Brochure

Best practices for cloud-based information governance

Autonomy Cloud solutions

Information governance in the cloud

Key advantages to cloud computing

Cloud computing alleviates adoption complexity, reduces IT overhead, and enables you to drive information governance programs directly from the cloud.

- Increase the predictability of costs through consumption-based pricing
- Scale up or down as information governance, and litigation and compliance burdens change
- Achieve ROI faster by having less to build, maintain, and upgrade
- Increase agility to meet business needs
- Deploy gradually to cloud-based information governance by module or department, allowing for hybrid deployments that mix cloud and on-premise capabilities, depending on unique business requirements and without disrupting users
- Simplify and optimize the IT environment by having less to own and operate
- Ensure data integrity and disaster recovery with sophisticated, automated data protection capabilities
- Allow organizations to drive a range of information governance capabilities directly from the cloud

"By 2020 more than a third of the Digital Universe will either live in or pass through the cloud."

—IDC

The modern organization faces greater IT challenges today than it did just five years ago. Expanding access methods include networks, the cloud, laptops, and a range of mobile devices such as smartphones and tablets. Data is diverse: in different languages, various formats including structured and unstructured—and information is generated from locations around the globe.

The exponential growth of data and increased use of rich media and multi-channel communications are driving new and sophisticated regulations. These regulations focus on interaction-based models, which signal the need for systems that not only monitor and capture data in all its forms, but understand its meaning. This need is driving lawyers, compliance professionals, records managers, and technologists to reconsider how interactions are managed—whether between employees, with customers, or among a range of constituents.

The challenge of how best to meet these diverse demands, while achieving optimal performance, often comes down to how to execute at the technology infrastructure level. When meeting these challenges, the direction chosen by a CIO, CISO, or manager can set the course for how an organization manages information.

More varied deployment choices are also changing the information landscape as more companies opt for cloud-based solutions to meet their most stringent privacy and security requirements for archiving, eDiscovery, compliance, records management, and data protection. Cloud computing can provide new levels of security, collaboration, agility, speed, and cost savings for businesses of any size and type. Shifting from on-premise software to an on-demand, cloud-based solution can enable you to lower costs and mitigate risk, while allowing you to defensibly enforce comprehensive information governance (IG) enterprise wide.

HP Autonomy's private cloud offers you a range of capabilities to address new demands in information management. We can help you to reduce IT complexity and provide you with capabilities to drive governance programs directly from the cloud with unmatched security. Unlike generic cloud deployments, Autonomy's cloud-based suite of Meaning Based Governance solutions enable organizations to understand the meaning of structured and unstructured data while enforcing defensible governance in archiving, eDiscovery, compliance, records management, and data protection.

Evaluating cloud deployment

Cloud computing uses the web server facilities of a third-party provider on the Internet (the "cloud") to store, deploy, and run applications, and it represents one of the hottest areas of technology today. When considering a move to the cloud, it is wise to research the costs, risks, and benefits of public and private deployments to determine which route best meets your unique legal, regulatory, and business needs. Private clouds can offer a range of capabilities that public clouds cannot address, such as the ability to replicate critical security and operational requirements, ensure data segregation between clients, and enable adherence to regulatory requirements on behalf of customers. Straightforward disaster recovery and streamlined backup are also common offerings, though the extent to which these services can be provided may vary greatly between private and public cloud services in terms of how the capabilities integrate with the software solutions being used by the organization.

Additionally, with storage and server needs in the hands of a third-party, an organization essentially shifts the burden from in-house IT to their provider. This allows internal IT departments to focus on business-critical tasks without having to increase costs in manpower and training. Specifically in the area of eDiscovery, systemized, repeatable, and defensible processes are key to reducing costs and risks, and therefore any new solution must provide these capabilities to ensure the organization operates efficiently and in compliance with regulations. With the latest capabilities available through cloud computing, the advantages afforded through an on-premise deployment—cost, ease of set up, scalability, security, and ROI—can not only be matched, but also exceeded in the cloud.

This paper defines cloud computing, explains how a private cloud benefits organizations in achieving their information governance goals, and offers best practices for secure cloud adoption.

Public and private clouds

For enterprise, legal, and government organizations, the option to deploy cloud computing overwhelmingly indicates the use of secure, private cloud services. These organizations cannot risk exchanging critical security capabilities and overall system flexibility for any potential savings offered by a public cloud service.

Public cloud – Public cloud computing is typically the option reserved for traditional mainstream consumers, most commonly found in sites such as Facebook and Twitter, as well as through sources such as Amazon Web Services, Google, and Microsoft. Public clouds are not typically recommended for information management and governance because the processes used for security, data segmentation, and data disposition are not sufficient. While a public cloud's lower cost structure is attractive, the lower levels of security, accessibility, and scalability make it unfeasible for most companies.

Private cloud – The term "private cloud" refers to an on-demand, scalable environment that is either a technology subset of an organization's current technology infrastructure or an isolated network environment hosted by a provider. Private clouds offer the highest levels of security, scalability, accessibility, and flexibility and are the option used by the world's leading organizations. Private clouds provide the greatest benefit when a specific solution is just one of many hosted applications leveraging the same corpus of data.

HP Autonomy has over 50 petabytes of data under management, with data and eDiscovery processing centers that are Safe Harbor-certified, span the globe and are audited to Statement of Accounting Standard number 70 (SAS 70 Type II). The data centers are under 24/7 surveillance and protected by biometrically controlled doors, exterior and interior CCTV cameras, glass break and motion detectors, alarm panels, audible alarms, lights and silent alarms.

To enable deployment flexibility, HP Autonomy customers can leverage a hybrid model that allows a gradual transition to cloud-based information governance by module or department, depending on unique business requirements and without disrupting users.

Better management of resources

The ability to remain agile when business disruptions arise is vital to sound information management practices. In the case of mergers and acquisitions, organizations may need to quickly bring on board massive data stores. Using an on-premise solution could make the process prohibitive, requiring extensive time and resources to deploy additional infrastructure elements. Cloud computing offers benefits for governance and meeting business obligations during regular and peak times to ensure information is properly retained, preserved, and disposed of according to legal, regulatory, and business requirements. Cloud-based solutions can help you to retire unused applications or licensed databases entirely, eliminating the licensure cost but allowing you to holding the information if needed in the future, but at a greatly reduced cost.

Information governance solutions in the cloud

At the core of any discussion on information governance in the cloud is an understanding of the definition of information governance which is "a process that ensures the effective and efficient use of information in enabling an organization to achieve its goals."[1] Information governance encompasses every phase of the Electronic Discovery Reference Model (EDRM) from archiving and legal hold, to identification, preservation, early case assessment, review, and production. It is often the central driver behind compliance, records management, and data protection programs.

Cloud computing offers organizations a way to drastically reduce infrastructure costs, and add a level of predictably by allowing cloud expenses to be budgeted at least in the near term. As organizations seek to streamline IT and enforce governance best practices, the cloud offers benefits from risk mitigation to more secure access and reduced IT complexity.

Electronic discovery in the cloud

In the area of eDiscovery, having on-demand capacity to grow as needed allows you to pay only for what you consume as part of an operational budget, rather than making considerable investments in infrastructure. Cloud-based eDiscovery also streamlines the exchange of information between inside and outside counsel. Organizations can give outside counsel access to data, eliminating risky handoff methods, such as physical shipments. Managing all information in a central cloud location dramatically reduces the risk of spoliation between eDiscovery phases.

Autonomy eDiscovery solutions unify identification, collection, early case assessment, document review, and production in a single offering that leverages Meaning Based Coding, advanced analytics, and policy-based, automated workflow. The solution operates seamlessly with Autonomy Legal Hold and a range of components from Autonomy's Information Governance solutions to deliver a complete end-to-end solution.

HP Autonomy's cloud-based technology and services are used by top law firms and legal service providers globally as a trusted choice for addressing complex litigation challenges. Autonomy data centers manage more than 50 petabytes of data, with 30 billion messages stored, six billion pages in active litigation review, and three million files processed per hour. Autonomy offers the most scalable and secure hosted eDiscovery offering in the market in scalability, speed, and security.

[1] For a definition of information governance, see the ARMA International Maturity Model for Information Governance, at http://www.arma.org/docs/bookstore/theprinciplesmaturitymodel.pdf (last accessed 5/7/13).

Archiving and records management in the cloud

More organizations are shifting away from legacy archiving models that operate as standalone, isolated installations or permanent content storage centers maintained regardless of business need. In records management, burdening users with classification duties, exchanging physical files, or managing records in disparate silos offer inefficient, risk-laden options. The modern demands of managing diverse electronic data require intelligent archiving and records management solutions as part of a pan-enterprise information risk management platform, and the cloud enables organizations to achieve these goals.

The role of the next generation archive is to serve as an anchor to mission critical solutions for eDiscovery, records management, risk mitigation, and information management.

Autonomy Consolidated Archive (ACA) – Greater awareness about the pitfalls of legacy archiving methods are changing the mindset that archives should exist as standalone, isolated, or permanent storage installations. Organizations can now deploy cloud-based archives that are closely integrated with eDiscovery, records management, and information management solutions.

Autonomy uniquely unlocks the value of archived content by understanding the meaning of human information. With ACA, you can drive a range of programs directly from the cloud on archived data, including advanced analytics, defensible legal compliance, and information governance best practices. ACA offers Anywhere Access for end users, providing valuable knowledge to all devices (laptops, smartphones, tablets) from the archive, including folders, and synching all changes made by the user.

With ACA, the lifecycle of any organizational asset can be governed based on the meaning of its content. ACA provides a scalable, unified, multichannel content archive that controls and manages electronically stored information including audio, video, and social media.

Application Information Optimizer – Database archiving software helps control the growth of mission-critical databases by automating the migration or retirement of data while preserving its business value and meeting the desired access requirements. Data can be relocated to a separate, online database for fast, transparent access, or to standards-based XML or CSV documents for long-term retention based on retention rules and policies that align with business needs. Application Information Optimizer includes an integrated set of components that facilitate design, deployment, and ongoing management of archiving processes throughout the lifecycle of applications and data. In addition, they deliver capabilities that address different levels of application complexity, data volumes, and archive access requirements.

Autonomy records management solutions – With the number of organizational records reaching into the tens to hundreds of millions, relying on individuals to manually classify each record is no longer feasible. To effectively streamline and automate the process of capturing, classifying, and declaring records according to a defined policy, a solution that addresses legal and end user requirements and supports current business processes is needed. Available as a cloud-based deployment, HP TRIM offers scalable enterprise document and records management that simplifies the capture, lifecycle management, security, and access to information. TRIM helps organizations comply with governance and regulatory obligations and provide authoritative records of business activities, while ensuring transparent, policy-based lifetime management of all information, regardless of format, system, or source. TRIM provides knowledge about information that helps organizations know what to retain, what is needed for legal and operational purposes, and what is ready for disposition.

To accommodate unique business requirements, organizations can maintain a hybrid deployment for archiving and records management that includes a combination of cloud and on-premise information, allocating data to each environment based on policies and company strategy. This allows you to move to the cloud in stages, for instance, if a business prefers to manage email over six months old in the cloud and keep new types of application data, such as SharePoint, on premise.

Autonomy WorkSite – Information intensive organizations must have the ability to implement working practices consistent with their policies while enabling collaboration across distributed teams. With Autonomy WorkSite, both paper and electronic documents—records, e-mail messages, and other media—can be consolidated into a central library that is easy to navigate and effective in ensuring that all content remains accessible, sharable, and reusable. Users or file owners manage access and security to workspaces, encouraging collaboration and reducing the demands on IT. WorkSite can enable accessibility to authorized individuals from any device or access point, including desktops and laptops, the Internet, client-facing extranets, and mobile devices including the iPad.

Social media and electronic communication governance in the cloud

Large banks, hedge funds, and private equity firms are required to monitor, investigate, and analyze electronic communications subject to oversight requirements by the SEC, FINRA, the FSA, and other regulators around the world. HP Autonomy provides the most advanced capabilities for compliance across all forms of electronic communication, including email, instant messages, Bloomberg, and Thomson Reuters data. Seamlessly connected with IDOL, the Autonomy Intelligent Data Operating Layer, we enable you to supervise across your enterprise as well as social networking and collaboration environments.

Autonomy Supervisor – Autonomy Supervisor takes an automated, intelligent approach to monitoring and surveillance of all electronic communications and incorporates flexible, easily configurable sampling profiles, integrated with the most precise policy module available. Going beyond keyword-based solutions to identify potential violations, Autonomy Supervisor includes advanced lexicons and conceptual search and classification tools.

Autonomy Social Media Governance – As communications increasingly move to the social realm, it is important to be able to automatically identify critical patterns across all customer touch points. Autonomy Social Media Governance can help you meet information governance obligations across customer contact centers, web properties, brick and mortar locations, and social media sites and derive actionable insight. By consolidating all customer interactions, whether direct or indirect, structured or unstructured, HP Autonomy's unique Meaning Based Computing based solutions can identify patterns in historical customer behavior to enlighten future actions, or review a website visit, survey response, grouping of successful sales calls, commentary on blogs or social media sites, overly emotional support calls, or even notes from a storefront representative.

These same interactions become very important when considering legal, regulatory, and business obligations that must be met for social media compliance. The use of social media sites to communicate, market, and conduct business has heightened governance and eDiscovery for many organizations.

Data protection in the cloud

Autonomy Connected Backup – Organizations today are comprised of a disparate and increasingly mobile workforce. While agility provides businesses the flexibility needed to succeed, it often leaves data unprotected. The increased risk of loss and vulnerability due to theft, hard-drive failures, and human error are real. In fact, the average cost of a lost laptop can be as high as $50,000 when considering the value of the hardware and content, without including the potential incalculable costs of security breaches or intellectual property losses.

Connected Backup eliminates the risk of data loss from enterprise desktops and laptops, whether protected locally or remotely. By automatically protecting data in the background, Connected Backup ensures complete data protection without interrupting users. A secure web-based access portal and mobility support enables users to easily retrieve data, without helpdesk intervention. HP Autonomy utilizes advanced encryption and other security technology to safeguard enterprise data during transmission, storage, and recovery. Choosing HP Autonomy for backup and recovery gives you an industry-leading technology partner with a proven track record of successful data protection. We currently manage over seven petabytes of endpoint device data and have more than 4 million devices under management worldwide.

Autonomy Live Vault – LiveVault allows you to protect critical application data in the cloud and manage the long-term retention needs—addressing both of these concerns in a secure multi-tenant global, geographically dispersed cloud storage grid. The LiveVault agent encrypts all data before transferring it from the servers. All data remains encrypted at HP Autonomy's secure, offsite, underground data centers, as well as on the optional TurboRestore™ appliance which resides in the customer data center. To ensure the physical security and availability of stored data, the LiveVault service mirrors all data to a second, geographically dispersed data centers, for full failover and redundancy.

Cloud computing factors to consider

The cloud offers huge benefits in its ability to flexibly meet the needs of the organization, and is well illustrated within the framework of the manufacturing industry. Since production facilities often have a maximum level of output, once the threshold is met, the manufacturer must either give up additional sales based on production limitations or invest in a new facility. Consequently, the new facility may likely be underutilized at first and present an unsupported fixed cost if the anticipated increased product demand does not materialize.

The same holds true in the world of governance where similar hardware constraints and purchasing occurs as demand for capacity rises and falls with the flow of litigation, investigations, regulatory requirements, or headcount. As a result, maintaining on-premise capacity that only supports baseline requirements will often mean insufficient available resources when demand increases. Similarly, investing in on-premise capacity to meet the worst-case scenario of a very large litigation could mean sunk costs that may never be fully utilized. Ultimately, the flexibility and on-demand capacity of a cloud-based governance solution make it ideal for many organizations. Beyond handling changing litigation demands, the cloud significantly increases business agility by enabling an organization to deliver business solutions, enforce information governance, and derive greater value from information.

When selecting cloud-based deployment, there are a number of factors to consider, as outlined in the following sections.

Search and identification of data
With massive increases in enterprise data, efficiently locating content regardless of format, language, or source repository can be a challenge. Often common in on-premise deployments, there are a variety of repositories, applications, and databases in use at any given time. This collection of applications can make it difficult for users to interact with the entire corpus of content because information may be hidden behind an application wall due to the lack of appropriate connectors. Without intelligent search software, it may be impossible to understand all format types or link to all databases, which can compromise accuracy and efficiency when searching and identifying data for governance purposes, driving up costs and turnaround times. In the cloud, the location of information becomes homogeneous, maximizing the strength of solutions used to access, search, and identify information.

With innovative solutions based on Meaning Based Computing (MBC), HP Autonomy enables your organization to form an understanding of virtually all your information and interactions, recognizing relationships that exist within them—regardless of format, repository, or type. MBC makes it possible for computers to process all types of human information—or unstructured data—including social media, email, video, audio, text, and web pages, as well as structured data such as call detail records, click streams, and sensor data. This allows computers to harness the richness of human and extreme information, bringing meaning to all data, regardless of what it is or where it resides.

At the heart of Autonomy's infrastructure software is IDOL, the Intelligent Data Operating Layer. As the information processing layer, IDOL automatically analyzes any piece of information from over 1,000 content formats, over 400 sources, and more than 150 languages.

Cloud security
Security is often a concern for organizations considering a cloud deployment, and must be a major factor in decision making, whether for archiving, eDiscovery, compliance, records management, or data protection. Moving important business information outside the walls of the enterprise demands serious forethought, as it can bring a certain level of risk. Hosted services should provide the same, if not higher, levels of security and control as established, internal information governance practices. For this reason, cloud service providers should be fully vetted to validate their methods of securing and controlling information. Important aspects of security include encryption and authentication methods used by the provider, as well as data location options, which can become important to meet jurisdictional laws and requirements.

Evaluating cloud security

When evaluating cloud security, organizations must consider a range of factors from how users access systems to the way various and law and regulations come into play related to managing data in the cloud. Following are few key points to consider:

Authentication
Proper authentication is required to ensure only authorized users can access information. Usernames and passwords offer one method for limiting access to resources, but are not enough. Authentication also extends to other areas of cloud services, such as technical support or requests for administrative changes. The highest authentication standards are required to prevent someone from posing as an employee of the company and requesting info or to change a user/password. HP Autonomy's multi-factor authentication method verifies users via location-based parameters or validation using rotating and even biometric data based on the user's unique physical characteristics to provide the highest levels of security. We also have the ability to not provide support or guidance to anyone calling without the appropriate authentication credentials.

Data location and privacy
Organizations of all types face an increasing number of regulations at local, state, federal, and international levels regarding data privacy and management. Regulatory requirements, laws, privacy requirements, and customer contracts make it necessary to know the location of data in the cloud.

Corporations that operate around the world know that privacy controls for their data may vary from region to region, with different countries placing different levels of restrictions on the transmission of data. For example, concerns over privacy and particularly the scope of the US Patriot Act, have led European, Canadian, and Asian governments to pass legislation prohibiting their citizens' personal data from being stored outside of their home country. Cloud providers should have data centers in multiple countries to meet this requirement. Choosing a provider that can commit to storing and processing data in a desired location or jurisdiction is a critical point that can typically be memorialized via a contractual commitment.

With data and processing centers spanning the globe, HP Autonomy can handle the most geographically dispersed organizations. Customers can proceed confidently knowing that the HP Autonomy cloud can help you to legally satisfy data privacy requirements required by the EU and other similarly situated jurisdictions.

Data deletion and disposition

In the Federal Rules of Civil Procedure, Rule 37 provides "safe harbor" when electronic evidence is lost and unrecoverable in the matter of regular business processes. This rule protects organizations from spoliation claims for data destroyed prior to the attachment of a duty to preserve. While a duty to preserve may require the suspension of normal retention policies for the duration a matter, the conclusion of a matter may release the duty to preserve and allow for that data to be subjected to the normal retention policies.

To avoid the pitfalls of tardy deletion or disposition, it is imperative to ensure that data is deleted and or disposed of according to retention and disposition guidelines. In Tomlinson v. El Paso Corp., a federal district court held that the defendant had a duty to preserve and produce data held by a third-party human resources organization.[2] The implications of this are that any third-party contracted to possess the organization's data, including cloud-based storage and email providers, may be subject to similar discovery. Without proper procedures to delete data from within the cloud environment—as well as any backups—that data may be indefinitely discoverable for future litigations. The fact remains, data that should have been deleted but wasn't does not shield or alleviate counsel's duty to preserve and produce.

On-demand scalability

A key benefit of the cloud is scalability, enabling organizations to flexibly scale up or down when changes occur in data volumes, litigation and compliance burdens, or cost structures. For example, most organizations are reticent to invest in infrastructure to manage matters of excessive size or involving a large, multi-party litigation. During these peak periods of demand, the flexible aspects of the cloud allow you to scale and reduce costs. This is especially critical in today's corporate environment where budgeting is closely watched, especially for infrequent spikes in demand for computing resources.

Leveraging its unique, split-cell architecture and grid-based design, HP Autonomy delivers massive, enterprise-wide, petabyte scalability without compromising performance, data security, or accessibility under any load. With 30 billion messages stored, six billion pages in active litigation review, and three million files processed per hour, HP Autonomy offers the most scalable and secure cloud solution available.

Data access methods

Once the decision is made to move to the cloud, the question of how data will be transferred is critical. If a cloud provider does not offer media restoration from backup tapes, and data is on tapes, this could present a roadblock. Organizations must work with a hosted services provider that understands and addresses its unique needs and implications for eDiscovery and information governance processes. For instance, it would not be feasible to work with a provider that relied solely on physical shipment of data, which is a poor method for transferring information.

HP Autonomy supports all data transfer methods to ensure the safe, secure, and seamless movement of data to the cloud. Access methods include but are not limited to the following:

- Media restoration
- Tape cataloging
- Data migration
- Bulk electronic transfer
- Real-time/burst streaming

[2] Tomlinson v. El Paso Corp., 245 F.R.D. 474 (D. Colo. 2007).

Evaluating a cloud provider: additional considerations

This section covers additional considerations that organizations should take into account when considering the use of cloud-based services for information governance.

Ownership of data
Who owns the data stored in the cloud—the corporation or the cloud provider? It is critical that any agreement with a cloud provider include terms that ensure the organization retains ownership of any data that is sent to the provider. This is not only important to ensuring intellectual property and sensitive information is not distributed, but may also have implications in the context of claims of privilege. If such an arrangement is being considered, it should be researched with outside legal counsel.

Technology ownership
The question of whether a cloud provider owns their technology and/or source code is of critical importance. It is not uncommon for service providers to license technology developed by other software developers and integrate it into their own products rather than attempting to develop it from scratch. While this may work satisfactorily in some industries, there could be consequences when this occurs in the context of cloud-based information governance. Providers and their clients could be put at risk if the provider's services are dependent on the success of other companies. For example, if a provider licenses a database technology from a company that goes out of business, discontinues support, or increases the license cost, the provider may be unable to update or fix issues that are essential to its services.

Experience and customer support
The experience, amount of time in business, and levels of support provided vary greatly between cloud providers. For these reasons, it is important to understand what is available. HP Autonomy provides customer support and training programs to help organizations with data handling for information governance and support for a diverse and global customer base along with the assistance of a worldwide professional services team.

Platform approach
A critical success factor with cloud-based solutions is the ability to leverage a platform approach rather than a point-solution approach. Point solutions address one or two aspects of information governance and eDiscovery processes, but could leave an organization needing additional solutions for early case assessment, legal hold, legal review, archiving, records management, and so on. Each point solution will have its own search methodology, set of reports, and security models. In large enterprises, using a point solution approach is guaranteed to make eDiscovery and governance processes overly complicated, inefficient, and hard to defend.

By comparison, HP Autonomy offers a platform approach designed to streamline information governance and dramatically increase the defensibility of business processes. With a platform approach, end-to-end eDiscovery and information governance processes leverage the same platform with one security model, set of audit trails, and index. Autonomy's modular architecture also makes it easy for you to add new functionality such as legal review or records management, as needed. Moreover, with a platform approach, there is no need to transfer data between applications, minimizing risk, ensuring chain of custody and avoiding expensive data loss.

Service Level Agreements
As with any business engagement, organizations need to understand the level of service a cloud provider will supply and whether it meets the needs of the organization. Due to the critical and often time-sensitive nature of eDiscovery, Service Level Agreements (SLAs)—which define expected service levels in terms of responsiveness, system availability, and system performance—should be highly detailed and include required levels of service and remuneration in instances where service levels are not met.

Best practices for selecting a cloud provider: at-a-glance

The chart below summarizes five key challenge areas that organizations should weigh when evaluating a private cloud provider.

Challenge	Concern	Recommendation
Add new ESI sources	Corporation will need to add a new solution or outsourced services provider for eDiscovery.	Make sure your eDiscovery Solution has the ability to easily add ESI sources to the process—file shares, SharePoint, Database, Audio, Video etc.
Multi language support	Solution will fail to find preserve potentially responsive non-English ESI.	Validate multi-lingual support via a proof of concept or other credentials that the vendor provides.
OEM components OEM (Original Equipment Manufacturer) components are software components developed by a 3rd party that an eDiscovery vendor may embed in their solution. File viewers for example, are typically OEM components.	OEM eDiscovery components require two layers for customer support which could cause a failure to produce ESI on time due to a component failure.	Look for vendors that develop all their own technology.
Financial viability and dedication to the eDiscovery space	Vendor could go out of business or get acquired by larger company that lacks commitment to the eDiscovery space.	Choose vendors that show profits and growth over several years. Also look for vendors where eDiscovery is a large percentage of their revenue. Pinpoint a vendor's dedication to the eDiscovery space for years to come.
Trained staff to run the system and interface cross functionally	Incomplete preservations and holds leading to sanctions.	Hire an eDiscovery Subject Matter Expert that will serve as a liaison between legal and IT and also oversee the entire eDiscovery process.

Conclusion

There are benefits and significant ROI to be gained by choosing a cloud-based deployment for performing information governance processes. In part, reasons such as complexity, up-front expense, and rigidity that can be common to on-premise solutions are spurring the shift to cloud solutions. More and more organizations are taking advantage of the flexibility and ROI that cloud computing offers. Industry analysts estimate that 50 percent of the email archiving market will be delivered via cloud solutions by 2014.[3]

Whether organizations choose the flexibility of a cloud solution or the control that an on-premise solution provides, a holistic-platform approach as described in the previous section is key to ongoing compliance with new regulations, addressing organizational growth, and taking advantage of new opportunities for ROI.

[3] Gartner, Inc., "Market Trends: E-Mail Archiving Strong Growth Continues," October 2010, available for purchase at http://my.gartner.com/portal/server.pt?open=512&objID=260&mode=2&PageID=3460702&id=1446030&ref=

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** to find out more.

autonomy.com

20130508_RL_BR_HP_AUT_Best_practices_for_cloud-based_information_governance