

Creating Information Advantage in a Cloudy World

Intelligent Governance Strategies for Cloud Agility

Report and recommendations based on discussions with the
Leadership Council for Information Advantage

William Awad Senior Vice President and Chief Technology
Officer, The Hartford Financial Services Group

Dave Blue Senior Manager, Enterprise Data Services, The
Boeing Company

Guy Chiarello CIO, JPMorgan Chase

John Chickering Vice President, Fidelity Investments

Dimitris Mavroyiannis General Manager – Group CIO,
Eurobank EFG Group

Sanjay Mirchandani Senior Vice President and Chief
Information Officer, EMC Corporation

Joe Solimando Senior Vice President, Global Operations
and Technology, CIO, Disney Consumer Products

Deirdre Woods Associate Dean and CIO, The Wharton
School, University of Pennsylvania



Contents

About the Leadership Council for Information Advantage	3
Executive Summary	4
Cloudy Days Ahead	7
Rising Clouds: A Perfect Storm for Information?	8
Governance Strategies to Maximize Information Advantage in the Cloud.....	9
#1: Find a good test case	10
#2: Own the information, even if you own nothing else	13
#3: Don't take terminology for granted	14
#4: Hope for standards, but prepare to integrate	14
#5: Control cloud platform proliferation	15
#6: Make your information "cloud ready"	16
#7: Master solution integration	17
Conclusion.....	17
Appendix: Leadership Council for Information Advantage Member Biographies	18



About the Leadership Council for Information Advantage

The rapidly shifting dynamics of competition coupled with the unprecedented, exponential proliferation of information have made it extraordinarily challenging for business leaders to make informed decisions about how their companies can best compete and grow. This lack of insight is especially perilous now, when volatile business conditions leave little room for error. Change is essential as the strategies set in motion today will determine which organizations lead their markets tomorrow.

While most information technology leaders recognize the need to better leverage information for business advantage, many still struggle to translate this aspiration into concrete strategies and action plans. This is why EMC is working with some of the top information technology leaders in the world to identify winning strategies for information advantage: strategies for leveraging information to compete more efficiently, increase customer loyalty, grow market share, and identify new sources of business value.

EMC has convened the [Leadership Council for Information Advantage](http://www.councilforinformationadvantage.com), an advisory group made up of global information leaders from “information-advantaged” enterprises—organizations from a variety of industries that are successfully using information to revolutionize how they compete and do business. We are conducting in-depth interviews with the members of this Council and publishing their ideas in a series of reports that provide candid lessons learned, proven best practices, and expert guidance on how to transform information into business value.

This report, the second in a series from the Leadership Council for Information Advantage, provides top-level guidance on how organizations can begin enacting the organizational, technological, and cultural changes required to achieve information advantage in cloud environments. Future reports will explore other critical focus areas required for information advantage success.



EMC invites you to join this important conversation. Please visit www.councilforinformationadvantage.com to download Council reports and to contribute ideas for future reports.

Information advantage defined

When an organization leverages information to revolutionize how it competes and transform how it does business, it has gained an information advantage.



Executive Summary

Within today's context of rapidly compressed business cycles, greater customer choice and globalizing competition, information is more essential than ever to gaining competitive advantage. The cloud promises to greatly improve and speed our ability to access, process, and share information by abstracting the underlying infrastructure so that information and content can flow unfettered.

Private clouds have been the first to be adopted, particularly since many organizations can realize immediate operational and cost benefits while still preserving control over the applications and information residing in their private clouds. Yet, some organizations are already looking to the next step: integrating external technology providers to further enhance the service capabilities and operational efficiency of their cloud environments. As the prospective benefits of leveraging external service providers continue to grow, many enterprise clouds will integrate outside cloud infrastructure or platform services. Some will even integrate whole public cloud services to create new hybrid models of cloud computing. We already see examples of this happening now, including in some of the companies represented in the Leadership Council for Information Advantage.

The rise of external service providers introduces new complexities, as well as benefits, into the delivery chain for cloud services. The leading areas of concern, according to a survey from IDG Research Services, relate to managing and safeguarding corporate information in clouds with externally hosted components. This is particularly true as information and application control moves off-premise to third-party providers. Without early planning and consideration, the evolution of more complex hybrid models could lead to the following concerning conditions, which are weighing on the minds of today's CIOs and IT professionals:

- Growth and proliferation of incompatible cloud services
- Isolation of valuable corporate information within cloud-based silos
- Escalating potential for vendor lock-in
- New complications in enforcing information security and policy compliance

If not planned for, these emerging conditions will impede the flow and value of corporate information for years to come. The main driver behind these problems is the classic challenge of information silos – the lack of cloud interoperability standards, lack of shared services that underpin multiple applications, and lack of tools to access information across applications. Like in on-premise installations, these gaps present a serious challenge in sharing information between applications, systems and even across cloud environments. Today's solutions providers are busy tackling the barriers to interoperability: embracing open standards, building shared services and creating standardized technology platforms, as well as creating APIs that help automate the integration of services across clouds.

Although solutions providers are making progress on the technology front, CIOs still see a gap between where cloud services are and where they need to be, particularly when they involve outside service providers. While they look forward to a time when standards have evolved and cloud platforms are fully enterprise ready, they don't want to sit on the sidelines waiting for cloud maturity and lose the competitive and cost advantages of moving IT services to the cloud today. Additionally, business units in some organizations are forcing IT's hand by independently provisioning public cloud services – sealing the deal with a corporate credit card and a user terms and conditions checkbox. As a result, organizations increasingly find themselves supporting hybrid environments in which some information resides in public clouds, some resides in externally hosted private clouds and some resides within the enterprise, either in traditional or virtualized data centers.

The net result is that organizations are at risk of fragmenting their information architecture, isolating valuable corporate information within disparate applications and cloud services. It's not unlike the enterprise data silo problems of the '90s, when information was locked within ERP and CRM applications, requiring massive systems integration efforts. However now, the business consequence of siloed data is more urgent: in today's climate, if you can't access and use your information, you've surrendered your business agility and lost an important competitive edge.

Fortunately, in spite of the rapidly rising rate of cloud adoption, the missteps leading to cloud information fragmentation have only just begun. To keep it from devolving into an unmanageable state, organizations must move quickly to establish a technology strategy for the emerging heterogeneous cloud landscape and a uniform set of policies that will preserve the integrity, utility and value of their corporate information in the cloud.

The [Leadership Council for Information Advantage](#) makes three fundamental assertions in this report about creating cloud-based information advantage:

1. Organizations that actively shape their cloud deployment strategies and extend strong information governance practices into the cloud will maximize their ability to leverage information for business advantage.
2. The move to the cloud does not change information governance requirements, but it does transform the risk factors and will increasingly challenge IT creativity in developing new strategies and mechanisms for policy compliance and enforcement. This is particularly the case for hybrid cloud environments, in which IT services are delivered through a mix of internal cloud resources and external service providers.
3. Best practices for information governance in the cloud will require less of an owner-operator mindset and more of an emphasis on solutions integration and vendor management. IT organizations that mobilize now to integrate flexible cloud platforms and adroitly manage complex chains of relationships, both internal and external, will ensure their businesses reap extraordinary benefits and achieve true information advantage.

The Council also lays out a road map for successfully achieving information governance in a cloudy world:

#1: Jump into the cloud with a good test case. Start out slow and identify a pilot project to begin developing your organization's cloud capabilities and experience in managing externally operated cloud services.

#2: Own the information, even if you own nothing else. Assert your organization's right to own the information, even if you don't own the infrastructure, application or service associated with that information.

#3: Don't take terminology for granted. Review information governance policies to identify areas of highest risk. Then, establish authoritative definitions for key vocabulary in those areas and require external partners to comply with your standards.

"We're standing at the doorstep of a new computing strategy with the cloud. If we're not careful, we're poised to recreate many of the mistakes we made in the mid- and late-1980s. Businesses today can choose a variety of cloud services for their ad hoc needs, creating isolated services with their own islands of information. This approach may serve their short-term needs, but they'll create challenges that may persist for years."

—John Chickering, Fidelity Investments



Classifying Internal, Private and Public Clouds

Private cloud describes an IT infrastructure in which a shared pool of computing resources—servers, networks, storage, applications and software services—can be rapidly provisioned, dynamically allocated and operated for the benefit of a single organization. Private clouds are similar in many ways to the traditional IT service delivery model, with three key differences:

1. IT resources are virtualized, leading to much more efficient use and flexible allocation. Most notably, virtualization enables the dynamic transfer or sharing of services within the cloud infrastructure and the secure partitioning of services for multitenancy. “Tenants” sharing a server or application can be either completely different companies in an external cloud scenario or different business functions or groups within internal clouds.
2. The organization needn’t physically own or operate the IT assets that form its private cloud. Some assets can be outsourced to cloud providers: for instance, outside data centers may be leased to run specific applications. Nevertheless, the organization still effectively “owns” its private cloud by controlling and setting policies governing how virtual IT assets are operated, with cloud vendors guaranteeing specific levels of service and conformance to agreed-upon standards for information security and compliance.
3. Within a virtualized environment, just about everything can be measured, including CPU cycles and bits transmitted. As a result, clouds can be monitored

at a highly granular level beyond the typical latency- and performance-based measurements of traditional IT environments. This opens up the potential for usage-based billing or charge backs, something that’s already common with public cloud services, such as Amazon’s Elastic Compute Cloud (EC2).

Internal clouds are a type of private cloud in which all aspects of IT service delivery are physically owned and operated by the organization itself. In terms of monitoring and proving compliance with information policies, organizations presumably have complete visibility, transparency, and control over their internal clouds, because they own and maintain the entire cloud infrastructure, from servers to services.

Public clouds refer to shared cloud services that are made available to a broad base of users. Although many organizations use public clouds for private business benefit, they don’t control how those cloud services are operated, accessed or secured. Popular examples of public clouds include Amazon EC2, Google Apps and Salesforce.com.

Many organizations have adopted different cloud models simultaneously, leading to a hybrid cloud environment in which some IT assets and services are hosted in internal clouds while others are delivered through externally hosted private clouds and public clouds.

The cloud is used throughout this report by Council members to refer to cloud computing and cloud services in the aggregate, regardless of type.

#4: Hope for standards, but prepare to integrate. Anticipate the need to integrate cloud-based information down the road and lay the strategic groundwork for future data integration activities now.

#5: Control cloud platform proliferation. Look for shared requirements in standardized business functions such as finance, HR, and CRM, and consolidate services organization-wide on a limited number of cloud platforms wherever possible.

#6: Make your information “cloud ready.” Encrypt information and reorganize data sets so they’re accessible and usable across multiple platforms.

#7: Master solution integration. Shift IT’s focus from owning and operating IT systems to becoming master information service integrators.

Cloudy Days Ahead

Without a doubt, we have entered the Era of the Cloud. A recent [Pew Research survey](#) found that more than 70 percent of technology industry thought leaders and practitioners expect to access and share information primarily through the cloud by 2020, versus using applications on desktop computers.¹ Other IT industry analyses and surveys show that organizations across the globe are virtualizing their IT infrastructure and applications right now. A CIO Market Pulse survey commissioned by EMC’s Information Intelligence Group revealed that 74 percent of organizations either have IT services already running in clouds or are planning to implement cloud services in the next year².

Organizations are moving to the cloud because they believe it will give them a business advantage: the cloud positions them to provision and scale IT services quickly and conveniently, oftentimes for a much lower cost. This is why virtualized data centers and private clouds have taken off so quickly. But while enticed by the potential benefits of the cloud, many companies are reluctant to adopt off-premise cloud services because of information risks. They’re unsure whether they’ll be able to manage corporate information to comply with corporate policies and government regulations, including security requirements. The study from IDG Research revealed an overwhelming 91 percent of organizations expressed serious concerns about information management, security, compliance, and e-discovery in deploying applications and information in cloud environments.

In response to organizations’ varying appetites for risk, complexity, utility, and cost, different types of cloud services have emerged (see “Classifying Internal, Private and Public Clouds” in previous section). All private clouds, whether enterprise-owned (an internal cloud) or externally hosted, afford high levels of flexibility, control,

1 “The Future of Cloud Computing,” [Pew Research Center’s Internet & American Life Project](#) and [Elon University’s Imagining the Internet Center](#) (June 2010)

2 “Cloud Computing: A CIO Market Pulse Survey,” CIO Custom Solutions Group and IDG Research Services (Aug. 2010)

“People choose a cloud service because it’s faster and more pragmatic and easily available and cheap. And I think all the structures and planning have the potential to go out of the window because of that.”

—*Deirdre Woods, The Wharton School*

“A lot of the early migration to the cloud was driven by economics. But closely intertwined with this driver was the possibility of supporting a better level of service. Now, I think service quality is really the driver. It has never been purely a decision based on how you can wring out costs. The win-win of the cloud is that I get better service, I provide a higher quality, and because we can aggregate the (standardized) needs of various business units or segments, we should achieve a scale that gets us a better price.”

—*Joe Solimando, Disney Consumer Group*

“The cloud is the new frontier of efficiency. You can either take a wait and see view or develop a strategy to lead the charge. In the financial services industry, we spend 10 to 12 percent of our net revenue on technology, so there’s a lot at stake. We need to keep making our operations and technology more efficient. We can’t afford to wait.”

—*Guy Chiarello, JPMorgan Chase*

“The potential value of the cloud is in being able to expand or contract capacity rapidly. This is especially true in areas of your business with highly volatile volumes of data or information that drive demand for more resource, whether for storage or for CPU cycles. That’s where cloud provides good economic return, because you won’t have to worry about being stuck managing a lot of excess capacity.”

—Dave Blue, *The Boeing Company*

“There are huge logistical issues with moving terabytes of data from data centers into a cloud. It’s not an easy proposition to move data at a certain scale. Once this data is no longer in your data center, if you wanted to change cloud providers, you would need to be comfortable that there were the infrastructure and processes in the cloud to allow for the portability of data.”

—William Awad, *The Hartford*

“Some people are concerned that their information may get locked away within a cloud offering and become less reusable or accessible. Well, that’s a problem. You’ve basically abdicated your responsibility to manage that information for your company, and you’ve really limited your options in terms of information portability and changing cloud service providers.”

—Dave Blue, *The Boeing Company*

and customization. They’re typically customized services, built to order for your organization’s specific needs and requirements. As a result, private clouds may cost more than provisioning similar off-the-shelf services from public clouds, but the customization and increased control make private clouds better suited to business applications and processes handling sensitive corporate data.. Public clouds, on the other hand, often provide best-in-breed features at very low costs. Because they’re designed for the general requirements of many corporate customers, public clouds offer standardized functions with limited configurability. In general, public cloud users understand the trade-off for high utility and low cost is “you get what you get and you don’t get upset.”

As cloud offerings mature, some of the trade-offs between private and public clouds will become less pronounced. Clouds are evolving rapidly, and the sheer number and variety of service options, combined with the current lack of interoperability among them, challenges CIO’s to develop a cohesive, efficient cloud strategy for the enterprise.

Rising Clouds: A Perfect Storm for Information?

The cloud promises to improve and speed our ability to access, process, and share information. Yet, a “perfect storm” of conditions are emerging that threaten to impede the flow and value of corporate information:

1. Growth and proliferation of incompatible cloud platforms and services—The ease and convenience of adopting public cloud infrastructure and software services make it increasingly likely that smaller groups within organizations will independently go with such services without considering how they may fit into the enterprise’s IT infrastructure as a whole. Sometimes, this results in different parts of the same organization using incompatible business applications for similar functions, which not only detracts from potential economies of scale, but also increases the number of systems and services that internal IT needs to integrate and support.
2. Data Silos 2.0—Without planning and integration, a cloud’s information repositories aren’t readily accessible to the organization’s other IT systems, business processes or groups. This can lead to cloud-specific silos of information that aren’t backed up, particularly in public clouds. The problem is exacerbated by the increasingly common practice of business users provisioning new cloud services with only their ad hoc requirements and a corporate credit card. Information access and portability will be major concerns as organizations move their IT services to the cloud. If cloud-based information silos are allowed to take root, integrating these silos may require future integration efforts of an epic scale.
3. Escalating potential for vendor lock-in—Cloud providers provide custom APIs for porting services and data to their platforms. While a few, such as Salesforce.com, have achieved sufficient market success to become de facto standards within their segments, the overall market for cloud services is still highly fragmented. Selecting a cloud platform can mean, for all practical purposes, a long-term vendor

commitment. Although switching to another cloud platform may not be as costly and time-consuming as shifting from IBM UNIX to Wintel servers, the potential for lock-in is remarkably similar to what we saw with IT hardware 15 years ago.

4. Complex chains of custody for information management and security—As organizations shift different IT services to various clouds, they complicate the chain of custody for information, which may now reside both in-house and in external private or public clouds. Cloud vendors throughout the service delivery stack must be monitored to ensure they're managing enterprise information appropriately and enforcing policies regarding information security, privacy, e-discovery, archiving, and backup.

These four emerging patterns make it highly challenging for organizations to effectively access, assimilate, analyze, and apply their valuable corporate information. In today's business climate, information is tantamount to business advantage. It's imperative that organizations maximize their ability to tap information for clearer market insight and faster response times.

Organizations that allow their information to become scattered and locked within various clouds risk losing its full utility and value. This problem can be minimized with some foresight, planning and strategic technology investments. Organizations should take action now to unify their information architecture while taking advantage of the cloud's benefits in terms of convenience, speed, scalability, and cost.

Governance Strategies to Maximize Information Advantage in the Cloud

To maximize the accessibility, utility, and value of corporate information, you need a set of guidelines to ensure information is treated in a consistent way, regardless of whether it resides within traditional enterprise data centers or in clouds. Historically, such guidelines in enterprise environments have been called "information governance." (See sidebar.)

The basic tenets of enterprise information governance can and must be extended to the cloud to help preserve the integrity and usefulness of cloud-based information. If you're just virtualizing your data center to form an internal cloud, the governance changes required will be very minor. For externally hosted private clouds and public clouds, policies around security, access, compliance, archiving, and information life cycle management don't change: you're still accountable for meeting the same regulatory, privacy, and administrative requirements. However, the controls used to enforce those policies and requirements will change: due diligence in vendor selection, performance and indemnity clauses in SLAs, vendor reports and activity logs, third-party audits and certifications. These controls may be different from the governance controls organizations had when everything belonged to them and they could physically recover a hard disk if a server went down. But while these vendor-oriented controls are different, they're not difficult. Managing vendor relationships is a skill every IT department has fine-tuned over the years.

What is Information Governance?

Information Governance is policy-based management of information designed to lower costs, reduce risk and ensure compliance with legal, regulatory standards, and/or corporate governance. It governs how information is accessed, secured, and handled throughout the organization, regardless of whether the information resides in paper documents or in encrypted data streams in the cloud.

Information governance policies set the right conditions for people, processes, and technologies to efficiently manage, locate, and deliver information when and where it's needed: What information does my organization have? What information does my organization need to keep? Is information synchronized and consistent? Do the right people have access to the right information at the right time?

The ultimate goal of information governance is to make it faster and easier for organizations to extract actionable insight and value from information in support of their business strategy.

The first Leadership Council for Information Advantage report, [Creating Winning Strategies for Information Advantage](#), presented some recommendations for organizations seeking to improve their information governance practices.

“Information management strategy is about seeking the value-add in information and in commodity processes or functions and integrating them in a manner that creates unique business value better, faster, cheaper than your competition.”

—John Chickering, *Fidelity Investments*

“Cloud computing offers tremendous scale, mobility, and agility. However, if information, governance and compliance policies do not evolve in the cloud, it can create complexity in your IT environment. IT professionals need to spend time defining these policies, so there are rules for capabilities, such as information mobility, to satisfy business demands and governance obligations.”

—Sanjay Mirchandani, *EMC*

“We need to recognize that policy needs to be a living document that grows with the business. As the business changes and as tools and techniques create new opportunities, policy must similarly be able to adapt.”

—John Chickering, *Fidelity Investments*

“Responsibility for information ultimately lies with the owner. The responsibility of the cloud service provider should simply be to ensure the functionality of their service, including enforcement of the technical controls, perform to spec. If they are performing within that specification and a problem occurs, then perhaps the owner has a gap in policy or an error in the configuration of that service.”

—Dave Blue, *The Boeing Company*

Instead, the guidance in this report focuses on uncovering and avoiding the hidden danger zones—some of the easy-to-miss stumbling blocks that can hurt your ability to harness and use information in the cloud. Many of these observations and lessons apply regardless of whether your IT resources are in-house or in a public cloud. Nonetheless, these recommendations can help your organization adapt its information governance practices to a cloudy world and keep control over enterprise information as more and more of it travels through the cloud.

#1: Jump into the cloud with a good test case

Organizations have different appetites for risk and different views on what types of applications, services and information are right to outsource to the cloud. Regardless of their specific concerns and limitations, most organizations should be able to identify a safe way to begin developing their capabilities in managing cloud services. Gaining experience now with cloud services is essential to taking advantage of higher-value future opportunities emerging in the cloud.

Finding a low-risk test case may not be as straightforward as it sounds. Information and IT services that seem like they'd be easy to deploy in the cloud sometimes aren't. Following are four questions to ask when evaluating which IT services lend themselves to “cloudsourcing,” particularly as external private clouds and public clouds.

Can compliance requirements be balanced safely with other priorities? Once you move regulated information to private clouds with external components or to public clouds, the chain of custody for information becomes more complex. Because of this, many IT professionals assume that policy compliance is harder in the cloud. We think it's a matter of perspective. Even though you have to factor in cloud vendors' logs and attestations in assessing your overall compliance posture (which certainly complicates compliance reporting), you no longer have to bear responsibility for maintaining the IT assets running your services. It's a trade-off.

While failing to meet compliance requirements is never an option, IT leaders need to help their organizations assess new sources of risk, such as chain of custody exposures, introduced by the cloud. Then, once new risk sources are

understood, organizations can explore whether compliance obligations may be met in new ways so the organization can reap the benefits of the cloud. In our experience, cloud services rarely pose insurmountable challenges for compliance; they simply change the mechanisms for monitoring and enforcement. The real question is, are the perceived benefits of the cloud great enough to justify changes in organizational processes and compliance procedures?

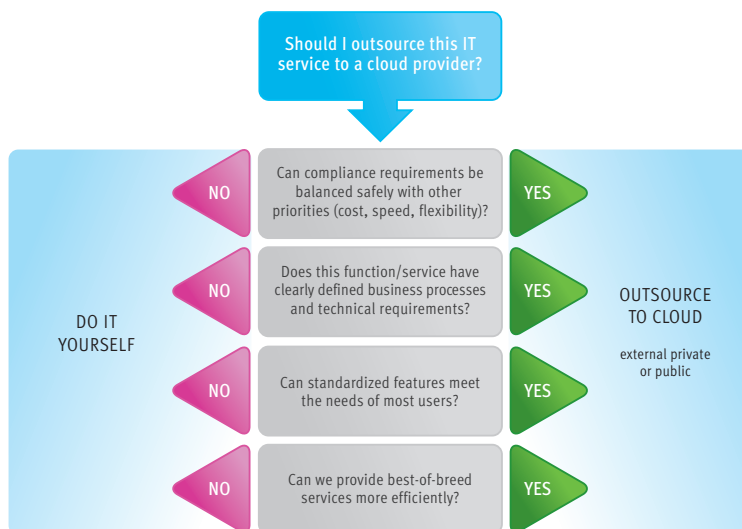
A good illustration of this is e-mail outsourcing. Many organizations today are struggling with whether to move their e-mail to the cloud. Organizations are choosing between hosting their own Exchange servers to meet various e-mail requirements or outsourcing e-mail and learning how to audit e-mail vendors for compliance reporting. For some companies, the potential cost-savings and improved service availability of partnering with an outside service provider more than offset the extra steps in compliance assessments.

In addition to chain-of-custody complications, the cloud introduces new compliance challenges in controlling the transmission of regulated information across national boundaries. For instance, banks keeping financial records of Canadian government employees cannot transmit these records or any related correspondence outside of Canada. Many European countries have similar regulations requiring certain information about their citizens be stored only within their national boundaries. Multinational organizations and cloud providers must conform to these requirements by operating their cloud data centers in specific countries. Furthermore, backup and disaster recovery, e-discovery requirements, as well as information access by cloud administrators based in foreign jurisdictions, must be carefully handled to comply with local regulations. Most cloud providers are familiar with the unique information requirements of the countries where they operate, and they've tailored their cloud services accordingly. For most organizations, addressing the boundary-specific challenges introduced by the cloud is a matter of choosing service providers with experience in regulated jurisdictions and writing restrictions and penalties for non-conformance into contracts.

“It’s not about if you use a public cloud, it’s about when to leverage a public cloud and how you execute it. One of the top issues we all face with this execution is the privacy and protection of information. We have to solve these challenges to move our cloud strategy forward.”

—Guy Chiarello, JPMorgan Chase

Decision-making model for “Cloudsourcing”



“I believe that to outsource something to the cloud, you first need to master it yourself. You need to know the details and challenges so clearly that you can specify exactly what you need.”

—Dimitris Mavroyiannis, Eurobank EFG Group

“A successful implementation of cloud computing requires a clear vision of how you want to leverage it and what it takes to get it done. For [our collaboration service], we had clarity of vision, understood the steps to take and recognized that leveraging a public cloud dramatically improved our time to market. We found a partner we knew had the skill and product sets, previous experience and commercial backing to make it work.”

—Guy Chiarello, JPMorgan Chase

“Computing, networking, and storage infrastructure are very important to us, but these assets are largely standardized across business units and segments. This means we not only can get better economies of scale but they’re also further along the evolution path where it makes sense for us to buy them as a service.”

—Joe Solimando, Disney Consumer Group

“Going with a cloud service is like buying an asset with an out-of-the-box functionality. Three or four years ago, our bank would never have accepted software without customization, because the perception has always been we do things differently here. Now, to reduce costs, everyone is willing to go without customizations, and they’re realizing that out-of-the-box functionality is not so bad. That’s an amazing cultural change for us, and it paves the way to do more with [public] clouds, where the room for customization is much less.”

—Dimitris Mavroyiannis, Eurobank EFG Group

“The cloud is not an infinitely flexible concept. The reason it makes economic sense for someone to build it is because there’s a limited number of options for it to support.”

—William Awad, The Hartford

Is it an IT function or service your internal organization has mastered? Organizations often are tempted to outsource things they don’t fully understand, thinking vendors can provide all the requisite expertise and solutions—essentially a magic bullet. Looking for outside solutions to poorly defined problems can be especially tempting when time is of overriding importance in getting an IT service up and running. While building from a ready-made cloud platform or outsourcing IT services to cloud vendors can save valuable time, if program requirements aren’t clearly understood, costs inevitably balloon and the organization often ends up stuck with an imperfect solution. When assessing which IT assets to move to the cloud, it’s best to start off with a function or process your organization already knows inside and out. That way, you recognize the conditions for success, can lay out detailed requirements for what matters, and you know what exactly to look for in prospective vendors.

Can you use a standardized service? Processes or functions that are standardized across companies or business units naturally lend themselves to the cloud. Public cloud services often provide best-in-breed functionality for lower cost. The downside is less customization and control, but that might not be a big deal for many standardized services and functions. Salesforce.com is a classic example of this. Its features are well suited to managing customer information and sales processes, whether you’re selling paper or professional services. Nevertheless, we’re seeing a trend toward configurable public cloud services as cloud providers increasingly offer industry-specific permutations or more granular controls to tailor their offerings to a wider range of customers.

Is the pilot project easily implementable? In scoping out projects for public or externally hosted private clouds, if you have to choose between process complexity and technical complexity, choose the latter. In our experience, the technical aspects of cloud adoption—experimenting with APIs, systems

integration and service testing—are the easy parts. Business process and service delivery issues tend to be more challenging.

Many IT teams think that just because the application or service they're moving to a cloud isn't "mission critical," the process will be quick and straightforward. This isn't always the case. If your organization hasn't worked with a cloud provider before and you're setting up a private cloud with custom features, it may take time to delineate what the service provider is responsible for and what your obligations are. Compliance and liability issues can be major sticking points. Defining compliance conditions and establishing liability for intellectual property protection with cloud providers are issues that span well beyond IT. Consequently, they can take a lot of time and coordination to resolve.

Previously, it seemed private cloud service providers offered more expansive liability clauses. Nowadays, standard liability clauses are more restrained (and arguably realistic), setting limits for financial compensation or stricter conditions on determining fault. IT teams should expect process challenges to occur even in seemingly straightforward projects that aren't handling any regulated or sensitive information.

While it seems process issues should present more of a challenge in public clouds, they often don't. Users typically sign up for services ad hoc, agreeing to strict terms and conditions in which public cloud providers typically promise nothing and assume minimal, if any, liability.

#2: Own the information, even if you own nothing else

Once you know what you're moving to the cloud, assert your organization's right to own the information, even if you don't own the infrastructure, application or service associated with that information. Externally hosted private cloud and public cloud services may offload the hassles of owning and maintaining expensive IT assets, but they don't offload information liability. If a privacy breach occurs with your consumer information in an external cloud, it's your company and brand that takes the hit.

Because your organization is liable for its information regardless of where it resides, your organization must have the means to manage it appropriately. Ironically, the people who often must be made to understand this are not your cloud vendors; they're your own employees.

It's unrealistic to prevent business units from provisioning their own cloud applications—a niche finance application here, a public cloud CRM service there—but the organization must institute policies and procedures to ensure the organization has the ability to monitor how cloud-based information is managed and, if needed, bring in that information for use within the enterprise.

Any new public cloud service that employees activate will inevitably involve the IT department at some point. When that happens, the organization's information governance policies should kick in. If the new service handles sensitive or regulated information (probably unlikely, but possible), is it clear that the organization has done the due diligence and put the contractual terms in place to safeguard that information? Has the organization trained employees on how to handle such information in cloud environments?

"If they haven't already, it's important for [IT groups] to start gaining experience delivering IT products and services in a virtual environment. The skill sets are different and you can't adopt this framework overnight. You need to invest now and be committed to it for the long haul."

—Guy Chiarello, JPMorgan Chase

"If the cloud is new to your organization, and you are able to, you should start with relatively low-risk areas where it's easier to get agreement, work through processes and build some success in the model area. Nothing breeds success like success."

—Joe Solimando, Disney Consumer Group

"Any company information you put in a vendor application—SaaS or otherwise—should be yours by right and you should be able to get it out. If it is an off-premise SaaS application you must manage your risk by replicating and/or extracting the information into your own managed environment. If you ever choose to switch vendors, you can transfer the information to someone else."

—Sanjay Mirchandani, EMC

“We need to educate our user communities about using cloud services. Just telling them they can’t do it isn’t enforceable. So, we need to advise people on how to manage their services as things go in the cloud, making sure they understand the need for backup and encryption. Education and guidance is essential. “Just say no’ doesn’t work.”

—Deirdre Woods, *The Wharton School*

“The cloud simply becomes an extension to your world: that’s how you have to look at it. We want to make sure we have ownership of our data (in the cloud) and can restore that data, if necessary. And the reason why we’d want to back it up internally is because we’re not comfortable with data portability.”

—William Awad, *The Hartford*

“We have worked with various parts of the organization to identify the few vital terms for technical controls and policies that demand additional rigor—those terms we absolutely have to perform to. By establishing an authoritative vocabulary around very important policies, we’re creating consensus on what needs to be uniform, what needs to be controlled for success.”

—Dave Blue, *The Boeing Company*

“The most important thing is to have a really good, clear understanding with your cloud provider about things like, where are your data living? How is backup done? How are your data actually encrypted? What does business continuity and disaster recovery look like in the cloud? Variations in these service details cost money, and if you do it cheap, it’ll often bite you.”

—Deirdre Woods, *The Wharton School*

How is backup handled by the service provider and is the information important enough to be duplicated within the enterprise? Because it’s often hard to forecast future uses for information, err on the side of caution by making sure cloud-based data and content can be brought back into the enterprise, even if you ultimately choose not to keep it.

#3: Don’t take terminology for granted

In working with cloud service providers, it’s often easy to overlook basic things like whether you define important terminology in the same way. Even though policies and regulations often detail how information should be handled, there’s always room for interpretation as to how to comply. For instance, Rule 17a-4 of the Securities Exchange Act requires instant messages and emails to be kept “in an easily accessible place” for two years. Your email cloud provider might have a very different interpretation of “easily accessible” than you do.

As a simple hypothetical, if a financial institution is asked to disclose all its dealings with a particular client within the last four years, will the search interfaces and message retrieval functions from the firm’s email provider be sufficient to support e-discovery and related report generation? Or will the cloud provider dump four years of raw data into that company’s lap and let them figure out how to sort and correlate the information?

Organizations should review their information governance policies to identify the elements of highest risk and establish authoritative definitions for key vocabulary in those areas. This should be done not only to ensure vendors’ expectations are aligned with your own, but also to help your internal organization focus on what’s absolutely essential to control. Once the definitions and key control points are identified, it makes it easier to figure out what IT assets need to be allocated or reconfigured to ensure everyone and everything performs to spec, outsourced or not.

#4: Hope for standards, but prepare to integrate

We’d all like assurance that cloud investments made today will interoperate with other clouds, now and in the future. But in reality, the cloud simply isn’t mature enough to have

developed standard specifications for platform interoperability and data exchange. XML as a data format is a useful carry-over from the web, but it's not compatible with legacy data formats used in many enterprise back-end systems. Various proposals for interoperability standards have been put forth for cloud components such as virtual machine metadata, service provider APIs, and identity management, but it's still very much early days.

In the meantime, organizations entering the cloud do so with some risk. If they invest in porting a lot of their information and applications to a particular cloud vendor's API, they risk vendor lock-in. But staying out of the cloud probably isn't a realistic option either, since it's so easy for users with a credit card and a perceived business need to provision their own cloud services. Just as the Web compelled us to integrate e-commerce systems to legacy ERP and open source spawned a mass porting of code from proprietary UNIX, IT teams must proactively anticipate and plan for the next stage of information integration in the cloud.

The trick is to lay the strategic groundwork early for data integration down the road. Organizations should insist their cloud vendors provide clear documentation on the data formats and schemas used to store information in their systems. Preferably, organizations should keep information architecture top-of-mind as they select cloud service providers.

#5: Control cloud platform proliferation

In the absence of cloud interoperability standards, the best way to limit information fragmentation—and head off a huge integration effort years down the road—is to try to minimize the number of different cloud platforms that require support. Admittedly, this is much easier said than done. Business groups need the flexibility to choose IT tools that support their work, and IT needs to support the business's ability to differentiate and gain a competitive edge. Rarely does that involve standard tools.

But to the extent possible, IT teams should help business units look for shared requirements in standardized business functions such as finance, HR, and CRM. Then, teams can identify cloud platforms that meet these various needs and consolidate the organization's services on them wherever possible. This should not only improve your organization's ability to share information across business units, it should also result in greater negotiating leverage for favorable contract terms and pricing, as you'll be offering up a bigger piece of business.

As discussed in the [first Information Advantage report](#), standardizing information platforms is very hard to do without buy-in at the top levels of the organization. It's up to the CIO and other business leaders to prioritize information architecture in the selection of new IT systems and services—including cloud platforms—and to support measures to maximize the utility of information within their organizations. With these goals in mind, it's crucial for IT leaders and business executives to collaboratively develop a strategic plan for how the organization will make use of the cloud. The major components required for this kind of proactive planning are outlined in the sidebar on the next page titled "Creating a Cloudsourcing Roadmap."

"It will take time for the cloud to mature. We need to start at a small scale. This will give cloud providers the chance to work with clients and evolve and mature their capabilities over time to a point where a comfort level is there around the APIs, portability and security."

—William Awad, *The Hartford*

"We can't wait afford to wait for industry standards around cloud computing. To meet our business challenges, we need to get closer to the efficient frontier, and leveraging the cloud will help. To accomplish this, we are already down the path of private clouds and beginning to use public clouds. While you build an ecosystem of partners, you need to develop your own capabilities and frameworks. This helps you increase your efficiency while you are learning."

—Guy Chiarello, *JPMorgan Chase*

"We really try to accommodate special requirements in business functionality, because this is what allows for innovation. One of the elements of innovation is doing something differently in our business than in the business next door. And I know that the business next door can copy my idea in six months, but it gives me six months' competitive advantage."

—Dimitris Mavroyiannis, *Eurobank EFG Group*

Creating a Cloudsourcing Roadmap

1. Perform an analysis of what IT services, business applications or processes you want to deploy in the cloud and identify the optimal cloud service model to support it (e.g., internal cloud, private cloud using external data centers, public cloud, etc.). Sequence the services to be deployed over each of the next five years in a roadmap.
2. Define requirements for each service to be cloudsourced. Requirements should include service-level metrics such as response time and uptime and as well as security, regulatory, and other information policy restrictions that must be satisfied.
3. Conduct a financial cost/benefits analysis to establish a rationale for why each service should or should not be moved to the cloud. Consumption models should be clear: what is the unit cost component?

Please refer to an earlier section of this report, [#1: Find a good test case](#), for additional guidance on which IT services are ripe for cloudsourcing.

“With many cloud applications, you need to re-architect your stack in order to see real financial benefits. This requires a big investment up front. The reengineering of your internal processes and infrastructure to accommodate cloud services is the hidden cost of the cloud.”

—Dimitris Mavroyiannis, Eurobank EFG Group

“We look at virtualization and our private cloud as being a key enabler for the portability of information. When you’re working within a virtualized infrastructure of a private cloud, the mobility of your information becomes unlimited, constrained only by policy.”

—Sanjay Mirchandani, EMC

#6: Make your information “cloud ready”

The process of information integration is often much harder than the technology of data integration. It can be very difficult to muster the organizational will to tackle information integration projects. In some cases, it’s hard to prove potential ROI. In other cases, data integration projects are hard to justify in the face of competing priorities.

However, organizations that have organized their data sets well enough to use them across multiple platforms will be best positioned to take full advantage of cloud services. They’ll be able to migrate enterprise information to cloud services more easily. Organizations without well-integrated information will likely find themselves confined to infrastructure-level cloud services such as computing and storage. In the cloud, the companies that have already figured out how to use their information for business advantage will quickly widen the gap between themselves and the companies still struggling to make sense of their data and content.

This is why it is essential for companies to redouble their efforts to integrate their information and make it “cloud ready.” This means getting into the habit of encrypting data, a practice that’ll become especially important as more of your corporate information travels through externally operated resources in the cloud. It also means redoubling efforts to tag fixed data and consolidate storage repositories. Transformation technologies such as ETL tools (extract, transform, load) can simplify the conversion of data from one format to another. The goal should be to convert information into one common format—probably XML, the gold standard for the cloud. Information preserved as XML becomes more portable and broadly searchable, qualities that remain intact as you migrate services to the cloud, even if XML schemas differ between cloud solutions.

Furthermore, organizations should consider decommissioning outdated or underutilized legacy applications. Research from various IT research firms estimate that 10-20 percent of overall IT budgets support underutilized or aging applications. That’s a lot of money spent on shelfware. Decommissioning such applications not only creates opportunities to move data to XML, which can be more broadly used, it also can save organizations millions of dollars in system consolidation. Lastly,

companies should insist that their technology partners demonstrate deep understanding of these growing requirements and are equally passionate about making their own products and services cloud ready.

#7: Master solution integration

As fewer IT assets reside in internal data centers, technology professionals need to shift their focus from owning and operating IT systems to becoming master information service integrators. Along with linking legacy databases to SaaS, IT teams will also need to connect their various private and public clouds, creating a seamless service environment that works like a single cloud custom-made for the enterprise. This transcends solutions integration. It requires greater synchronization between IT departments and their vendors. It also requires IT managers to act less like a part of the service delivery chain and more like an orchestrator of the entire service experience.

In a cloudy world, service integration will become one of the corporate IT team's most important roles and responsibilities. By focusing on activities that add value to the business as opposed to simply managing an operational infrastructure, IT can truly become a partner to business.

Conclusion

It's probably unrealistic for most IT organizations to expect to fully control their organizations' entry into the cloud: most business units need some autonomy in selecting their IT tools and public cloud services are now so easy to provision that they often are in use before the IT group even knows it. Regardless of whether IT can dictate conditions for entering the cloud, IT nonetheless bears responsibility for organizing the data and content generated by cloud services so they support the company's broader business and information requirements.

Creating a unified view of information, whether it resides in-house or in public clouds, is paramount to creating business insight and, thus, achieving a competitive advantage. Even though early conditions in the cloud suggest that cloud services may fragment information more than unify it, this doesn't need to be the case. The key to protecting and increasing the value of corporate information assets lies in good information governance. The cloud won't change information governance requirements, but it will transform the risk factors and increasingly challenge IT creativity in developing new strategies and mechanisms for policy compliance and enforcement.

The IT organizations that can flexibly integrate new services and technologies and adroitly manage complex chains of relationships, both internal and external, will reap extraordinary benefits in a cloudy world. By integrating best-in-breed cloud solutions from external providers with in-house IT assets, technology leaders can create a seamless blend of information and services that help their organizations achieve true business agility and an information advantage.

"I'm shaping our IT group to become better at integrating services versus owning all the processes, development, applications, and infrastructure. I think it takes a higher level of management sophistication to integrate cloud services, even though it seems like a cloud service should be simpler."

—Joe Solimando, *Disney Consumer Group*

"You want the talent of your staff actually doing innovative, very strategically aligned work. Sending more commoditized work out on the cloud might free up your people to focus on things that are more important to your mission."

—Deirdre Woods, *The Wharton School*

Appendix: Leadership Council for Information Advantage Member Biographies

William Awad

Senior Vice President and Chief Technology Officer, The Hartford Financial Services Group

William Awad drives technology strategy and policy across The Hartford Financial Services Group. He defines overall architectural direction and standards for the company and has management responsibility for technical strategy, architecture, IT standards, vendor management for technical products, technical innovation, and architecture governance. Prior to The Hartford, Mr. Awad was CTO at Travelers for more than three years, leading the engineering, IT operations, and enterprise infrastructure technical architecture areas. He previously served as CTO of Travelers Personal Lines, where he led the delivery of their strategic speed-to-market program. From 1995 through early 2004, Mr. Awad was a senior executive in Accenture's Financial Services Operating Group, where his responsibilities ranged from large program management of complex system implementations to developing enterprise architecture models and implementing roadmaps to the design and implementation of high-performing technical architectures with a focus on distributed multi-tier/multi-channel technical architectures. Mr. Awad received a B.S in Computer Science and Mathematics from Lebanese American University and a Master of Science in Computer Science and Applied Mathematics from the University of Illinois at Chicago.

Dave Blue

Senior Manager, Enterprise Data Services, The Boeing Company

Dave Blue leads the delivery of enterprise data services within Boeing Information Technology. He previously led Boeing Information Architecture, where he was responsible for developing and communicating the vision, strategy, and architecture supporting information management disciplines and for applying this architecture to projects. As a member of the Chief Architects Council (CAC), he helped ensure that information architecture was integrated within the overall enterprise architecture. Mr. Blue's Boeing career has been in information technology, with progressively broader responsibilities in application development and maintenance, information management, and architecture disciplines.

Guy Chiarello

CIO, JPMorgan Chase

Guy Chiarello has worldwide responsibility at JPMorgan Chase for information technology functions. Mr. Chiarello joined the firm in November 2007 and is a member of its executive committee. Before joining JPMorgan Chase, Mr. Chiarello was chief technology officer and chief information officer for Morgan Stanley for seven years, responsible for the global strategy and execution of information technology for both its securities businesses and corporate functions. He joined Morgan Stanley in 1984 and served in a number of information technology roles over the majority of 23 years. Mr. Chiarello began his career in information technology in 1981 with the Treasury Department for the State of New Jersey. Over the past 10 years, he has been an executive advisor for leading public and private technology companies on business strategy and technology innovation. He has garnered industry and private sector recognition through various awards including Top Financial IT Executive by CIO Forum, Computer World Premier 100 Leaders, 2008 CIO of the Year by NASSCOM, and a special Alumni Citation Award from the College of New Jersey. Mr. Chiarello has a BS in business from the College of New Jersey.

John Chickering

Vice President, Fidelity Investments

John Chickering's experience as a consultant, software vendor, end user, and lecturer gives him a unique perspective on applying technology to manage information. He is a Vice President at Fidelity Investments, where he is currently working with document management, archive, and records management solutions. Mr. Chickering has delivered solutions in the public sector and financial services industries and has served as CIO at two human resource services companies. A former licensed merchant marine engineering officer, he began his IT career at American Management Systems, where he was a founding member of the firm's imaging practice. After nearly ten years, he moved on to spend two years at a workflow software vendor before joining Fidelity. Mr. Chickering has authored several articles and has spoken at both industry conferences and continuing education seminars hosted in academia. He is a member of AIIM's Board of Directors and its Emerging Technology Advisory Group. He is also an active volunteer with several community service organizations. Mr. Chickering holds an MBA (Operations Research) from the University of Maryland and a BS (Marine Engineering) from the United States Merchant Marine Academy.

Dimitris Mavroyiannis

General Manager – Group CIO, Eurobank EFG Group

Dimitris Mavroyiannis oversees all of Eurobank EFG Group's IT units, ensuring the various units are working as a whole to help achieve the bank's overall business objectives, as well as maximize the value of IT investments, optimize the utilization of IT resources, and assure information systems and the technological infrastructure are able to support the company's innovative business initiatives. Mr. Mavroyiannis joined the bank in 1999 to develop its Internet strategy and banking channel, a role that evolved into his leading a subsidiary specializing in e-business and e-commerce consulting and implementation services for the Greek market. Mr. Mavroyiannis was the CEO of this services group until 2004. He then served in various leadership roles for Eurobank EFG Group, including CIO of the bank's operations in Greece. Prior to Eurobank EFG Group, Mr. Mavroyiannis worked for IBM Consulting Group in Europe, as well as for smaller companies in Greece and abroad. He has an MBA from Imperial College London, an MSc from University College London, and a BEng from the University of Sussex.

Sanjay Mirchandani

Senior Vice President and Chief Information Officer , EMC Corporation

Sanjay Mirchandani is responsible for extending EMC's operational excellence and for driving technological innovations to meet the current and future needs of EMC's business. He also leads EMC's network of global delivery centers in India, China, Russia, and Israel. These centers support EMC's worldwide research and development efforts and provide customer support and shared services. Mr. Mirchandani most recently served as the senior vice president leading the EMC Office of Globalization. In this role, he identified global growth opportunities and built the EMC processes and infrastructure required for global expansion. He was also responsible for bringing in new strategic international partners into EMC's Global Alliances program. Prior to joining EMC, Mr. Mirchandani was Microsoft's Regional Vice President, Enterprise Services, Asia, where he worked with the region's largest customers and partners. He also held multiple management positions during his tenure with Microsoft, including President, Asia Pacific Region; President, South Asia; and Managing Director, India. Mr. Mirchandani earned an MBA from the University of Pittsburgh and a BA from Drew University.

Joe Solimando

Senior Vice President, Global Operations and Technology, CIO, Disney Consumer Products

Joe Solimando defines the strategic direction for information technology across all of Disney Consumer Products' (DCP) lines of business, which include licensing for toys, apparel, and hardlines products; retail stores; worldwide publishing; and e-commerce. He also serves as DCP's segment representative on The Walt Disney Company IT Leadership Board, which oversees The Walt Disney Company's information technology direction, standards, and company-wide IT initiatives. Mr. Solimando joined Disney in 1998 as vice president, operations & technology of Disney Consumer Products. In this role, he managed DCP's Shared Applications Services group responsible for the implementation and support of shared financial and HR business applications. He also led the planning, development, and implementation of operations and technology systems for several business units as the IT business partner for vertical businesses, including Walt Disney Art Classics, Disney Direct Marketing, Walt Disney Records, and Disney Worldwide Publishing. Prior to joining Disney, Mr. Solimando held the position of senior manager of information technology in the management consulting practice at Ernst & Young. In his 10 years with this firm, he worked on IT strategic planning, system evaluation, selection and implementation projects for many top consumer products, retail, entertainment and manufacturing companies. Mr. Solimando has also held information technology and project management positions at Wicke's Companies and Fluor Engineers. He holds both an MBA and a BS in Civil Engineering degree from The Pennsylvania State University.

Deirdre Woods

Associate Dean and CIO, The Wharton School, University of Pennsylvania

Deirdre Woods leads a 120-person organization at Wharton Computing in developing and maintaining technologies that further The Wharton School's leadership in research, knowledge creation, and teaching. In her years at Wharton, Woods has been instrumental in bringing student and faculty satisfaction with IT services to the highest level and has served as a strategic driver for some of Wharton Computing's most innovative technologies. As Associate Dean and Chief Information Officer, Woods ensures that all of the school's various technology initiatives and programs are effectively implemented.

EMC²
where information lives®

EMC Corporation
Hopkinton
Massachusetts
01748-9103
1-508-435-1000
In North America 1-866-464-7381
www.EMC.com

EMC², EMC, and where information lives are registered trademarks or trademarks of EMC Corporation in the United States and other countries.
All other trademarks used herein are the property of their respective owners. © Copyright 2010 EMC Corporation. All rights reserved. Published in
the USA. H4895 10/10