Internal Audit’s Role in Cloud Computing
Introduction

There are numerous risk factors that must be managed to ensure the availability of a public, private, hybrid or community cloud solution.

Cloud computing has transformed the way businesses approach the consumption and delivery of IT services. It is a form of standardized IT-based capability – such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or Software as a Service (SaaS) – offered by a service provider (e.g., “public” cloud) and intended to provide end-user access via the Internet from any computer. It is – in theory, at least – always available, can dynamically scale to adjust to demand, has web- or programmatic-based control interfaces, and enables full customer self-service. As this white paper discusses, there are numerous risk factors that must be managed to ensure the availability of a public, private, hybrid or community cloud solution.

With cloud computing, applications and data are available to an organization’s user base, wherever and whenever users choose to connect. This means the business does not have to maintain the hardware and software required to deliver those services – or provide all the support to keep those infrastructure components updated, secure and available. Other potential benefits to organizations that embrace the cloud computing model are¹:

• Decoupling and separating the business service from the infrastructure needed to run it (i.e., virtualization)
• Flexibility to choose multiple vendors that provide reliable and scalable business services, development environments and infrastructure that can be leveraged “out of the box” and billed on a metered basis – with the potential for no long-term contracts
• Elastic nature of the infrastructure to rapidly allocate and de-allocate massively scalable resources to business services on a demand basis
• Cost-allocation flexibility for businesses using the cloud that want to move capital expenditures into operating expenses
• Reduced costs due to operational efficiencies
• More rapid deployment of new business services
• Operational risk reduction, if availability of services and operations are adequately protected within a contract

The use of cloud computing does pose risks to the enterprise; but if key risks to the business are understood and planned for from the outset, they can be managed. Before moving to the cloud, companies should assess the following:

- **Privileged user access** – How will the provider control access to our data? How can we be assured they will not abuse that access?
- **Regulatory compliance** – Our business must adhere to regulatory requirements. How will we know if the provider is complying with those requirements?
- **Data location and ownership** – Once our data is “in the cloud,” where exactly will it reside? Is the provider’s data center located in a jurisdiction in which we don’t currently operate? Do we understand the requirements of that jurisdiction? Do we have contracts with any customers that prohibit our company from storing data in certain jurisdictions? If there is a problem, or a legal matter, what rights do we have to the data?
- **Data segregation** – If the same servers are used to store data from multiple customers, how will the provider ensure other customers cannot see our data – and that we will not see theirs? Can other people access and change our data once it is in the cloud?
- **Recovery** – Can the cloud go offline? If so, who is responsible for getting it back online? How quickly can that be done? What happens while we are waiting? Could our data be lost in the process? Do recovery capabilities support our obligations to stakeholders and/or customers?
- **Investigative support** – What happens if we receive a legal hold notice? Will the cloud service provider help us secure the data? How do we know legal holds will be properly processed? What about other types of investigations?
- **Long-term viability** – If our cloud service provider goes out of business, how do we get our data back? If our provider is a startup, do they have the long-term funding and business model to serve us? And if we are fully leveraging the cloud (SaaS, PaaS and IaaS), do we even have the capability to get the data back? How would we restore our data and applications if we did get it back?
- **IT general controls** – Will our cloud environment be supported by fundamental IT general controls? How do we know the environment is secure? What is our provider doing to protect us from third parties hacking into our data? Can we perform periodic audits of the vendor’s environment? What if we need to perform testing to support Sarbanes-Oxley or other regulatory requirements?
- **Unknown cloud services** – Do we know all the cloud services already in use in our organization? (Fifty-five percent of U.S. respondents do not, according to a 2010 *Security of Cloud Computing Users* study by Ponemon Institute.) Due to increasing consumerization (employees’ introducing and adopting technology in the enterprise) of cloud services, business units already may be using these services without IT’s knowledge – or any thought of data security.

---

INTERNAL AUDIT IS WELL POSITIONED THROUGH ITS ROLE AS AN ASSURANCE FUNCTION OF THE ORGANIZATION TO HELP MANAGEMENT AND THE BOARD IDENTIFY AND CONSIDER THE KEY RISKS OF LEVERAGING CLOUD COMPUTING TECHNOLOGY.

INTERNAL AUDIT’S ROLE IN THE CLOUD COMPUTING DECISION

The risks outlined above are generally applicable throughout the cloud computing life cycle, whether an organization is thinking about moving to the cloud, is in the process of implementing a cloud-based solution, or is already working in a cloud environment. (Some companies may be in various stages of all three.) Regardless of which stage your company is in, internal audit is well positioned through its role as an assurance function of the organization to help management and the board identify and consider the key risks of leveraging cloud computing technology. Internal audit also can help the business determine whether those risks are being appropriately mitigated.

Defining a Cloud Strategy

Internal audit should engage company management to determine if a cloud computing strategy has been defined and communicated. If not, internal audit may be able to assist management in this process by helping to address the following questions:

- **What is the business case for moving to the cloud?** Organizations need a true understanding of the value they seek to gain by moving to the cloud, and determine if they can fully mitigate or accept the risks associated with working in this environment. Consider the following: Does your organization have a complex application infrastructure? Are your applications no longer supported by the vendor or reliant upon legacy systems? If so, cloud vendors may not be able to support these applications or the servers on which they run. However, if your business looks to become increasingly scalable and efficient while reducing costs, a cloud hosting solution may be appropriate.

- **Would this decision align with business needs?** Before migrating to a cloud environment, companies should determine if such a move would align with their overall business strategy and objectives. Are your IT assets aging or reaching the point of retirement? Is there a strategy in place to reduce the cost of IT assets? If your organization is looking for ways to decrease operational or labor costs, the business may be able to realize some cost benefits by selecting a cloud solution.

- **Do we understand the current state of systems and data to be moved to the cloud?** It is important to understand what exactly is being moved to the cloud. Would your company be moving sensitive and/or critical data? Will the business be able to continue complying with data retention requirements? Are there other applications or infrastructure that will have to be re-architected from a communications standpoint? Is your transaction volume going to exceed your (or the provider’s) available bandwidth?

Evaluating Vendors

After weighing the potential benefits and risks of moving to the cloud computing model, the next step is to select the right vendor. Companies are often tempted to leverage the first cloud vendor they identify, or opt for the most popular provider. However, as is the case with any vendor relationship, many risks merit attention to help ensure your organization’s specific risks and controls are addressed. When evaluating potential cloud providers, companies should consider the following questions:

- **Who will manage the vendor relationship?** Companies that use third-party cloud providers should determine who will act as the liaison between the company and the vendor. This will help to ensure
there are clear lines of communication between your company and the vendor’s legal department, IT organizations and account managers.

- **How are assets protected?** Information is arguably an organization’s most valuable asset – as well as a potential liability. Cloud vendors should be able to describe the internal data security controls in place to protect data – from intellectual property to customer information to internal bank account numbers. Your company should understand how the vendor manages its own security – both physical security and logical security (e.g., access rights, user identification) – by requesting security policies, vulnerability and penetration test results, and attestations on internal control environments. SSAE 16s (new industry standard that replaces the legacy SAS 70) and reports on compliance often provide insight into the vendor’s control environment and any considerations a prospective client might need to address. Where SSAE 16s or other assessment reports are not available, it is still important to determine how you will obtain assurance that the vendor’s security practices meet your business needs.

- **How is responsibility divided?** Your company needs a clear understanding of which party is operationally responsible for data stored in the cloud. Determine up front who is responsible for monitoring and controlling the servers, applications and data hosted in the cloud. Monitoring activities may include measuring bandwidth, monitoring server performance, applying patches and updates, managing network infrastructure, monitoring backups and providing intrusion detection services. Also, determine who is financially and legally responsible for the data, security and uptime.

- **How will moving to the cloud impact disaster recovery planning?** Disaster preparedness is growing in priority and significance for businesses of all types. One benefit of a cloud computing model is that many providers guarantee defined uptime and failover capabilities as a component of their business model and signed contract. Your company should request the prospective vendor’s business continuity and disaster recovery plans and determine if they align with your business needs and recovery objectives.

- **How does the vendor manage multiple tenants?** In the cloud, your data may be stored on the same physical machine with other clients’ data. Your company should know what controls are in place to logically and even physically (whether on separate devices, sectioned off in separate cages or in completely separate bays) separate your data from other clients’ data.

- **How would this change the technology environment?** Implementing a cloud solution may change your organization’s technology environment, including network topology, interaction between systems and the flow of data. It is necessary for your company to understand which data sits on and flows between which devices. Also, determine who owns each of those components and who is responsible for governing the environment in each step along the way.

- **Where is data physically stored?** Cloud hosting providers can host data in a variety of locations, and your company should understand where your data will reside. If the vendor hosts data internationally, this may impose additional regulatory, international and ownership risks, depending on the country in which the vendor maintains its servers.

- **How do the company’s risks and controls align with the prospective vendor’s?** By performing a gap analysis, your company will be able to determine if there are any control or process gaps in place, which may expose your organization to additional risks. Reports on compliance, SSAE 16s or other assessment reports from the vendor can provide additional insight into known deficiencies, operational risks and user control considerations.

**Implementing a Cloud Computing Model**

Once due diligence activities are complete, and a cloud service provider that aligns with the company’s strategy, objectives and control framework has been selected, internal audit may shift to evaluating the implementation process. Internal audit can be integral in determining whether the level of planning was adequate to reduce project risk, while also providing independent feedback about the migration process.
Internal audit should evaluate implementation activities for adherence to the company's system development life cycle, project management and change management methodologies. Where deviations from these internal policies, processes and methodologies are required, it should be confirmed that all updates follow expected approval procedures. In addition to ensuring that fundamental cloud computing risk areas have been identified, this evaluation may provide an opportunity for internal audit to help assess the effectiveness of mitigation strategies/controls prior to implementing a cloud computing model.

Questions the business should consider when implementing a cloud computing model include:

- **What are the service level and operating level agreements (SLAs and OLAs)?** While SLAs and OLAs are important for services hosted internally, these agreements have additional significance when the service is hosted in the cloud. With this objective measurement, there is a defined expectation of the level of service being provided. When the SLAs and OLAs were drafted, was the business involved in the decision-making process, or did IT unilaterally decide what was acceptable? Are there any legal, regulatory or contractual compliance requirements that must be taken into account? As the amount of permitted downtime (or other measure) decreases, the cost to the provider – and presumably, the customer – increases.

- **What are our (and our cloud provider’s) compliance responsibilities?** There are many legal (e.g., legal hold, e-discovery), regulatory (e.g., Payment Card Industry Data Security Standard, Health Insurance Portability and Accountability Act, Gramm-Leach-Bliley Act, the European Union’s Data Protection Directive), and contractual compliance requirements that organizations need to consider when moving to the cloud. Outsourcing the hosting of a service to a third party does not change these requirements, which should be incorporated into the contract to provide a solid base for establishing necessary controls. How does the vendor prove compliance with relevant regulatory requirements? How will customers be notified of a security breach?

- **How are incidents managed?** What is the process for identifying and escalating an issue (e.g., a data breach) in a timely and efficient manner? Are you responsible for initiating contact with the vendor, or does the service provider have proactive monitoring in place so that it knows when something goes wrong? Establishing these basic processes and understanding escalation procedures and expected time to resolution are important.

- **Who determines user access rights to data?** Depending on the type of service purchased, user provisioning may be automated or manual. If it is a manual process, it may be executed by the organization, the provider or both. Developing and defining a process for all situations, including end users and administrators, is important so that expectations are universally understood. While the process may not be identical to that of your organization’s internally hosted services, the same core principles should exist.

- **How often is data backed up?** Who is responsible for that process? Depending on the responsibilities defined between your organization and the cloud vendor, backup and recovery processes that formally assign responsibility for monitoring backups; identifying, resolving and escalating errors and failures; and rotating data and media to a separate location for recovery purposes should be defined. If a daily backup routine fails, what happens?

- **How will we inform and train end users?** As with any significant change to an IT environment, end-user training is critical for ensuring process owners and other users in the organization have adequate knowledge of newly defined processes and fully understand their roles in helping the business to meet data security and compliance expectations.
Monitoring the Vendor

Once your company integrates the planned systems and data into a cloud environment, internal audit may evaluate whether the defined owner is adequately monitoring and controlling the vendor relationship. By this time, the organization should be formally monitoring and reporting on the agreed-upon service levels, while investigating and resolving any variances. As a component of monitoring activities, your company should routinely review any documentation provided by the vendor relating to internal control assessments (whether from SSAE 16s, vulnerability scans or penetration tests). Additionally, internal audit should routinely evaluate regulatory requirements and determine if they are being addressed adequately by the cloud vendor and the company.

In monitoring the cloud vendor relationship, the following should be confirmed:

• **How the company’s relationship with the vendor is managed** – A single person (i.e., relationship manager) should be identified as the primary point of contact with the cloud provider. That person (and any necessary backups) should regularly communicate with a counterpart at the provider. This existing relationship should be used to address issues that arise with the service (e.g., the breach of an SLA or OLA) and to reach resolution.

• **Who is confirming the accuracy of invoices** – Prior to being paid, invoices should be reviewed to confirm pricing terms are consistent with the contract and the quantity of services being billed is accurate. Independent reports should be obtained to confirm the accuracy of any quantity on the invoice.

• **Whether SLAs and/or OLAs are being monitored and reviewed** – Where SLAs and OLAs have been agreed to, they should be recalculated to confirm that the values provided by the cloud vendor are accurate. Additionally, penalties or incentives obtained due to SLA/OLA deviations should be recalculated to confirm the accuracy of the resulting payments and/or credits.

• **How contractual control requirements (e.g., regulatory, security, privacy) are being monitored** – Contractual control requirements should be evaluated using the means made available through the contract, including “right to audit,” assessment reports (e.g., SSAE 16s, reports on compliance) and other evaluations. These methods should be used as frequently as possible, based on the terms of the contract, and the evaluation should be documented.

**CONCLUSION**

Cloud computing will continue to transform the way organizations manage IT – increasing efficiencies while reducing costs – but there are risks. Proactively identifying and understanding relevant risks before signing a contract and committing to a cloud hosting implementation is essential for success and for ensuring both data security and adherence to compliance demands.

Organizations should establish processes to routinely re-evaluate and monitor risks once the business is working “in the cloud.” Internal audit should consider the risks and controls outlined in this paper and ensure management has evaluated potential risks and taken steps to address them proactively.

Further, it is the responsibility of the chief audit executive to understand the security risks facing the organization, and to work as a conduit to ensure the audit committee understands the risks and how well management is mitigating them.
protiviti (www.protiviti.com) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit. Through our network of more than 70 offices in over 20 countries, we have served more than 35 percent of FORTUNE® 1000 and Global 500 companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

protiviti is a wholly owned subsidiary of Robert Half International Inc. (NYSE: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

About Our IT Internal Audit Services
protiviti's IT internal audit services help organizations understand their key technology risks and how well they are mitigating and controlling those risks. We also provide insight into the threats inherent in today's highly complex technologies. protiviti provides a wide range of services for IT internal audit outsourcing and co-sourcing. The protiviti methodology, which is both COSO- and CobiT-based, facilitates an overall IT internal audit management team (either protiviti-led, client-led, or in combination) with execution of individual projects by subject-matter experts in each IT audit area.

Other Thought Leadership from Protiviti
Visit www.protiviti.com to obtain copies of these and other thought leadership materials from Protiviti:

- 2011 IT Audit Benchmarking Survey
- 2011 Information Technology Capabilities and Needs Survey
- 2011 Internal Audit Capabilities and Needs Survey
- Using High Value IT Audits to Add Value and Evaluate Key Risks and Controls
- Powerful Insights (protiviti's podcast series)
  - IT Audit – Assessing and Managing Risks Effectively within the IT Environment
  - The Importance of Strong IT Governance During a Financial Crisis
  - Social Media Use in Companies – Managing the Risks Effectively
  - Technology-enabled Audits – Increasing Productivity and Delivering More Timely and Reliable Results
  - Internal Audit Quality Assessment Reviews – Required as well as Beneficial
  - The Benefits of Outsourcing the Internal Audit Function
- Board Risk Oversight – A Progress Report (from COSO and Protiviti): Where Boards of Directors Currently Stand in Executing Their Risk Oversight Responsibilities
- Changes to the IIA Standards: What Board Members and Executive Management Need to Know
- Testing the Reporting Process – Validating Critical Information
- Internal Auditing Around the World (Volumes 1-7)
Brian Christensen
Executive Vice President – Global Internal Audit
+1.602.273.8020
brian.christensen@protiviti.com

David Brand
Managing Director – IT Audit Practice Leader
+1.312.476.6401
david.brand@protiviti.com

Australia
Gary Anderson
+61.3.9948.1200
gary.anderson@protiviti.com.au

United Kingdom
Jonathan Wyatt
+44.20.7024.7522
jonathan.wyatt@protiviti.co.uk

United States
David Brand
+1.312.476.6401
david.brand@protiviti.com
### THE AMERICAS

**United States**
- Alexandria
- Atlanta
- Baltimore
- Boston
- Charlotte
- Chicago
- Cincinnati
- Cleveland
- Dallas
- Denver
- Fort Lauderdale
- Houston
- Kansas City
- Los Angeles
- Milwaukee
- Minneapolis
- New York
- Orlando
- Philadelphia
- Phoenix
- Pittsburgh
- Portland
- Richmond
- Sacramento
- Salt Lake City
- San Francisco
- San Jose
- Seattle
- Stamford
- St. Louis
- Tampa
- Washington, D.C.
- Woodbridge

**Europe**
- France
  - Paris
- Germany
  - Frankfurt
  - Munich
- Italy
  - Milan
  - Rome
  - Turin
- Spain
  - Madrid
- The Netherlands
  - Amsterdam
- United Kingdom
  - London

**Middle East**
- Bahrain
  - Manama*
- Oman
  - Muscat*
- United Arab Emirates
  - Abu Dhabi*
  - Dubai*

**Asian-Pacific**
- Argentina
  - Buenos Aires*
- Brazil
  - Rio de Janeiro*
  - São Paulo*
- Canada
  - Kitchener-Waterloo
  - Toronto
- Mexico
  - Mexico City*
  - Monterrey*
- Peru
  - Lima*
- Venezuela
  - Caracas*
- Singapore
  - Singapore
- South Korea
  - Seoul

**Australia**
- Brisbane
- Canberra
- Melbourne
- Perth
- Sydney
- Indonesia
  - Jakarta**
- Japan
  - Osaka
  - Tokyo

---

* Protiviti Member Firm
** Protiviti Alliance Member