Deloitte.

Will risk rain on your move to the cloud?
The role of Internal Audit in the Digital Enterprise

Preface

Organizations today are embracing new digital technologies to leapfrog or keep pace with growing competition in the marketplace. Powerful platforms — such as mobile, analytics, social media, cloud, and cyber intelligence — can potentially impact every facet of the organization, leading to new opportunities. But these emerging technologies and platforms can also introduce significant disruptive forces into the business. The convergence of these macro forces is reflecting a new basis for competition, changing the environment in which we both live and work, and becoming the core of the "Digital Enterprise." Therefore, it is critical to understand the risks of integration as constantly changing digital technologies become the norm.

This whitepaper is part of our series on the Digital Enterprise, which focuses on how organizations can leverage the disruptive forces of digital technologies, mitigate emerging risks, and capitalize on breakthrough thinking. We encourage you to share this whitepaper with colleagues — executives, board members, and key managers at your company. The issues outlined herein can serve as the starting point for the crucial dialogue on helping your organization achieve its goals as a Digital Enterprise.

Table of contents

Mitigating the risks of cloud computing 4

Cloud computing defined 5

Cloud computing on the rise 6

Getting to the heart of risks 7

Internal Audit: Taking on the challenge 9

 Cloud computing – Not a “whether” forecast 10

Mitigating the risks of cloud computing

When confronting the challenges of cloud computing, internal auditors may need to stretch beyond their traditional audit roles.

Cloud computing has taken the business world by storm. And with it comes a potential deluge of risks. As confidentiality, security, service continuity, and regulatory compliance become even more critical to the business, what role should Internal Audit (IA) play in addressing these risks?

In this paper, we discuss the growing importance of the cloud and pinpoint the risks the organization should take to heart. Cloud computing presents a new frontier for many organizations — and for IA as well. When confronting the challenges of cloud computing, internal auditors may need to stretch beyond their traditional audit roles, adding greater value as they assist the organization in building the required control environment to mitigate risks associated with the cloud.

To help prevent surprises and ward off regulatory and compliance fines that may have a damaging impact on brand and reputation, IA can conduct a cloud readiness assessment of existing vendor procurement and contract processes to identify cloud control gaps. We also offer five proactive steps IA functions should consider as the organization adopts cloud computing initiatives:

1. Engage stakeholders in informed discussions about the risk implications of cloud computing
2. Review the current organizational risk framework based on cloud risks that have been identified
3. Develop risk-mitigation strategies to help minimize the risks that accompany cloud computing
4. Review and better understand the organization's data governance program, as this is a key component in the treatment of data in the cloud
5. Evaluate potential cloud vendors from a risk perspective

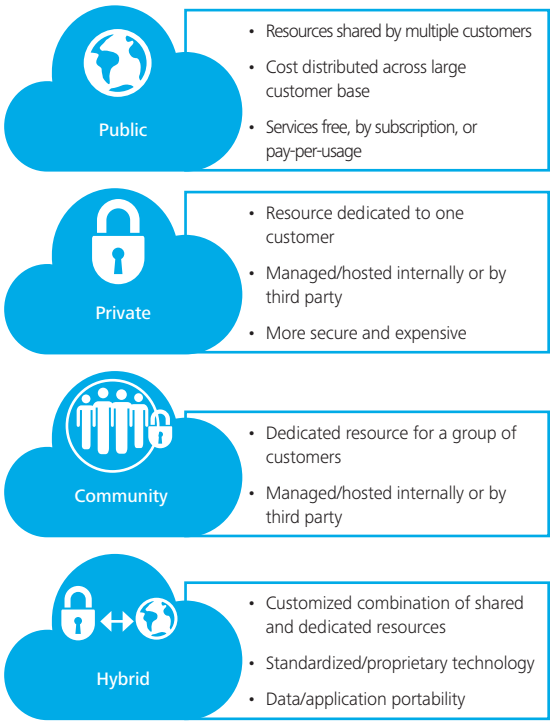
Cloud computing defined

As defined by the National Institute of Standards and Technology (NIST), "Cloud computing is a model for enabling ubiquitous, 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."[1] Cloud computing vendors can provide a complete application or a specific slice of technology that enhances an organization's existing technology capabilities.

According to NIST, cloud computing has five key characteristics:[2]

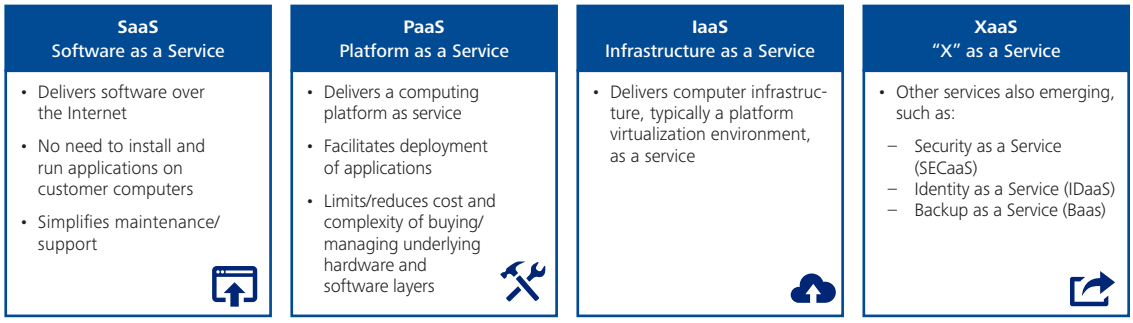
- Predictable pricing: The organization incurs a charge only when it consumes resources. The price is based on a flat subscription fee or a pay-as-you-go usage model, not on perpetual licensing or a long-term contract.
- Ubiquitous network access: The service is available wherever and whenever the network is available and can be accessed from a range of devices (PCs, laptops, mobile devices, tablets, etc.).
- Resource pooling and location independence: The provider pools its computing resources to serve multiple consumers using a multi-tenant model. The customer organization generally has no control over or knowledge of the exact location of these resources.
- Self-service: Users can access the service directly, provisioning is on-demand, and services are delivered in near-real-time.
- Elasticity of supply: Capabilities can be scaled up or down to meet resource demands, with seemingly limitless upper bounds. This allows the organization to rapidly increase or decrease its information technology (IT) infrastructure costs based on changing business needs.

Figure 1: Common cloud deployment models



Organizations typically leverage one or more of the four common cloud computing models shown in figure 1. There are also three major cloud service delivery types. But other services have begun to emerge — often referred to as "X as a Service." (See figure 2.) In essence, anything can be "as a service," and some cloud vendors now offer slivers and combinations of traditional services.

Figure 2: Common service delivery types



[1] Mell, Peter and Grance, Timothy, "The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology," Special Publication 800-145, National Institution of Standards and Technology, U.S. Department of Commerce, September 2011.

[2] These attributes are an adaptation of the NIST characteristics.

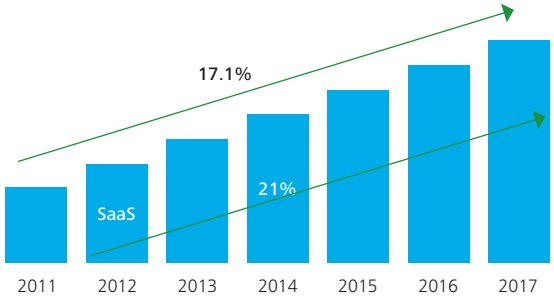
Cloud computing on the rise

However you define it, cloud computing is clearly on the rise. A 2013 Gartner report predicted that total spending on public cloud services could grow 18 percent by year end, reaching $131 billion, with a compound annual growth rate (CAGR) of 17.1 percent from 2011 through 2017. Gartner also projects that the cloud application software-as-a-service (SaaS) market will increase at a steady CAGR of 21 percent from 2012 through 2017.[3] (See figure 3.)

Companies are migrating to the cloud in such numbers, of course, because of the significant advantages it can provide — from increasing speed to market and achieving better economies of scale to improving organizational flexibility and trimming technology infrastructure and software licensing spending. No longer are organizations faced with the task of creating and maintaining large data centers and developing proprietary complex systems. The expense of software upgrades or application patches is carried by the provider, which can allocate these costs across a wide customer base. Potentially freed from large up-front capital investments, time-consuming installation, and hefty maintenance costs, IT departments can focus on value-added activities that promote the business.

It is important to note, though, that the amount of investment and savings will vary on cloud deployment models. In some instances, actual up-front costs can rise as the level of customization and privacy requirements increase. But cloud computing can allow companies that see a new market opportunity to pick and choose vendors, turning to a top-of-the-line provider and entering the marketplace quickly. In fact, technology research firm IDC foresees that "the primary driver for cloud adoption will shift from economics to innovation as leading-edge companies invest in cloud services as the foundation for new competitive offerings."[4]

Figure 3: Compound annual growth rate of cloud services spending



Source: Gartner, "Forecast Overview: Public Cloud Services, Worldwide, 2Q13 Update."

The growing consumer use of social media and mobile technologies has also added to the demand for cloud services, as businesses seek better and faster ways to reach out to existing and potential customers. For example, a bricks-and-mortar video and game rental company failed to grasp the implications of cloud computing. When competitors began offering consumers immediately downloadable programming, the company was too slow to react and eventually folded.

Some companies go beyond using the cloud to provide customer services. In an effort to focus its IT operations on business services, an online video rental and streaming company moved its internal applications to a cloud service provider and began using SaaS applications. Even governments are getting in on the game: A large metropolitan city equipped all its employees with an application for both email and cloud-based collaboration.

[3] Gartner, "Forecast Overview: Public Cloud Services, Worldwide, 2Q13 Update," August 28, 2013.

[4] "Worldwide and Regional Public IT Cloud Services 2013-2017 Forecast," IDC, August 2013.

Getting to the heart of risks

Companies that ignore the potential pitfalls of moving to the cloud do so at their peril. The shift to cloud computing has essentially extended the boundaries of the traditional computer processing environment to include multiple service providers. This brings a complex set of risks to an organization's data as it travels through the cloud. When a company opts for the speed and convenience of moving to the cloud, it often relinquishes control not only of its own data, but that of its customers. Confidentiality, security, and service continuity become critical considerations, as does regulatory compliance, which remains the responsibility of the business.

The organization should scrutinize risks throughout the technology life cycle — not only those inherent in migrating to the cloud, but also those that affect vendor selection, implementation, and ongoing monitoring. In our work with clients, we have found that a broad risk framework tool can prompt management to consider the potential pitfalls of moving to the cloud from a variety of perspectives.

Such a tool can get to the heart of risks by providing a view on the pervasive, evolving, and interconnected nature of risks associated with cloud computing. These risks range from governance and compliance to infrastructure security and from data management to IT operations. (See figure 4.) This risk framework tool can also help:

- Spur discussions about such risk management topics as risk identification, prioritization, measurement, and mitigation
- Facilitate the connection of risk management silos
- Identify redundant efforts in place to manage risk
- Improve efficiency in compliance and risk management efforts
- Develop risk event scenarios that require integrated responses

Not every cloud has a silver lining

Organizations contemplating a move to the cloud should be aware of the problems that can occur. Here are just a few potential risks:

Data breaches: Particularly in multi-tenant cloud service databases. A flaw in one client's application could give an attacker entrance to other clients' data as well. Breaches could expose email databases, putting email accounts of thousands of end customers at risk of increased spam and phishing scams. Worse yet, data breaches could also reveal customers' passwords, and even personal and financial information, to hackers.

Data loss: Malicious hackers, natural disasters, or lapses in provider services could result in a loss of customer data. For example, bugs in web-based email services could lead to the disappearance of users' messages, folders, inboxes, or entire email accounts. Data loss could be particularly detrimental to organizations that are required to store information in compliance with industry regulations, such as healthcare organizations that must comply with the Health Insurance Portability and Accountability Act.

Downed reservations systems and websites: Whether due to denial of service attacks, severe storms, or technical glitches, outages could result in thousands of inconvenienced customers (for example, airline travelers) and the disruption of traffic (and commerce) at client websites.

Reduced levels of control can also be attributed to IT departments being bypassed, as some business owners opt to obtain services more quickly and cheaply by creating their own "rogue" technology environments via the cloud.

To be more effective, the tool can be customized to include regulatory, geographic, industry, and other specific issues that impact the organization.

In short, a cloud risk framework tool can stimulate discussion about an action plan for vetting providers, monitoring performance, and mitigating risk. Consider a conversation about data management risks, as one example. Because organizations may have to relinquish control over their data to cloud providers, it is crucial that they have a full understanding of how data will be handled in the cloud environment. To that end, they should ask a range of questions, such as:

- Will the complexity of multiple cloud data stores compromise data retention?
- What is the risk of unauthorized access to or inappropriate use of sensitive data, and how will this be handled? How will we be notified of a violation?
- Will transfer of data between jurisdictions violate any data privacy laws?
- Will we be able to remove data from multiple cloud data stores?

With the increasing migration to the cloud, IA should be at the forefront, engaging in discussions with business and IT in the preliminary stages to address potential cloud risks and opportunities. If IA is consulted too late in the process — and the organization has already made the move to the cloud — a prime opportunity may be missed to assess and mitigate risks, and IA reports may have findings that management is unable to remediate.

Figure 4: Cloud risk framework: A recommended approach

Internal Audit: Taking on the challenge

Implementing a cloud strategy changes the risk landscape in profound ways. As some risks are minimized, others spring up in their place. Recognizing and responding to this morphing organizational risk profile is the purview of IA. Internal auditors understand the interplay between business processes and risk. So they can not only help business leaders articulate their appetite for risk, but they can also help develop strategies for mitigating it.

Furthermore, while an organization's information security group can build cloud monitoring capabilities, IA can assess the effectiveness of the control environment — helping to prevent the IT department from being left out of the loop.

IA, then, should make sure it understands the organization's current cloud footprint, conducts cloud audits by starting at the procurement process, and recognizes the conditions that prompt business users to bypass the IT shop and sign up for cloud services directly. It should also develop and leverage a customized framework tool to help identify the organization's top cloud risks and drill down to key statements.

As the company adopts technology initiatives that involve cloud computing, IA should take the five proactive steps outlined below:

Keeping an eye on the cloud, post-migration

Of course, the risks don't end when the migration is complete. Continued monitoring is critical. Once the organization has moved its data, applications, or other technology to the cloud environment, internal auditors should audit these initiatives using a cloud risk framework tool and then adjust the degree of testing based on the cloud deployment model and service.

Auditing the cloud presents new challenges in how IA assesses controls. What part of the technology stack is subject to the cloud audit? What is the universal sample to make selections from within an ever-changing environment? And how can historical data be tested if it is no longer there?

Also, services may change in the cloud. Therefore, internal auditors should understand and test the controls the organization has in place on an annual basis to reevaluate the company's cloud risk profile.

Figure 5: Proactive steps for Internal Audit

1 Engage stakeholders	• Encourage IT and business executives to begin an informed conversation about the move to the cloud. • Help stakeholders understand the potential for rogue IT environments. • Proactively explore which applications and data are candidates for transfer to a cloud environment and be prepared to discuss the risk implications of the move.
2 Review the organizational framework	• Make changes to the company's risk framework based on the new risks that have been identified, minimizing the emphasis on those that are no longer a concern. • This new or modified framework tool should measure the organization's current cloud capability state across the different cloud risk domains.
3 Develop risk-mitigation strategies	• IA can be part of the risk equation, assisting the organization with developing a risk-based approach to the use of cloud computing. • This entails not only understanding the risks involved but suggesting ways to help minimize risk.
4 Review data governance	• IA can review the organization's current data governance program and implementation across various systems to assess if policies are in place to meet regulatory and compliance laws. • By understanding the data governance program and its implementation within the organization, management will be able to make risk-informed decisions about moving services and data to the cloud.
5 Evaluate potential cloud vendors	• IT will be familiar with the range of vendors, and the business leaders will be able to articulate the objectives of a move to the cloud. • IA should be engaged in risk discussions, along with your organization's security, risk, and compliance groups. • Internal auditors can help the organization develop an assessment profile for vendors that explores such issues as vendor controls, disaster recovery capabilities, the handling of multiple customers' data, and roles and responsibilities.

Cloud computing – not a "whether" forecast

Cloud computing is changing the technology landscape, and the changes are only likely to intensify in the years to come. For many organizations, the question is not whether the cloud should be part of their technology strategy, but when and how. Under pressure to provide solutions, organizations may be tempted to leverage cloud services quickly, without weighing the associated risks. As the third line of defense, and as a function that understands risks, IA can help provide the context and risk framework an organization should consider when moving to the cloud.

A broad risk assessment should be integral to decisions that entail moving applications or infrastructure to the cloud and determining which vendors are a good fit. Similarly, cloud providers should also perform a risk assessment of their services. By engaging in these discussions, internal auditors can help IT and business leaders be better prepared for the full range of risks when migrating to the cloud.

As the third line of defense, IA can help provide the context and risk framework when moving to the cloud.

Contacts

Michael Juergens
Principal
Deloitte & Touche LLP
+1 213 688 5338
michaelj@deloitte.com

Charlie Willis
Senior Manager
Deloitte & Touche LLP
+1 215 299 4534
chwillis@deloitte.com

This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this document.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2014 Deloitte Development LLC. All rights reserved.
Member of Deloitte Touche Tohmatsu Limited