A point of view for risk and security officers, audit executives, and those who deploy cloud services

Cloud Assurance series

Managing risk in the cloud—the role of management

pwc

Contents

Managing risk in the cloud—management's role

Business use of cloud services continues to increase, yet many businesses have no idea how many and which cloud services—authorized or not—are actually in use across their enterprises. Such an incomplete picture of the cloud services in place challenges organizations' ability to adequately address the risks associated with cloud services, including data security, customer privacy, reliability of critical business processes, and compliance risks. Business leaders' engagement is essential to move organizations toward greater cloud service awareness and a trusted, organized, and predictable approach to cloud use.

The use of cloud services has become mainstream across many industries as organizations come to realize that the potential benefits are simply too great to ignore. Used properly, cloud services may offer significant competitive advantages by helping businesses achieve operational efficiencies, enjoy instant scalability, institute price elasticity, gain expanded computing and processing power, and achieve cost reductions.

Adoption of cloud services also can help transform various business processes such as those involving customer portals, payment platforms, and sensitive modeling and engineering. Essentially, the cloud can transform any legacy process. In fact, 55% of organizations across industries and around the world now use some form of cloud computing, according to PwC's Global State of Information Security Survey 2015.[1]

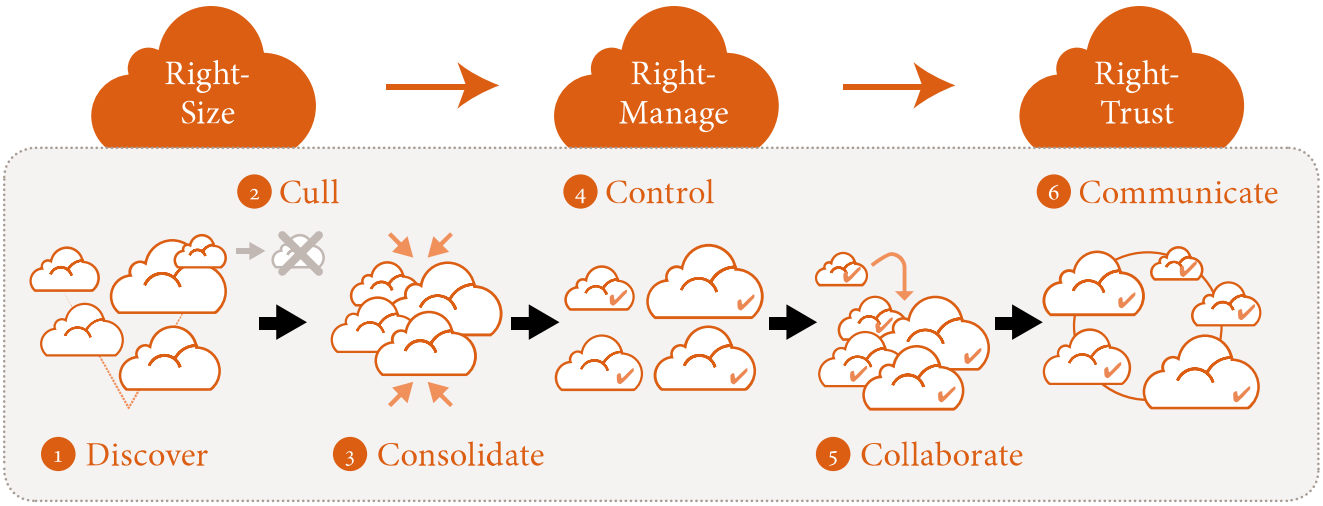
For many organizations, early implementation of more basic cloud services has given way to large-scale deployment of business functions such as customer relationship management, talent management, payroll, and enterprise communications and collaboration. But the quick deployment and low cost of cloud service subscriptions have also resulted in investment in cloud services at will by employees at all levels and in all business units, effectively permitting the purchase of enterprise information technology applications by anyone with a credit card. Such ad hoc dissemination contributes to an increase in so-called shadow IT: information technology (IT) implemented without the knowledge of or approval by corporate IT. And therefore, many companies are unaware of either the extent of cloud services they're using or who's using each service. As a result, many executives still worry about the security of company and customer information in the cloud, as well as cloud services' reliability for being entrusted with mission-critical business functions.

As cloud adoption continues growing, the risks can no longer be ignored. Knowing the extent of cloud services in use is a critical starting point. Assessing those services—including understanding how they're used, knowing the value they deliver to the company, and being familiar with the security measures in place—is essential to addressing those risks. At the same time, establishing, sharing, and championing new cloud adoption guidelines are necessary steps for driving future cloud service adoption. Different areas of the organization play different—and vital—roles in shepherding a company through the steps in that process—a process that must be undertaken in a way that does not disrupt but instead aligns with business operations and goals.

Those who make the commitment to the journey and take a programmatic approach to using cloud services can more effectively use the cloud to drive business innovation.

Knowing the extent of cloud services in use is a critical starting point. Assessing those services—including understanding how they're used, knowing the value they deliver to the company, and being familiar with the security measures in place—is essential to addressing those risks.

1 The Global State of Information Security Survey 2015: http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.



Enter the lifecycle approach for cloud risk assurance

An enterprise wide cloud risk assurance approach is necessary for learning (1) which cloud services are in use across the enterprise and (2) any related issues that have arisen. The enterprise cloud risk assurance approach is based on the cloud user's actual service use (both deployed and planned), with a framework connecting the enterprise's cloud services work flow.

Instead of being clamped on as purely corporate governance measures, this approach instead builds risk assurance throughout various cloud services and reinforces the enterprise's cloud governance, risk management, and compliance (GRC) stance with operational feedback that also offer measurements of cloud services' success. How can a business accomplish all this? The answer is, by taking a lifecycle approach to cloud services that applies the right risk management measures at each stage of development. Such an approach is (1) right-sized, with a cloud services scope appropriate to the organization's use; (2) right-managed, with an appropriate level of attention to cloud security; and (3) right-trusted, with continual pursuit of trusted cloud services.

Discover

The discovery stage is a critical first step in the lifecycle approach to cloud risk assurance. The approach begins with discovery (phase 1) of the entire portfolio of cloud services to determine what is in use across the enterprise: both known (sanctioned by the organization and IT) and unknown (unsanctioned shadow IT) services. Discover will define the scope of the enterprise cloud, identify the actual usage characteristics of each service, and set the stage for the assessment of risk exposures.

The elements of the discovery process and the information gathered feed directly into development of a proper cloud risk assurance strategy that covers establishing policies; prioritizing the cloud security program; building in the necessary elements for privacy; defining the information risk management stance, guidelines, and review for adopting cloud services; and scheduling thorough audits and compliance reporting.

A manual approach to cloud discovery can be a painstaking, time-consuming process, but many tools are available to assist organizations with cloud service discovery. Such companies as Skyhigh Networks, CloudLock, and Netskope provide insights into shadow IT. Google, Amazon Web Services, Microsoft Azure, Salesforce.com, and others offer insights and audit capabilities for their hosted applications.

Cull and Consolidate

For an organization that's embracing the lifecycle approach to cloud risk assurance, it's now time to right-size the expanse of physical, virtual, and extended cloud organizations and ecosystems. This part of the process begins with culling (phase 2), eliminating risky cloud services, and then consolidating redundant cloud services (phase 3). The task is ongoing; evaluation of cloud services must be in a continuous mode of discovering emerging services, culling them, and consolidating the duplicates.

Control and Collaborate

The next step consists of bringing the right-sized services into a fully right-managed form. The knowledge gained

in the discovery phase is the basis for mapping and locking in the appropriate controls (phase 4). Those controls could be based on guidelines or requirements provided by an organization such as the Cloud Security Alliance, or a regulation, or, in an advanced case, a strict technology platform that permits engagement of cloud services only in accordance with certain policies, procedures, and processes that manage risks associated with the services. Such a system enables business units and partners to understand and adhere to the criteria required for bringing additional cloud services into the enterprise and lets purchasing agents work from preformulated checklists and written contracts, thereby ensuring that the service will comply with the organization's IT needs and its GRC requirements during the collaboration stage (phase 5) between IT and the users, vendors, and buyers of the new cloud services.

In this phase, the control element has to do not only with blocking unauthorized cloud services but also with enabling an organization to take advantage of cloud services that have adopted or can be integrated with solutions that support the organization's control needs. For example, various proprietary platforms such as Amazon Web Services, Microsoft Azure, and Salesforce.com are being designed with encryption and key management systems in mind—in addition to offering auditing capabilities and access control federation.

Communicate

Finally, it's time to assemble the components of trust across the operations lifecycle. This is a major communications step (phase 6), wherein the company provides stakeholders with well-articulated evidence of the improvements made to the enterprise's cloud risk profile. The communication should focus on giving all stakeholders confidence in several areas related to cloud services and on building right trust in the forms of:

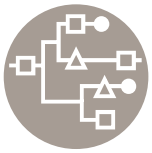
- Confidence that systems are secure, data is protected, privacy issues have been dealt with, and ongoing risks are understood and will be well managed
- Confidence in the benefits that will accrue from the things that data can reveal about business operations
- Confidence in the alignment of the organization's cloud with business systems and services, including that systems have in place the right controls and strict monitoring to ensure they do what they're supposed to do
- Confidence in the resilience of the organization's overall IT and that all digital platforms will be available when required
- Confidence that the organization's cloud services will enable the enterprise to deliver a digital transformation program to move from legacy systems to modern systems involving cloud, mobile, social media, or other services and functions in ways that result in the expected benefits—on time and on budget and taking maximum advantage of the strengths of cloud services
- Confidence based on deep understanding of the nature and management of risk in the organization's cloud services lifecycle, which in turn increases trust in the organization, its operations, and its brand

The new confidence is the foundation for building cloud trust—but only when operations are communicated openly and are transparent to all of the organization's stakeholders.

> The new cloud operations lifecycle based confidence is the foundation for building cloud trust.

Management's role

Because cloud services have implications across the entire enterprise, the lifecycle approach



CIO

CISO

CFO/COO

CAE/CCO/CLO

BUSINESS EXECS

described here has steps business leaders must take to move their organizations toward secure and trustworthy cloud usage. Following are examples of business leader roles and main considerations throughout the lifecycle.

The CHIEF INFORMATION OFFICER (CIO) must lead the effort to discover the cloud services currently in use across the organization and their impact on operations. At this stage, the CIO focuses on learning the current number and types of cloud services in use and how those services are being used. The effort requires extensive discovery of cloud services, including the applications running in them, the data they contain, where they're running and how, who's connected to them, who's using them, and what sort of anomalous behavior patterns might be associated with their use.

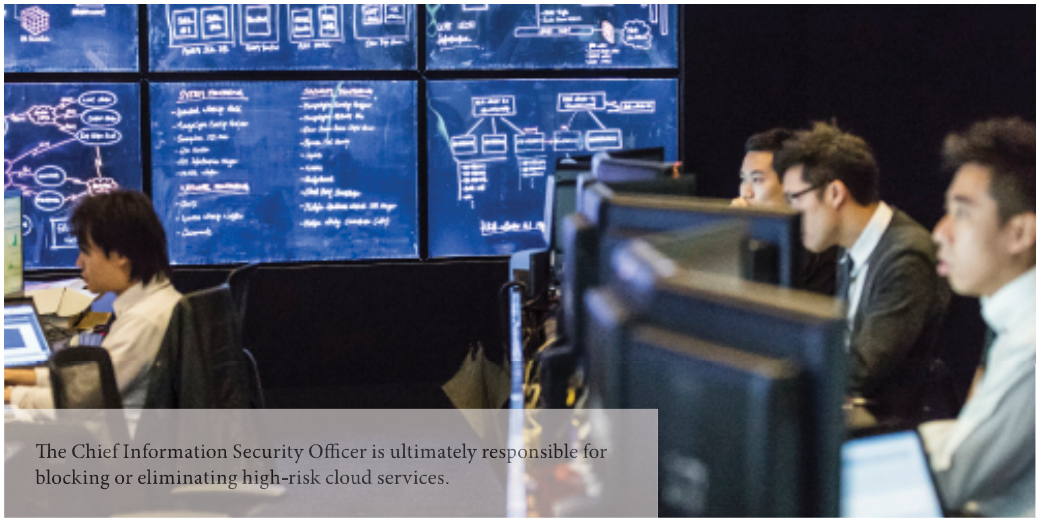
CIO

Key Cloud Considerations

- How do I know employees are using sanctioned services?
- How do I make the people directing existing IT investments more cloud aware?
- Am I operating on the fewest possible cloud services to minimize risk yet utilizing the ones necessary for the organization's success?

The CIO of a multibillion-dollar global corporation with IT and business operations around the world had no knowledge of the extent of the company's cloud service usage before engaging in the discovery process. Although the results of the discovery might have been surprising, they also provided a fact-based understanding of (1) how business units and staff were using cloud services and (2) the maturity levels of existing cloud security programs. That knowledge lay the foundation for a new, more precise cloud risk management program that fit the company's cloud operations lifecycle.

The CHIEF INFORMATION SECURITY OFFICER (CISO) is ultimately responsible for blocking or eliminating high-risk cloud services. With an understanding of what the organization is doing in the cloud, the CISO can lead the effort to immediately shut down, eliminate, or block cloud services that present high risks. This elimination phase can involve either policy or governance mandates, and it immediately produces the benefit of reducing cloud risk. After learning from evidence of



The Chief Information Security Officer is ultimately responsible for blocking or eliminating high-risk cloud services.

the organization's cloud use, the CISO can make security, privacy, and data protection controls more robust.

The CISO of a large US healthcare provider struggled with (1) selecting the right security tools to invest in and (2) judging the effectiveness of those in place. Was security a technology issue, a people issue, a process issue, or even a policy issue? Discovery revealed not only all of the cloud services in use but also the presence of shadow IT, the inability to definitively block access to several blacklisted services, and rampant unauthorized data transfers due to lack of restrictions on maximum-capacity uploads or downloads. In addition to revealing core security solutions, the discovery process pointed to the need for improvements in existing systems' policies, configurations, testing, and controls. Discovery also identified gaps where existing tools did not function well with cloud services in use, audit logs that were hard to get or incomplete, and policy orchestration that was hard to verify. New investments would be needed, along with prioritizing of custom scripting to bind the policies and controls together. Discovery and evidence-based understanding of security issues at all stages of the lifecycle helped design and validate a cloud cybersecurity road map.

The CHIEF FINANCIAL OFFICER (CFO) or CHIEF OPERATING OFFICER (COO) will have an interest in moving unsanctioned cloud services into sanctioned ones and creating more-cost- and more-business-efficient cloud use. In this cost consolidation phase, the CFO or COO leads the effort to eliminate duplication of cloud services by consolidating into a more manageable number the cloud services the organization is using. There's no point in paying for redundant cloud services, particularly when many are unmanaged.

CISO

Key Cloud Considerations

» What are the risks in the use of cloud services?

» Which cloud services do I need to block, and how do they rank by priority based on their risk to the enterprise?

» Is sensitive data passing through the cloud?

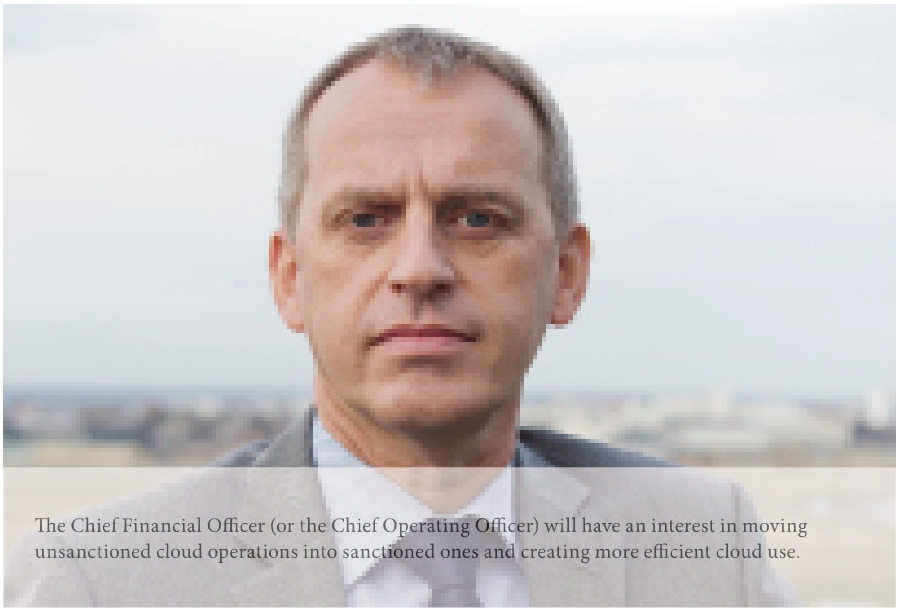
CFO/COO

Key Cloud Considerations

- Are our cloud services compliant with contract guidelines?
- Can I eliminate redundant use of cloud services and optimize cost and performance based on business needs?
- Can I get visibility into cloud risks that have an impact on my financial or operations reporting and build controls around them?

The CFO and COO of a $5-billion retail firm became most disturbed by hundreds of services that popped up in a financial report on cloud subscriptions. Costs were running amok, and the two suspected that not all of the services were sanctioned. Audit trails based on cloud discovery led to detailed information on usage patterns, possible unauthorized data transfers, personal usage, and shadow IT arrangements. The two executives then focused on remediation, culling of unwarranted or high-risk services, consolidation of redundant services, control policies, and enforcement processes. Related cloud service costs fell in line quickly thereafter.

The CHIEF AUDIT EXECUTIVE (CAE) or CHIEF COMPLIANCE OFFICER (CCO) ensures that the right control framework, monitoring, and assurance are in place for cloud activities. With cloud services right-sized to a manageable group, the CAE or CCO can impose the right controls on the organization's cloud use. By anticipating cloud service trends, regulatory compliance directions, and business forecasts, a company can build in the necessary controls on future cloud services rather than having to bolt them on later.



The Chief Financial Officer (or the Chief Operating Officer) will have an interest in moving unsanctioned cloud operations into sanctioned ones and creating more efficient cloud use.

The CCO at a large technology corporation weighed whether a new financial module being added to a cloud platform service should be held within scope or to what extent employees and processes using the module and the service should be tested. Cloud service discovery would identify the users who subscribed to the service, their usage patterns, their authority to change business rules, and the availability of easy-to-use logs for access to factual information and user behavior patterns. Discovery also would reveal how much data users uploaded, downloaded, and accessed. Of thousands who had access to the system, only a hundred or so were actually authorized to change system or business parameters. Additional data showed there was potential for further reducing the number authorized to execute system or business changes with little impact on business processes because those users used the system only infrequently. The detailed cloud-service-usage trails that discovery found also enabled evidence-based assessment of foreign exchange and revenue recognition impacts for Sarbanes-Oxley reporting.[2]

2 PwC recently published a white paper entitled A guide to cloud audits, which examines balancing risk and reward in the cloud: http://www.pwc.com/en_US/us/risk-assurance-services/publications/assets/internal-cloud-audit-risk-guide.pdf.

All BUSINESS LINE EXECUTIVES should reinforce cloud service guidelines and promote platforms for adding new cloud services. Executives across the C-suite can now apply their new cloud policies and guidelines as their organizations bring on new cloud business partners. And those partners that meet the guidelines can potentially get their services onboarded faster and more cheaply as executives effectively and transparently fast-track the adoption of qualified cloud services to drive business innovation.

With cloud services right-sized to a manageable group, the CAE or CCO can impose the right controls on the organization's cloud use.

CAE/CCO/CLO
Key Cloud Considerations

» How do I comply with regulatory requirements?

» How do I assess whether cloud services are and remain within my audit scope?

» Do I need to deploy continuous and automated auditing capabilities for selected services?

BUSINESS EXECS

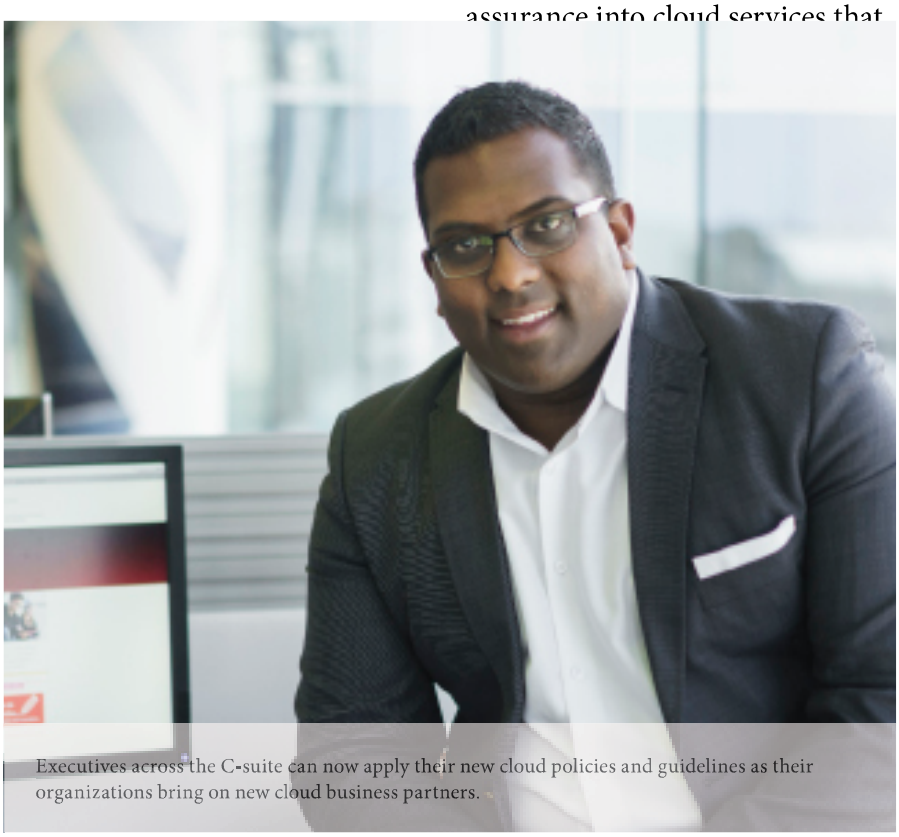
Key cloud considerations

- Am I promoting the right cloud services that offer me the best time to market and effectively connect my business with my customers?
- How do I encourage my staff to work closely with IT in onboarding cloud services sustaining the enterprise's security, data privacy and compliance objectives?
- Do I have a good sense of progress in terms of best practices and the operations metrics of how securely my organization is using cloud services?

A CMO and a vice president/general manager in a manufacturing-sector company considering a certain new cloud service vendor for managing customer service calls with customer relationship management tools wanted to fast-track the qualification and adoption of that particular service provider. Previously, the company had crafted cloud service adoption guidelines covering performance, security, privacy, operations, and compliance as a collaborative venture. It was decided that members of the same team could be tapped to assess the vendor under consideration against the adoption guidelines. Not only did the process get fast-tracked, but it also provided a frame of reference for conversations with the vendor about some missing functional elements. For instance, the vendor provided the company direct access to user logs even before the function was generally available, thus meeting an important audit and compliance criterion as well as company cloud service guidelines.

The journey to cloud risk assurance maturity

A lifecycle approach to cloud risk assurance combines the benefit of streamlined cloud services with risk assurance that's built alongside cloud activities as they get planned and implemented—not applied in a scramble later as bolted-on afterthoughts. The lifecycle approach builds the risk assurance into cloud services that



Executives across the C-suite can now apply their new cloud policies and guidelines as their organizations bring on new cloud business partners.

Achieving cloud security, and through it trust, takes time.

more effectively to meet strategic goals and promote innovation.

The cloud risk assurance effort covers such areas as security, privacy, data compliance, regulation, best practices, and industry standards to manage and decrease risk in cloud services. That effort—achieving cloud security and through it, trust—takes time. It's a journey, though each step on that journey brings benefits.

In addition to time, the process requires commitment by the entire C-suite; but the rewards come—in the form of trustworthy cloud services functioning in a way that fits the nature and strategy of the business.

The lifecycle approach builds the risk assurance in cloud operations that is essential to using cloud services more effectively to meet strategic goals and promote innovation.

www.pwc.com

To have a deeper conversation about how this subject may affect your business, please contact:

Piotr Urban, Partner
Poland Risk Assurance Leader
+48 502 18 4157
piotr.urban@pl.pwc.com

Rafał Jaczyński, Director
Cyber Security Consulting Leader
+48 519 50 7122
rafal.jaczynski@pl.pwc.com

Patryk Gęborys, Manager
Cyber Security Consulting
+48 519 50 6760
patryk.geborys@pl.pwc.com

Jacek Masny, Senior Manager
IT Risk Assurance
+48 502 18 4640
jacek.masny@pl.pwc.com