Insights on IT risk
Business briefing

April 2012

Ready for takeoff

Preparing for your journey into the cloud

Ernst & Young
Quality In Everything We Do

Contents

Managing risks in the cloud

Many organizations are looking to cloud computing to increase the effectiveness of IT initiatives, reduce cost of in-house operations, increase operational flexibility, and generate a competitive advantage. Through an effective strategy, cloud computing can enable many companies to do much more with IT by becoming strategy focused and not operations focused. Cloud-based services are nimble and adaptive, increasing capability to read and react to changing marketplace conditions by responding to customer needs and competitors' actions.

Savvy business professionals recognize the speed and efficiencies that embracing cloud technology can bring. Organizations that are disinclined to focus on IT recognize the tremendous value of being able to concentrate on their core business competencies. This is attained by shifting to a user of IT services, as they no longer need to build and maintain complex internal IT infrastructures. Cloud computing is evolving at a fast pace, giving companies a variety of choices when looking to restructure their IT organization.

However, like most technology changes, cloud computing presents its share of risks and challenges, which are too often overlooked or not fully understood by businesses that are quick to embrace it. Implementing cloud computing requires a considerable shift from traditional computing methods and business processes. Organizations considering cloud computing should conduct due diligence based on the needs of the business and the capability of IT in order to determine readiness for adoption of the platform. A clear and attainable strategy for migrating to the cloud is then required, taking into consideration the associated risks and challenges while providing robust internal capabilities to address such matters.

In this paper we will discuss the cloud risk universe or — in other words — the most important risk areas that need to be addressed while moving into the cloud. As part of this discussion we will provide a framework to conduct a cloud risk assessment.

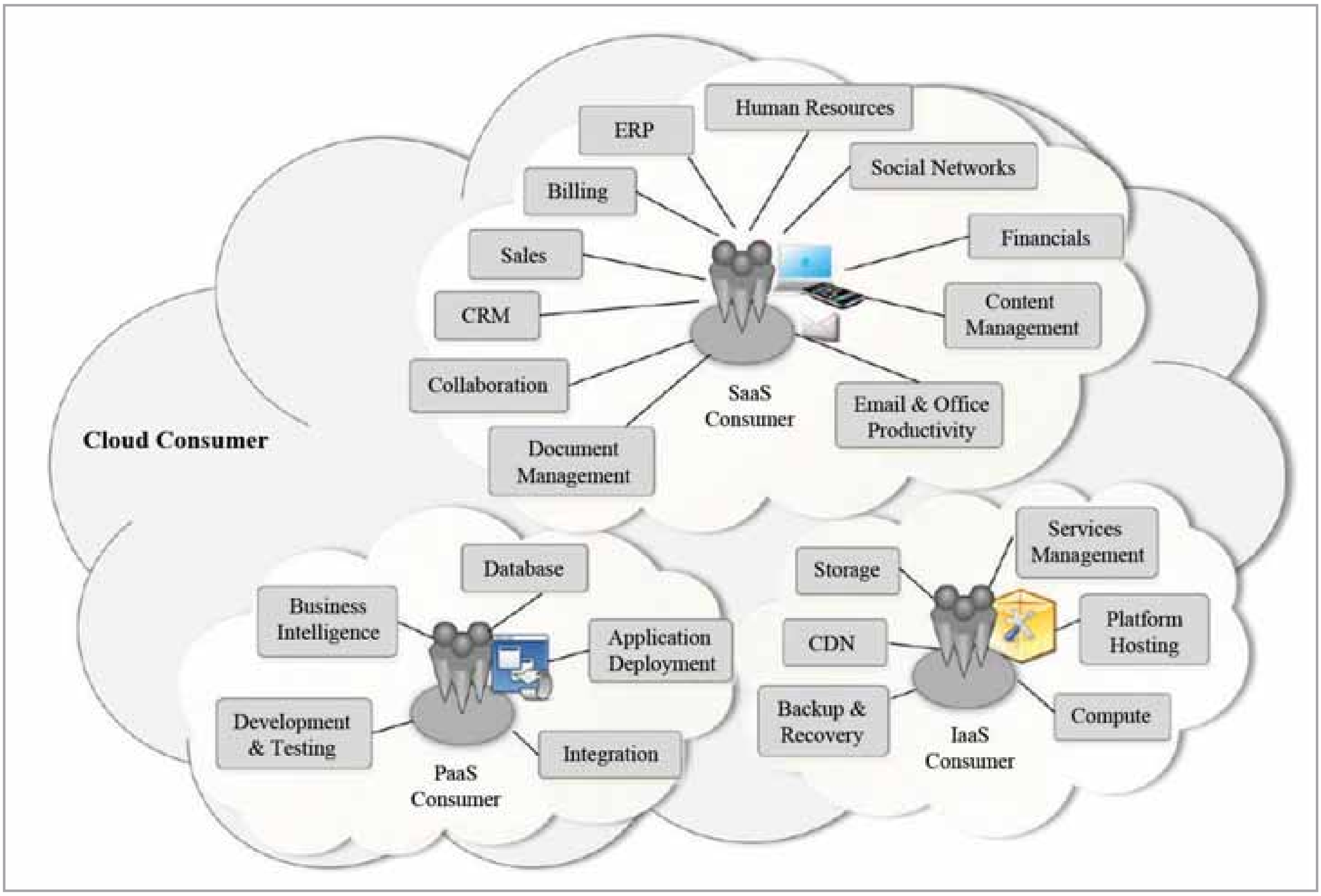
> According to MarketsandMarkets.com, Cloud Computing Market — Global Forecast (2010 — 2015), the global cloud computing market is expected to grow from US$37.8 billion in 2010 to US$121.1 billion in 2015 at a CAGR of 26.2% from 2010 to 2015.

The sky is the limit for cloud services

Cloud computing services are available across the entire computing spectrum. The US National Institute of Standards and Technology (NIST) published a definition of cloud computing as 'a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.' While the US NIST definition[1] includes three primary service models, the market has evolved so that you can buy as a service just about any slice of the computing "stack" within the three, which are as follows:

1. **Infrastructure as a service (IaaS):** The capability provided to the consumer is to provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications and possibly limited control of select networking components (e.g., host firewalls).
2. **Platform as a service (PaaS):** The capabilities provided to the consumer is to deploy onto the cloud infrastructure, consumer-created applications or applications created using programming languages supported by the provider. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems or storage, but has control over the deployed applications and possibly application hosting environment configurations.
3. **Software as a service (SaaS):** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

[1] The definitions of cloud computing and its essential characteristics, service models and deployment models are excerpted from the US National Standards and Technology's widely referenced definition, NIST Definitions of Cloud Computing v15. The full text is available at the NIST website at: http://nist.gov/itl/cloud/upload/could-def-v15.pdf.



Source: National Institute of Standards and Technology (NIST) graphic, Cloud Computing Reference Architecture, Special Publication 500-292, http://csrc.nist.gov.

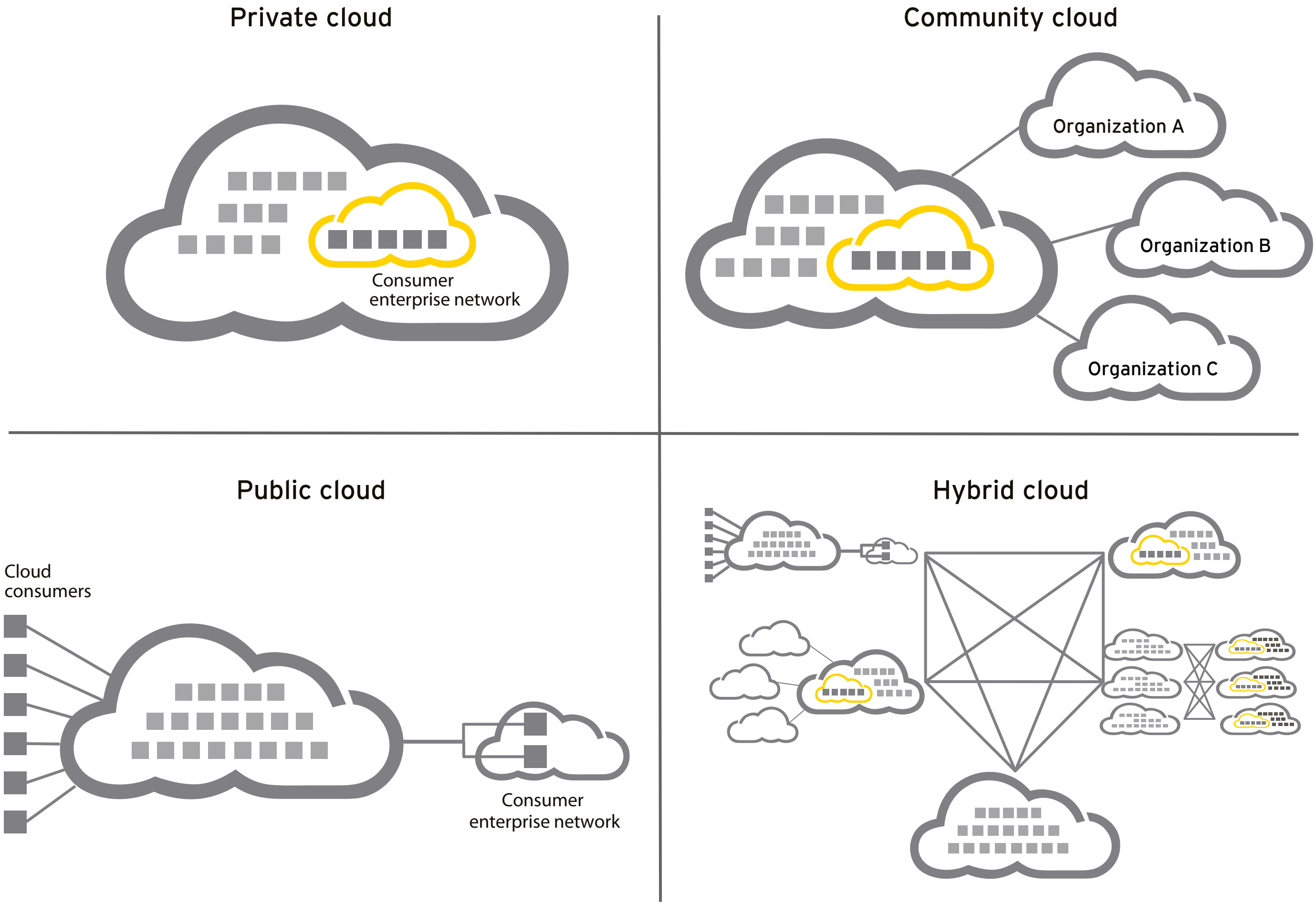
In addition, a fourth service model is evolving called Business Process as a Service (BPaaS), albeit more slowly at present than the primary three. BPaaS combines multiple components of each of the three to deliver an entire business process. Today, services such as payroll and billing already are outsourced using traditional methods. Looking ahead, we expect higher-value business process services to evolve, differentiated from traditional business process outsourcing because they will be enabled by multiple underlying cloud services.

These primary service models can be implemented via private, public, hybrid or community cloud platforms.[2]

- **Private cloud:** The cloud infrastructure is provisioned by a single organization. It may be owned, managed and operated by the organization, a third party or some combination of them, and it may exist on or off premises.
- **Public cloud:** The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
- **Community cloud:** The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy and compliance considerations). It may be managed by the organization or a third party and may exist on premise or off premise.
- **Hybrid cloud:** The cloud infrastructure is a composition of two or more clouds (private, community or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

The NIST also defines five essential cloud computing characteristics, which we have included in its entirety (see Appendix, page 17).

[2] The definitions of cloud computing and its essential characteristics, service models and deployment models are excerpted from the US National Standards and Technology's widely referenced definition, NIST Definitions of Cloud Computing v15. The full text is available at the NIST website at: http://nist.gov/itl/cloud/upload/could-def-v15.pdf.



Note: Illustration based on NIST service deployment models (Cloud Computing Reference Architecture, Special Publications 500-292).

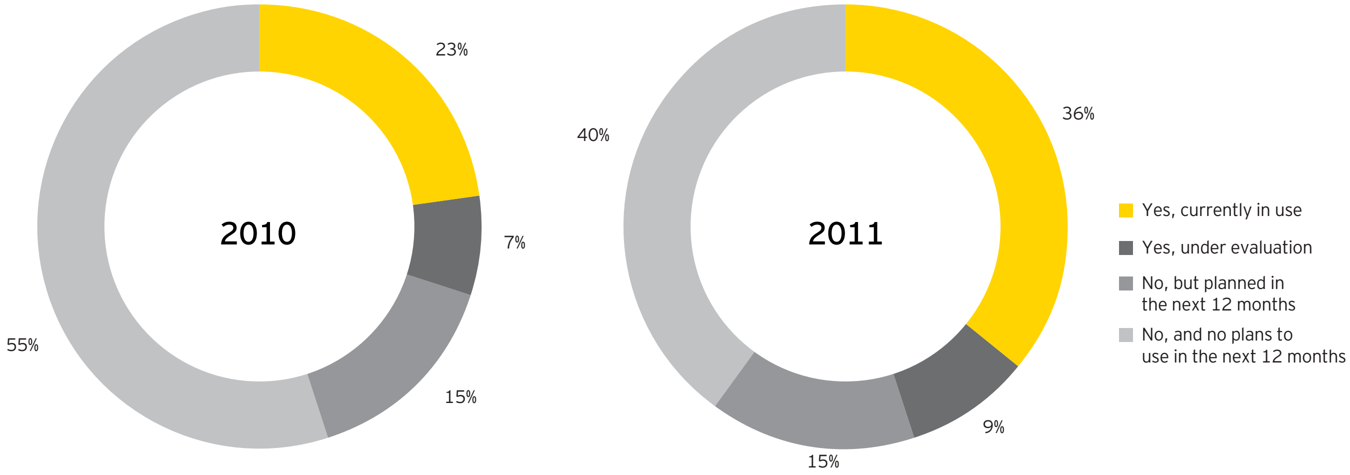
Lift off for cloud adoption

The operations shift from physical to virtual has allowed businesses to capitalize on deploying new technologies, driven by a need to reduce costs while increasing business agility. According to our publication *Into the cloud, out of the fog: Ernst & Young 2011 Global Information Security Survey* (GISS 2011), the number of organizations using cloud-based services in 2011 increased by 50% from the previous year.

To embrace highly configurable, rapidly deployable, externally managed applications, an ever-increasing number of companies are moving from the more traditional outsourcing contracts to cloud service providers (CSPs). In fact, our survey revealed that 61% of respondents are currently using, evaluating or planning to implement cloud-based services within the next 12 months.

As organizations realize the benefits of bringing their business into the cloud and confidence in the cloud business model increases, they will have the assurance that critical services and, in some cases, their entire IT infrastructure footprint can exist in the cloud. By moving into the cloud, organizations now have the potential to greatly reduce or even eliminate their IT operations, thereby forever altering their business model (GISS 2011).

Figure 1: Results showing extent of organizations utilizing cloud computing today



Shown: percentage of respondents (GISS 2010 and GISS 2011).

Drivers for cloud computing

Business agility	Perhaps the major accelerant for cloud adoption is the ability to elastically scale IT resource availability up — and down — depending on the momentary or capacity needs of the business. This resolves a long-standing dilemma for large organizations, which forecast demand for their IT resources yet typically end up with more capacity than they need — or worse, less than they need — because of business changes during the installation process. Cloud-based IT services can grow or shrink as business requirements change, without requiring long implementation times or aggressive capital investment.
Pay-as-you-go versus install-and-own	The shift in up-front capital requirements from the user to the service provider is extremely attractive to large and small organizations alike. This flexibility allows them to remain as a cloud customer and buy access to the infrastructure and application they need, as they need them. Instead of paying for it all up front, including more capacity than they may need right away, cloud customers pay only for what they use — and only when they use it.
Cost saving	A report by the Brookings Institution found that government agencies can save 25% to 50% of their IT cost and increase their business agility by migrating IT infrastructure to cloud services.
Innovation platform for growth cloud	Cloud computing services reduce IT barriers to entry, allowing start-ups to emerge with lower infrastructure start-up costs than were necessary pre-cloud. This cost saving allows for increases in innovation. This will likely allow organizations to allocate more time to strategy and enablement by leveraging the cloud.
Infrastructure utilization	Better network efficiency results in lower power consumption and smaller carbon footprints. This comes from virtualizing hardware and software resources and providing them as a service to multiple users simultaneously.
Public investment	Governments worldwide are investing to create economic regions of cloud technology development (China, Japan), supporting cloud-related standards development (e.g., EU, US) or migrating their own IT infrastructures to cloud services in an effort to lead by example (US, UK, Japan).
Market research	Research points to ongoing rapid adoption of both public and private cloud services, which tends to become a self-fulfilling prophecy.
Security	Forrester Research projected that within five years cloud security will become one of the primary drivers for adopting cloud computing.[3] There already is a growing view that using a CSP enhances security.[4] A CSP's viability depends in part on establishing a reputation as trustworthy. According to this view, the CSP will devote significantly more resources to security and data protection than a typical business, whose IT departments are cost centers that often face diminishing budgets. In fact, this is being seen already: leading CSPs view security as among the most important issues for broad adoption, and the measures they are taking are effectively "setting the standard" for others.
Standardization efforts	Standards are likely to reduce or eliminate risk from many current barriers to cloud adoption. Many government, industry and public–private coalitions are racing to fill the standards void and, thus, ease risk management for CSPs and their cloud users.
Cloud brokers	Emerging cloud services brokers simplify an organization's transition to the cloud by helping to overcome specific security, privacy and compliance issues and helping achieve interoperability across multiple public clouds, private clouds and in-house IT infrastructure.
Risk of missing out	Organizations that do not adopt cloud computing along with their competitors risk missing out on expected benefits such as the flexibility and agility afforded by on-demand services and access to the latest versions of technologies. This is because CSPs typically perform more timely upgrades than most private organizations.

[3] *IDC Predictions 2011: Welcome to the New Mainstream*, International Data Corporation, December 2010

[4] *Borderless Security: Ernst & Young's 2010 Global Information Security Survey*, Ernst & Young, 2010

Navigating the cloud risk universe

A holistic viewpoint

As previously stated, cloud computing is well on its way to mainstream adoption. However, many organizations are still unclear on the implications and are concerned with the risks and challenges associated with it.

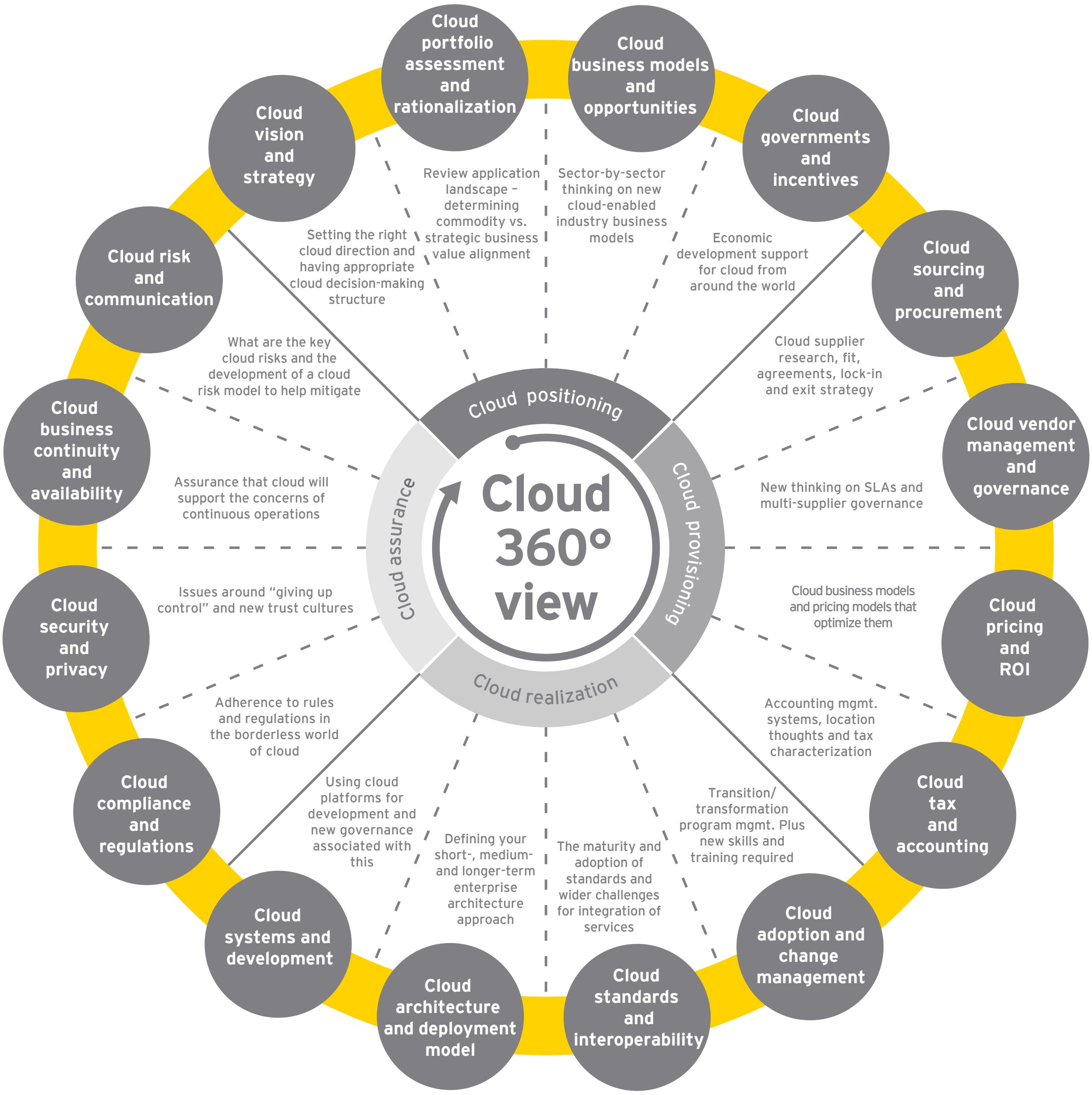
Ernst & Young's Cloud 360° view (Figure 2) provides a holistic view of the areas that organizations should consider when exploring cloud computing. The four main areas of the Cloud 360° view (depicted in the center) are cloud positioning, cloud provisioning, cloud realization and cloud assurance. Each category is further divided into four components giving a total of 16 areas of focus.

As shown in the diagram, implementing a cloud solution can have an effect on many areas of an organization.

A decision to migrate to the cloud should not be taken lightly. Organizations should first have a clear vision of what they want to accomplish, in terms of where they are going. There is also a need to understand the risks and implications to the organization as a whole, not just the IT side of the business. They should also include design for adequate measures and mitigation strategies to manage associated risks and challenges.

> Moving to the cloud is not just another change program — it is nothing less than a complete transition of business processes.

Figure 2: Cloud 360º view


Cloud 360º view
Cloud positioning
Cloud provisioning
Cloud realization
Cloud assurance
Cloud portfolio assessment and rationalization
Cloud business models and opportunities
Cloud governments and incentives
Cloud sourcing and procurement
Cloud vendor management and governance
Cloud pricing and ROI
Cloud tax and accounting
Cloud adoption and change management
Cloud standards and interoperability
Cloud architecture and deployment model
Cloud systems and development
Cloud compliance and regulations
Cloud security and privacy
Cloud business continuity and availability
Cloud risk and communication
Cloud vision and strategy
Review application landscape – determining commodity vs. strategic business value alignment
Sector-by-sector thinking on new cloud-enabled industry business models
Economic development support for cloud from around the world
Cloud supplier research, fit, agreements, lock-in and exit strategy
New thinking on SLAs and multi-supplier governance
Cloud business models and pricing models that optimize them
Accounting mgmt. systems, location thoughts and tax characterization
Transition/ transformation program mgmt. Plus new skills and training required
The maturity and adoption of standards and wider challenges for integration of services
Defining your short-, medium- and longer-term enterprise architecture approach
Using cloud platforms for development and new governance associated with this
Adherence to rules and regulations in the borderless world of cloud
Issues around "giving up control" and new trust cultures
Assurance that cloud will support the concerns of continuous operations
What are the key cloud risks and the development of a cloud risk model to help mitigate
Setting the right cloud direction and having appropriate cloud decision-making structure

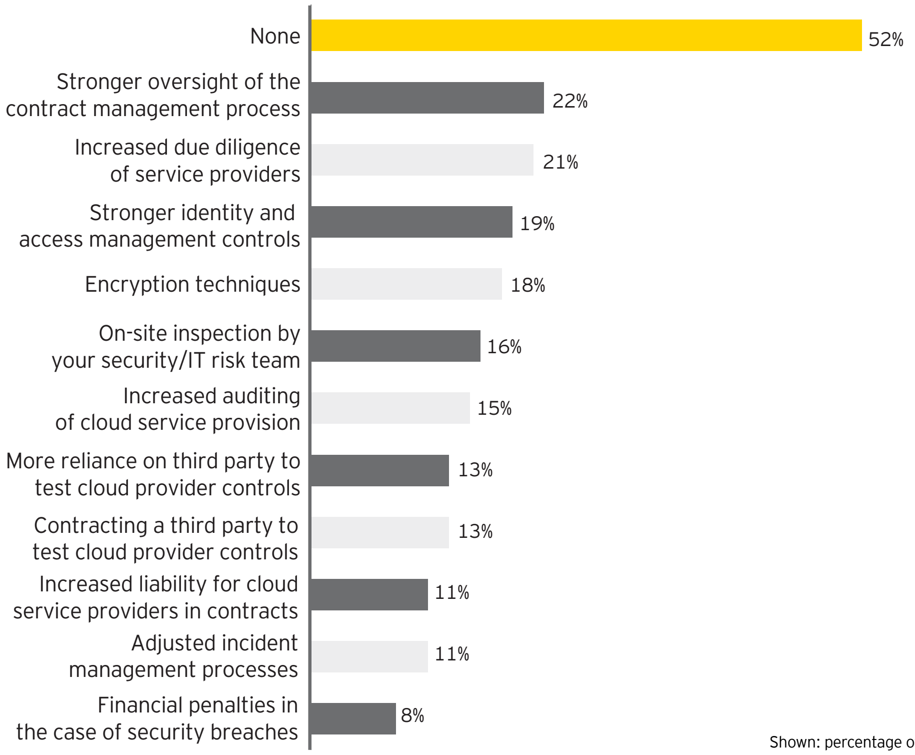
The implications for business

Moving to the cloud is not just another change program — it is nothing less than a complete transition of business processes.

If ill-prepared, organizations may struggle with the integration of external cloud computing into their business. In the GISS 2011, 48% of respondents listed the implementation of cloud computing as a difficult or very difficult challenge, and just over half have not implemented any controls to mitigate the risks associated with cloud computing. Organizations, uncertain about their control options, select and may only implement a subset of those available, or sometimes none at all. The most frequently taken measure is stronger oversight on the contract management process with cloud providers, but even this is only done by 20% of respondents, indicating a high and possibly misguided level of trust.

In the absence of clear guidance, many organizations seem to be making hasty decisions, either moving to the cloud prematurely without appropriately considering the associated risks, or avoiding it altogether. The results of the survey indicated that although many organizations have moved to the cloud, many have done so reluctantly, evidenced by 80% of respondents who admit to being challenged to deliver information security initiatives for new technologies such as cloud computing and virtualization.

Figure 3: Controls implemented to mitigate cloud computing risks



Shown: percentage of respondents.

Risk areas of cloud computing

Cloud architecture and deployment	Infrastructure and architecture risks arise if the provider does not achieve performance requirements that organizations and the provider agree to and define in the service level agreements at the outset of the contract. These risks may include availability and reliability issues in the form of unplanned outages or compromised bandwidth because organizations are sharing the infrastructure with other clients during peak hours.
Cloud standards and operability	CSPs typically develop customized services that meet the desired needs of their target audience. But to effectively interact with the provider's applications, architecture and infrastructure, it is vital that the organizations systems and those of the provider can communicate with one another. If the systems cannot talk with one another, processing continuity, application performance, the inability to customize applications and the overall efficiency of desired services are at risk. Industry standards, often a risk management safety net, are lagging behind the rapid growth of cloud services. The lack of specific standards, especially in the areas of security, privacy and availability, can create a high degree of uncertainty about the risks users are assuming. Many government, industry and public-private coalitions are racing to fill the standards void and, thus, ease risk management for CSPs and their users. Standards development however, is a consensus-driven and, therefore, lengthy process and the cloud standards process has begun only recently.
Cloud compliance and regulations	Organizations are increasingly required, by law or industry standard, to store, track and/or transfer certain information. Often, this information is confidential, classified or proprietary. Accordingly, safe transfer and storage of information is paramount. This type of requirement is seen across many industry sectors and is embodied in legislation such as the Sarbanes-Oxley (SOX) Act and the Health Insurance Portability and Accountability Act (HIPAA). For organizations that have to comply with these regulations, security, availability, privacy and data integrity are crucial. Organizations may encounter additional legal, regulatory and compliance risks around data privacy, search and seizure, subpoena and e-discovery legislation depending not only on the organization's jurisdictions, but also those of the cloud provider. Moving data to the cloud does not absolve an organization of responsibility for regulatory compliance — quite the contrary. Regardless of where the data resides, the organization remains accountable for its regulatory and compliance obligations. As such, you will need to thoroughly understand the legal and regulatory requirements in each jurisdiction in which the organization and the provider operate.

Company suffers massive data loss

A large telecommunications company faced a major setback when they experienced a cloud outage that lasted just over a full working week, leaving about a million of its customers without access to their calendar, address book and other key features of the services they provided. Additionally, the system failure caused loss of data in the core and the backup database.

Risk areas of cloud computing (continued)

Information security and privacy risks	A few of the most significant Information security risks when processing in a cloud environment include: ‣ Unauthorized access to both logical and physical areas of the network ‣ Unauthorized modification of systems or data ‣ Unauthorized deletion of data Many organizations are concerned about relinquishing control of their business information to cloud providers — relying on them to provide secure authentication, user credentials and role management, or data management. Their concerns are not unfounded. Organizations using cloud computing services, and particularly SaaS, have lower transparency and ownership over security controls and processes that providers implement. When it comes to privacy, maintaining the confidentiality and integrity of the personal information an organization holds is often paramount to its survival. A single data breach could significantly harm the organization's brand, tarnish its reputation and limit its future growth, in addition to the direct costs of the breach. Jurisdictionally appropriate privacy policies and controls are critical for both the organization and the provider. When we think of data risks, the focus is usually on the inherent security risks associated with transferring data over public networks and storing it in facilities that may be operated by third parties other than the cloud provider with which the organization has a contract or housed in a foreign jurisdiction where privacy protections are more lax. However, data issues may also arise from improperly entered or recorded transactions if a cloud computing service is not properly implemented.
Cloud vendor management and governance	Contractual risks stem primarily from the types of contracts that clients enter into with CSPs. These service level agreements or end-user level agreements are often binding contracts that stipulate a client's ability to audit a provider, any legal recourse they have for incidents and which party owns data stored in the cloud. They also often contain crucial details regarding key elements of service, such as the level or percent of availability and storage space allotted. These terms are often non-negotiable, especially for users of commodity service offerings. In the continuing cost-conscious environment, organizations cannot afford to make mistakes when it comes to IT investments, nor can they afford to be noncompliant when it comes to industry, state or country-specific regulations. When embarking on the journey into the cloud, organizations will want to make sure they have a clearly defined strategy for cloud services that is aligned to the broader business strategy, is compatible with existing architecture, adheres to all applicable laws and regulations within each jurisdiction in which the organization operates, and provides the desired return on investment the organization seeks. Without a sound governance strategy that applies to both the organization and the CSP, organizations risk ineffectiveness, loss of control and potential harm to their reputation from negative legal or regulatory action.

Service support	Whether SaaS, PaaS or IaaS, service in cloud computing should mean not having to worry about the risks or the uncertainty because the provider has already thought of them and has solutions at the ready. However, while some of the largest providers invest heavily in technology support (in some cases for a fee), for many providers, customer support may be an afterthought.
Business continuity and availability	Continuity of the business is critical. It is, therefore, important to understand the geographical coverage of a cloud provider and how this may affect cloud users. In addition, cloud users are depending on their CSP's business continuity program and disaster recovery capabilities. The cloud user is also dependent on the CSP's capabilities when it comes down to operations and support processes such as incident management and service desk.
Cloud adoption and change management	Moving to the cloud is not just another project. It is a major transformation of the business. Organizations need solid transformation management including structured program governance and organizational change management.
Strategy alignment and governance	When embarking on the journey into the cloud, organizations will want to determine how this fits in with their overall business goals in terms of both the benefits and the risks. Organizations, therefore, need a governance model and a cloud strategy including a cloud risk management approach. Standards, leading practices, and guidance for cloud users and CSPs are under development with several independent bodies. However, there is no agreed-upon baseline currently available.

Company in breach of data protection laws

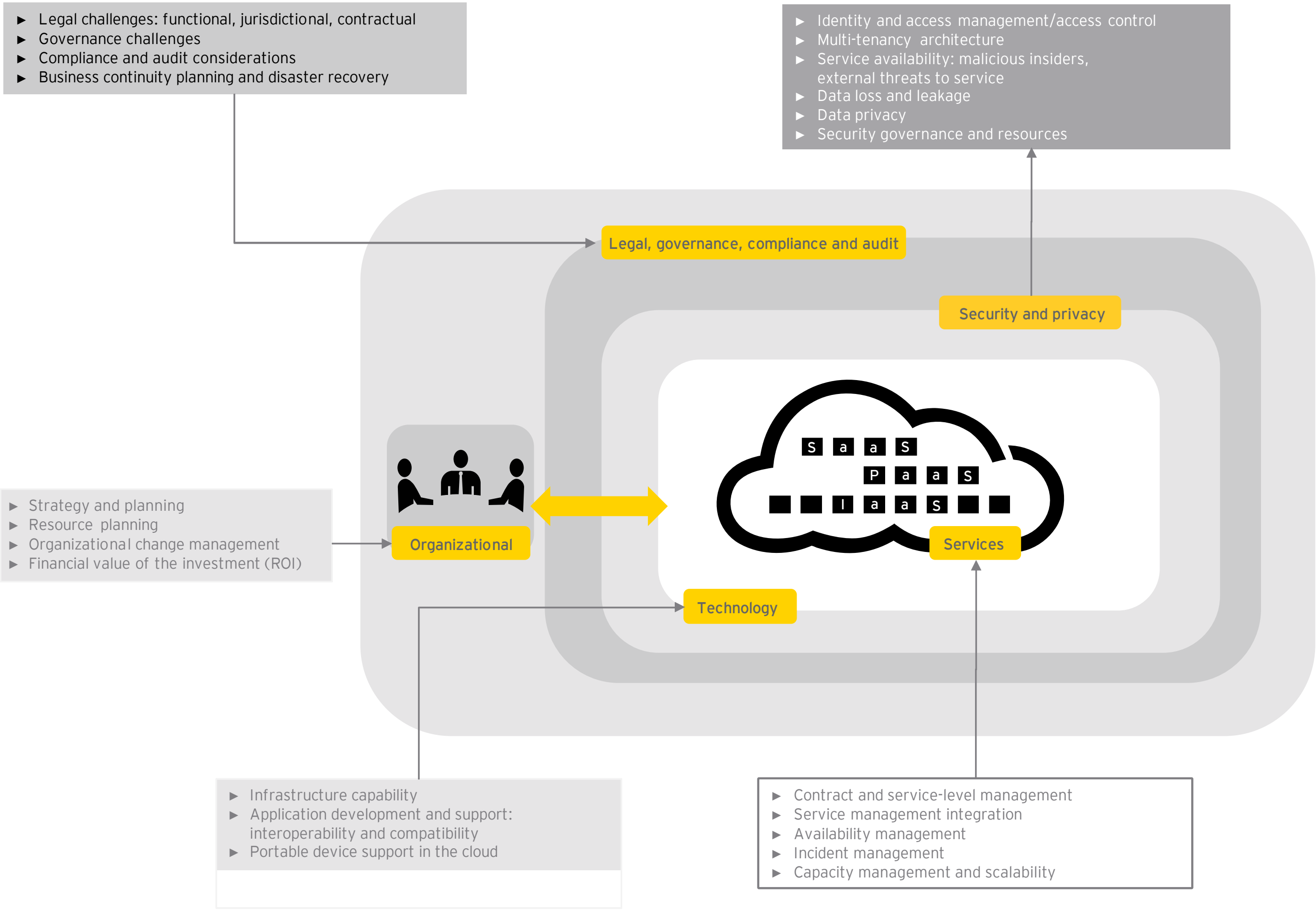
The owners of a company discovered that they were in breach of data protection laws when they discovered that their CSP relocated their data centers outside the permitted geographic location without notifying the company.

As a result of the CSP relocating their data center, the company incurred penalties for breaching data protection laws and was forced to change CSP as their requirements could no longer be met.

Fasten seat belts – assess your cloud risks

Cloud adoption offers numerous benefits to organizations but requires a considerable shift from traditional computing methods and business processes. Due diligence from both business and IT groups within an organization is necessary, and several factors such as industry drivers, size of the organization, business needs, security policies and the existing IT base of the organization need to be considered when identifying a cloud model that best fits an organization's needs. Migration to the cloud should follow a strategic roadmap that supports an organization's vision and business imperatives.

Figure 4: Cloud risk assessment framework



- Legal challenges: functional, jurisdictional, contractual
- Governance challenges
- Compliance and audit considerations
- Business continuity planning and disaster recovery

- Identity and access management/access control
- Multi-tenancy architecture
- Service availability: malicious insiders, external threats to service
- Data loss and leakage
- Data privacy
- Security governance and resources

- Strategy and planning
- Resource planning
- Organizational change management
- Financial value of the investment (ROI)

- Infrastructure capability
- Application development and support: interoperability and compatibility
- Portable device support in the cloud

- Contract and service-level management
- Service management integration
- Availability management
- Incident management
- Capacity management and scalability

Organizations may need to consider some of the following factors in order to evaluate which applications or services can be moved to the cloud:

- Maturity of infrastructure and services with respect to the level of customization, and in-house support required
- Capabilities to effectively integrate with existing systems
- Data management and security issues related to defining data sensitivity and how it is handled
- Personnel to support the new cloud deployment and operations of systems

Ernst & Young's cloud risk assessment framework covers all aspects of moving to the cloud and the implications on business areas including organizational; technology; security and privacy; legal, governance, compliance and audit; and services. This framework relates to concerns for all cloud service types: IaaS, PaaS and SaaS.

Overview of cloud risk assessment framework

Organizational	Organizational factors often overlooked during cloud risk assessments are crucial for successful migrations to the cloud environment and should be given due consideration. Organizations should evaluate parameters such as strategy and planning, resource planning, organizational change management and financial value of the investment (ROI).
Technology	Cloud computing can bring transformational changes to an organization's IT portfolio, based on the services an organization may be looking to move to the cloud. Organizations will have to develop capabilities that can support these changes in terms of understanding, deploying and eventually using different technology. An assessment of technology should focus on infrastructure, application development and deployment capabilities as well as existing features such as portable device support.
Security and privacy	In the cloud, organizations face numerous security and data privacy challenges related to identity and access management (IAM), multi-tenant architectures, service availability (malicious insider, external threats to service), data loss and leakage, data privacy issues related to transborder information flow, and security governance and resources issue. Organizations should be cognizant of and plan well in advance to mitigate threats associated with these challenges.
Legal, governance, compliance and audit	Organizations need to focus on various legal, governance, compliance and audit aspects to ensure that cloud services do not violate any laws or agreements. Organizations should conduct a careful industry-specific assessment of legal and compliance mandates before moving their IT to the cloud. In addition, organizations should consider business continuity/disaster recovery (BC/DR) planning as part of this to minimize the impact of an adverse event on business processes.
Services	Organizations should conduct a due diligence review of the CSP prior to purchasing any services to ensure that their requirements can be met, taking into consideration organizational; technological; legal, governance, compliance and audit; and security and privacy requirements. In addition, a successful cloud migration should be supported by effective service management measures related to service levels, contingency plans in case of failure, liability agreements, extended support, and the inclusion of other terms and conditions as part of the service contracts, as well as availability, incident, and capacity management and scalability.

Taking action

Despite the risks, the widespread adoption of cloud computing is inevitable because organizations can achieve real business agility with regards to IT. However, successful migration requires an overhaul of organizational structure, processes and technology and an understanding of the business impact and risks posed. The cloud risk assessment can help your organization understand what these are in advance of migrating to the cloud.

Ready for takeoff

After reading this article, could you answer the following sample questions for your organization?

Organizational

- Is your cloud integration strategy in line with the management's risk appetite?
- Does your organization have personnel with the right skills and experience level for a successful move to the cloud?

Technology

- Has your organization's IT and security infrastructure and architecture been tested to verify whether it is cloud compatible?
- Is your organization's network capable of supporting additional network traffic that will result from accessing applications over the internet?

Security and privacy

- Has a business impact assessment been conducted for the services moving to the cloud to support business continuity planning and disaster recovery?
- Does your organization have secure authentication protocols for users working in the cloud?

Legal, governance, compliance and audit

- Has your organization considered all the legal requirements with respect to transborder information flow?
- Has your organization defined minimum criteria for service termination (including data, asset return, data privacy, destruction and migrations) in contractual arrangements?

Services

- Has a due diligence review of the CSP been conducted to determine that the organization's requirements can be met?
- Does your organization have processes to maintain regulatory compliance in key areas such as change control across internal and cloud-based operations and services?

Appendix[5]

Essential cloud computing characteristic

1. **On-demand self-service.** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.
2. **Broad network access.** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
3. **Resource pooling.** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
4. **Rapid elasticity.** Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
5. **Measured service.** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

[5] The definitions of cloud computing and its essential characteristics, service models and deployment models are excerpted from the US National Standards and Technology's widely referenced definition, NIST Definitions of Cloud Computing v15. The full text is available at the NIST website at: http://nist.gov/itl/cloud/upload/could-def-v15.pdf.

Ernst & Young

Assurance | Tax | Transactions | Advisory

About Ernst & Young
Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 152,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit www.ey.com.

About Ernst & Young's Advisory Services
The relationship between risk and performance improvement is an increasingly complex and central business challenge, with business performance directly connected to the recognition and effective management of risk. Whether your focus is on business transformation or sustaining achievement, having the right advisors on your side can make all the difference. Our 25,000 advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to deliver a powerful and superior client experience. We use proven, integrated methodologies to help you achieve your strategic priorities and make improvements that are sustainable for the longer term. We understand that to achieve your potential as an organization you require services that respond to your specific issues, so we bring our broad sector experience and deep subject matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where the strategy is delivering the value your business needs. It's how Ernst & Young makes a difference.

EYG no. AU1159

In line with Ernst & Young's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM Limited nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.

ED None.

How Ernst & Young makes a difference

At Ernst & Young, our services focus on our individual clients' specific business needs and issues because we recognize that each is unique to that business.

IT is a key to allowing modern organizations to compete. It offers the opportunity to become closer to customers, allows for more focused and faster responses, and can redefine both the effectiveness and efficiency of operations. But as opportunity grows, so does risk. Effective ITRM helps you to improve the competitive advantage of your IT operations by making these operations more cost efficient and managing down the risks related to running your systems. Our 6,000 IT risk professionals draw on extensive personal experience to give you fresh perspectives and open, objective advice – wherever you are in the world. We work with you to develop an integrated, holistic approach to your IT risk or to deal with a specific risk and information security issue.
We understand that to achieve your potential, you need tailored services as much as consistent methodologies. We work to give you the benefit of our broad sector experience, our deep subject-matter knowledge and the latest insights from our work worldwide. It's how Ernst & Young makes a difference.

For more information on how we can make a difference in your organization, contact your local Ernst & Young professional or a member of our team listed below.

Contacts

Global		
Norman Lonergan (Advisory Services Leader, London)	+44 20 7980 0596	norman.lonergan@uk.ey.com
Paul van Kessel (IT Risk and Assurance Services Leader, Amsterdam)	+31 88 407 1271	paul.van.kessel@nl.ey.com

Advisory Services		
Robert Patton (Americas Leader, Atlanta)	+1 404 817 5579	robert.patton@ey.com
Andrew Embury (Europe, Middle East, India and Africa Leader, London)	+44 20 7951 1802	aembury@uk.ey.com
Doug Simpson (Asia-Pacific Leader, Sydney)	+61 2 9248 4923	doug.simpson@au.ey.com
Naoki Matsumura (Japan Leader, Tokyo)	+81 3 3503 1100	matsumura-nk@shinnihon.or.jp

IT Risk and Assurance Services		
Bernie Wedge (Americas Leader, Atlanta)	+1 404 817 5120	bernard.wedge@ey.com
Manuel Giralt Herrero (Europe, Middle East, India and Africa Leader, Madrid)	+34 91 572 7479	manuel.giraltherrero@es.ey.com
Troy Kelly (Asia-Pacific Leader, Hong Kong)	+852 2629 3238	troy.kelly@hk.ey.com
Giovanni Stagno (Japan Leader, Tokyo)	+81 3 3503 1159	stagno-gvnn@shinnihon.or.jp