Insights on IT risk

March 2011

Building trust in the cloud

Ten cloud computing risks and how to manage them

Ernst & Young

Quality In Everything We Do

Five questions for the C-suite

1. What shouldyour organization try to achieve through cloud computing?
2. What specific areas within your organization are most appropriate for cloud computing?
3. What are the most significant data privacy and security issues that you will likely face?
4. How would existing resources — technology and people — be reallocated for maximum impact?
5. What are the broader cultural and operational implications of this approach?

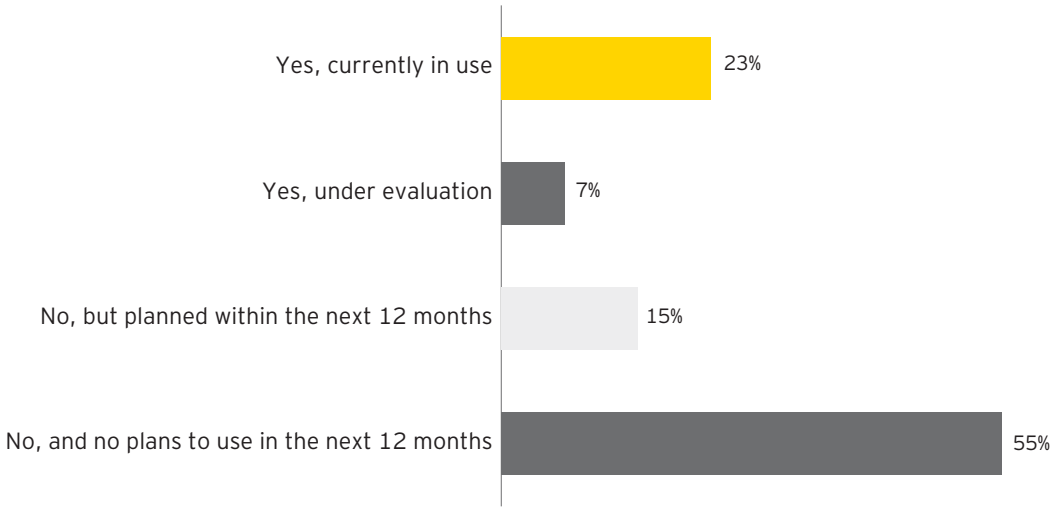
CIOs everywhere are facing a similar dilemma: pressure to reduce IT spending while improving the flexibility and speed of implementation. They are looking for computing services that don't need as much investment or ramp up time, fewer skilled internal IT resources and lower operating costs and they know they need to implement a different computing model to get it.

The benefits of cloud computing are undeniable:

- Minimal up-front costs
- Shorter contract terms
- On-demand scaling of resources
- Leading IT services within a constrained budget

And cloud computing is gaining momentum. In *Borderless security: Ernst & Young's 2010 Global Information Security Survey*, 23% of respondents are currently using cloud computing services, 7% are evaluating its use and 15% are planning to use within the next 12 months.

Does your organization currently use cloud-computing-based delivery solutions?



Shown: Percentage of respondents

Borderless security: Ernst & Young's 2010 Global Information Security Survey

This is a significant trend given that there are so many unanswered questions regarding issues of reliability, regulation, liability, contractual oversight, legal discovery and the security of many cloud services. These questions — and more importantly, the risks — leave many CIOs unwilling to trust the cloud environment.

We believe with the right risk-based approach, organizations can not only manage the risks, but use them to their advantage when selecting cloud computing providers and services appropriate to their organization's needs and its appetite for risk.

At a glance

Cloud computing service models

Service models include pay-as-you-go, on-demand and self-service utilities, but are generally categorized as:

- **Software-as-a-service (SaaS).** Customers access their provider's software applications, which are managed, controlled and hosted on the service provider's cloud infrastructure. Within this environment, customers don't need to own the software. Instead, they pay per usage through a web application programming interface (API). Customers benefit by not having to pay the in-house costs ongoing maintenance, daily technical operation and software support.
- **Platform-as-a-service (PaaS).** An outgrowth of the SaaS application delivery model, PaaS enables customers to deploy applications on the service provider's infrastructure. Customers can implement and maintain controls of tools and programming languages — if they are supported by the service provider — while the service provider maintains controls of the infrastructure. The value to customers is the availability of an integrated suite from the internet, with no software downloads or installation requirements for developers, IT managers or end users.
- **Infrastructure-as-a-service (IaaS).** IaaS service providers offer customers the use of virtual machines, on which customers can run its preferred applications and processes. Customers can also maintain control of parts of the network, including firewalls, deployed services, operating systems and storage. Customers benefit by not having to purchase servers, software, data center space or network equipment, but instead buy those resources as a fully outsourced service.

Cloud computing deployment models

Cloud computing has evolved from an amalgam of grid computing, automation and virtualization technologies. Deployment models include pay-as-you-go, on-demand and self-service utilities, but are generally categorized as:

- **Private cloud.** The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
- **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 organizations or a third party and may exist on premise or off premise. Could be defined as somewhere between a private cloud and a public cloud
- **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.
- **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).

The level of risk to your organization will depend on the model you choose. For example, in a public cloud, multi-tenancy and the vendor's ability to segment and protect company data from being inappropriately accessed while in transit can be high. However, the same risk is much lower when choosing a private cloud model.

Ten cloud computing risks

Understanding the risks associated with moving to the cloud is a first step to managing them. It is important to note that many of risks are not new. In fact, organizations may be able to apply lessons learned from managing other IT outsourcing contracts, or from similar services, like virtualization that IT functions have implemented behind the firewall. Virtualized environments, in particular, can be subject to attacks that can go virtually undetected by traditional monitoring systems. Customers need to look for a system that will enforce security policies across dynamic and scalable applications residing in the cloud and at data centers.

The following represent the 10 most significant categories of cloud computing risks and how your organization can manage them.

1 Policies, standards and controls

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.

Managing policies, standards and controls risks

Because of the rate of development and innovation in cloud computing and a lack of widely accepted normative models for controls in a cloud environment, assessing the impact of outsourcing to a cloud service provider can be difficult. This difficulty is often increased due to the reluctance of CSPs to permit tenant audits of the controls over their cloud environments and lack of availability of independent third party reports on the controls. Often, organizations have require CSPs to provide SAS 70 reports in order to obtain some confidence in the controls over the cloud environments, even though reports prepared in accordance with SAS 70 are intended only to address the controls as they related to the financial statements of users.

With the release of SOC 2: Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2) from the American Institute of Certified Public Accountants (AICPA), cloud tenants have a new tool for assessing controls over a cloud environment. A SOC 2 report provides users with a description of the CSP's cloud services and an independent CPA's opinion on the fairness of the description, the suitability of the design of the CSP's controls and, in a Type 2 report, an opinion on the effectiveness of the controls. The AICPA is also working with the Cloud Security Alliance (CSA) to provide a framework for integrating SOC 2 reports with the CSA's Consensus Assessments Initiative Questionnaire and Cloud Control Matrix.

2 Regulatory and compliance risks

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 like 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 your organization's jurisdictions, but also those of the cloud provider. Moving your data to the cloud does not absolve your organization of responsibility for regulatory compliance — quite the contrary. Regardless of where the data resides, your 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 you and the provider operate.

Managing regulatory and compliance risks

Carefully examine the following areas and prepare appropriate action to address these risks:

- **Cloud provider controls.** Carefully review controls implemented by the cloud service provider, which will detail the terms of the services and whether they have the necessary controls, infrastructure and certifications to meet regulatory guidelines.
- **Industry relevance.** Investigate whether the provider currently has other relevant industry clients to determine their level of experience in managing the types of storage, reporting and tracking of information you need to meet compliance requirements.
- **Diversity of jurisdictions.** Thoroughly review laws and regulations in each jurisdiction in which your organization and the provider operates and set your reporting, security and ownership standards to the most stringent legal environment. Understanding your organization's exposure to the diversity of laws, which vary from state to state and country to country, will help providers to provide service levels that meet legal requirements. Given the ever changing legal landscape of information laws, it is important to notify your cloud provider if services need to be adapted to match new regulatory guidelines or expectations.

Examples of country-specific regulations include:

- US. Sarbanes-Oxley (SOX), The Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH), Payment Card Industry Data Security Standard (PCI/DSS) and other laws mandate compliance requirements based on industry.
- Europe. European Directives provide guidance to European Union member states without mandating how to achieve a particular result. One example is Directive 2004/48/EC which outlines parameters for enforcing intellectual property rights. The Privacy and Electronic Communications (EC Directive), another EC Directive, makes it illegal to use automated messages through the telephone for direct marketing purposes, without the prior consent of the subscriber.
- UK. The Data Protection Act 1998 (DPA) outlines a company's legal obligations in handing and protecting personal information.

3 Governance risks

In the continuing cost-conscious environment, organizations cannot afford to make mistakes when it comes to IT investments. Nor can it afford to be noncompliant when it comes to industry-, state- or country-specific regulations. When embarking on the journey into the cloud, your organization will want to make sure it has a clearly defined strategy for cloud services that is aligned to the broader business strategy, compatible with existing architecture, adheres to all applicable laws and regulations within each jurisdiction in which your organization operates, and provides the desired return on investment your organization seeks.

Without a sound governance strategy that applies to both your organization as well as the cloud services provider, the organization risks ineffectiveness, loss of control and potential harm to its reputation from negative legal or regulatory action.

Managing governance risks

To manage governance risks, consider developing a strategy and implementing a governance framework that aligns to the following five major domains of governance and global standards:

- **Aligning to business objectives**. As stated above, begin by analyzing your reason for moving to the cloud and making sure that your organization's IT strategy is aligned to that of the broader business strategy. Develop a committee that focuses on IT governance before and after an implementation, gives strategic direction of the cloud services engagement and reviews the overall investment. Additionally, assess your business requirements and compare them to the benefits and the risks associated with cloud services. It is possible that cloud computing may not be the best solution for the business.
- **Value delivery.** Create an environment of collaboration with the cloud provider to achieve the desired business goals. Work to optimize cloud services delivery expenses by taking full advantage of ownership that the provider is offering.
- **Cloud risk management.** Assess the cloud computing risks that may have an impact across the enterprise. Also, review the provider's governance structure prior to implementation. Pay particular attention to Non-disclosure agreements (NDAs), escrow contracts, penalties and contractual terms.
- **Ownership and accountability.** Be clear about who owns and has rights to the data and the systems, as well as roles and responsibilities internally, and with the provider.
- **Performance measurement.** Develop metrics and standards to monitor the impact the cloud services may have on your business. Create auditable documentation of the findings and implement periodic reviews to ensure the provider is maintaining appropriate performance levels.

4 Information security 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

In *Borderless security: Ernst & Young's 2010 Global Information Security Survey*, 52% of respondents identify data leakage, 39% cited the loss of visibility to what happens to company data, and 34% worried about unauthorized access as increasing risks.

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 software-as-a-service (SaaS), have lower transparency and ownership over security controls and processes that providers implement.

Security threat matrix

[text to come]
[text to come]
[text to come]
[text to come]
[text to come]
[text to come]

Managing information security risks

Start by asking for a copy of the provider's IT security policy, as well as business continuity and disaster recovery plans. Based on their IT security policy and corporate strategic plan, you can develop a security strategy with the cloud computing provider. This strategy must clearly articulate what constitutes an acceptable level of risk based on your organization's risk tolerance. The cloud services provider should also have third-party audit certification validating that the provider has implemented proper operating controls for data security.

Acceptable audit reports may include ISO 27001certification or the new Service organization control report, SOC 2, performed by a registered auditing firm.

Consider mapping which security measures are critical and how they align to the varying levels of security controls the provider is implementing. As well, it is important to ensure that the provider continually demonstrates adherence to strict requirements for confidentiality, integrity and availability. Define which controls are critical to the business at the outset, and work with the provider to address them as part of the initial contract negotiation. SLAs, their underpinning contracts, and controls should include at a minimum:

- **Information risk appetite and tolerance.** Given the sensitivity of information your organization may be moving to the cloud, it is critical to understand the types of risks that may materialize as well as their business impact. With that knowledge, define your organization's risk appetite and establish a set of risk management strategies that manage the risk to the prescribed tolerance level. From there, compare the provider's risk management methods to determine if they meet the organization's risk tolerance. If they do not, additional risk management measures may be necessary.
- **Security policies and procedures.** Work with the provider to mirror as closely as possible your organization's security policies and procedures. This will enable you to establish consistent, effective and secure solutions. These may include centralized guidelines, standards, procedures and metrics. You will also want to ensure that the provider has measures in place which will protect, detect and react (PDR) to potential threats or breaches against your logical and physical assets. The information may be held in the cloud, but you remain accountable for its protection, control, and due diligence with regard to all governing regulations. There should also be a provision to mitigate threats beyond the traditional security perimeter. Cloud computing extends a security perimeter outside traditional boundaries, which can challenge traditional PDR mechanisms.

- **Application security.** Use assessment tools to determine security levels of applications and underlying dependencies. Consider direct application security-specific metrics such as vulnerability scores and patch coverage to assess the quality of application coding. Indirect data handling metrics, such as the percentage of data encrypted, can validate that providers are making responsible decisions in terms of application architecture.
- **Identity and access management.** Client management protocols should address requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges with a set of user account management procedures. Discuss terms of services from the provider and communicate roles and responsibilities for personnel and users to distinguish between authority, responsibilities and accountability. Limit user access to information on a need-to-know basis.
- **Authentication.** Consider authenticating users through your identity management system. This authentication can be augmented with an industry single sign on (SSO) standard such as security assertion markup language (SAML) to then access the provider's cloud environment.
- **Continuity of operations.** Business continuity is critical. Determine what procedures the provider has in place to sustain service at all times. At a minimum, providers should have some form of system restoration to earlier states, as well the ability to restore valid configuration as far back as 6 to 12 months, or in adherence to other requirements that may apply based on geography.
- **Cloud resilience.** Using exceptional fault tolerance can mitigate the risk of catastrophic failure. However, fault tolerance does not address other critical areas of business resilience. Consider addressing this risk by answering the following key questions: What happens if the cloud provider goes out of business? Can you back up from the cloud? Can you restore your business if cloud services fail? You need to understand what control you have if a catastrophic failure occurs.
- **Encryption.** Identify which data is essential to encrypt to optimize processing while still providing a secure communication channel. When possible, segregate encryption key management from the cloud provider hosting the data. This will minimize the provider's ability to misuse information. It will also protect your organization and the provider from conflicts should either party be compelled by law to provide access to data. It is also important to ensure the security of encryption keys used to secure data. These keys should be kept in an area that is segmented, with limited logical and physical access, and with access only by user privilege. Data should be encrypted in rest and in motion.
- **Security incident handling.** Make sure incident detection and analysis tools are compatible with your systems. Incompatibilities could result in issues related to investigations, forensics and legal discovery should there be legal action or government intervention. To prevent security incidents, processes must be in place to proactively test and monitor policies, procedures and controls you have you have implemented. Periodically, reevaluate security measures to make certain that the provider is maintaining the approved enterprise's information security baseline.

5 Privacy risks

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 your organization, as well as the provider.

Managing privacy risks

Privacy and personal information policies should include how soon the cloud provider needs to alert you in the event of a suspected breach so that you can take appropriate actions to notify relevant regulatory bodies and impacted individuals. You will also want to be clear about retention periods, where the data can or cannot be transferred, logging of access by cloud administrators and the ability of other parties to access the data for market research or other secondary activities. Other areas to consider include:

- **Data identification and classification.** Prior to engaging a cloud services provider, develop a corporate data dictionary with data syntax rules, data classification and security levels. Establish a classification scheme based on data criticality and sensitivity (e.g., public, internal use, proprietary, highly confidential and top secret), including data ownership. Classification schemes should tie to an appropriate security level and protection controls with data retention and destruction requirements. It is also important to identify any regulatory requirements that apply to outsourced data so that you can specifically ensure that the provider meets these requirements as part of the contract negotiations.

- **Encryption.** Proper encryption can help to ensure data privacy. Prior to engaging a cloud services provider, decide what data to send to the cloud and what should be kept in-house based on criticality. Criticality can also determine what data needs to be encrypted and at what stage. All data should be encrypted when transmitted. Confidential data should be encrypted while stored. Additionally, implement policies with the provider regarding generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys.
- **Regulatory monitoring.** Regularly monitor and measure the provider to ensure that it is adhering to emerging regulation and legislation regarding data privacy and confidentiality.
- **Deleted data.** Deleted data doesn't necessarily disappear. CSPs and their clients alike need to be concerned with the fact that data sometimes persists in servers through which it has traveled, even after having been "deleted." Only forensic analysis can reveal whether deletion of data is truly "permanent."

6 Data risks

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 whom you've contracted, or housed in a foreign jurisdiction where privacy protections are lax. However, data issues may also arise from improperly entered or recorded transactions if a cloud computing service is not properly implemented.

Managing data risks

Because data risks have both operational and legal ramifications, you will want to ensure that active measures are clearly outlined in the following areas:

- **Data handling procedures.** As part of the planning process, openly communicate to the provider your procedures for effective and efficient data storage, retention and archiving, and destruction of data. As well, data needs to be authorized and identifiable. This will prevent future "bad data."
- **Penalties for non-compliance.** Use the SLA to specifically outline data requirements and associated penalties if the provider fails to meet the required baselines.
- **Data integrity controls.** Implement access management and hashing controls to prevent unauthorized modification of data.

7 Service support, operations and development risks

Whether it's software-as-a-service (SaaS), platform-as-a-service (PaaS) or infrastructure-as-a-service (IaaS), the key words in each are "as-a-Service." Service in cloud computing should mean not having to work 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.

Managing service support, operations and development risks

To prevent support risks, address the following key areas as part of your contract negotiations with the provider:

- **Capacity planning.** As part of the due diligence process when selecting a provider, you will want to ensure that the provider can meet your support requirements. Review the provider's capacity and performance resources to see whether they can meet your desired service levels. To minimize the risk of service disruptions because of insufficient capacity or performance degradation, consider advising the provider in advance of estimated future performance and capacity needs, giving consideration to normal workloads, trends, contingencies, storage requirements, tenant workloads and IT resource life cycles.
- **Right to audit.** You will also want the right to audit the provider at periodic intervals, upon disruption of service or you are not satisfied with the level of service being offered. An audit may highlight issues that will increase service levels.
- **Incident management.** Verify that your selected provider has established service desk procedures, call centers or help desks, as well as tiered escalation procedures based on the urgency of the issue for incidents that cannot be resolved immediately with a clear line of accountability. Establish at the outset what you consider an incident (data breaches, perhaps) versus an event (a suspicious intrusion detection alert) and that you understand how you would communicate, log, track, correct and report incidents that arise.

8 Contract and legal risks

Contractual risks stem primarily from the types of contracts that clients enter into with cloud service providers. These service level agreements (SLAs) or end-user level agreements (EULAs) 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 nonnegotiable, especially for users of commodity service offerings.

Managing contract and legal risks

Contract risk management needs to begin with a holistic understanding of your organization and why you are choosing cloud computing services. This should include knowledge of your internal systems interdependencies, as well as the capability to manage business-critical provider contracts. Review the following areas:

- **SLAs and EULAs.** Examine the SLAs and EULAs to determine whether your needs and expectations match the services a provider is willing or able to provide. If the agreement fails to meet your requirements, request a say in determining SLA terms and conditions. When negotiating the SLAs, also make certain that you address all critical IT services based on your predetermined requirements and IT capabilities.
- **Risk assumption and transference.** Understand who assumes risk where and when. Often, providers use insurance policies as risk transference mechanisms. This can also occur through Underpinning contracts (UCs) that reflect agreements between cloud providers and their third-party providers. Where possible, examine these contracts with the same degree of scrutiny as that of the cloud provider's SLA, since the third parties may be providing critical aspects of the services you are negotiating with the provider.
- **Service delivery metrics.** Develop key performance indicators (KPIs) or other service delivery metrics to measure performance and service delivery. Begin by identifying which metrics you deem most important. KPIs should include availability, time to resolve service requests, transactions processing time and memory use. Often, providers will have the capability to deliver these metrics in an easy to evaluate dashboard that you can use as a real-time scorecard. While this type of self-reporting is good, you will also want to conduct periodic audits to verify that the provider is delivering the agreed-upon services at the agreed-upon levels.
- **Termination of services.** Ensure the contract addresses termination of services. This should include provisions for how the provider returns or destroys your organization's data.

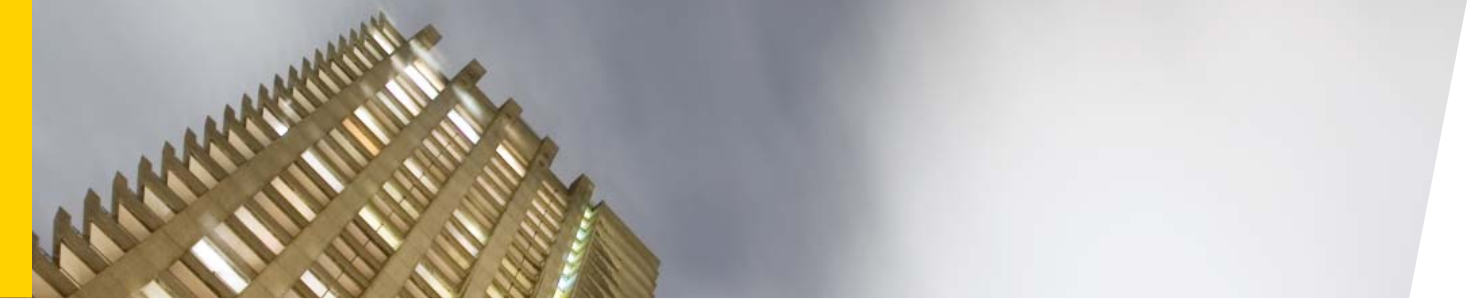
9 Infrastructure and architecture risks

Infrastructure and architecture risks arise if the provider does not achieve performance requirements that your organization and the provider agree to and define in the SLA at the outset of the engagement. These risks may include availability and reliability issues in the form of unplanned outages or compromised bandwidth because you are sharing the infrastructure with other clients during peak hours.

Managing infrastructure risks

There are certain steps you can take with your provider to minimize infrastructure risks. These include:

- Understand your baseline usage. When seeking cloud services it is important to evaluate and analyze current baselines of usage to which you can compare future requirements. This will enable you to provide forecasted capacity and availability estimates for which the provider can prepare and scale to, if needed.
- Planning for the future. Scalability requirements so that, as the company grows, you have assurance that the cloud services provider will be able to meet these demands. Clearly articulate responsibility for IT and security function. Document explicit responsibilities for traditional IT and security services, including application, data, runtime, middleware, operating system, virtualization, server, storage, networking, provisioning, and incident response.



Managing architectural risks

Architectural risks are dependent on services and infrastructure. Thoroughly study the following systems infrastructure of each prospective provider to determine compatibility with your current in-house systems prior to finalizing the engagement.

- **Multi-tenancy.** Many cloud services providers have a multi-tenant structure in which a single application or platform serves multiple clients. This model may not be appropriate for every organization, particularly if the organization is bound by special regulatory requirements or has customization requirements that cannot be extended to other tenants. Where a multi-tenant structure is a viable option, be aware of how co-tenant activities can affect you. For example, if a tenant is under investigation, the hardware containing the suspect data may be seized, or processing frozen. If you share hardware with this tenant, your use of that hardware may be compromised. Similarly, if you are operating during another client's peak usage period, this increased traffic could limit your bandwidth. Insist on contingency plans that include dynamic allocation of computing resources and robust load balancing techniques.
- **Cloud provider privileges and access.** To avoid provider employees from accessing data, determine who has access to your data, as well as their respective rights, privileges and the conditions under which such rights are granted. Ask for a report from the provider's HR department outlining the methods the provider uses for vetting its employees. Additionally, keep "default deny all" policies and enforce "least privilege" principles so that data access is given only to the necessary users and that only those rights needed to complete their respective jobs is granted. Both your employees and those of the provider should be bound by these policies. Ensure to reflect these policies in the contract you negotiate with the provider.
- **Data and application lock-in.** If you attempt to move the services performed by an external provider in-house, or to another provider, you may be unable to access your data. To avoid this problem, accurately understand your provider's systems architecture. As part of your contract negotiations, request advanced notifications if the provider plans any major architectural changes.
- **Embedded security architecture.** Despite the effective management of defined controls, the underlying infrastructure, systems and business processes may not have been designed with embedded security. To address this risk, look for indicators that security is build-in and not bolted on. Key indicators are robust service provider design and implementation procedures (SDLC), with security and architecture stakeholders and gates.

10 Integration risks

Cloud service providers 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 your 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.

Managing integration risks

Minimize integration risks by focusing on the following key areas:

- **Transition services.** Negotiate transition services into the contract with the selected provider. This should include the provider's full cooperation in all transition activities, as well as allocations of associated costs.
- **Technology changes and upgrades.** Plan for changes in technology or architecture by the provider that may affect the operability of the systems or require you to make changes. You will also want to set strict parameters around data extraction should you wish to terminate your agreement with the provider.
- **Testing.** Test systems for interoperability prior to integration. This helps evaluate and analyze whether the provider is able to deliver the expected outcome and value.

Moving forward

Despite the risks, we believe the success of cloud computing is inevitable, because companies will be attracted to its flexible, pay-as-you-use business model. That model allows companies to manage their technology costs more efficiently, enables deployment of new technology faster and easier than other models, and allows management to focus on delivering business value. Cloud computing is the future of both information technology and information security – and the future is here.

Glossary of terms

Application service provider (ASP) is a termused to describe computer-based services delivered over the internet in the late 1990s. The term has since been replaced by "on-demand software" and "software as a service."

Cloud computing[1] is 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. This cloud model promotes availability and is composed of (A) five essential cloud characteristics, (B) three service models and (C) four deployment models.

A: Essential cloud computing characteristics

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 datacenter). 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.

B: Cloud computing service models

1. *Cloud 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 fromvarious 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.
2. *Cloud platform as a service (PaaS).* The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools 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. *Cloud 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).

C: Cloud computing deployment models

1. *Private cloud.* The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
2. *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 organizations or a third party and may exist on premise or off premise.
3. *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.
4. *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).

Grid computing is a form of distributed computing in which a large set of geographically remote computers work together to perform a single task. Although it started out as a more general term, today it applies primarily to super-computer level tasks and is used mostly in the scientific community. Mash-ups are new, innovative combinations of existing services, usually on the internet,that create new business value, whether through open public means or via service agreements.

Time-sharing is the process in which multiple users share the processor time of a main-frame computer system. It faded out of use beginning in the 1980s after the PC emerged.

Utility computing is the provision of computing resources as a metered service, similar to a public utility. The term is an ancestor of cloud computing; it was most popular in the 1980s and early 1990s.

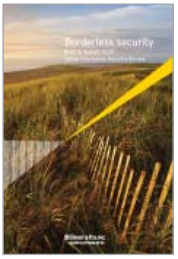
Service level agreements (SLAs) are written contracts between information technology service providers and their customers that stipulate details such as system availability and customer service response time, as well as penalties for failure to meet the agreed-on service levels.

Related thought leadership

Thought leadership at ey.com/informationsecurity

Privacy trends 2011: challenges to privacy programs in a borderless world

Executives are investing more money to protect the privacy of personal information. But are they spending it in the right places? Read this year's report to find out which privacy issues you need to be thinking about in an increasingly borderless world.



Borderless security: Ernst & Young's 2010 Global Information Security Survey

In our 2010 Global Information Security Survey, more than 1,600 participants from 56 countries share their greatest strengths and most critical risks in today's information security environment.

Countering cyber attacks

Traditional information security solutions are not enough to protect against persistent threats and attacks. This updated report discusses the measures organizations should consider to detect and react to successful cyber attacks.

A risk-based approach to segregation of duties

Segregation of Duties (SoD) is top of mind for many professionals, due in part to control-driven regulations worldwide and the executive-level accountability for their successful implementation. This document outlines a practical, risk-based approach to SoD compliance.

Information security in a borderless world: time for a rethink

Traditional security models that focus primarily on keeping the bad guys out no longer work. It's time to rethink how organizations can keep their most valuable assets safe. Read this report to learn how you can transform your information security program to enable enterprise-wide business performance and build trust in a borderless world.

Plugging the leaks: managing threats to confidential data

Over the last five years, organizations have experienced a rise in the volume of intentional and unintentional data leakage. This new whitepaper explains how a program that includes both behavior and technical controls can give responsible employees an outlet for escalating concerns while protecting confidential data from being leaked by those with malicious intent.

GTC report "Cloud computing: issues and impacts" to come

Ernst & Young

Assurance | Tax | Transactions | Advisory

About Ernst & Young
Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 141,000 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 20,000 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. xxxxxx

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.

www.ey.com

About Ernst & Young

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 and more focused and faster in responses, and can redefine both the effectiveness and efficiency of operations. But as opportunity grows, so does risk. Effective IT risk management 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 40 71271	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
Paul van Kessel (Europe, Middle East, India and Africa Leader, Amsterdam)	+31 88 40 71271	paul.van.kessel@nl.ey.com
Troy Kelly (Asia-Pacific Leader, Hong Kong)	+85 2 2629 3238	troy.kelly@hk.ey.com
Giovanni Stagno (Japan Leader, Chiyoda-ku)	+81 3 3506 2411	stagno-gvnn@shinnihon.or.jp