

# Internal audit

An accompanying piece to 10Minutes

## Navigating the risks of cloud computing

### Highlights

Cloud computing elevates risk as tried and true internal IT privacy and data controls and compliance processes are replaced

Yet a cloud strategy vetted and supported by internal audit will help companies take advantage of the compelling cost benefits while managing new risks

Internal audit can provide business insight by identifying and communicating internal changes, external dependencies, and overall progress on objectives. Assessing the impact of the cloud starts with understanding the cloud model—private, public, or hybrid—that your company plans to adopt

With small steps, or in wholesale shifts, companies are adopting cloud computing. The economics are too compelling to ignore: standardized IT processes at reduced costs can free up IT resources to focus on differentiating the business.

Yet risk is elevated because a broad cloud implementation requires changes in processes, people, and systems.

### CAEs have a significant role to play

Chief audit executives should proactively engage the C-suite and business leaders to understand what data and applications may be moved to the cloud. They then should investigate specific risks and controls for near-term cloud adoption.

As critical IT functions move to the cloud, new risks will arise. Internal audit (IA) should re-evaluate its annual risk assessment, audit scope, and resources to support its company's cloud strategy.

### A proactive lead on risk management

CAEs should partner with business leaders to perform “preventive auditing” as their company executes its cloud adoption plan.

By identifying the controls and key performance indicators needed to manage risks and provider performance, CAEs can take an early lead in cloud strategy planning and maximize the value of cloud computing for their organizations.

Important roles for Internal Audit may include:

- 1. Manage the risks of internal change.** Roles and responsibilities change as a cloud model is adopted because existing processes and controls become obsolete. IA's knowledge of business risks, processes, and controls, combined with a proactive assessment of post-cloud processes, will enable early identification of areas of change and risks.
- 2. Manage risks of external processes and systems on the cloud.** Responsibility for managing risks—including legal, regulatory, or reputational—remains with the company, not the cloud provider. Security is top of mind, and IA should be prepared to recommend oversight requirements governing the cloud provider for security and other prevalent risks.
- 3. Provide strong governance over cloud implementation.** IA can provide real-time assurance and insight on attainment of the objectives.

### New risks to consider

The cloud model requires that IA understand the technology and processes underlying cloud computing, as well as the complex processes used to assess provider performance. IA should understand its company's contractual,

## Consider how the cloud can impact your business:

- *How will your data be protected?*
- *What changes will the cloud bring to IT?*
- *How will cloud computing impact new revenue recognition?*
- *How will cloud affect your tax deductions?*
- *What control assurances does your cloud provider offer?*

operational, and regulatory requirements that might be affected. IA should proactively engage technology, security, and regulatory specialists to help assess the impact of cloud adoption.

### Success through governance

A broad adoption of cloud computing can change virtually every business function, and IA can play an essential role through governance. IA should develop an assessment strategy that defines the “as is” and “to be” processes for assessing service level agreements, monitor the implementation to identify interdependencies or new risks, and document and evaluate metrics to measure progress toward objectives.

### Steps CAEs should take now

1. Discuss the cloud strategy with the C-suite, and gather details from functional leaders for small- and large-scale adoption.
2. Develop an education plan on cloud computing for internal audit resources.
3. To get your arms around rapidly evolving practices, engage an adviser to keep you abreast of trends in technology, enterprise risk, governance, security, and privacy relevant to the cloud.

4. For existing cloud implementations, engage an independent party to help assess the controls at your cloud provider.

### How PwC can help

To have a deeper discussion about cloud computing, please contact:

#### Dean Simone

Internal Audit Services Leader  
Phone: 267 330 2070  
Email: dean.c.simone@us.pwc.com

#### Michael Pearl

US Cloud Computing Leader  
Phone: 408 817 3801  
Email: michael.pearl@us.pwc.com

#### Cara Beston

Third Party Assurance for Cloud Computing  
Phone: 408 817 1210  
Email: cara.m.beston@us.pwc.com

### Ireland

#### Ciarán Kelly

Consulting Leader  
Phone: +353 (0) 1 792 6408  
Email: ciaran.kelly@ie.pwc.com

#### Kieran Mongan

Senior Technology Advisor  
Phone: +353 (0) 1 792 8632  
Email: kieran.mongan@ie.pwc.com