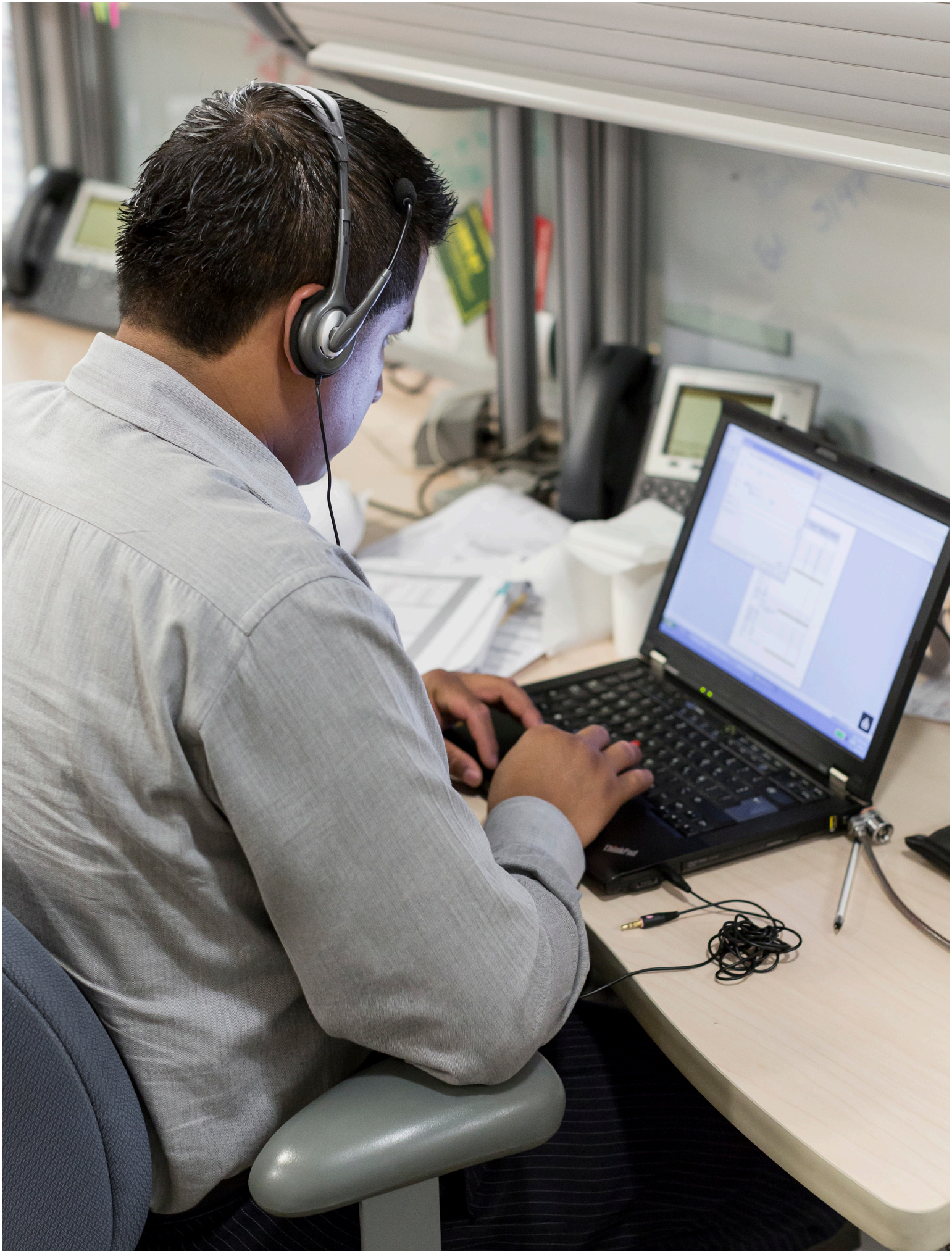
A guide to cloud audits

Internal audit's role in balancing risk and reward in the cloud

October 2014

pwc



Cloud: The new normal

Digital keystone skills

The following eight skills represent the top new, must-have areas of expertise for successful IT departments.

- Enterprise and technology architecture
- Project and program management
- Business requirements management
- Quality assurance
- Vendor management
- Prototyping
- User experience design
- Security

Source: PwC, Reinventing Information Technology in the Digital Enterprise, Jan 2014 http://www.pwc.com/us/en/increasing-it-effectiveness/publications/new-it-platform.jhtml

Today, Internal Audit is in a state of rapid transformation, thanks largely to cloud technologies. IT is rapidly modernizing our data centers from virtualization to software defined data centers so as to build out increasingly sophisticated private clouds. Inevitably, these too are connected to public clouds. The net effect is that the perimeter of the audit's control environment is increasingly virtual and hyper-extended.

No doubt the rise of cloud adoption has been phenomenal in the past few years and there are no signs of its slowing down. What was once a niche solution for start-ups can now be found in information technology (IT) road maps and business strategies throughout the corporate world. In other words, the corporate cloud is the new normal. With sensitive company data passing through third-party cloud providers and into the cloud, questions of security and risk have become paramount: Who decides what information should be shared in the cloud? Who safeguards company data in the cloud and manages the associated risks? Who is responsible for monitoring changes in the risk profile of a company's cloud position? Cloud services are also creating new responsibilities for vendor management and IT operations, giving internal audit departments an important role to play and making cloud-related risks a priority.

Cloud activity carries a host of benefits, such as cost reduction, productivity increase, and scalability. But companies are increasingly seeing the cloud movement through the lens of traditional risk management, with concerns around privacy, reliability, and resilience: Who might be watching or listening to the enormous flow of data both into and out of the cloud? What types of information are safe to hand over to a cloud provider, and what are the risks that sensitive data might get lost or compromised once data goes off premise? What controls are in place so that organizations can be sure legal, regulatory, and compliance requirements are being met and the company brand is being protected? Plus, cloud computing is changing the ways IT is procured, operated, managed, and maintained.

As organizations thus transform, internal audit will be pivotal in guiding an organization through change because leading functions will be able to provide management with an independent point of view of the organization's governance and controls structure. To be effective, many internal audit functions will have to broaden their skill sets to include those new digital keystone skills (see box) that are being added by IT departments worldwide. Is your internal audit department keeping up with the rapid pace of cloud adoption and adding value to your organization?

How is the corporate cloud used?

To incorporate cloud operations into your internal audit department's 2015 strategic planning process, you must first know where the cloud is being used. From our experience, corporate cloud consumption—in typical medium- and large-size organizations—falls into three main areas as follows, shown with a few illustrative but not exhaustive examples of common uses of cloud services.

For internal audit, a move into the cloud introduces new issues of risk, controls, data ownership, and privacy into the audit plan.

Office productivity

- Productivity solutions have switched to the cloud, often accompanying a move to enterprise-cloud email combined with document management and storage. Examples are Microsoft Office 365 and Google Apps
- Many organizations have migrated their telecommunications to cloud solutions such as Jive, Telligent, and Unison
- File sharing has been the nemesis of many an enterprise project, and cloud providers have proliferated in response. Such providers as Dropbox and Box paved the way with solutions that make the sharing of large files both simpler and mobile
- Project management often requires collaboration that is well suited to cloud base solutions. Providers include Clarizen, Basecamp, and Zoho

Business process, data and analytics

- Core business processes have gained inordinate efficiencies with cloud services in areas such as talent management with Workday, SuccessFactors, and Taleo; procurement and expense management with Ariba and Concur; customer relationship management with SalesForce.com; and so on
- Rich enterprise data is being collected from various public and internal sources in big data warehouses supplied by Google, Lexis, Reuters, public agencies; with IT data integration and quality improvement solutions from cloud providers such as Informatica
- Intelligent decision making is based on sophisticated analytics from GoodData and Tableau for precise trends in purchase patterns, demographics and regional performance; and with big data analytics from Cloudera

IT, innovation, and research and development

- The streamlining of IT support to reduce time spent and infrastructure costs has been addressed by such services as ServiceNow, Zendesk, Jitbit, and Desk.com
- Product development processes requiring tools to support more-agile development processes require a higher level of automation. Solution providers include GitHub and Atlassian.
- Continued demand for high levels of processing power for the analysis or stress testing of new products and solution development, such as conducting clinical trials prior to the release of a new medication, is supported by cloud solutions from Amazon, Google, Cloudera, and Basho

Internal audit's pivotal role

With such radical changes under way, it's vital that internal audit play a role in helping identify the most-serious cloud-related risks that already exist and then in guiding business and IT users become better prepared for new cloud-related risks. How can your internal audit department add value by helping your company avoid the pitfalls associated with cloud adoption?

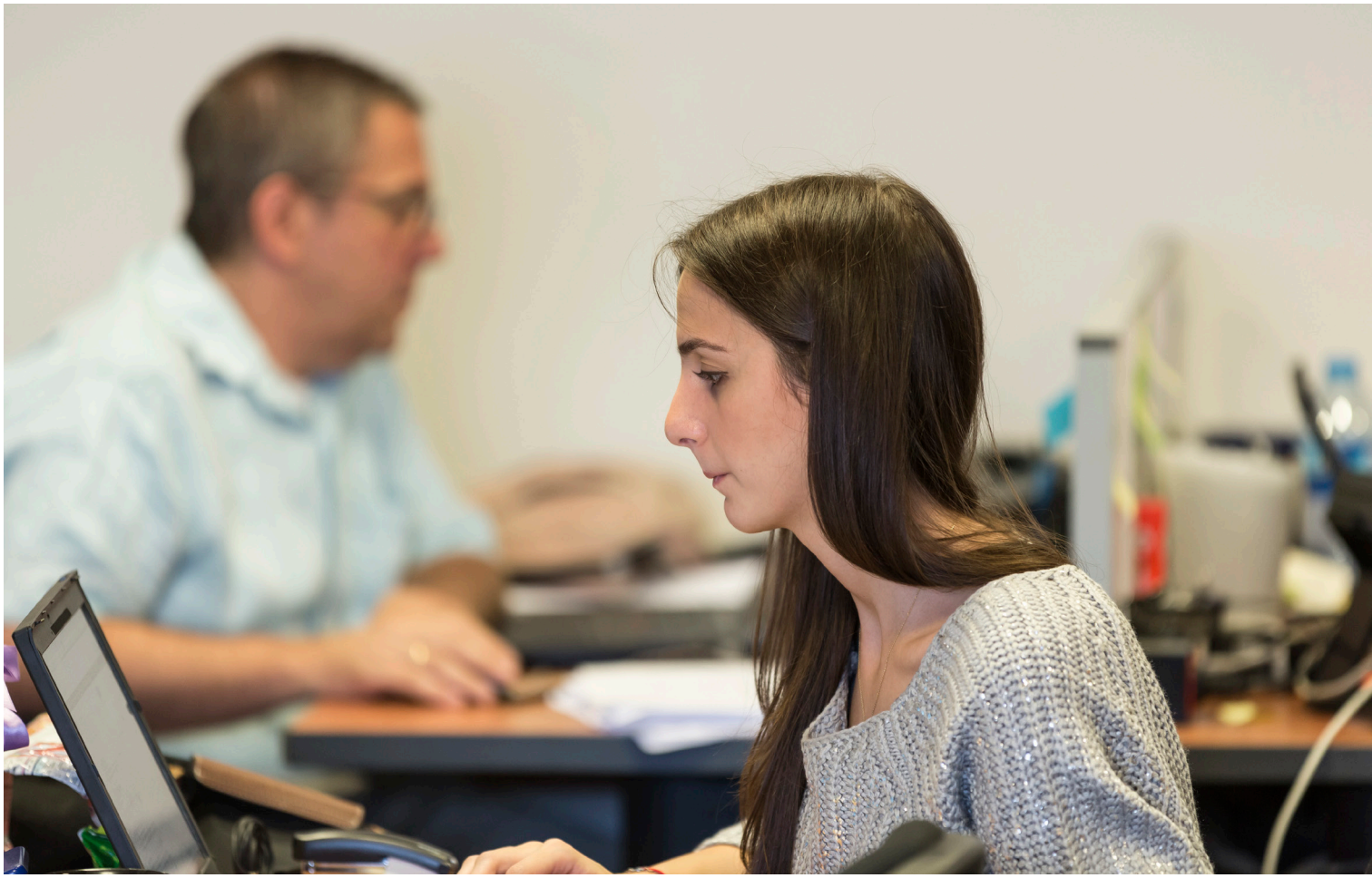
We've identified a few places to get you started.

Finding where cloud activity already exists

Discovery. This is the first action step—and it can be a tremendous one. In global companies, employees around the world may have signed up and paid for cloud services outside the typical procurement process. Many such services are priced so low (e.g. $5 per month) that the decision seems nominal. Across the organization, however, those purchasing decisions may increase costs through duplicated services and may introduce security, privacy, and data ownership issues. For many enterprises, reaching a full understanding of which cloud services are in use, by whom, and for what purpose represents a significant undertaking.

In the discovery phase, internal audit looks for previously unknown cloud providers; and informs management of potential gaps regarding cloud governance, policies, and intellectual property; and may even offer recommendations to remediate gaps and improve policy, but identification of every cloud solution that is hiding in the shadows isn't necessary to get started. As internal audit conducts its regularly planned activities, adding a few inquiries about the business or IT management's knowledge of existing cloud-based solutions can yield a representative list in just a few months of normal audit activities. That traditional discovery approach is a painstakingly manual process, consisting of interviews, manual scanning of expense reports, and so on. Internal audit organizations can now turn to third-party solutions to scan the network to identify previously unknown cloud services, discover applications, data, and people trails in the cloud, and thus help with the task. The result is the uplift in an organization's capability to discover, index, classify, and categorize risks even more granularly.

Governance. Once current cloud service providers have been identified, internal audit has an important role in advising management on development of structures for governance of those providers and on creation of improved structures and contractual agreements for future adoption of cloud services. Many cloud providers want to serve a variety of industries but may not have solutions designed to help various kinds of companies meet their unique needs. Internal audit can help management establish consistent guidelines for assessment of new cloud providers and evaluation of existing ones to ensure that best-of-breed providers get chosen and retained, respectively. This results in a consistent method for IT to directly manage its cloud services portfolio and to cull, consolidate, and build cloud service offerings for its line of businesses and the enterprise.



Policies. As cloud providers get identified and inventoried, assessment of the state of current policies and procedures for procuring, managing, monitoring, and operating cloud services becomes needed. Internal audit departments can provide objective advice and guidance in the development of company wide policies for governing cloud adoption, including changes to existing IT security policies and procurement rules.

Companies that have completed the discovery phase are finding a surprising number of cloud services in use—well beyond what was initially estimated. During this phase, breaches of company policies may get identified, such as instances when sensitive presentations containing company or customer information were stored or processed in a cloud service. In those cases, given that clouds are evolving technically, functionally, and creatively, it is essential to have a process to transform our cloud polices as often and as deeply as required in order to reduce risk.

Managing risk among known cloud providers

Even though organizations may be aware of sanctioned cloud services already in place—many of which are more akin to traditional hosting services because they are single tenant—they may not yet have the resources to respond to the risk management issues presented by an increasing volume of providers or by the diversity of types of cloud solutions already adopted. It's common to find a company's business units subscribing to an external cloud service without fully understanding the contracting risks or the service-level agreements and privacy policies agreed to on behalf of the company. In many cases, internal audit hasn't had the opportunity to consider controls and auditing procedures for cloud operations, even when those operations were widely approved. This phase of planning is important because it involves examination of the organization's known cloud IT efforts and their incorporation into the audit plan. Following are essential areas of focus recommended for any internal audit function whose company is operating in the cloud.

Targeted reviews and audits. Each cloud provider may have its own method of audit and compliance, from self-assessment to sophisticated methods aligned with industry-specific and other frameworks developed over the past few years in an attempt to reign in the compliance and audit process. Others are taking more-traditional approaches and applying them to the cloud architecture and service model, such as the American Institute of CPAs' trust services principles and criteria. Targeted reviews of cloud providers encourage consistency in the monitoring and auditing of key risks, thereby reducing the burden of full-scope reviews.

Vendor risk assessment. Cloud providers show varying compliance with security standards. Risk factors therefore must be examined for each known cloud provider, with obligations spelled out in contracts and service-level agreements. Vendor controls and contingency plans in the event of a data breach or loss would be clarified during the assessment.

Contract compliance. Internal audit will have a central role in assessing how well a cloud provider performs according to its contractual obligations regarding security and privacy. The monitoring of vendor performance in traditional areas such as security, resilience, and reliability is paramount in painting the overall risk management picture, which internal audit can help assess as more and more cloud providers get brought on board.

Business unit use of cloud. Whereas IT-driven cloud projects are likely to be known and incorporated into risk management planning, the growing use of cloud provisioning at the business unit level adds significantly to the overall risk management task. The discovery phase of planning will reveal many decentralized cloud activities, and policies and procedures should be developed that incorporate any new cloud provisioning into ongoing audit plans.

Across a range of companies and industries, leading internal audit departments are beginning to take responsibility for reviewing or initiating cloud policy development, for overseeing cloud security measures and practices, for developing provider contracts and service-level agreements, and for setting forth the purchasing procedures for cloud activities. They are also evaluating the risks of moving applications to the cloud—taking into account the financial, user acceptability, security, and compliance risks.

When the enterprise builds its own cloud

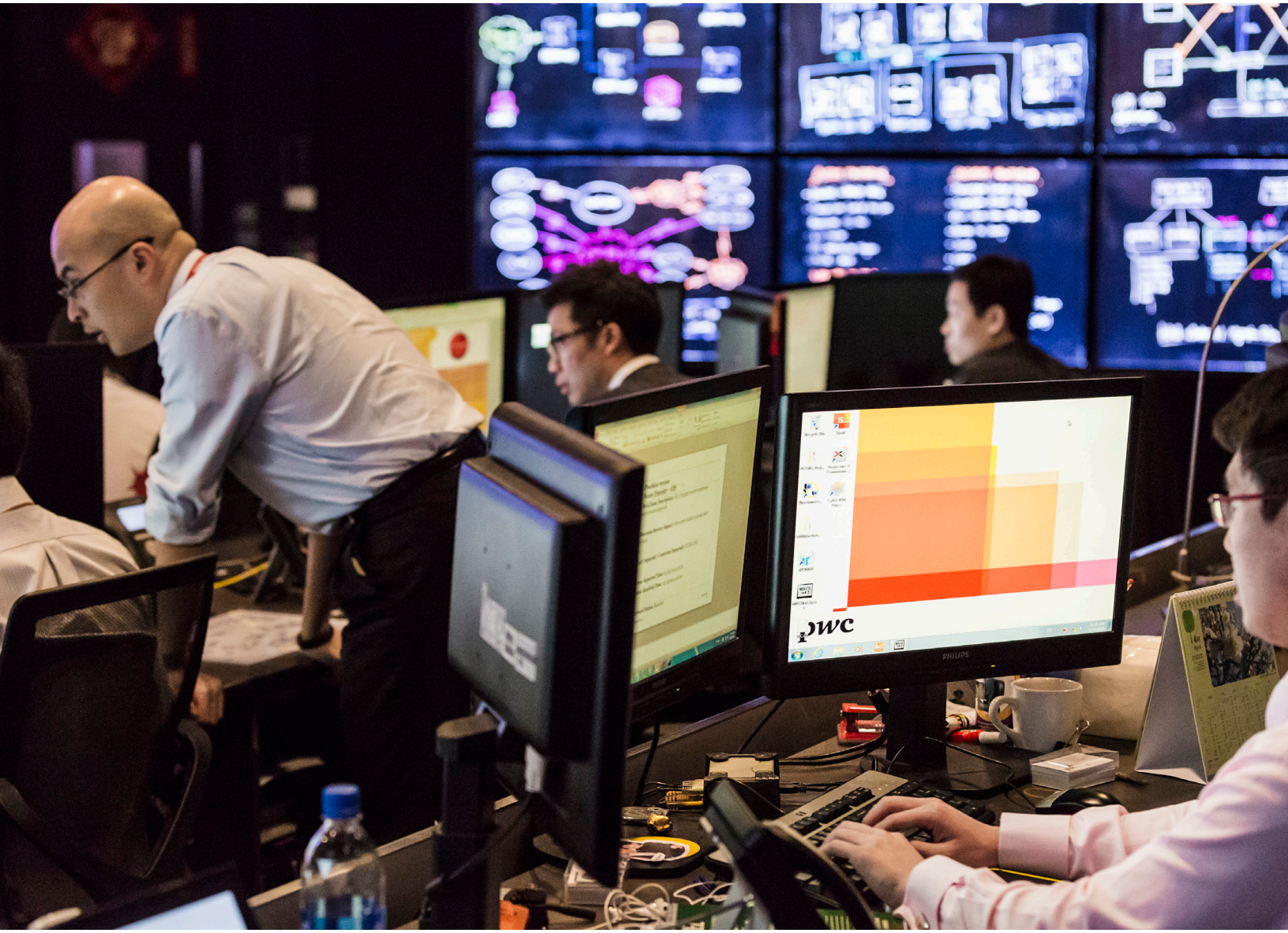
Some organizations have decided to build their own internal cloud applications and services. Internal audit has a role in that activity as well—and it can get extremely technical. For example, internal audit may want to review the internal technical architecture and weigh in on development plans with respect to controls, security, and other auditing concerns. Considerations include:

Technical architecture. Questions about interoperability and scalability; about whether various software components will be open-source ones, proprietary ones, or hybrid blends; and about the ways data will be managed and stored are matters likely to be debated before architecture choices get settled on. Internal audit has a say in such discussions, again bringing its unique perspective on controls such as automatically maintaining consistent root of trust, policy and compliance in the system; risk management particularly when change occurs; and other auditing matters such as advanced monitoring and analytics for auditing.

Vulnerability assessment. Considerations of security within each system layer—while striking a balance with accessibility and availability of the cloud application as a whole—will be reviewed in an assessment of vulnerability. And internal audit may have a lead role in bringing risk management concerns to the forefront.

Development operations. As more and more organizations adopt formal development operations methods of software development and deployment, internal audit will be creating audit models suited to standards-based and communication-centric methodologies. As standards get accepted and implemented for cloud computing, having a workable audit model that covers development through life-cycle management will be increasingly useful.

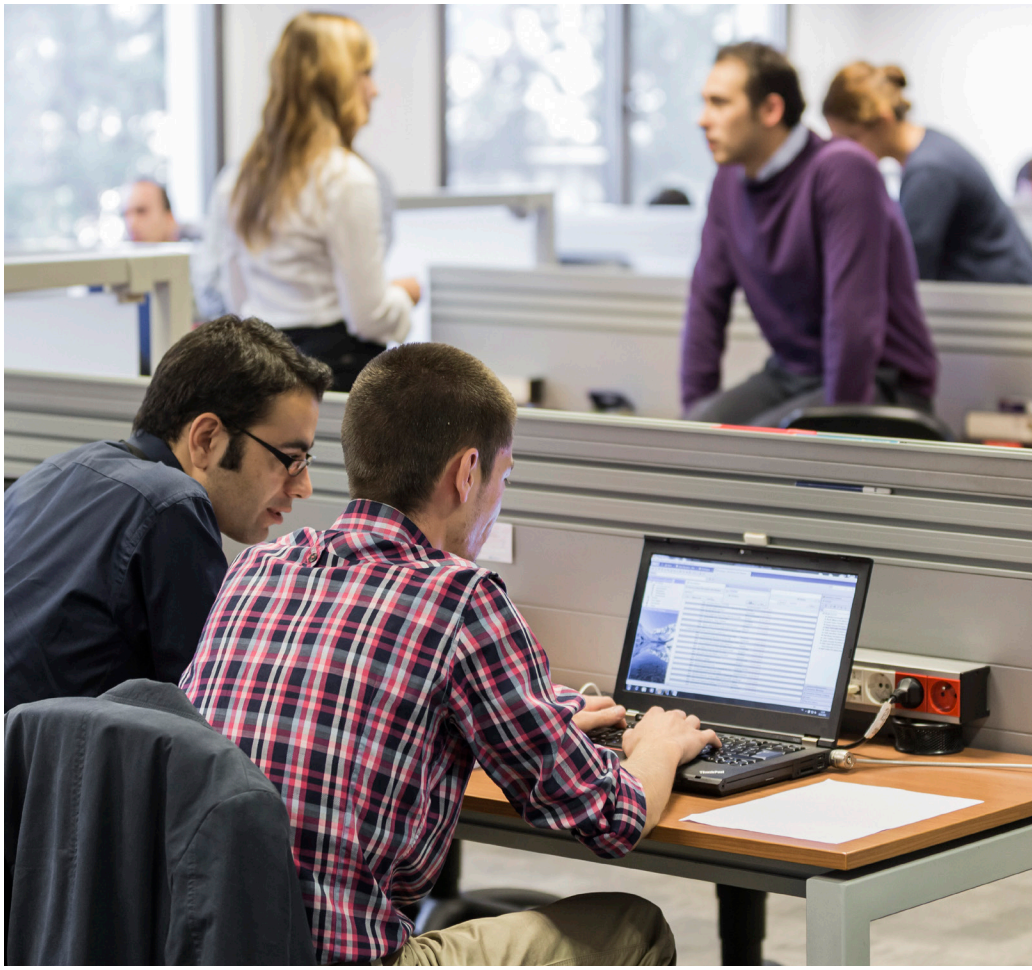
While continuing to work closely with its own IT department, this is the stage when internal audit turns to external expertise to address issues outside its core knowledge. Internal audit may also rely on outside security firms to handle certain logistics. We have seen internal audit departments asked to review technical architecture, checking for security and compliance as well as industry regulations such as Sarbanes-Oxley or US Food and Drug Administration or Health Insurance Portability and Accountability Act requirements.


pwc
PHILIPS

What's next?

With the growing adoption of cloud computing, the acceptance of off-premise, vendor-provided information technology services is becoming the new normal within the enterprise. Internal audit's role in creating a trusted cloud framework and auditing plan—same as its role in traditional IT operations—is of great importance, yet there is little time to ramp up given the explosive acceleration in cloud adoption. If your internal audit department is not quick to acknowledge this imperative movement and not careful to build a robust program around it, the situation could rapidly deteriorate, leaving your company vulnerable to security risks, privacy issues, and operating hazards.

For internal audit practitioners, therefore, the path is clear: know where to find the cloud within your enterprise and how to add value by taking an expanded approach to your otherwise traditional responsibilities in overseeing IT risk management, security, and privacy. Is your internal audit department ready for the new normal?



To have a deeper conversation on shadow cloud activity in your organization, please contact:

Cara Beston
US Cloud Assurance Leader
(408) 817-1210
cara.m.beston@us.pwc.com

Eric Tan
US Cloud Assurance Director
(408) 817-7980
eric.tan@us.pwc.com

Satchit Dokras
US Cloud Assurance Director
(408) 817-5720
satchit.dokras@us.pwc.com

Jason Pett
US Internal Audit Leader
(410) 659-3380
jason.pett@us.pwc.com

Brian Brown
US Risk Innovation Center Partner
(949) 437-5514
brian.brown@us.pwc.com

Michael Pearl
Technology Consulting Leader and
Global Cloud Computing Leader
(415) 378-8133
michael.pearl@us.pwc.com

www.pwc.com

MW-14-0583