OPTIMIZING THE JOURNEY TO THE CLOUD: BALANCING TRUST, ECONOMICS, AND FUNCTIONALITY

Cloud adoption has taken off. The business benefits are compelling, cloud technology has matured rapidly, public cloud offerings have proliferated, and private cloud has proven a robust and secure platform for all kinds of business applications. It's no longer a question of whether to use the cloud, but how to use the cloud to optimize the cost-effective business performance of information systems and technology.

The question today is: Where does each application, or set of related applications, belong? In the public cloud, a private cloud, a hybrid cloud, or the organization's legacy computing environment? Where can each of these "workloads" offer the best combination of performance, cost, and flexibility? In this perspective, we'll show you how to answer that question by assessing representative workloads through three essential filters—economic, trust, and functional—and help you chart and accelerate your course to optimizing business services in the cloud.

EMC²

INTO THE CLOUD

A recent CIO Market Pulse survey by IDG found that nearly three-fourths of IT organizations are running business applications in cloud computing environments now or are planning to do so in the next 12 months.[i] In a McKinsey survey, nearly half of the responding companies are already running collaboration applications in the cloud, over a third are running customer relationship management, over a third are running finance or human resource systems, and a fifth are running supply chain or resource planning systems.[ii]

Business leaders appreciate the benefits of the cloud. In the McKinsey survey of both business and technology executives, 75 percent believe that cloud computing could drive value in their companies (another 16 percent aren't sure yet). What kind of value do they anticipate? Increased business flexibility, improved systems scalability to meet business needs, lower unit cost for IT, and better business continuity—in that order.[iii] Compelling as the direct economic benefits of the cloud are, these executives recognize that cloud computing is very much a business performance proposition.

Some organizations are still understandably hesitant to move their sensitive information and mission-critical applications to the more open, more networked, and less familiar environment of cloud computing. Security, reliability, and regulatory compliance remain the most common concerns about the cloud; however, those concerns apply primarily to public cloud services, and many of the risks are overstated.

Executives today are distinguishing between the public cloud, where the enterprise cannot maintain full control over its information assets, and a private cloud, where it can. A recent Gartner survey found that 76 percent of IT organizations will be pursuing a private cloud strategy by 2012 (and another 20 percent said maybe they will). When asked for a planned investment breakdown, 75 percent said they'll spend more on private cloud than public, while only eight percent plan the reverse.[iv]

Cloud Types

Resources are owned and managed by the provider and shared across customers. Scale economies can be high and costs low, but for the customer organization both transparency and control can be low. A variation is the community cloud, a multi-company, members-only version of a public cloud, usually centered on a common business process (e.g., for use by a purchasing consortium).

Resources are owned and managed by the organization and shared across it. The organization has scale economies and cost advantages (though not on a par with the public cloud) together with more transparency and control. Private cloud resources are usually on premise; however, an external private cloud can be operated by an outside service and still offer high transparency and control, including over asset location and segregation.

Hybrid cloud is a combination of public and private clouds. Today, most applications run in one cloud or the other. In more complex configurations, selected data moves back and forth, for example when a public cloud customer relationship management application shares data with financial applications in a private cloud. Sometimes a public cloud part of the hybrid serves as an on-demand extension of computing and storage infrastructure to handle peak loads or transaction volumes.

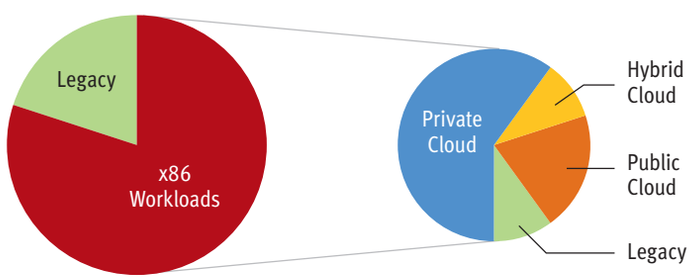
The most flexible and cost-effective computing environment today incorporates a federation of public and private clouds, with appropriate applications running in the public cloud, most mission-critical applications and those handling sensitive information running in a private cloud, and some applications crossing over and utilizing both public and private cloud services.

BUSINESS BENEFITS OF THE CLOUD

The potential economic benefits of cloud computing are certainly attention getting:

- With a private cloud platform, an organization utilizes its technology more efficiently and reduces the footprint and cost (including energy cost) of its physical infrastructure. Traditional data center costs can decline significantly.
- Commodity services like email and collaborative workspaces can be provisioned at lower cost thanks to the scale economies of the public cloud. With Software as a Service, the costs of using and maintaining business applications can be reduced. And with pay-by-usage, the ongoing cost of applications and other services can decline and align with real business need.
- By optimizing the distribution and management of workloads across public, private, and hybrid clouds, an organization can lower its total infrastructure and personnel IT spend by 25-30 percent.

AN OPTIMIZED CLOUD ENVIRONMENT YIELDS 25-30% SAVINGS IN TOTAL IT SPEND



As attractive as these direct cost and cost structure reductions may be, the greatest payback of cloud computing should be embedded in two other types of business benefits:

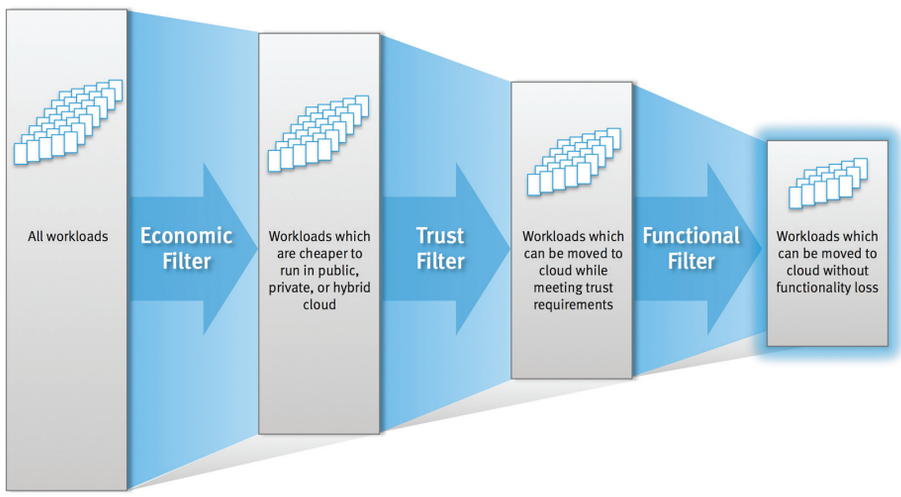
- **Productivity**. Business people have on-demand access to more information and the tools to use it. They can more readily collaborate and share information, expertise, and other resources. IT staff spend much less effort on the operations and management of everyday information systems and can focus more on technology-enabled business improvement.
- **Agility**. With on-demand access to modular information assets, people can assemble new business capabilities and bring innovations to market quickly. They can then scale those innovations up and integrate them into business operations with minimal disruption. They also can access, experiment with, and deploy new cloud-based business applications and services in record time.

By implementing a private cloud and chartering an associated center of excellence, a national transportation authority has been able to manage IT as a portfolio of services, monitor service levels in real time, and launch new technology-based business projects in a day instead of a month.

The cloud enables better business performance on multiple fronts simultaneously: cost, manageability, information access, new capability deployment, coordination and collaboration, business continuity and security, business innovation, and growth. It's the way for organizations to get the best mix of capabilities, performance, and cost from their computing environments.

WORKLOAD ANALYSIS USING THE THREE FILTERS

Businesses should evaluate specifically what applications and information are appropriate for cloud computing, and what type of cloud is the best destination for each. This involves looking at each asset and its potential migration to the cloud through three filters—economic, trust, and functional.



INITIAL WORKLOAD AND INFORMATION FLOW ANALYSIS

A workload is a specific asset, often corresponding to a business application or set of related applications together with the information they use. A workload can also be a service like email or collaboration workspaces, or a shared resource like a data warehouse.

Start by identifying the workloads that are candidates for movement to the cloud. Well-defined and modular workloads with few interfaces may be good candidates; difficult-to-reconfigure legacy systems would not. Analyze the data and applications associated with the workload. What are their business importance and value? Who uses them and how? In what workflows and in making what business decisions? Very importantly, where does the information originate and flow, both inside and outside the organization? And how important and sensitive is that information? The purpose of this initial analysis is to develop a working inventory of cloud-candidate workloads and understand them in sufficient detail to apply the three filters.

ECONOMIC FILTER

Assess the economic impact of moving each specific workload to the cloud. Look at its scale and transaction volume, including the number of users and the consumption of processing and storage resources—are these large enough to make a difference in terms of everyday operating cost?

Through consolidation, virtualization, and applications migration, a major European financial institution realized one-time savings of €500,000 and reduced annual cost per server by two-thirds.

The key to this economic analysis is deriving a reasonably accurate “all in” cost that includes the costs of both moving to the cloud and operating there. How much effort will be needed to retrofit the workload and its interfaces? How will the consumption of bandwidth and network management resources increase, including for backup and recovery, if the destination cloud is remote? How much will be saved in each of the basic IT cost categories after the workload moves to the cloud? What’s the bottom line for each individual workload?

TRUST FILTER

Before applying the trust filter, you should understand the characteristics and requirements of a trustworthy computing environment (see sidebar). And you should understand the different trust profiles of the potential destinations for workloads—public, private, and hybrid clouds, and the in-house legacy environment. In particular, recognize how a private cloud presents the opportunity to improve the trustworthiness of the computing environment through greater transparency, more granular controls, improved reliability and business continuity, and more precise and complete protection of sensitive information.

ANATOMY OF TRUST

A secure, compliant, and trustworthy computing environment, whether cloud-based or not, should meet six requirements:

These six requirements are not mutually exclusive. Protecting personally identifiable information, for example, is a privacy matter, a legal requirement, and a potential source of risk and exposure. However, you learn different things by looking through the lenses of each of these six requirements.

Compliance	The organization can meet specific legal requirements governing the management of information and can comply with industry standards and rules (e.g., GAAP, ISO) and meet service-level agreements.
Governance	The organization can monitor the computing environment; enforce management policies, procedures, and controls; and establish the responsibilities, accountabilities, and decision rights of the people using and managing information technology resources.
Risk Management	The risks associated with a computing environment range from direct threats (e.g., intrusion, hacking) to business interruption (e.g., when systems are unavailable) to derived exposures (e.g., the financial, reputational, and legal repercussions of information loss or theft).
Availability	This includes both everyday access to computing resources and the quick and complete recovery of resources following any kind of interruption or failure.
Integrity	To maintain the integrity of information and other assets, access must be secure, so only authorized people and systems can use specified information and applications; and the transactions processed (think of a funds transfer) must be certifiably complete, even though there may be many potential points of network or system failure.
Confidentiality/ Privacy	This includes protecting the confidentiality of personal data as required by law; protecting commercial data such as financials, trade secrets, and other intellectual property; and meeting the expectations of customers, employees, and others regarding how information about them is obtained and used.

Start with any specific regulatory requirements, standards, and rules governing the workload—the "compliance" category of trust. Then evaluate the workload's requirements in terms of the other five categories—governance, risk management, availability, integrity, and confidentiality/privacy. What conditions and standards must be met? How well does the current computing environment meet them? Which among the cloud deployment options can meet them adequately—or perhaps better than the current environment can? Take note of needed improvements independent of planned migration to the cloud.

Workloads with lower trust requirements naturally have more flexible cloud deployment options. Some workloads will be quickly disqualified from the public cloud on compliance and governance, if not other grounds. With a private cloud, it's much less of an all-or-nothing proposition. You need to ask: What exposures are reduced by migration to the cloud? What exposures are increased? What risk mitigation tactics might enable the workload to run trustfully in a private cloud? How can we leverage migration to private cloud to improve the trust profile of the workload?

A large state social services agency was able to realize the cost savings of virtualization while increasing the protection of private and sensitive information about citizens. Key actions included classifying information, standardizing and extending security controls, and implementing more comprehensive risk management.

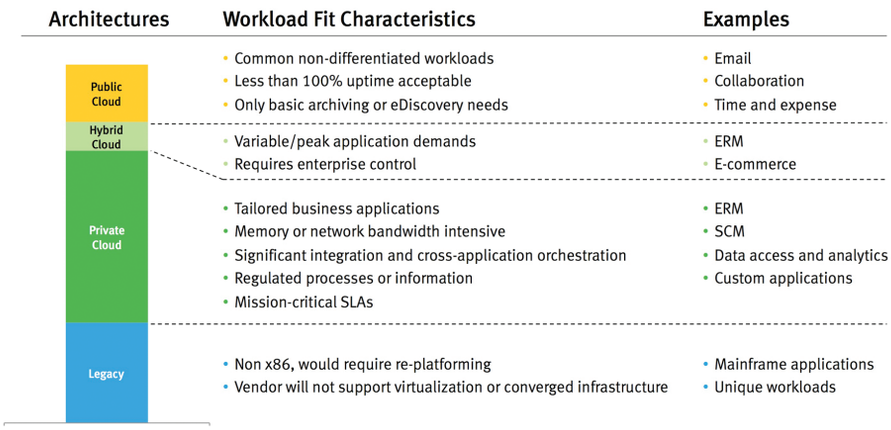
FUNCTIONAL FILTER

Can the workload operate in the cloud at least as well as it does today? Will it lose functionality because of restrictions on interfaces with other less cloud-compatible applications or because of restrictions on information availability and movement? Can its basic performance characteristics such as response time be maintained? Will access by authorized users outside the company, especially customers, be complicated (or facilitated) by movement to the cloud?

Basic content and applications code should be unaffected by movement of a workload to the cloud, but other things can change, especially around access and interfaces. So anticipate the workload's entire performance context. Will functionality be reduced or lost? And remember to consider ways in which functionality, performance, and flexibility can be enhanced by movement to the cloud.

MAPPING TO CLOUD OPTIONS

As the three filters are applied, the field of candidates (especially for short-term cloud migration) narrows, and the preferred cloud deployment destination of each workload emerges. Combine the results from the three filters, and then make adjustments based on their interplay. For example, "all in" cost may change if there is added expense to maintain the workload's functionality or to adjust its trust profile through security enhancements. Keep in mind that marginal economic payback may not be a disqualifier for a workload that belongs in the cloud for business performance and agility reasons.



MAPPING WORKLOADS TO CLOUD OPTIONS

In general, you'll find that widely used but non-differentiated workloads where less than 100 percent availability is acceptable fit the public cloud (for example, email, collaboration spaces, and time and expense reporting). Most core business applications—especially those that are tailored, are closely integrated with other applications, or must perform to mission-critical service-level agreements—belong in a private cloud. Market-facing workloads such as e-commerce applications may need a hybrid cloud for rapid scaling to meet peak demand. And highly specialized and fine-tuned workloads such as operational control systems stay in the legacy environment. However, that's painting with a very broad brush. There are many variations, and an organization must evaluate its workloads in detail.

After assessing workloads individually, assemble the composite picture. What will the new distribution of workloads across platforms look like? How will key information have to flow across workloads and platforms? How will the interfaces work? What will be the overall impacts in terms of economics, trust, and functionality?

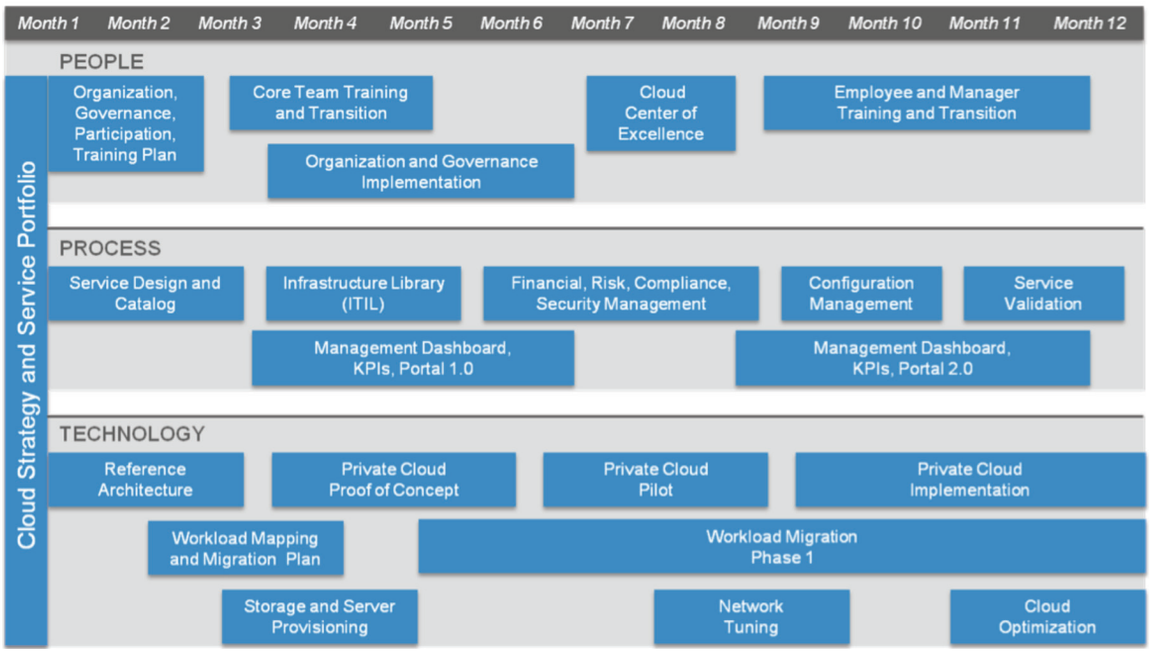
What Not to Put in the Cloud

- Self-contained and highly specialized business applications, such as realtime manufacturing control systems and analytical trading systems in financial services. These tend to be complex "workhorse" systems within specific business functions, and the value of pooling these resources is limited. They may regularly connect to cloud-based systems for up-to-date information, but that's as a customer of cloud services, not a resource managed in the cloud.
- Applications and databases that must absolutely be "walled off" from the rest of the computing environment for legal or regulatory reasons, such as local privacy laws. Companies tend to segregate such resources physically to be safe. However, with the help of state-of-the-art virtualization management methods, enterprises can usually manage more of these sensitive assets in a private cloud than they assume.
- Applications that have been written, and their performance optimized, for specific (and sometimes proprietary) systems architectures. Over time, you may choose to retrofit such assets to be shared and run in the cloud.

ROADMAP TO THE CLOUD

This process culminates in a readiness assessment and roadmap for putting the new pieces in place—from technology and automation, to process changes and staff training, to the migration of specific workloads to their cloud destinations—under the guidance of a clear governance structure. A roadmap establishes scope, objectives, and measures. It details implementation actions, sequences, dependencies, milestones, alternatives, and triggers of alternative action. And it details the means of tracking progress and performance, as well as capturing what's learned along the way.

Cloud adoption is a journey, not a one-time implementation. The consolidation and virtualization of technology, and the re-automation of its management, will happen early in the journey and yield immediate financial benefits. But workloads will migrate to private, public, and hybrid clouds over time as both the workloads and their cloud destinations are ready. People will learn to work, collaborate, and use information and applications in new ways. Business performance and agility benefits, as well as economic gains, will accumulate and amplify.



Implications for IT Management

Cloud computing represents a different and more productive way for technology services to be provided, consumed, and managed. Technology assets are defined and packaged differently—modular, interconnectable, and virtualized. IT's work is structured and provisioned differently, as a catalog of business services. Business people access and consume services differently, often through a self-service portal, and they often pay by actual usage. IT and the business together can manage the technology environment and its services differently with greater transparency into business performance and value.

For the IT organization, cloud computing also offers the opportunity to reduce complexity, raise efficiency, and finally break the pattern of devoting 70 percent or more of its budget and energy to maintaining resources and "keeping the lights on."

To realize these benefits, to really enter the cloud, requires specific changes to how IT works—including virtualizing assets, automating operations, organizing around services, and enabling self-service. Recent Forrester research found that most IT organizations' ambitions around private cloud exceed their readiness and operational capability. Most are not investing enough effort in automating their virtual environments, deploying self-service portals, or implementing the resource tracking and cost allocation systems needed to support self-service and pay-by-use. For companies short on these necessary capabilities, an externally hosted private cloud may be the fastest and most effective way to get started.[v]

Research by IDG for the Leadership Council for Information Advantage explored perhaps the biggest gap in IT capability—lack of information governance policies for cloud computing. Existing policies can be leveraged for a private cloud environment, where information and applications remain under the direct control of the enterprise. But public and hybrid clouds need new approaches. And only one-third of companies surveyed have specific governance policies for cloud-based information (though another 38 percent said they are planning to develop them).[vi]

Without such policies, a company may find itself with a proliferation of incompatible public cloud platforms and services, new forms of fragmentation and isolation of information assets, and lack of control over the chains of custody for information and its security. Without policies that span cloud platforms and the computing environment as a whole, complexity grows and benefits are diluted.[vii]

Wherever the capability gaps may be—technology architecture, infrastructure automation, information management, service orientation, cloud platform federation, or IT governance, policy and management—IT can accelerate the journey to the cloud and its business benefits by partnering with experts.

CONCLUSION

The steps outlined in this perspective are a cloud-focused extension of what organizations should already be doing periodically. Review the important information and technology assets, determine whether they're doing the best job they can for the business, and evaluate how the computing environment amplifies or inhibits their performance. Then plan the next-generation computing environment, move steadily toward it, and realize business benefits along the way.

If your organization hasn't made this asessment lately, then let the business opportunities of cloud computing be your reason to do it now. Use the economic and performance benefits of the cloud as the driver to take a fresh look at your IT assets, raise their business value, and enhance the economics, performance, and trustworthiness of your organization's computing environment. Optimize your use of the cloud.

EMC® Corporation is at the forefront in deploying robust and secure cloud computing solutions. EMC Consulting, with our information-centric approach to meeting business and technology challenges, can be your guide to the business benefits of cloud computing.

"EMC IT's Journey to the Private Cloud: serving 48,000 employees over the globe. The benefits to our organization in revenue and efficiency are dramatic. We are realizing the promise of running IT as a Service—everything—with speed, efficiency, and cost-transparency."

SANJAY MIRCHANDANI, SVP AND CHIEF INFORMATION OFFICER, EMC CORPORATION

EMC CONSULTING

As part of EMC Corporation, the world's leading developer and provider of information infrastructure technology and solutions, EMC Consulting provides strategic guidance and technology expertise to help organizations exploit information to its maximum potential. With worldwide expertise across organizations' businesses, applications, and infrastructures, as well as deep industry understanding, EMC Consulting guides and delivers revolutionary thinking to help clients realize their ambitions in an information economy. EMC Consulting drives execution for its clients, including more than half of the Global Fortune 500 companies, to transform information into actionable strategies and tangible business results.

CONTACT US

To learn more about how EMC Consulting services can help solve your business and IT challenges, contact your local EMC Consulting representative, or visit us at www.EMC.com/consulting.

[i] "In the Race to the Cloud, Do Your Organization's Governance Policies Stack Up?" 2010, page 1.

[ii] "McKinsey Global Survey Results: How IT is managing new demands," 2010, page 8.

[iii] "McKinsey Global Survey Results: How IT is managing new demands," page 7.

[iv] "Private Cloud Computing Plans From Conference Polls," Thomas J. Bittman, 30 April 2010, pages 3-4.

[v] "Companies Building Private Clouds Focus On Infrastructure But Not Operations," James Staten, November 23, 2010, pages 7-8.

[vi] "In the Race to the Cloud, Do Your Organization's Governance Policies Stack Up?" 2010, page 1.

[vii] "Creating Information Advantage in a Cloudy World," October 2010, pages 4, 8-9.

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

EMC²