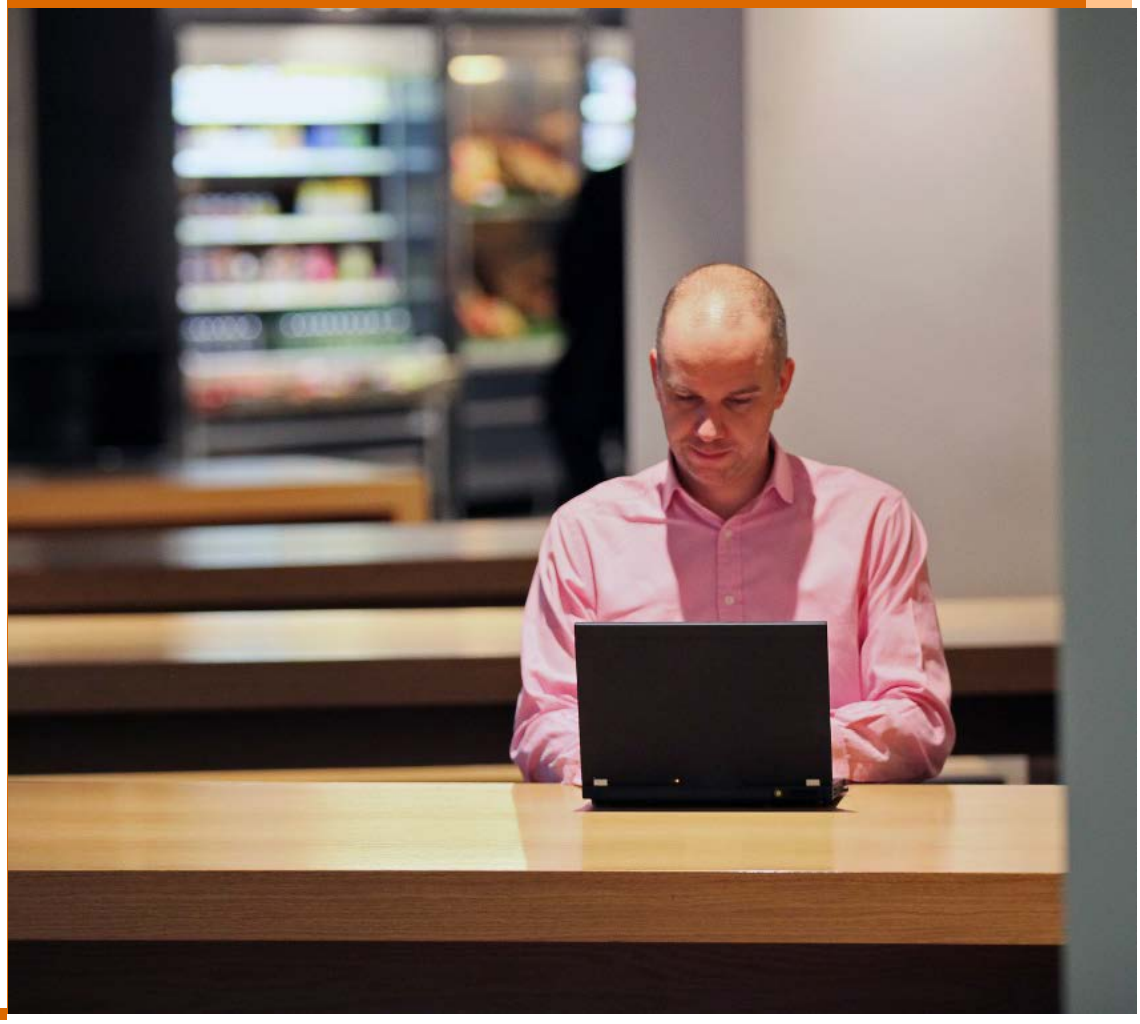
Managing the Shadow Cloud

Perspectives from Australia and New Zealand

June 2015



pwc

skyhigh

Shadow IT is not a new concept and organisations are well aware of the traditional risks associated with unauthorised IT activity.

From shadow IT to shadow cloud

The gap between the business and the traditional IT department is widening. With ever increasing pressure to perform, business units, frustrated by rigid organisational structures, are circumventing the CIO organisation to achieve their own IT outcomes. This is known as "shadow IT." Shadow IT is not a new concept, IT departments have despaired for many years at users and business groups who download and install their own software to get the job done. The recent explosion in Shadow IT though has been dramatic. The culture of consumerisation 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the enterprise–having what you want, when you want it, the way you want it, and at the price you want it—coupled with outdated technologies and IT models, has accelerated the adoption of cloud computing by business units and individual users. Shadow Cloud, the unsanctioned and uncontrolled use of cloud services, has now emerged as today's equivalent of the Shadow IT problem creating both risks and opportunities for business.

What does this mean for business and IT organisations? The days of big IT are gone, but successful IT departments will be those that work with the business to solve the organisation's most important problems. IT therefore must move from a centralised authority to an advisor, broker, and orchestrator of business services.

New shadow, new risks

Shadow Cloud has arisen from the business unit's need for technology platforms which help them achieve their business goals, drive a deeper user experience and which create competitive advantage. 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 the potential deterioration of the control environment.

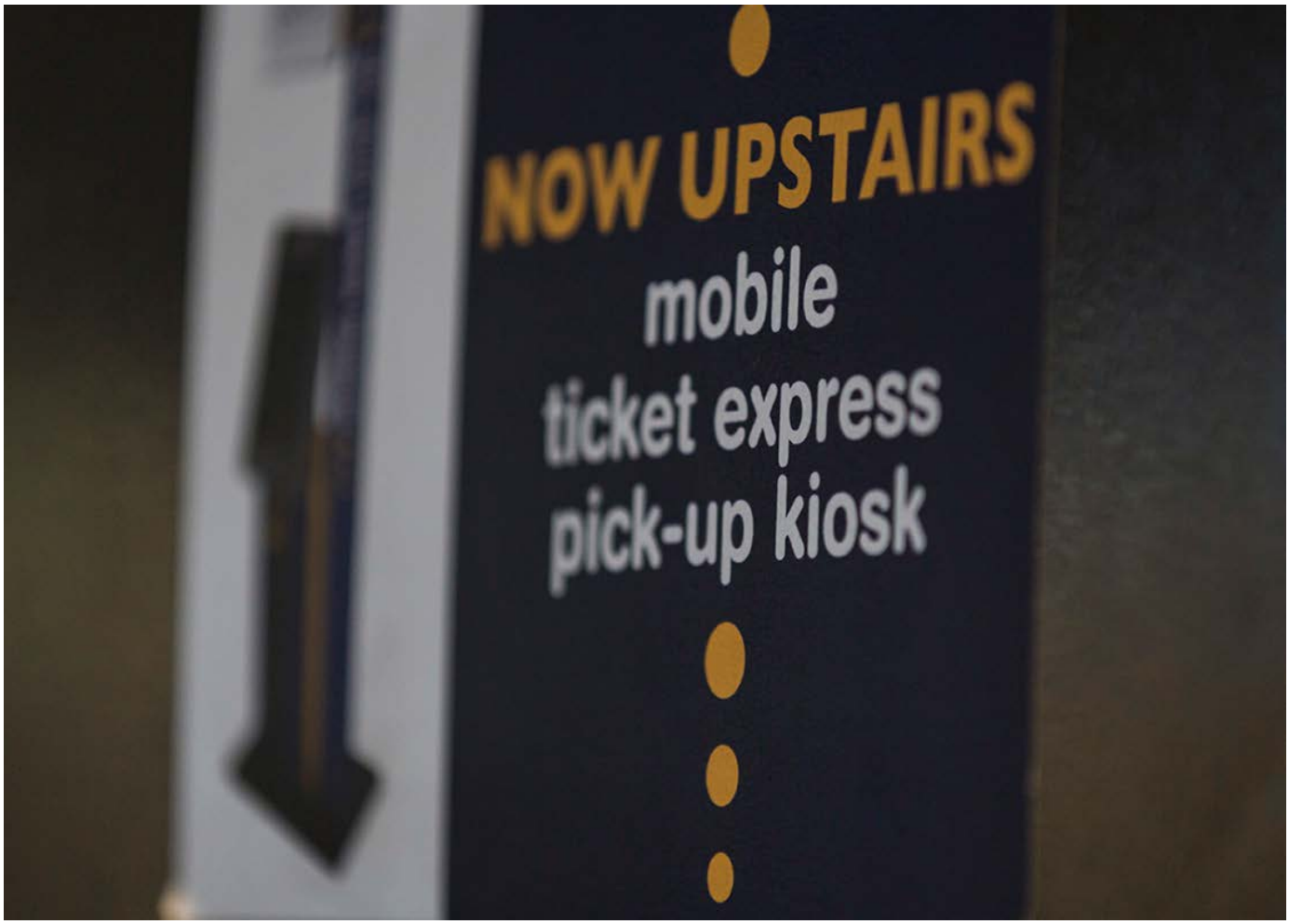
The difference is that the risks associated with shadow IT were largely confined to individual computers running a solution to support discrete day-to-day activities. While rampant in some organisations, the impact was limited to within the traditional perimeter of the company. Contrast that with Shadow Cloud. Services 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. In Cloud computing the traditional perimeter is dissolved and company information assets are now pushed outside historical

geographic boundaries to services delivered potentially from anywhere. Multiply that by 10, 20, 100 different services 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 a potential increase in redundancies.

If left ungoverned, such decentralised, 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 happened with shadow IT, it is bringing innovation, speed and efficiency to the enterprise.

Executives have begun to realise that Shadow Cloud activity cannot be ignored, but with the proliferation of cloud usage across many large organisations, propelled by drastically decreased budgets during the most 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, realising 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.

Australia and New Zealand lead cloud adoption internationally but at what cost?

From our research with the global PwC network and the major cloud vendors we have formed the view that Australia and New Zealand are leading cloud adoption globally. Through this research we note that the key driver for this level of adoption has been to improve agility to minimise the time to market for new products and solution.

With this early adoption and the level of innovation being driven through these platforms we are increasingly seeing users consuming unsanctioned or Shadow Cloud services. It is our view that this unsanctioned cloud usage is largely due to outdated governance and risk frameworks and a lack of skilled personnel in the cloud market.

Through PwC's alliance with Skyhigh Networks we have delivered a number of cloud discovery (cDiscovery™) assessments across Australia and New Zealand. These assessments involve the analysis of our client's Internet traffic and provide a data driven view of the current state of Shadow Cloud in our market. From the outset, it has been apparent, with every client assessment, that the scope of the cloud usage has been far greater than anticipated, with an average of 670 per organisation.

We have also discovered a series of fascinating insights into the distribution of the 670 services per organisation. Cloud storage is a category that we believe poses a significant and unique set of compliance, security, insider threat and loss of collaboration capability risks. We find on average organisations using 28 services in this category alone.

We have also discovered some stark figures with respect to organisations attempts to effectively control cloud usage. From this data, we can only conclude that organisations are not aware of the shadow cloud challenge and are currently not effectively equipped to address it.

Average number of cloud services per A/NZ organisation

Average number of cloud services per employee

85%

Percentage of high risk services not being blocked

Average number of high risk cloud services per organisation

28

Average number of cloud storage services per organisation

0%

The percentage of organisations who's cloud use matched their policy

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 organisation. 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 organisations.

Assess

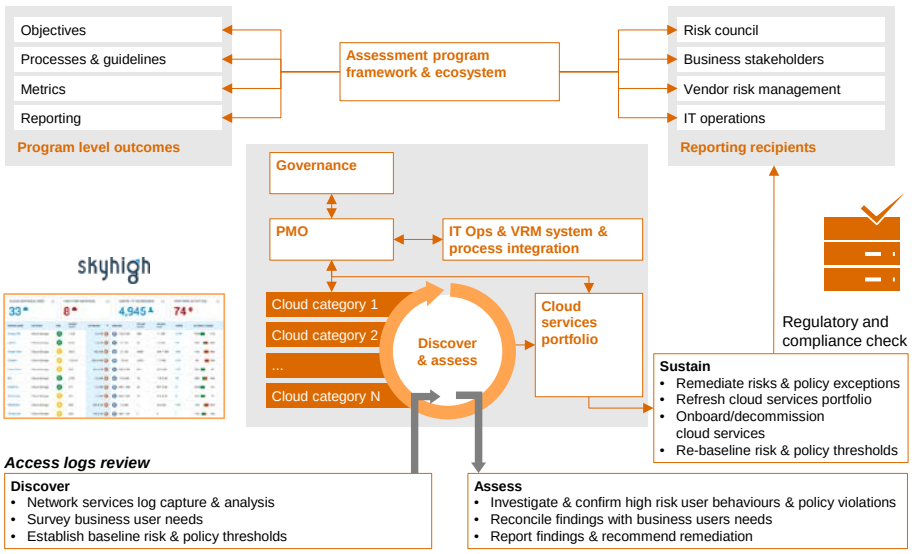
Once all shadow cloud activity has been uncovered, the next step is to categorise it and create a cloud services portfolio. Categorisation can vary, but firms often choose to group cloud providers by level of risk to the firm and sanctioned level of access:

- Cloud providers that should be banned or restricted
- Cloud providers that have significant usage throughout the organisation— 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



Ten steps to manage the clouds our employees use

Organisations must find ways to discover, analyse, 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 ***Discover and Assess***

As noted in the previous section, the elasticity of cloud services and the ease of their deployment makes it is very difficult to know all of your enterprise cloud services, how they are being used and by whom. In order to manage the risks associated with these services you must conduct a systematic discovery to build a complete inventory of services so that you can clearly assess your current risk profile.

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***

Organisations collect massive amounts of data and as with any other asset, data has a useful life and must be categorised 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 maybe 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 organisation.

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 realisation 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.

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.

Organisations 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.

Research between Skyhigh Networks and the Cloud Security Alliance has shown some initial promise from adopting this approach, namely a 97% reduction in data sent to high risk cloud services, an 83% increase in the use of low risk cloud services and a 17% average improvement to the IT satisfaction index.

As organisations 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 recognised standards and controls both within and outside the traditional technology perimeter.

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

Australia

Peter Quigley
Sydney
+61 (2) 8266 3917
peter.j.quigley@au.pwc.com

John Taylor
Melbourne
+61 (3) 8603 1021
john.g.taylor@au.pwc.com

Adam Wood
Canberra
+61 (2) 6271 3666
adam.wood@au.pwc.com

Leon Fouche
Brisbane
+61 (7) 3257 8696
leon.fouche@au.pwc.com

Ryan Menezes
Perth
+61 (8) 9238 3045
ryan.menezes@au.pwc.com

New Zealand

Steve McCabe
Wellington
+64 (4) 462 7050
steve.c.mccabe@nz.pwc.com

Adrian van Hest
Wellington
+64 4 462 7109
adrian.p.van.hest@nz.pwc.com

www.pwc.com

.