## TABLE OF CONTENTS

Executive Summary ........................................................................................................ 3

Establishing Trust in the Era of the Cloud: Today’s Challenge for Regulated Industries ...... 4

How Do We Remove the Fog? Definitions, Standards and Recommended Practices ........... 5

Cloud Computing Definition and Characteristics ......................................................... 6

Cloud Services Categories ......................................................................................... 6

Four Main Types of Cloud Infrastructure ................................................................. 6

Information Governance in the Cloud: Assessing Your Options .................................. 8

Six Key Elements of Building a Cloud Strategy .......................................................... 9

Why Viewpointe? A Trusted Partner to Meet Information Governance Needs .............. 14

Conclusion ............................................................................................................... 19

Appendix: Assessing an Information Governance Platform: Evaluating Cloud Readiness ...... 20
Large, complex organizations often handle sensitive and protected information. Financial, health and proprietary commercial data are among the most protected types of digital content, and enterprises are continually challenged to find new ways to store, secure and manage this information in an ever-changing world of computing.

Tech-savvy customers are adopting mobile, social and other online communication methods at an unparalleled rate, contributing to the acceleration of data growth. As a result, companies are experiencing higher costs, poorer performance, and increased compliance and litigation risk from these expanded information footprints.

Many organizations are facing pressures to improve efficiency, store data more securely and reduce costs. Moving from an on-premises information management infrastructure to a cloud platform is a viable option for more and more businesses. However, uncertainty surrounding the types of cloud services that are available, their characteristics and the variety of infrastructure types can lead to confusion and lack of action. Understanding how information governance can be enabled for content stored in a cloud is a top concern.

Public cloud or private cloud? Hybrid or community? Software-as-a-Service or Platform-as-a-Service? An analysis of your business – as well as compliance and Information Technology (IT) requirements – can help cut through the jargon to find an approach that meets the needs of a large enterprise. IT executives, legal staff, records managers and senior business managers can work collaboratively on requirements for a cloud strategy. Security needs, compliance mandates and information governance policies are factors that should drive your assessment of potential cloud service providers, as it can be a complicated vendor landscape for regulated industries.

Is there a way to eliminate the complexity? The answer is yes. Vendor-neutral parties such as the Federal Financial Institutions Examination Council (FFIEC) and National Institute of Standards and Technology (NIST) provide meaningful definitions, guidance and recommendations to organizations seeking to educate themselves on the advantages of cloud computing and move forward with a cloud strategy.

Information can indeed be safely stored and managed in this new world of cloud computing – it is a natural evolution of the utility computing services and virtualization platforms that independent service providers have offered for years. The era of cloud computing has indeed reached a level of maturity that can deliver on the needs of regulated businesses. If your business is an enterprise that must manage large volumes of sensitive data, execute upon content lifecycle policies and demonstrate a defensible approach to the disposition of corporate information, there is no need to face these challenges alone. Trusted cloud service providers with a track record of success in highly-regulated industries are ready to provide guidance for safe, secure cloud adoption.
Trust is the foundation of business. Whether your business serves the needs of commercial entities or those of individuals, it must provide safe, secure channels for the exchange of ideas and information. When customers share their financial, health or confidential commercial data, they expect that such information will be stored, secured and handled by a trusted provider within the parameters of legal and industry best practices.

Enterprises that are trusted with sensitive information – such as those in banking, insurance, investments and healthcare – must comply with external regulations in order to continue business activities. These compliance requirements compel enterprises to develop rigorous internal controls and policies to govern information holdings. Investment companies must abide by disclosure and communication rules from Financial Industry Regulatory Authority (FINRA), while banks must ensure that stringent customer privacy regulations are met as mandated by the Gramm–Leach–Bliley and Fair Credit Reporting Acts. Healthcare providers must respect the patient data protection obligations of Health Insurance Portability and Accountability Act (HIPAA). A common theme runs through these regulations: large companies must protect the data they create for their clients, securing it from leaks or tampering, and disposing of it safely when no longer needed in the course of business.

But the world of computing is changing. Individuals are becoming increasingly tech-savvy. Customers demand new ways to engage in digital, mobile and social transactions with their banks, insurance providers, investment companies and other essential service providers. Thus, the volume of electronic content continues to grow exponentially, and the information footprint that has grown drastically must be right-sized. Cost accelerates, performance suffers and decisions are more difficult to make. To complicate matters, these types of businesses also have significant compliance, security and data protection requirements. Innovations enabled by cutting-edge technologies can open the door to better online client service and provide competitive advantage, but the same innovations may also open a door to unacceptable levels of information governance risk.

By 2015, 60% of information workers will interact with content through a mobile device.


IT executives and compliance officers are sure to face even more uncertainties and anxieties as the computing market continues to debate the risks and benefits of cloud, mobile access and social media. The rapidly increasing volume, velocity and variety of digital content you are compelled to manage and protect continue unabated. Security, availability, integrity, confidentiality and privacy are the essential governance concerns that your organization must assess before moving to a new computing paradigm.
Can a balance be achieved? Can your team prepare itself to serve ever-changing markets, reduce costs and still be assured of appropriate governance of your information holdings? Is there an approach to information storage that delivers cost reductions and platform flexibility, but still provides rigorous controls for compliance and security? Can the same technology that helps your company meet regulatory obligations also transform your information into a competitive advantage? With all of these challenges, how can your business begin to make this shift, discovering both economic and security benefits of a cloud platform for your sensitive information holdings?

This whitepaper outlines today’s market challenges for financial institutions, as well as other regulated industries. We’ll share insights into industry best practices for safe, policy-driven cloud computing, and the steps that you can take to achieve the goal of enhanced information security while decreasing the capital costs of IT. Yes, the world of technology is changing rapidly, but information governance platforms from trusted cloud-computing service providers have proven that business transformation can happen safely and securely.

The cloud services vendor landscape can be complicated for institutions that require a high level of security, governance and lifecycle management for their critical content. Some of this complexity, however, can be eliminated by using the recommendations and guidelines provided by vendor-neutral professional bodies. Organizations should seek a cloud platform provider that can meet and/or exceed the recommended due diligence criteria including:

- a proven track record of managing large volumes of sensitive data,
- the capability to execute content lifecycle and management policies, and
- a deep understanding of the rigorous compliance obligations faced by regulated industries.

**HOW DO WE REMOVE THE FOG? DEFINITIONS, STANDARDS AND RECOMMENDED PRACTICES**

Businesses can make informed decisions about cloud services. Requirements for secure information governance and archiving should include the recommended practices from objective, vendor-neutral organizations such as FFIEC and NIST. Large enterprises that are investigating cloud platforms need to ensure due diligence is done on prospective vendors and service providers. IT executives, compliance officers and records managers must become comfortable with the vocabulary of the cloud marketplace in order to have an informed discussion with prospective service providers, as well as with each other. Governance and protection of core business data and customer information should never be risked in the name of cost reduction or lack of education.

Cloud is a natural evolution of the utility computing services and virtualization platforms that have been around for many years. Trusted service providers have been operating for years before the buzzwords about cloud computing began, providing hosted or managed services in independent data centers for services that extend from check archive to hosted email.
The decision to adopt a cloud infrastructure is often prompted by a need to consolidate IT projects, focus on core business activities and take advantage of operational budgets rather than investing capital. Never, however, should requirements for data preservation, classification, segregation and security be risked solely for the sake of cost savings. Selecting the cloud architecture and service provider who can balance these needs will be a key to success.

CLOUD COMPUTING DEFINITION AND CHARACTERISTICS
Cloud computing can be defined as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable resources.” There are five essential characteristics of a cloud computing platform:

- **On-demand self-service**: Unilateral provisioning of computing capabilities
- **Broad network access**: Capabilities are available over the network and accessed through standard client platforms such as laptops, workstations, phones or tablets
- **Resource pooling**: The platform provider pools computing resources to serve multiple customers using a multi-tenant model, dynamically assigning resources according to customer demand
- **Rapid elasticity**: Capabilities can be elastically provisioned and released to scale rapidly
- **Measured service**: Resources are controlled and optimized by metering services, allowing resource usage to be monitored, controlled and reported, ensuring transparency to both the service provider and the consumer

These five characteristics describe the core attributes of cloud computing, but there are also very different approaches to cloud service infrastructure. Choosing the appropriate cloud service infrastructure for your enterprise will be the critical decision, particularly when challenged to manage very large volumes of sensitive, confidential or commercial proprietary information. Regulated industries, particularly those with rigorous information governance and security mandates, can safely make the decision to adopt cloud computing. But your team must perform the due diligence on prospective service providers and determine the appropriate type of cloud infrastructure for your needs.

CLOUD SERVICES CATEGORIES
The three most common categories of cloud services are applications, platforms and infrastructure tools. Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) are terms that you and your decision-making team should understand to ensure a cloud services provider delivers the right mix of tools needed to meet your requirements.

Many new and unproven solution providers are latching on to the term “cloud.” These service providers, often targeting the consumer market, may provide terms of service that are unsuitable for sensitive business content. It is important to look beyond the hype; no cloud platform is one-size-fits-all. Instead, focus on cloud as the logical evolution of utility computing and learn how it can securely meet your large enterprise needs.

FOUR MAIN TYPES OF CLOUD INFRASTRUCTURE
We can identify four main types of cloud infrastructure in today’s market. According to NIST, they include:

- **Private cloud** infrastructure is “provisioned for exclusive use by a single organization.”
Private clouds can be owned or managed by the customer organization or by a third party, and may reside on premises or be hosted by the platform provider.

- **Public cloud** infrastructure "is provisioned for open use by the general public. It may be owned, managed and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider."

- **Community cloud** infrastructure "is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns."

- **Hybrid cloud**, which is the "composition of two or more distinct cloud infrastructures," such as an application that spans a private and a public cloud instance with some form of technology integration or interoperability.

The decision to adopt a private, public, community or hybrid cloud infrastructure is best determined by the enterprise’s requirements for security, data preservation, classification and segregation, as well as cost and service level commitments.
Large financial services organizations may find that a private cloud platform, hosted by a provider with specific expertise in regulated industries, achieves the right balance of cost and risk reduction, without sacrificing the cloud’s promise of increased agility and flexibility.

The adoption of secure cloud services by banks for check archiving and transaction processing has been accelerating over the last decade. Taking this proven archiving model to a broader range of electronic information is a logical evolution for these platforms as their cloud architectures are already built for the rigorous security demands of regulated environments. IT executives, legal or records managers, and senior business managers can work collaboratively on such a decision, and adopt industry best practices for executing an information governance program.

Information governance has been described by Gartner, Inc. as, “the specification of decision rights and an accountability framework to encourage desirable behavior in the valuation, creation, storage, use, archival and deletion of information. It includes the processes, roles, standards and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals.” This key concept of accountability often underpins the cloud services provider for information governance selection. Enterprise information managed in a cloud platform must be subject to the same – or better - level of stewardship and security as any traditional on-premises content repository.

To help your organization understand its information governance roles, responsibilities and stakeholder needs, a reference model can be used to help map out your needs. One of the more widely used reference models for information governance has been developed by an electronic discovery expert community and published on the “Electronic Discovery Reference Model” resource web site EDRM.NET. This expert community published this reference model to provide a common, practical framework, helping organizations develop and implement an effective information management program. Understanding the needs that your business, legal, records, privacy, security and IT managers have across the lifecycle of your corporate information is an important step towards improved governance. These requirements will be important when moving essential information to a cloud platform and can be met without sacrificing governance or risking non-compliance. Synchronization of priorities will help your organization select the cloud platform best suited to meet your unique business, IT and governance needs. Balancing the requirements for security, information stewardship, system reliability, cost and business agility is essential. Today’s reality of constant technology change means finding a trusted cloud platform provider that has proven that it can evolve and adapt as your digital communication and content – and that of your customers - evolves.

Assessing cloud platforms for information governance and secure repository services is not an easy task when done in a vacuum. Organizations should look to existing standards, guidelines and recommendations as a foundation upon which to build their requirements. A helpful set of considerations for financial service institutions was issued by...
the FFIEC in July 2012. These recommendations can also benefit other regulated industries who seek to understand the risks and benefits of cloud computing in an environment subject to heavy compliance obligations.

Financial institutions and regulated industries can improve and accelerate their decision-making process by getting to the heart of the governance, security and risk management issues when assessing a cloud service provider. Choosing a trusted vendor is important. Their technology, domain expertise and experience must be demonstrated as part of your selection process. The right platform provider will understand the unique challenges of regulated industries, have expertise in governing information across its lifecycle, and demonstrate a proven track record of handling high volume secure content stores and transactions. Many consumer-oriented public cloud service providers may struggle to meet these criteria. Many on-premises software vendors that are new entrants to the cloud service market will also face this same challenge.

**SIX KEY ELEMENTS OF BUILDING A CLOUD STRATEGY**

Let’s review the six key elements of building a cloud strategy when information governance and security are essential requirements.

1. **DUE DILIGENCE – UNDERSTAND HOW YOUR INFORMATION IS PROTECTED**

   Pushing administrative, storage and hardware costs to a third party is a significant business driver for institutions who adopt a cloud platform for information control. Use of a third party, however, “does not diminish the responsibility” of your business leadership to ensure that activities are conducted safely, soundly and in compliance with applicable laws and regulations. Use of a third party that has

---

**Figure 3: Information Governance Reference Model- Used Under Creative Commons Attribution 3.0 United States License**
extensive experience hosting data for regulated businesses can become critical.

Information – whether data, transactions or other digital records – runs through all aspects of your business. Sensitive information may include corporate or personal financial data, health or insurance records, or confidential commercial secrets. Sensitive data must be protected from disclosure that could invite risk or embarrassment to an institution or its clients. Segregation of hosted information is important to meet the needs of regulated industries who handle sensitive content.

Hosted information is also subject to the same eDiscovery obligations as any other electronic content. Large organizations will often face the need to hold and preserve content related to a real or threatened legal action. Understand how a cloud service provider can fulfill a demand to retrieve, hold and produce your data to protect it from unauthorized deletion or alteration.8

Adoption of a private cloud platform can deliver this higher degree of integrity and confidentiality. A trusted cloud provider should also be available to offer its expertise for information migration as the cloud services are adopted. Assessing your enterprise content for value, risk and sensitivity levels, and enabling the disposal of low-value information that is at the end of its business lifecycle can be tremendously valuable services. Return-on-investment estimates or other performance indicators can be fast-tracked by analyzing the value of content during the platform adoption process.

2. VENDOR MANAGEMENT – UNDERSTAND HOW YOUR RELATIONSHIP IS GOVERNED

There are advantages to selecting a cloud service provider that has a track record of meeting the rigorous needs of industries that must comply with a vast array of regulations. The FFIEC recommendations advise that service providers that lack this experience “may present risks that the institution is unable or unwilling to mitigate.”9 A cloud platform provider that is unable or unwilling to adjust its practices to protect your customer or other sensitive data will often need to be ruled out as a viable option. Once again, ensure that IT, legal, records and business stakeholders can align their needs for an information governance strategy – particularly when moving to a new paradigm such as cloud.

Nearly 70% of large organizations (those with over 5000 employees) view private cloud as the best way to meet their information management needs.

Financial services organizations may be subject to laws or regulations that cover the “ownership, location(s) and format(s) of data.”10 Ensure the cloud platform provider can verify the jurisdiction in which your information is held and respect your need for transparency into its residency. Select a cloud services provider that understands that these unique compliance challenges must be addressed. Your organization has an obligation to understand your cloud service provider’s architecture, physical data center locations, and how your company data is managed. Privacy and data protection laws as well as the need to comply with eDiscovery orders should be top considerations when moving to a cloud archiving platform.
3. AUDITABILITY – KNOW HOW THE PROVIDER’S INTERNAL CONTROLS PROTECT YOUR CONTENT
Determine if a prospective cloud platform provider is equipped to answer the tough questions your audit team may need to pose. A defensible information governance strategy must extend to any third party, cloud or hosting service provider that is entrusted with customer or other sensitive commercial content. Be proactive when reviewing the adequacy of a service provider’s internal controls and practices. According to the FFIEC recommendations, organizations must ensure that “auditors assist in this evaluation by assessing whether those controls are functioning appropriately.”11 Understand the cloud provider’s practices, and educate your internal audit teams on how to adapt their assessment activities to new cloud computing realities.

4. INFORMATION SECURITY – PROTECT, MONITOR AND ENFORCE YOUR POLICIES
The risk of a security incident can be reduced by ensuring that a prospective cloud platform provider can monitor, report, and investigate perceived threats. Regulated industries must verify that “data are satisfactorily protected and access to their data is appropriately controlled.”12 Establishing a relationship with a cloud provider who cannot demonstrate security measures is “ill-advised,” according to the FFIEC recommendations. Whether this data is structured information in databases, stored in line-of-business applications, or residing unstructured in email or other electronic documents, you must verify that proper controls, security and handling procedures are clear and executed consistently.
5. COMPLIANCE CONSIDERATIONS – UNDERSTAND YOUR REGULATORY ENVIRONMENT

Adopting a new platform for information governance presents an opportunity to review your information governance strategy and tune specific programs or policies. Ensure any renewal of an information governance strategy takes the requirements of business, IT and compliance/legal officers into full account. How well does a cloud platform provider understand the importance of the legal, regulatory or internal quality obligations faced by your organization? Do they understand the reputational risk or threat of sanctions for leaked or unencrypted non-public personal information (NPPI)? How ready are they to perform the hold, identification, review, production and delivery of your electronically stored information (ESI) in the event of an eDiscovery order or threat thereof?

Financial services organizations and other institutions holding sensitive information will have important decisions to make regarding the storage of data overseas and the applicability of any laws or regulations that can affect a cloud provider with a globally-distributed infrastructure. Your business can, however, choose to mitigate this risk of data residency by looking at private, segregated platforms, and by using a cloud provider who understands the risk of inviting legal obligations from unexpected jurisdictions. According to the FFIEC guidelines, an organization’s “ability to assess compliance may be more complex and difficult in an environment where the cloud computing service provider processes and stores data overseas or comingles the financial institution’s data with data from other customers that operate under diverse legal and regulatory jurisdictions.”

Know what obligations your business faces regarding privacy, confidentiality, legal holds, freedom of information requests or eDiscovery orders, and ensure your cloud platform provider is able to guide and assist with a plan to address these non-negotiable protection and preservation requirements.
A vendor that can provide domain expertise in the area of information governance offers value far beyond that of a typical storage services provider. Can your new services provider help you identify content that is subject to regulations? That needs particular levels of protection? Or that is ready for disposition in line with approved lifecycle management rules? Question, document and assess the ability of the cloud platform provider in these essential areas of governance; vet their experience and track record thoroughly. A particularly risky area for regulated industries is the “potential that data are not completely removed or deleted from the servicer’s storage media”14 at the end of a contract. Validate and verify the disposition, destruction and lifecycle management practices of the cloud platform provider.

6. BUSINESS CONTINUITY – MINIMIZE DOWNTIME AND PROTECT YOUR MISSION-CRITICAL INFORMATION

Business continuity is the process of ensuring that your enterprise’s key activities and information can be recovered, resumed and safely maintained – including that content held by a cloud service provider.15 Unexpected disruption can result in lost revenue, diminished customer satisfaction, and delayed processing of mission-critical transactions. Ensure that you have all of the information you need to be confident not only in the cloud service provider’s back-up and recovery procedures, but in its ability to deliver sufficient redundancy, load-balancing or other fail-safe measures to minimize downtime in the first place. Service level agreements (SLAs) should outline the terms of service and provide benchmarks for performance, downtime and procedures for any scheduled maintenance, disrupted system availability and disaster recovery. Also, be assured of the cloud platform provider’s ability to monitor, support and scale your cloud instance as the information footprint grows and the value of your content increases. Experienced cloud providers should be seasoned in providing SLAs that support the specific governance and continuity needs for your jurisdiction and industry sector.
The cloud services vendor landscape can be complicated for institutions that require a high level of security, governance and lifecycle management of their critical content. You can reduce some of this complexity, however, by looking at the recommendations of the FFIEC, or professional associations for information managers such as ARMA International.

Consider partnering with a cloud platform provider that can meet recommended due diligence criteria including:

- the ability to manage large volumes of sensitive data,
- the capability to execute clients’ content lifecycle and management policies, and
- a deep understanding of the rigorous compliance obligations faced by regulated industries.

Viewpointe® meets these requirements with our OnPointe® information governance platform. For more than a decade, Viewpointe has been a trusted partner to large, complex organizations. We have helped businesses to manage, secure and monitor their data with our hosted digital archive. Viewpointe was founded by financial institutions, for financial institutions, and therefore intimately understands the regulatory and compliance challenges faced by heavily regulated organizations. OnPointe is the next generation of our trusted archive offering, representing the logical evolution of our expertise and experience managing large volumes of sensitive information.

We have successfully managed large private cloud archives for some of the world’s biggest financial institutions and this experience brings our unique technological capabilities and years of domain expertise to the information governance needs of regulated industries.
governance market with a well-established private cloud platform offering. The OnPointe information governance platform from Viewpointe is the secure, trusted choice for information governance in today’s era of the cloud.

A track record of trust sets Viewpointe apart from the legacy on-premises product providers now entering the cloud archive market. Ten years of technical and hosting expertise has been encapsulated in our information governance platform. OnPointe builds on the technical infrastructure that today hosts over 29 petabytes of data on behalf of large regulated institutions. Customer data is securely managed and retained across distributed Tier 3+ data centers to help ensure that it is protected and accessible.

Information governance is an integral part of the OnPointe platform. These governance capabilities help Viewpointe clients meet regulatory, legal and business requirements to protect and manage essential content. Automating and consistently applying your organization’s governance policies can result in improved compliance and response to eDiscovery orders, allowing you to restrict access to data, monitor its use, manage retention rules and establish defensible disposition procedures. Automation of these governance policies can also help reduce the risk and cost of managing critical content by eliminating redundant, obsolete information. Additionally, reducing your enterprise’s information footprint can result in lowered storage costs and improved decision-making. We provide proven methodologies and domain expertise to help create an approach that fits your institution. From content management and text analytics, to retention management, archiving and eDiscovery technologies, the OnPointe platform delivers the essential components needed to protect your information across its business lifecycle.

SECURITY PROVIDED BY PRIVATE CLOUD SERVICES
Segregation of your data and the customer information entrusted to your care is an important element of the FFIEC
To help ensure commitments are met and rigorous internal controls are in place, our services undergo an annual SSAE-16 (formerly known as SAS70 Type-II) review. Our internal controls and practices as a private cloud provider have been subject to this audit rigor for over a decade helping to ensure we provide consistent and secure operations. The OnPointe architecture includes multiple security layers that include physical, technical and operational safeguards.

Content archived with the OnPointe platform is encrypted on disk “at-rest” as well as during transmission “in-motion.” This helps protect your information from unauthorized access, without sacrificing the fast retrieval demanded by your business users. Enhanced auditing services validates content is used and accessed in accordance with your policies, with only authorized users obtaining access. Information that is regulated by privacy or disclosure laws, such as PII or NPPI, can be restricted, helping ensure compliance and reducing the risk of breach. OnPointe supports secure single sign-on and integration with your directory services to authenticate and identify users so that users are given access only to the content they’re authorized to see. Intrusion detection, firewalls and transaction monitoring are all services available with the OnPointe information governance platform.

**ON-DEMAND ACCESS TO YOUR ESSENTIAL INFORMATION**

Ensuring that accurate information is easily found is an important requirement in the fast-paced digital workplace. No one wants to consider trading security and savings for speedy access to data. Making decisions faster and better with a right-sized information footprint is a goal for many large, complex organizations. OnPointe includes sophisticated retrieval capabilities as part of its private cloud platform, allowing near-instant access to essential information. Our clients demand fast, accurate access to information to make decisions, share knowledge and to perform complex inquiries on large volumes of their managed data.

“Private clouds will dominate critical functions. Industries with the strongest adoption of private clouds are financial services, healthcare and diversified industrials... financial services and healthcare face heavy regulatory and compliance issues that are exacerbated, though not impossible to overcome, in the cloud.”

KPMG, “Clarity in the Cloud” – December 2011

**COST MANAGEMENT AND EFFICIENCIES**

Cloud usage models offer tremendous opportunity to uncover cost savings, reduce capital expenditures and provide transparency into how computing services are consumed across your business. Upfront investments in software licenses and hardware infrastructure coupled with ongoing spending on maintenance and installation services mean traditional acquisition and deployment models are often time-consuming, budget-burning
propositions. A private cloud platform for an information governance program can significantly lower total cost of ownership (TCO) for your organization and help projects get started faster. Less upfront investment and a consumption-based pricing model mean eliminating the high total cost of shelfware. Consumption-based models help you align business costs to your business priorities, not those of a license-driven technology vendor.

Insight into how information is being captured, stored and managed across business units helps your organization align its operational expenditures to the priorities of your organization’s leadership. Scale up or down as your business needs dictate, and as your information footprint expands or shrinks as content is consolidated and retention policies are executed.

**FLEXIBLE INTEGRATION WITH YOUR EXISTING BUSINESS APPLICATIONS**

Adopting an information governance platform can be accelerated by integrating to your key line of business systems. Enterprise applications are major sources of business content, and enabling content at its source helps ensure a more complete set of corporate records. Faster adoption translates into meeting your targets for compliance and cost reduction more quickly. The OnPointe application programming interface (API) ensures your private cloud platform adoption can continue to evolve. The broad spectrum of business applications includes those you have in-house today, as well as those that may be adopted in the future. As the digital workplace continues to evolve at an ever-accelerating pace, our platform flexibility helps assure consistent governance of information, regardless of the source. APIs deliver ease of integration into the secure, distributed OnPointe platform, accommodating your digital content regardless of format.
DOMAINEXPERTISEANDCONTENT
ASSESSMENTSERVICES
Support from our OnPointe platform experts is an integral part of the offering. Because we model our business on usage rates, your adoption success drives our success. But large organizations don’t simply obtain information governance “out-of-the-box” or “out-of-the-cloud.” Our domain expertise in the areas of regulatory and legal compliance, retention and disposition policies and eDiscovery practices for regulated industries can help accelerate success. Generic technology adoption – whether cloud or on-premises – is not enough to ensure that your organization meets its compliance obligations. OnPointe draws upon the track record of its corporate team to provide you with the subject matter experts who have extensive experience managing large volumes of client data. This expertise is available to our OnPointe clients. We are able to help you to fast-track your information governance objectives and achieve desired cost efficiencies.

Viewpointe provides one of the
nation’s largest trusted archive at
over 29 petabytes.

The Viewpointe Content Assessment service and methodology encapsulates our expertise and can prepare your organization for information governance readiness. We’ll get you started on the right path by prioritizing the content to be moved to the OnPointe platform in line with legal, regulatory and business requirements. We can assess your information governance strategy, ensure your migration experience is optimized and allow you to fully exploit our knowledge and years of hands-on experience serving regulated industries.
New approaches to computing will lead to new approaches to governance. Balancing compliance with cost reduction, auditability with agility, eDiscovery with efficiencies – these are the challenges you’ll face as you guide your business to the next level of governing corporate content. Large enterprises with complex governance requirements must adapt to the changing world of technology, but can only do so within the parameters of security, data protection and externally-mandated regulations. Finding a trusted provider for information governance in the world of cloud, mobile and social can be a significant challenge.

Are you ready to select a cloud platform provider who can serve the needs of not only your business, IT and compliance stakeholders, but those of your clients and their important information assets? There’s no need to take on this challenge alone. Viewpointe, and our team of OnPointe Advisors, will deliver the trusted private cloud services you need to achieve information governance in this era of the cloud.

**RECOMMENDATIONS FOR FURTHER READING**


### APPENDIX: ASSESSING AN INFORMATION GOVERNANCE PLATFORM: EVALUATING CLOUD READINESS

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Questions to Consider</th>
<th>Vendor Response</th>
<th>Comments on Vendor Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Due Diligence</td>
<td>Is the cloud platform provider audited for SSAE-16 (formerly known as SAS70 Type-II) compliance? If yes, is this an annual audit? Do we have access to the audit findings?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>How much managed data or content is hosted by the cloud service provider? (For example, the number of petabytes under management.) How quickly is this managed content store growing per year?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>How many years has the service provider been offering secure hosting and/or private cloud services?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>What percentage of the service provider’s clientele is regulated industry?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Management</td>
<td>Can the service provider provide segregated data or content repository services in line with FFIEC recommendations?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Can the service provider ensure that data or content resides in a particular jurisdiction?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>How does the service provider ensure that data or content is deleted and destroyed in line with your corporate disposal schedules? Does this include backups, archives, replicated or mirrored sites?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Describe any professional services expertise offered by the cloud platform provider to assist with migration and content assessments. What methodologies or industry standards are used in their services approach?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auditability</td>
<td>How will the cloud service provider allow your audit team to evaluate and validate their internal controls and processes?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Security</td>
<td>How does the cloud service provider conform to the FFIEC guideline to maintain a comprehensive data inventory? To maintain a data classification process?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>How does the cloud service provider ensure that access to your data / content is restricted?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Criteria</td>
<td>Questions to Consider</td>
<td>Vendor Response</td>
<td>Comments on Vendor Response</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------</td>
<td>-----------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td></td>
<td>List the key information or content types that can be migrated to the cloud service provider using packaged services or utilities. For example: Network file shares? SharePoint sites? E-mail inboxes? Messaging systems? Office applications? Print streams? Imaging or capture applications? Line of business applications (ERP, CRM, HRM, etc.)?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Describe the APIs or development toolkits available for the cloud service platform.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance Considerations</td>
<td>How does the cloud service provider protect Non-Public Personal Information (NPPI)?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>How will the cloud service provider place a hold on data or content that is subject to a legal hold order as part of eDiscovery or other formal investigation?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>How will the cloud service provider perform the analysis, retrieval and production of data or content that is subject to a legal hold order?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Considerations</td>
<td>Describe any disk encryption provided by the cloud service provider.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Describe the user authentication approach used by the cloud service provider. Is single sign-on supported?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Continuity</td>
<td>Does the cloud service provider offer service level agreements for system availability in line with your business needs? SLAs for performance? SLAs for issue resolution?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>How will the cloud service provider perform back-up, recovery, load-balancing or other fail safe measures to minimize downtime or information loss?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>How will the cloud service provider allow your organization to scale up (adding users or additional storage) or scale down (reducing users or eliminating storage) on demand?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
END NOTES

1 SOC 2 – “Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy” – A How-To Guide for Auditors, published by the American Institute of CPAs (AICPA).


4 Gartner, Inc. “Using the Cloud and Staying Secure” – 2012 Webinar delivered by John Pescatore, Vice President.


16 ARMA International is a not-for-profit professional association and the authority on managing records and information. Publications from ARMA include “Guideline for Outsourcing Records Storage to the Cloud,” 2010. Available from the ARMA bookstore.

Viewpointe®, a leading cloud provider of information governance and payments exchange services, is recognized for its national, trusted archive with more than 29 petabytes of data under management. With expertise in serving highly regulated financial institutions, Viewpointe offers the scale, security and state-of-the-art infrastructure needed to meet the most complex content management and information governance requirements. Viewpointe’s information governance platform, OnPointe®, leverages your existing technology investments and streamlines your information governance processes, management, access and storage via a private cloud, helping you mitigate risk, increase efficiencies and reduce costs.

If you would like to learn more about how OnPointe can help optimize your information governance, management and storage environment, contact an OnPointe Advisor today.

(800) 956-3807 | onpointeadvisors@viewpointe.com | viewpointe.com/onpointe