloud provider, as needed, to meet various needs such as making internal documents more easily available to users beyond the firewall, adding burst capacity on-demand for short-term storage or processing needs, or increasing fault tolerance. IT can typically manage access and security across both public and private elements of the hybrid cloud from a single console.

For all the hype around the cloud, it is not a single remedy for all that ails modern IT. Rather, it is an approach to delivering software that can solve a specific type of problem. Organizations should evaluate the cloud in the context of the real problems they need to address and decide for themselves whether a cloud solution is right for them.

---

**Engagement management in the cloud**

**Profile**
- Professional services/accounting firm
- 800+ users, 32 U.S. Offices

**Challenge**
- Provide a unified, engagement-centric view of content, communication, and workflows for audit and tax practices

**Solution**
- WorkSite for document and email management, coupled with Autonomy Process Automation (APA) to manage the engagement lifecycle
- Processes automated:
  - New client onboarding
  - New engagement opening
  - Specific transactional engagements
- Solution was fully integrated with the practice management system of the firm

**Benefits**
- Improved organizational efficiency through end-to-end process automation
- Comprehensive information management across the matter lifecycle to support collaboration and tracking
- Increased focus on client service by automating routine administrative processes

---

**Why move to the cloud?**

People often think of the cloud first in terms of the financial advantages of its cost model. Typically, a cloud provider offers its services for a monthly subscription fee based on users, features, provisioning, storage, or transactions. This eliminates initial capital expenses such as servers, operating system, and other infrastructure licenses, making it much easier for IT to build a business case and start delivering services to users. Because the monthly subscription scales with use, the organization pays only for what is used, instead of having to over-provision to accommodate uncertain future needs or risk getting caught short. Cloud services also reduce administrative costs, since operating system, database, and other server-side upgrades are handled by the provider and covered by the same subscription.

In a comparison of its private cloud hosting versus traditional on-premise deployment for a typical 100-seat configuration, HP Autonomy estimates that customers can improve capital utilization by upwards of 75% while reducing IT administrative costs on the order of 50% per year.
But the adoption of a cloud solution should be motivated by more than just cost. In some ways, the decision reflects a deeper understanding of the organization’s core competency. This is especially true in the legal field. Many small and mid-size law firms, and most corporate legal departments, do not consider IT and application administration to be a core competency, especially when compared with their primary focus on practicing law. Even large law firms may not want to take on the overhead of a live backup data center or the administrative requirements of a secure file-sharing solution.

Beyond financial considerations, the main drivers for cloud adoption generally fall under three headings:

1. Business and IT agility
2. Risk reduction
3. Collaboration and client service

Business and IT agility
Organizations that adopt cloud applications can respond more quickly to changing workloads and business requirements. With back-end infrastructure provisioned by the provider, you can measure time-to-value for cloud-based applications in weeks, not months. The provider can perform configuration and customization rapidly, with small changes applied in a matter of days, allowing a high level of fine-tuning to maximize the application’s value. This relieves the internal IT team from having to maintain infrastructure, allowing them to focus on solving business needs and servicing users.

Because you can upgrade cloud applications centrally, a provider can add new features continuously and make them available immediately so customers can take advantage of the latest innovations. Cloud services also benefit from the wisdom of “crowdsourcing” where the cloud provider monitors applications centrally and measures user patterns to provide insight into how to use various features and the adoption of new changes. This informs better product design and more relevant enhancements, and upgrades can become more frequent and effective.

Risk reduction
While the actual risk reduction benefits can vary widely from provider to provider, in principle a well-run cloud operation can offer legal organizations several advantages over in-house applications. One is reliability: Most cloud providers offer contractually committed uptime levels. Organizations can also architect cloud solutions to provide disaster recovery through a secondary infrastructure in a geographically discrete data center that becomes operational in the event of a catastrophic failure in the primary data center.

Although security is frequently cited as a concern by cloud computing skeptics, the reality is that how data is managed matters more than who is managing it. Leading cloud providers have adopted strict data security and information governance practices, adhering to standards including SAS 70, ISO 27001, and ISO 27002. For example, all HP Autonomy data centers are audited against the SSAE 16 attestation standard to ensure appropriate internal...
controls to maintain the security of customer data. This is as high or higher than the level of protection provided in many internal data centers, as it often works out to be more cost effective to have this level of security provisioned by the cloud provider than trying to adopt these standards internally.

Collaboration and client service
In addition to its benefits for IT, cloud computing has much to offer for users as well. Securely accessible over the public Internet by authorized users, cloud services can greatly simplify collaboration across the firewall for remote and mobile employees as well as third parties such as clients, co-counsel, investigators, discovery providers, contractors, and other business partners. Attorneys that are able to access resources from anywhere can also respond more quickly and effectively to client needs whenever they arise, and can better integrate work and life to achieve better balance.

Business risks, technical limitations, and other considerations
While the hype around the cloud promises simple, carefree adoption and use, there are several things organizations need to pay close attention to—including both technical limitations and legal implications.

Connectivity
The availability of a cloud solution depends greatly on your connection to the cloud data center. The reliability of your WAN service should be one of the first things you consider in evaluating a cloud approach. If you are entirely dependent on a single Internet connection and it goes down, your users will promptly lose access to their cloud applications and data. To mitigate this possibility, many companies secure dual Internet connections through different ISPs in key locations.

Latency and network bandwidth
Several network-related factors can affect the performance of a cloud application. In terms of the WAN, the distance between your gateway and the cloud data center can contribute to latency. This effect can be mitigated by maintaining multiple data centers in different geographies—a strategy used by most leading cloud providers—as well as by WAN acceleration technologies. More advanced cloud providers also have the ability to perform service updates incrementally, and synchronize customer data based on actual changes, to reduce the amount of data that needs to travel to the cloud.

Within the organization, the speed and bandwidth allocated to the application in the LAN can also affect performance. Mission-critical data related to the cloud service can end up competing for network resources with VoIP data, video downloads, email, and other network traffic. It’s important to allocate sufficient priority in your network infrastructure to ensure proper performance.
Security
While a cloud service can be just as secure as an on-premise solution, as discussed above, the reality can be very different. Inadequate security technologies or practices on the provider’s end can lead to leakage of sensitive data with catastrophic consequences—and all too many public cloud services fall far short of the enterprise security standard. In fact, the rampant adoption of unmanaged cloud services by rogue users contributes greatly to the urgency of providing a more secure alternative—one that combines the convenience of a consumer service with a higher level of security and control. In the Legal IT Professionals survey, 18% of respondents freely admitted to using public cloud services like Gmail and Dropbox in their work without the knowledge or approval of their firm. As the report notes, “it is also possible that less tech-savvy, iPad-owning users are using applications such as Dropbox without acknowledging that this is in fact the public cloud.”

To mitigate this risk, business processes, workflow, and security must be well integrated into the solution to safeguard access, data security, and integrity.

Data sovereignty
Law firms and corporate legal departments must also consider data privacy regulations and the implications of the legal domains in which cloud-based content is stored. For example:

- Many European countries do not allow certain types of data, such as personal information, to leave the European Union territories, or even the country.
- European clients may also be concerned about data stored within U.S. data centers, which under the U.S. Patriot Act can be acquired and inspected by U.S. law enforcement and intelligence agencies in contradiction to Europe’s strong data protection laws.
- Even the ability of support functions, such as systems administrators to access the data, may be deemed to constitute a transfer to the country from which the support is being provided. This can greatly complicate cross-border access to data residing in cloud data centers within these countries.
- Many Asia/Pacific countries such as Japan, Korea, and India have drafted similar data protection and privacy regulations.

Most global cloud providers offer mitigation strategies to address these concerns including hosting their data centers in multiple countries and restricting sensitive content to country-resident data centers. However, both the cloud provider and the “client” have responsibilities under most privacy regulatory regimes to ensure that personal data transferred across borders is properly safeguarded and processed. The primary responsibility to ensure that any such transfers are properly authorized by the law rests with the business client, as they are the party that owns and controls the personal and business sensitive data. Contact HP Autonomy for more information on this topic.
HP Autonomy cloud content management solutions for law firms and corporate legal departments

For organizations deciding to adopt a cloud strategy, HP Autonomy offers a comprehensive, but flexible set of cloud content management solutions to meet various needs of law firms and corporate legal departments. Autonomy WorkSite in the Cloud is designed for both primary and backup use cases:

- **Primary environment** – Organizations use WorkSite in the Cloud as their principal work platform. This approach is best for organizations that are interested in achieving the cloud benefits discussed above, or who do not consider the hosting of WorkSite to be one of their core competencies. In the primary deployment scenario, WorkSite is offered as a private cloud service that can be configured to interoperate with existing on-premise systems such as Microsoft Exchange servers. Alternatively, WorkSite can be deployed in a hybrid cloud configuration to interoperate with other hosted cloud services such as Microsoft Exchange 365.

- **Backup environment** – Organizations use an on-premise installation of WorkSite as their primary work platform, with a hosted implementation of WorkSite in the Cloud acting as a live disaster recovery (DR) site. This scenario is well-suited to firms and corporate legal departments of any size that want to implement a DR site without the up-front and ongoing capital expenses of maintaining a physical site, or that want their DR site to be a discrete distance from their primary site to avoid local risk factors such as hurricanes or earthquakes. For many firms and corporate legal departments, this use case offers an opportunity to gain experience with the solution to pave the way to broader adoption in a primary environment.

The diagram above shows different WorkSite cloud configurations supported by HP Autonomy.
Autonomy WorkSite 9.0 has been optimized for online delivery to provide consistent, high-quality service:

- Desktop components have been re-architected to fully utilize secure HTTPS in all communications between client and server.
- HTTPS communication between client and server is compressed to optimize throughput and minimize the effects of network latency.
- OffSite is an integral part of WorkSite in the Cloud, providing desktop file caching and seamless offline access. This further serves to minimize the impact of network latency.
- Enhanced web-based administration tools allow full management from the browser.

**Key advantages of WorkSite in the Cloud**

WorkSite in the Cloud is tailored to meet the specific requirements of law firms and corporate legal departments.

- **Rich Microsoft Office integration** – Going beyond simple Cloud Open and Cloud Save features, WorkSite in the Cloud integrates deeply with the Office suite to enable features such as Word Compare, Mail Merge, and Object Linking and Embedding (OLE). Extensive macro support includes the ability to use the WorkSite API for custom development.

- **Server-side integration with Microsoft Exchange 365** – Out-of-the-box integration with Office 365 mailboxes supports the growing number of organizations taking advantage of the cloud-based email service where the enterprise mailboxes are hosted in the cloud.

- **Seamless offline experience** – OffSite ensures that professionals can remain productive even when a network connection is not available. The module also enables content caching, which is critical for users connecting from overseas or over cellular broadband connections as it alleviates the bandwidth challenge when working with sizable content.

- **Best-of-breed search technology** – Like all HP Autonomy cloud solutions, WorkSite in the Cloud is powered by Autonomy IDOL (Intelligent Data Operating Layer), which provides concept-based, full-text searching capability. IDOL can process more than 1,000 different document formats, and is highly scalable to provide fast search speeds even for repositories of hundreds of millions of objects.

- **Rich ecosystem of third-party integrations** – WorkSite in the Cloud offers the same integrations as an on-premise WorkSite implementation through the legal software packages created by the HP Autonomy partner ecosystem. These include document comparison, document automation such as footer macros, metadata cleaning tools, and many more. The solution also fully supports the three-tier API over HTTPS, enabling third-party administration tools such as workspace generation.
• **Centralized facilitation of the global matter file** – All WorkSite libraries for an organization may be located and provisioned from one place to enable firms to embrace the single-instance matter more easily and eliminate multiple libraries containing ‘parts of the matter.’

**Architecture**

WorkSite in the Cloud provides economies of scale well beyond the possibilities of a traditional on-premise solution. A shared, secure underlying architecture for both database and storage reduces your cost while providing the ability to scale services up and down on demand. A single tenant, clustered application server infrastructure supports customer-specific instances of licensed applications. To ensure reliability, you can use Internet connectivity to the cloud or deploy dedicated connectivity as you choose, and your own devices (such as WAN acceleration devices) are supported within the HP Autonomy data center. SAN storage minimizes risk, providing high availability and increased security, primary and redundant data centers with real-time content replication, and an entire infrastructure built for high availability with no single point of failure.

**Conclusion**

The cloud-computing model is especially appropriate for law firms and corporate legal departments that prefer to focus their attention on the core competency of practicing law. While considerable uncertainty remains about the risks and benefits of the cloud among legal professionals, a well-architected cloud solution can be at least as secure and reliable as an on-premise application, while offering unique advantages in cost, agility, and productivity. With Autonomy WorkSite in the Cloud, organizations can combine the benefits of cloud computing with the proven functionality of the industry’s definitive document and email management solution.

Optimized for the web and architected to provide enterprise-class security, WorkSite in the Cloud helps legal professionals access the tools they need from anywhere with reliable high performance. Law firms and corporate legal departments can put best-of-breed technology to work for their clients—while remaining focused on their legal practice, not technology issues.

**About HP Autonomy**

HP Autonomy is a global leader in software that processes human information, or unstructured data, including social media, email, video, audio, text and web pages, etc. Autonomy’s powerful management and analytic tools for structured information together with its ability to extract meaning in real time from all forms of information, regardless of format, is a powerful tool for companies seeking to get the most out of their data. Autonomy’s product portfolio helps power companies through enterprise search analytics, business process management and OEM operations. Autonomy also offers information governance solutions in areas such as eDiscovery, content management and compliance, as well as marketing solutions that help companies grow revenue, such as web content management, online marketing optimization and rich media management.

Please visit [autonomy.com](http://autonomy.com) to find out more.
WorkSite in the Cloud: Technical Supplement

Data center security
The data center that hosts Worksite in the Cloud is audited against the SSAE 16 SOC 2 Type II standard. The SOC 2 Type II report focuses on non-financial reporting controls as they relate to the security, availability, processing integrity, confidentiality, and privacy of the system.

Physical controls
Extensive physical controls in the data center include:
- **Perimeter** – blast walls, gates
- **Exterior walls** – steel-reinforced concrete, reinforced and alarmed doors
- **Man-traps** – biometric authentication, 24/7 security officers, fixed cameras
- **Access Control** – metal walls, cameras, intercoms, biometric readers
- **Compartmented spaces** – data center rack space is individually locked, protected, and monitored
- **Positive access control** – identity verified by security officer before access is granted
- **Surveillance** – fixed and PTZ cameras, video recording

Internal controls and procedures
HP Autonomy’s information security policy and standards are based upon global security standards ISO 27001 and 27002. ISO 27002 provides best practice recommendations on information security management for use by those who are responsible for initiating, implementing or maintaining Information Security Management Systems (ISMS). All HP Autonomy security policies and related standards are built on a foundation of confidentiality, integrity and availability. Key principles include:
- **Accountability** – the process of tracing activities to a responsible source.
- **Audibility** – the use of informational markers and messages that can be reviewed to determine how effectively the security policy is enforced.
- **Least privilege** – the principle that security architectures shall be designed so that each system entity is granted the minimum system resources and authorizations needed to do its work. Need-to-know is related to least privilege and extends to knowledge of processes and information.
- **Separation of duties** – the practice of dividing the steps in a system function among different individuals. Properly implemented, this can provide the necessary checks and balances to mitigate against fraud, errors, and omissions.

Application security
HP Autonomy takes many steps at both the infrastructure and application levels to ensure the security and integrity of the data that customers entrust to us.

Infrastructure
- Third-party penetration testing
- Active log monitoring
- Vulnerability management
- Active firewall monitoring
- Web application scanning
- Malware monitoring

Application
- Encryption of data in rest and in motion
- Customer-specific dedicated storage LUNs with customers specific access control
- Customer-specific databases with customer-specific access control
- Customer-specific virtual instances of applications
- Customer data hosted on customer-specific LUNs—never commingled
- Separate service accounts for each customer database and storage location

These factors ensure the highest level of security and integrity for customer data. In the deployed cloud architecture, customer data can never be commingled and it is never possible for one customer to gain access to another customer’s data.