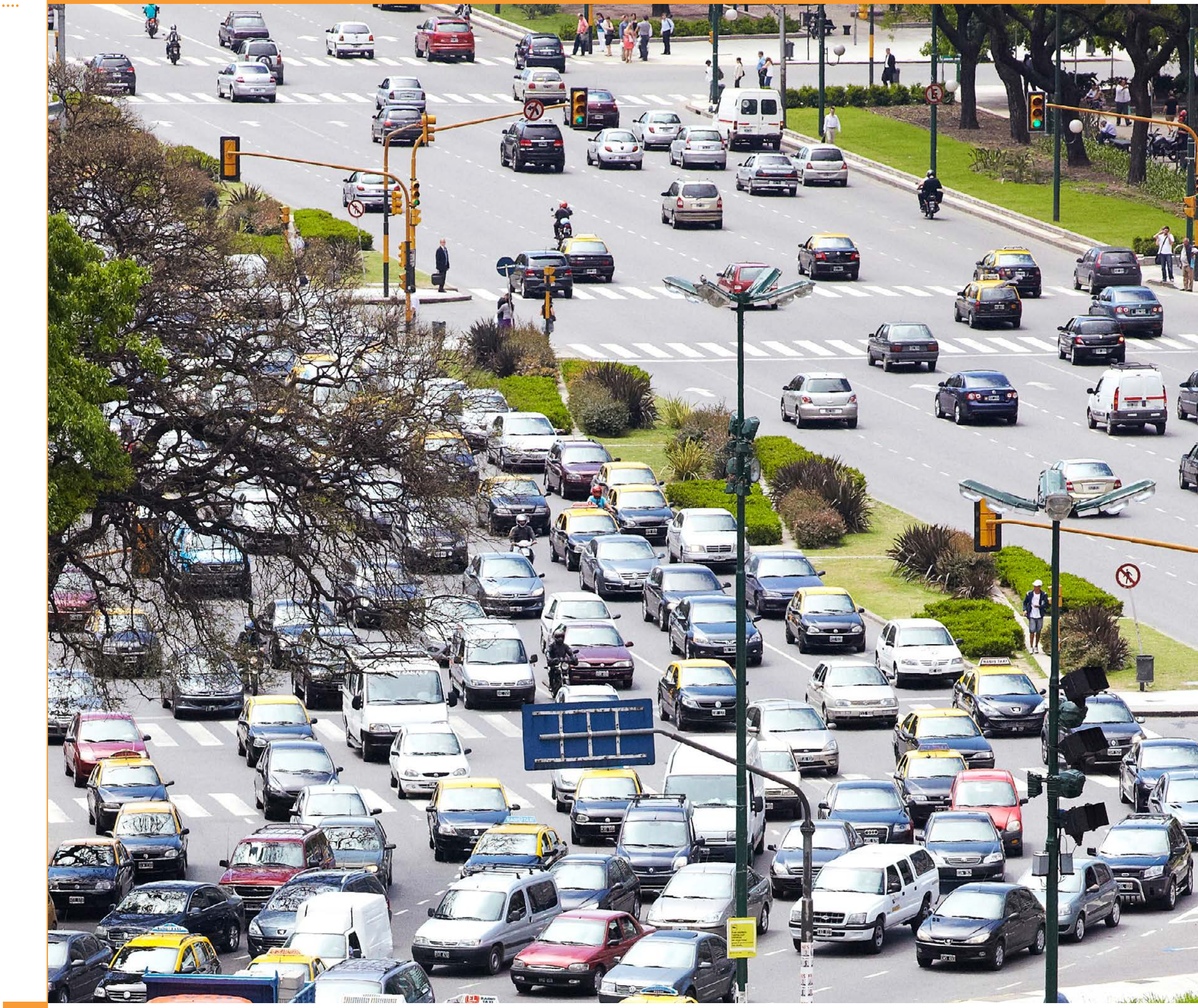
Managing the Shadow Cloud

Integrating cloud governance into your existing compliance program

August 2014



Shadow IT is not a new concept and organizations are well aware of the risks associated with unauthorized IT activity.

From shadow IT to shadow cloud

The gap between the business and IT is widening. With ever increasing pressure to perform, business units, frustrated by rigid organizational structures, are circumventing the CIO organization to get their own IT solutions. This is known as “shadow IT.” Shadow IT is not a new concept, but its recent increase has been dramatic. The culture of consumerization within the enterprise– having what you want, when you want it, the way you want it, and at the price you want it—coupled with aging technologies and outdated IT models, has propelled cloud computing into favor with business units and individual users. Shadow cloud has now emerged as a trend in business organizations. What does this mean for business and IT organizations? The days of “big IT” are gone, but successful IT departments will be those that work with the business to solve the organization’s most important problems: “IT will move from a centralized authority to an advisor, broker, and orchestrator of business services.”

New shadow, new risks

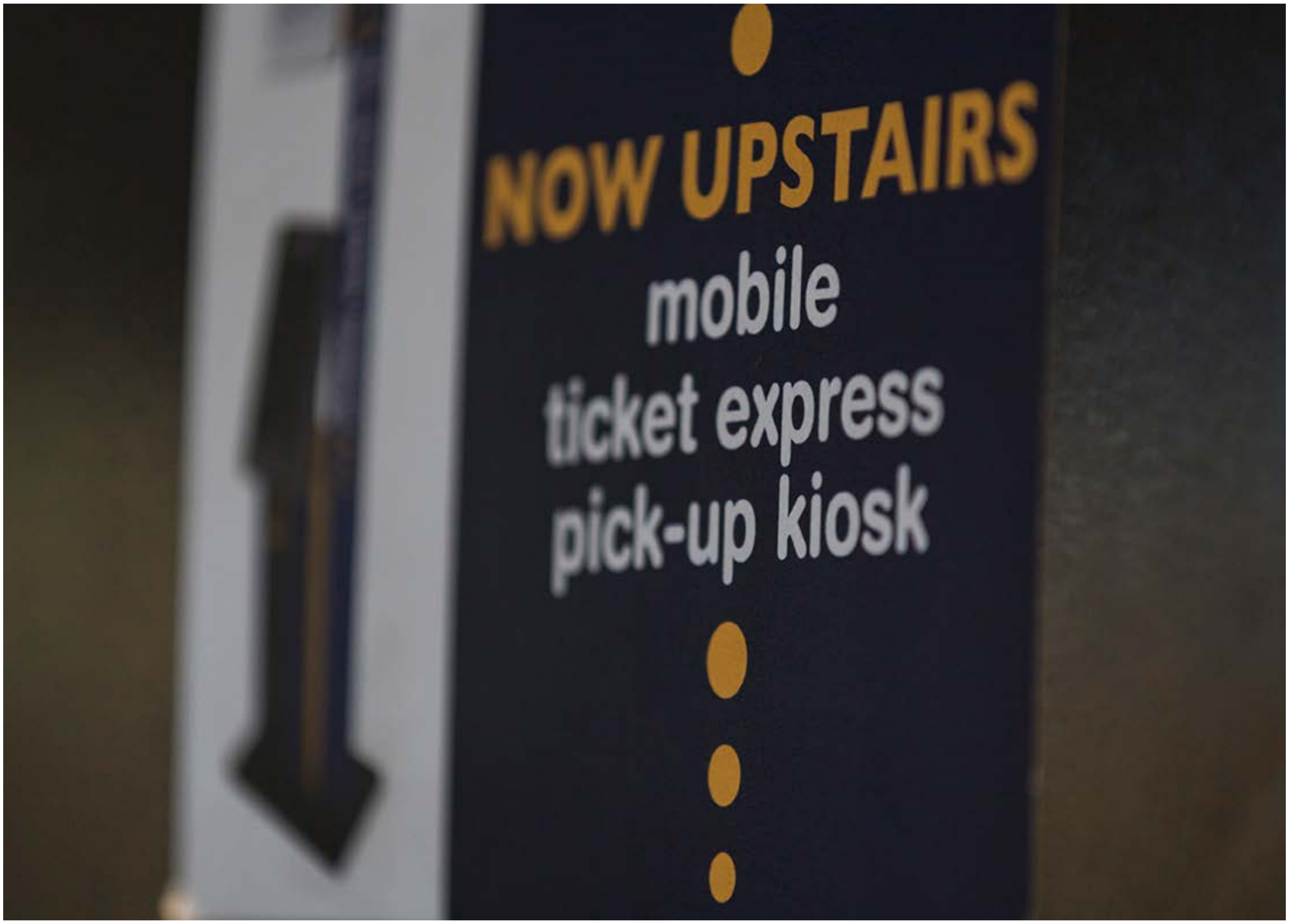
Shadow cloud arises from a business unit need for automated solutions and the existence of solutions that are within budget. On the surface, the concerns that companies face with shadow cloud are similar to shadow IT. Total cost of technology, when fully exposed, exceeds budgets. Process changes without the ability to update the solution lead to diminishing value, and a deterioration of knowledge about the solution results in failures in related processes.

The difference is that the risks associated with shadow IT were largely confined to individual computers running the solution to support discrete day-to-day activities. While rampant in some organizations, the impact was limited to the ‘inside walls’ of the company. Contrast that with shadow cloud. Automated solutions consumed from the internet process transactions and carry company information through a potentially intricate network of internal and external systems. No longer is the impact contained to the desktop or workspace of the individual user, rather one or more third parties are now in the loop. Multiply that by 10, 20, 100 different solutions that are procured across the enterprise under the guise that they are cheaper, faster, and more agile solutions to business issues. Suddenly, shadow cloud is a potentially pervasive gateway to new and unknown risks, spiraling growth of operating costs, and potential increase in redundancies.

If left ungoverned, such decentralized, unknown, and unmonitored activity presents a significant risk to any enterprise, particularly those companies operating in highly regulated sectors. These risks include issues with data security, transaction integrity, business continuity, and regulatory compliance, all of which are often exacerbated by the presence of third-party vendors. Yet cloud computing is becoming the new normal and as with shadow IT, is bringing innovation to the enterprise.

Executives have begun to realize that shadow cloud activity cannot be ignored, but with the proliferation of cloud usage across many large organizations, propelled by drastically decreased budget during the recent recession, a practical solution seems out of reach. Also, new and innovative cloud-based solutions are entering the market at a rapid pace as venture capital and capital market investors focus funding decisions toward cloud computing. This will further fuel the rate of adoption of cloud computing in the enterprise.

The world of computing has changed, and management must acknowledge that there is no going back to the days of traditional command and control IT. At the same time, realizing the benefits of the cloud with more confidence about the risk/rewards depends on knowing how to prudently say “yes” to the cloud.



The world of computing has changed, and management must acknowledge that there is no going back to the days of traditional command and control IT.

Ten steps to manage the clouds our employees use

Organizations must find ways to discover, analyze, and actively monitor new and existing cloud solutions that are entering the corporate environment. However, it is critical that the solution doesn't become a barrier to the innovation that is often associated with shadow IT.

Consider building a collaborative atmosphere of mutual trust with verification, in which both business and IT embrace change. A change where the business engages with IT partners for solution insights and IT assumes a role of computing advisor and orchestrator. This approach could help a beleaguered department stretch its capacity while providing valuable guidance to users in the evaluation, contracting and management of cloud solution providers. It can also encourage business and IT leaders to apply a practical, repeatable approach that can turn the shadow cloud into the strategic cloud.

1 Align strategy

Align business strategy and organizational performance goals to a cloud adoption strategy. Elevate cloud consumption decisions to a higher level in the enterprise that is not based on economics alone.

2 Tackle business requirements

Work with departments across the enterprise to understand functional requirements, business processes, and architectures that make sense. Be sure to get cross-functional stakeholder acceptance along the way, or the next iteration may go underground again. Navigating the world of cloud solutions can be complex—IT can guide their user community to the best choice.

3 Comply with standards and regulations

All IT solutions, whether in or outside the enterprise, need to meet applicable legal, contractual, regulatory and sector-based standards. Third party cloud services can often pose a challenge in this respect, increasing the need for stringent attention to compliance with policies and regulations. Implementing intelligent vendor management practices may help to mitigate vendor risk and address the need for adherence to varied compliance requirements across multiple vendors. As you corral shadow cloud activities and bring them into the fold, enterprise-wide benefits of baseline standards for control and adherence to IT governance and security practices will likely follow.

4 Establish SLAs and contracts

When choosing solutions for sensitive data sets or business transactions, it's especially important to find providers willing to commit to service level agreements (SLAs) and other contract terms that meet your needs. These can be used to define rights and responsibilities surrounding such things as right-to-audit vs. third-party assurance, breach notification, security, and privacy. Having established SLA expectations can help you more quickly assess similar cloud solutions.

5 *Manage the lifecycle*

Organizations collect massive amounts of data and as with any other asset, data has a useful life and must be categorized and managed accordingly. With the rapid agility and user friendliness of the cloud comes a potential lack of rigor with respect to data governance and lifecycle management. IT has mastered these lessons and this knowledge should be used to manage the data lifecycle exposed to the cloud.

6 *Lock it down*

Cloud providers may be overwhelmed with the data and transaction security needs of an enterprise user. To ensure the security of your information, identify who needs access to applications and create and manage an access control list; update current procedures to ensure that new users are on-boarded with the right protocols and approvals; ensure that encryption rules are applied as data is being transferred from your company to a cloud provider; and ensure that key management at the provider is assigned and available to you if and when needed.

7 *Make it resilient*

If a department has come to rely on a shadow cloud solution, it's important to put plans in place for crisis and incident response, including continuity and recovery procedures, in the event of an outage at the cloud service provider or disruption in service due to financial insolvency of the cloud provider.

8 *Keep it on the radar*

Adopting cloud solutions isn't a 'one and done' event. Managing and monitoring cloud service providers is a key aspect of value generation and risk management. Consider monitoring capabilities and incident escalation processes that will give you real time insight into business case gaps or conflicts, security issues, and other service metrics.

9 *Support the operation*

Shadow cloud is inherently isolated, creating a new form of disconnected IT. Develop an IT architectural vision for the consumption of cloud services that will allow efficient access management and service interoperability to enable an 'integrated cloud' for your organization.

10 *Manage cloud solutions*

Depending on the level of cloud activity across the enterprise, and the number of cloud providers involved, service orchestration may help improve benefits realization by enabling a more integrated set of IT processes across a varied set of cloud solutions. Leverage the IT architectural view to establish cloud administration procedures that use leading technology solutions to help automate monitoring and management responsibilities.

Successfully bringing cloud activity out of the shadows

Discovering and managing shadow cloud activities can be a daunting task. Many companies use the following model to successfully discover, assess, and sustain shadow cloud activity in their company. The key success factor is to embed cloud adoption into existing strategies, operational and governance processes, rather than creating a new and siloed process.

Discover

Given the large number of cloud services available, successful companies use a combination of automated and manual discovery methods to identify where the cloud is being used across their organization. In some cases, more than quadruple the number of shadow cloud providers have been found than was originally estimated. Automated methods are more robust and accurate, especially for large or complex organizations.

Assess

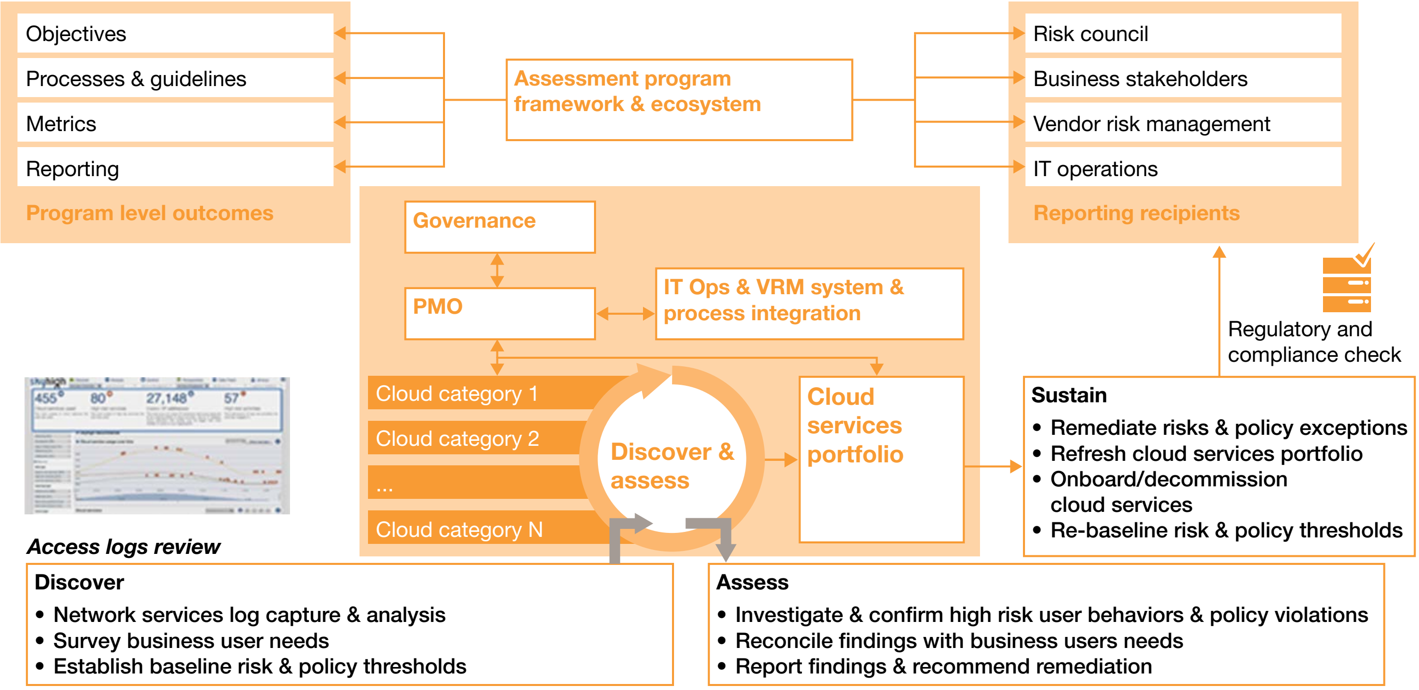
Once all shadow cloud activity has been uncovered, the next step is to categorize it and create a cloud services portfolio. Categorization can vary, but firms often choose to group cloud providers by level of risk to the firm and sanctioned level of access:

- Cloud providers that should be banned or restricted
- Cloud providers that have significant usage throughout the organization—a solution should be found that allows continued use, but that does not pose a risk to the firm
- Cloud providers that are known and sanctioned

Sustain

It is important to continually manage the cloud services portfolio as needs and issues are constantly changing. In companies where this has been done successfully, they have embedded the process within their existing risk framework. This shows a commitment and understanding that shadow cloud activity is the new normal and must be fully integrated into business operations.

Integrating cloud governance into existing compliance programs



Objectives

Processes & guidelines

Metrics

Reporting

Program level outcomes

Assessment program framework & ecosystem

Risk council

Business stakeholders

Vendor risk management

IT operations

Reporting recipients

Governance

PMO

IT Ops & VRM system & process integration

Cloud category 1

Cloud category 2

...

Cloud category N

Discover & assess

Cloud services portfolio

Regulatory and compliance check

Sustain

- Remediate risks & policy exceptions
- Refresh cloud services portfolio
- Onboard/decommission cloud services
- Re-baseline risk & policy thresholds

Access logs review

Discover

- Network services log capture & analysis
- Survey business user needs
- Establish baseline risk & policy thresholds

Assess

- Investigate & confirm high risk user behaviors & policy violations
- Reconcile findings with business users needs
- Report findings & recommend remediation

What's next?

The consumer culture driving IT consumption is a modern enterprise reality that is here to stay. With the burgeoning popularity of cloud providers, the risk unsanctioned IT presents grows exponentially. This risk should not be overlooked or underestimated.

Organizations willing to work with their business units, individuals, and cloud providers to better understand the levels of activity, risks and benefits, will ultimately gain from their efforts. As they work through a logical process and approach, and build a sustainable model, they will be better positioned to implement agile, workable solutions that adhere to recognized standards and controls both on and off the corporate campus.

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

Michael Pearl
Technology Consulting Leader and
Global Cloud Computing Leader
(415) 387-8133
michael.pearl@us.pwc.com

Shawn Panson
US Emerging Services Leader
(973) 236-5677
shawn.panson@us.pwc.com

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

Eric Tan
Cloud Assurance Director
(408) 817-7986
eric.tan@us.pwc.com

www.pwc.com