

WHITE PAPER

Information Governance in the Cloud

Sponsored by: EMC

Vivian Tero
September 2010

IDC OPINION

Organizations have an obligation to enforce their information governance policies consistently across their on-premise and cloud-based deployments. Cloud computing and virtualization change the risk profile of information assets. The layers of abstraction inherent in these technologies also pose challenges in effectively tracking and executing the technical controls around confidentiality, data integrity, and availability. These information governance issues impede higher adoption of cloud computing among organizations.

Services vendors, in partnership with EMC, have an opportunity to provide a broad range of value-added services that would enable organizations to plan for and address these information governance challenges effectively. These services should:

- Provide assurances on data provenance and integrity, on confidentiality, and on the users' identities and entitlements.
- Address data management, data security, and data segregation issues as part of the organization's cloud exit strategy.
- Assist organizations balancing the trade-offs between their operational and service-level objectives and their information security and compliance obligations.

Information governance value-added services and capabilities would enable services vendors to differentiate their solutions, create new revenue streams, enter new markets, improve their stickiness, and realize higher margins. To take full advantage of these opportunities, service providers should look to partner with ISVs whose application architecture and licensing models are able to support the various cloud architecture and deployment models.

IN THIS WHITE PAPER

This IDC white paper discusses the role of information governance in overcoming key impediments to the adoption of cloud computing technologies among organizations. The document concludes with recommendations on solutions that services vendors, in collaboration with technology vendors, like EMC Corporation, should offer to organizations so that they could effectively take advantage of cloud computing technologies to achieve their business, legal, operational, and security objectives.

SITUATION OVERVIEW

Aggressive data volume growth and the use of new technologies underscore the criticality of application delivery-agnostic information governance practices.

The 2010 *IDC Digital Universe Study* sized the 2009 digital universe at 800,000 petabytes and forecasts total volume to reach 1.2 million petabytes by the end of 2010. Unstructured data and metadata (also known as data about the data) are the fastest-growing categories. The use of cloud computing and virtualization technologies adds layers of abstraction and makes the tracking of dependencies across the information infrastructure and IT infrastructure particularly onerous. Understanding these dependencies is critical to ensuring and demonstrating adherence to a broad range of business, legal, regulatory, security, and operational requirements. The metadata infrastructure provides the critical glue that binds the information infrastructure to the underlying IT infrastructure. Sound information governance practices would take advantage of the metadata infrastructure to ensure that content and data are managed consistently and adhere to written policies, across on-premise and cloud-based environments. (Source: *IDC Digital Universe Study*, May 2010)

Global regulatory and legal regimes are expected to be more active and demand increased oversight and accountability. In 2008, 22–33% of the digital universe was high-value information, also known as data and content that are governed by security, compliance, and preservation obligations. IDC forecasts that high-value information will comprise 35–45% of the digital universe by the end of 2012. Siloed, regulation-specific compliance programs are costly and increase the probability of policy conflicts and runaway costs associated with hyper-enforcement. Sound information governance practices and tools would enable organizations to align their data retention, acceptable use and communication, data privacy, records management, and information security policies, processes, and technical controls. (Source: *Worldwide Governance, Risk, and Compliance Infrastructure 2010–2014 Forecast: Increased Regulatory Oversight, Privacy, Cloud Computing, and Smart Cities Drive Emerging GRC Obligations*, IDC #222214, March 2010)

Organizations are looking to realize cost efficiencies and improve business agility by taking advantage of cloud computing. IDC research concludes that there are marked differences in the motivation for employing cloud computing across SMBs and enterprises. Public cloud is an SMB high-volume play, while private cloud is the preferred consumption model among organizations with over 5,000 employees and where the IT environments are over 15% virtualized. Despite the differences in organizations' motivation, consuming information governance technologies through the cloud offers lower acquisition and deployment costs of critical governance tools via subscription fees instead of the perpetual license model. Organizations would also find the quick time to deployment and the ability to provision and scale up (or down) quickly as other appealing features of cloud computing technologies. (Source: *Cloud Computing Attitudes*, IDC #223077, April 2010)

Adoption Impediments to Cloud Computing

IDC research concludes that risk and compliance issues are the primary objections to cloud computing, including:

- ☒ Absence of sound legal and regulatory frameworks to address data privacy and data segregation requirements. Privacy and civil liberties advocates continue to express their reservations over the potential unchecked powers of governments to access personal information in the cloud.
- ☒ Data provenance, data traceability and audit, and managing identities and entitlements of authorized users in the cloud. Organizations want assurances that information is securely shared among authorized users and partners, that retention policies are adhered to, and that events, logs, and chain of custody requirements are properly documented. Organizations are also looking for more effective methods for conducting audits in on-demand and dynamic environments.
- ☒ Costs and risks associated with exiting the relationship with the cloud service providers. Organizations want assurances that data management, data segregation, and data destruction requirements are enforced and that content migration costs are addressed in the event that the relationship with the cloud service provider is terminated by either party.
- ☒ Need for sound framework and tools to enable organizations to balance the trade-offs between their operational cost efficiency and service-level objectives with information security and compliance requirements.

The dynamic, highly abstracted, and on-demand nature of cloud-based services poses challenges in executing the technical controls for information governance. These protocols and controls should enable organizations to consistently execute the organization's information governance policies across its on-premise and cloud-based environments.

(Source: *Managing and Securing Information In the Cloud: IDC Cloud Computing Forum*, IDC #220690, November 2009)

FUTURE OUTLOOK

Best Practices for Information Governance

As a best practice, information governance should include the following core components:

- ☒ Information retention and disposition program, including policies and technical protocols for records management, archiving, data privacy, and acceptable use and communications

- ☒ Legal hold program including policies and technical protocols for legal hold life-cycle management, as well as information management and storage protocols for the identification, preservation, and collection of potentially responsive ESI
- ☒ Policies and technical protocols to support data and application availability, as well as data confidentiality, provenance, and integrity requirements
- ☒ Common platform for governance tools, if available, to minimize the training, usage, and support costs that are associated with the adoption of new software solutions

Information Governance in the Cloud: Opportunities for Service Providers and Technology Partners

The services opportunities for cloud-related information governance services go beyond the storage, security, and IT infrastructure-related services. Examples of storage services include archiving, data protection, eDiscovery and litigation support, and business continuity. Security services include security strategy and planning, compliance road map and audit, benchmarking (e.g., ISO 17799), security policy assessment and development, network architecture assessment, incident response planning and forensics, security implementation, security operations, and education and training. Infrastructure-related services include those traditionally provided by telcos, ISPs, and IT outsourcing/IT managed services vendors focusing on areas like provision, billing, capacity, and utilization management; application workload management; and service-level management.

In concert with their ISV and hardware partners, service providers could potentially provide a myriad of information governance services associated with strategic planning and onboarding, implementation and deployment, application and IT infrastructure hosting and management services, and testing, training, and support for cloud-based environments. These cloud-related information governance services would include:

- ☒ Information discovery, audit, risk assessment, and policy planning.
- ☒ Business process and IT process planning and design.
- ☒ Information retention implementation and deployment solutions, including testing, training, and organization change management.
- ☒ Legal hold and eDiscovery implementation and deployment solutions, including testing, training, and organization change management.
- ☒ Monitoring, audit, and reporting for adherence to corporate information retention, legal hold, and eDiscovery programs, as well as operational risks and security compliance programs for PCI-DSS, cybersecurity and data privacy, antifraud and antimoney laundering, and Basel II compliance
- ☒ Corporate M&A processes involving information migration, management, and integration with existing corporate assets. Service providers may offer a more

efficient option for corporate customers that wish to transition and onboard employees with their associated data while not experiencing all of the challenges related to merging IT datacenters.

- ☒ Corporate alliance partnerships, where comingled files, data, and messaging are shared, may benefit from a third-party service provider offering rapid information availability of information, with associated permissions, and continuity of content.

Service providers could employ these information governance services as tactical differentiators on top of the standard application and platform cloud services (such as SharePoint and Exchange). By allowing organizations to differentiate the value of information, service providers could offer higher SLAs — such as higher levels of availability, more granular risk assessment and reporting, and more stringent layers of security controls — for the most critical information assets.

Among telcos, ISPs, and IT outsourcing and IT managed service providers, information governance is an opportunity to go beyond hosting the application to helping customers implement and manage information management policies. As more cloud-service providers enter and saturate the market, these value-added components would enable the service providers to differentiate their offerings from the low-cost cloud providers. New entrants (like Google, Rackspace, and Amazon) are gaining traction purely on cost. As more service providers introduce their own cloud services, competing on price becomes a losing strategy. Information governance offerings will be key to keeping customers, entering new markets, and protecting itself from price erosion. Keep in mind that there are many different flavors of cloud (private, public, hybrid, and community). The lower down the stack the cloud provider stops, the more information governance activities the consumer of the services will be tactically responsible for implementing and managing. Helping the consumer of cloud services understand, plan for, and manage the dependencies across the information, workloads, and underlying IT infrastructure in order to adhere to the consumer's security, data retention, preservation, data segregation/privacy, and operational objectives presents a huge transformational opportunity for service providers. These value-added components would also enable service providers to create new revenue streams and realize higher margins.

As service providers offer information governance in the cloud, it would also be useful for them to evaluate whether the application (such as archiving, records management, legal hold process management, search and text analytics) is able to support the various types of cloud architectures. It also needs to consider if the information governance application can support flexible licensing models (subscription versus perpetual license). Here, the service provider should evaluate if the multitenant cloud pricing and offering go beyond those that utilize virtual machine instances. Information governance applications with more flexible technology architecture and pricing and licensing models would enable the cloud service provider to expand its addressable markets.

EMC Information Governance Solutions

Service providers have an opportunity to work with technology enablers, like EMC, to address a broad range of information governance challenges. EMC offers a portfolio

of software, services, and hardware so that organizations can manage and enforce their information governance obligations consistently across their on-premise, private cloud, public cloud, and hybrid IT architecture deployments. This portfolio includes:

- ☒ **EMC Source One Family.** Includes the range of archiving, search, and text analytics software solutions for eDiscovery, retention management, email management, content reuse, and operational improvements.
- ☒ **EMC Storage Platforms (including offerings from Data Domain, EMC Centerra and Celerra, and V-Plex).** Includes hardware and software products that are intended to provide highly scalable storage pools, as well as better capacity, utilization, storage availability, data resiliency, and storage resource management.
- ☒ **EMC Consulting.** This division works with EMC's services partners by augmenting their capabilities around business and IT strategy, process and risk assessments, application and information governance strategy, program implementation, business continuity services, compliance and records management, eDiscovery consulting services, and cloud consulting services.
- ☒ **RSA Security.** The security division offers solutions for identity and access management, access control, data loss prevention, encryption, security information and event management, and GRC management.
- ☒ **VMware and EMC IT Infrastructure Management.** Includes software that spans datacenter operations and compliance, IT operation intelligence, service discovery and mapping, network and systems resource management, service and configuration management, storage resource management, and virtualized datacenter management.
- ☒ **Greenplum.** The data analytics and warehousing solution is the foundation of EMC's data computing product division within the information infrastructure business.

EMC announced that it is making modifications to its products and licensing model so that the technology architecture of its information governance applications can support various cloud architecture and deployment models. (For more on the cloud architecture and deployment models, see "*Security Guidance for Critical Areas of Focus in Cloud Computing V2.1*," Cloud Security Alliance, December 2009.)

CHALLENGES AND OPPORTUNITIES

Organizations, service providers, ISV and hardware vendors, technical standards bodies, and government agencies have to collaborate and harmonize efforts in order to address both policy and technical challenges to cloud computing.

First, the absence of a cohesive regulatory and legal framework to address potential conflicts in data privacy, segregation, archiving, and protection requirements across national and state jurisdictions could make the management of technical protocols complex and prohibitively expensive, thus obviating the promise of operational cost

efficiencies. Today, CIOs and cloud service providers continue to bemoan the typical 300-page cloud service contracts. Multiply these contracts by the number of jurisdictions and service providers and it becomes fairly obvious why this is not a sustainable strategy for managing cloud service relationships. In the United States, regulators (like the FTC) and legislative bodies (Congress and Senate) need to do a better job in providing guidelines for harmonizing the labyrinth of state and local data regulations. Globally, organizations and government agencies have to work together to encourage the adoption of retention management, information security, and data protection and privacy standards. Best practices and standards around cloud service management, cloud audits, and service assurance also have to be in place.

The on-demand, automated resource provisioning, and highly abstracted relationships that are inherent to cloud computing present technical challenges that must be addressed, including:

- ☒ Monitoring and remediating potential data management, segregation, and security compliance conflicts.
- ☒ Tracking dependencies and enforcing compliance to information governance policies across information and application infrastructure with metadata infrastructure and IT infrastructure.
- ☒ Managing user access, provisioning, and entitlements, and balancing these requirements against performance and budget constraints.
- ☒ Auditing and providing assessment, assurance, and reporting services across multiple cloud deployments can be cumbersome and potentially expensive since the development of a secure, open, extensible, and common interface is still in its infancy.

CONCLUSION

Organizations across a broad range of company size bands and industries would find the lower acquisition and deployment costs, the quick time to deployment, the ability to provision and scale quickly in response to rapidly changing business requirements, and the pay-as-you-go model as the primary benefits of cloud computing.

Cloud computing and virtualization changes the risk profile of information assets. The layers of abstraction inherent in these technologies also pose challenges in effectively tracking and executing technical controls around confidentiality, data integrity, and availability. These information governance issues impede higher adoption of cloud computing among organizations.

Services vendors, in partnership with EMC, have an opportunity to provide a broad range of value-added services that would enable organizations to plan for and address these information governance challenges effectively across their on-premise and cloud-based environments. These value-added services and capabilities would enable services vendors to differentiate their solutions, improve their stickiness, and realize higher margins.

As more cloud services enter the market, providers should look for ways to protect their competitive position. Information governance cloud services present huge transformational opportunities for service providers. To take full advantage of these opportunities, service providers should consider partnering with ISVs whose application architecture and licensing models are able to support the various cloud architecture and deployment models.

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2010 IDC. Reproduction without written permission is completely forbidden.