www.pwc.com

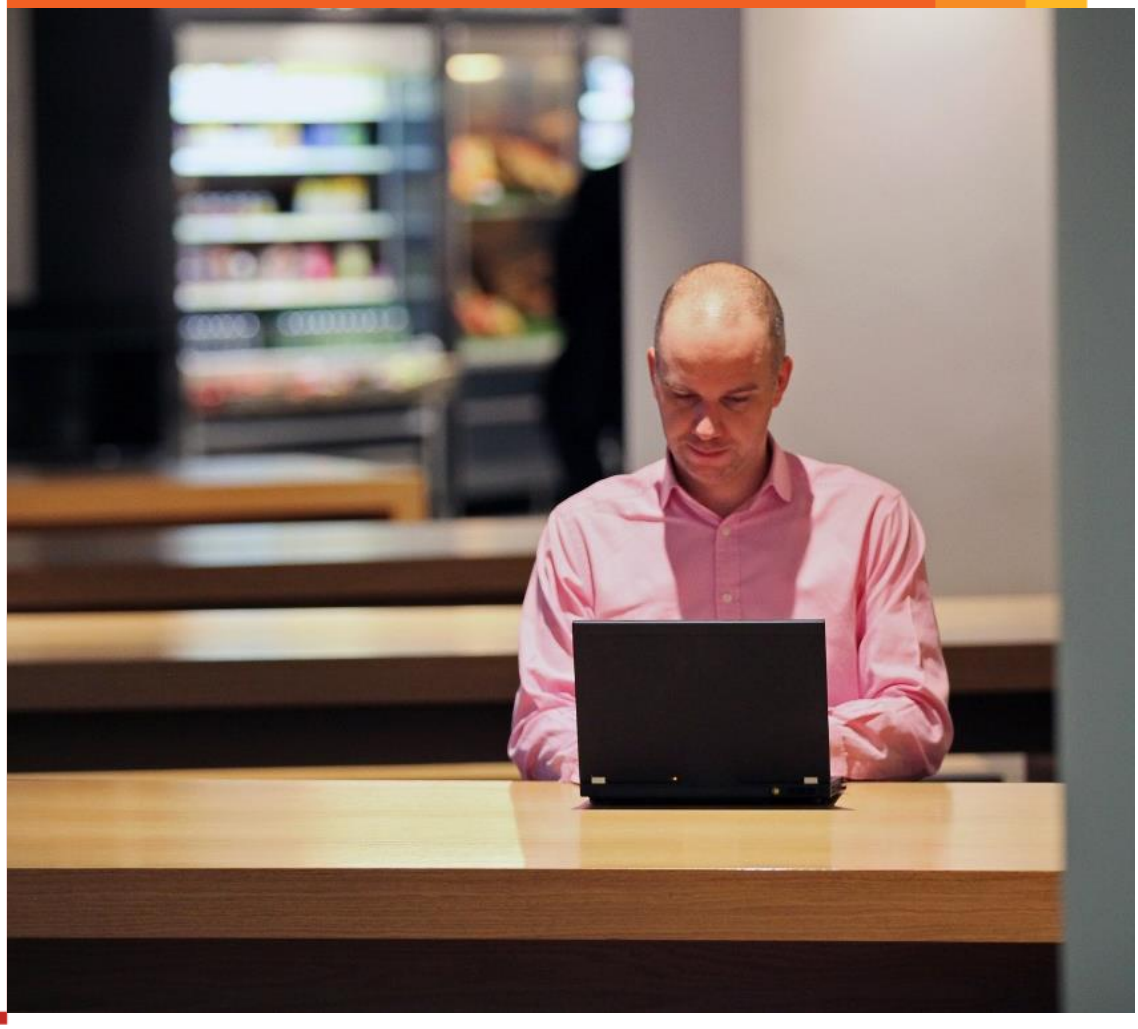
Managing the Shadow Cloud

Integrating cloud governance into European Compliance programs

November 2015

in association with

skyhigh



pwc

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

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.

From shadow IT to shadow cloud

The gap between business units and IT departments is widening. Increasingly, performance pressures and frustrations at rigid organisations can trigger business units to circumvent IT to procure their own solutions. Although not a new phenomenon, the explosion in such 'Shadow IT' has been dramatic. Consumerisation within the enterprise – having what you want, when and how you want it, at the price you want to pay – coupled with outdated technologies and IT models, has accelerated the adoption of cloud solutions by business units and individual users. Shadow Cloud – the unsanctioned and uncontrolled use of cloud services – has emerged as today's equivalent of the Shadow IT problem creating both risks and opportunities for business.

With the days of big IT all but gone, successful IT departments must realise that they are an investment in making the business work, and therefore collaborate with the business to solve the big problems: IT 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 need for cheaper, faster and more agile solutions to achieve business goals, engage users & clients and exploit new opportunities to create competitive advantage. Ostensibly, the concerns on Shadow Cloud are similar to those of 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 major difference is that risks associated with Shadow IT were largely confined to the organisation's traditional IT perimeter. Contrast that with Shadow Cloud, where services consumed from the Internet process company information across a network of internal and external systems. The impact is no longer confined to an individual user: the traditional IT perimeter is dissolved and information assets are now pushed to services delivered potentially from anywhere. Multiply that by 10, 20, 100 different services that are used across the enterprise and suddenly Shadow Cloud is a potentially pervasive gateway to new and unknown risks, particularly Cyber providing back-door access to user organisations, spiralling costs and a multitude of redundancies.

Left ungoverned, such decentralised, unknown and unmonitored activities present significant risks to any enterprise, particularly those operating in highly regulated sectors. These risks include data loss and security, privacy & integrity, business continuity, e-Risk 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.

Once aware of its existence, executives must quickly realise that Shadow Cloud activity cannot be ignored because the rate of enterprise cloud computing adoption is only likely to accelerate. The proliferation of cloud usage across many organisations – often adopted in response to drastically reduced budgets during the recession – is likely to increase as new and innovative cloud-based solutions enter the market at a rapid pace in response to venture capital and capital market investors focusing funding decisions toward cloud computing.

The days of traditional 'command and control' IT are over. To realise the benefits of the cloud with confidence over the risk / rewards, management must know how to prudently say "yes" to the cloud.

Cloud adoption in Europe is growing fast, and so are the risks

From our research with the global PwC network and the major cloud vendors we have seen that European adoption is rapid. This research shows that the key driver is 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, poor awareness of an organisation's risk appetite and tolerance levels – particularly relating to unapproved software – and a lack of skilled expertise on cloud.

The European Union (EU) has taken a lead in data privacy since 1995 and is strengthening the existing laws with expectations of a new Data Protection Regulation being agreed upon by the end of 2015.

One of the areas of the existing EU Directive and the new EU Regulation covers where data on European individuals can be transferred. A recent study conducted by Skyhigh Networks identified that European companies are using many cloud services that do not meet data residency requirements. Only 14.3% of the cloud services in use are hosted within the EU and 64.9% should not hold EU data. Understanding the potential impact is vitally important: an organisation that breaches the Regulation by using a cloud service provider that breaches the rules could be fined up to 5% of its global revenues.

Through PwC's alliance with Skyhigh Networks, we have delivered a number of cloud discovery assessments across Europe. These have highlighted that the extent of cloud usage is frequently far greater than anticipated: with an average of 987 cloud services in use per organisation, there is a massive potential for breaching the EU Regulation.

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 organisation **987**

23 ***Average number of cloud services per employee***

65%

Percentage of services unsafe for European Union personal data

Use of cloud services during the weekend **13**

28 ***Average number of cloud storage services per organisation***

0% ***The percentage of organisations whose 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 ten times 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

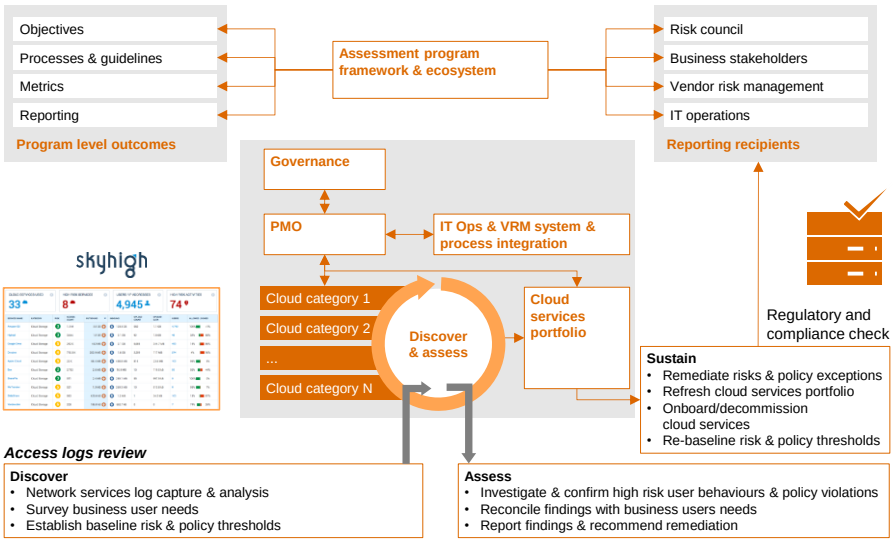
Once all shadow cloud activity has been uncovered, the next step is to categorise it and create a cloud services portfolio. Categorisation can vary, but firms often choose to group cloud providers by level of risk to the firm and sanctioned level of access:

- 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 together with clear reporting metrics particularly over usage, data transmissions and insider threat monitoring. 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



Six steps to manage the clouds that employees use

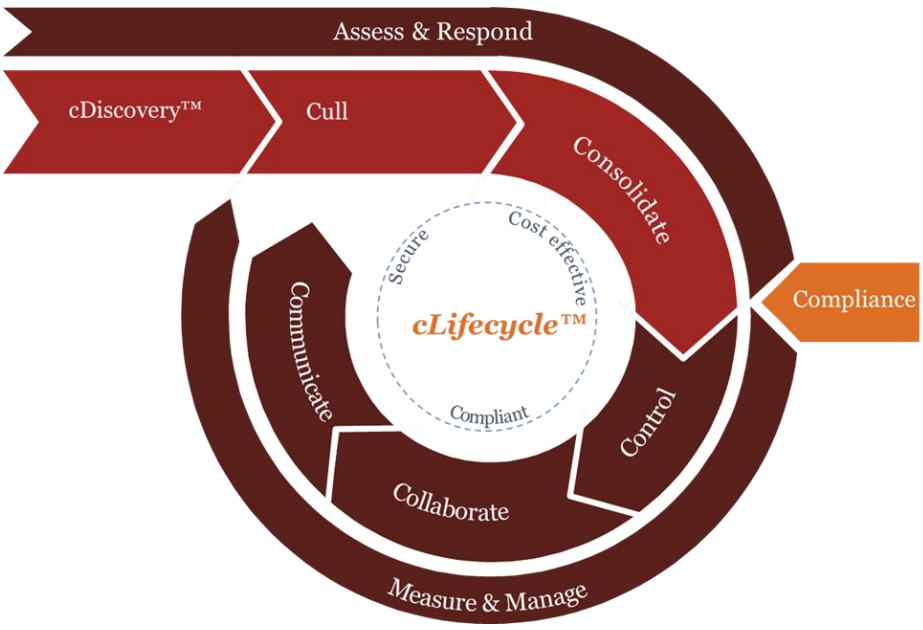
Organisations must find ways to discover, analyse, and actively monitor new and existing cloud solutions that are entering the corporate environment. However, it is critical that the solution doesn't become a barrier to the innovation that is often associated with shadow IT.

Organisations should 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 will help a beleaguered department stretch its capacity while providing valuable guidance to users in the evaluation, contracting and management of cloud solution providers. This will encourage business and IT leaders to apply a practical, repeatable approach that can turn the shadow cloud into a strategic cloud that is clearly aligned to broader IT and business strategy goals and objectives.

1. **cDiscovery™**: Start with discovering the current cloud services used in the enterprise.
2. **Cull**: Block and eliminate high risk services.
3. **Consolidate**: Move from unsanctioned cloud service providers to sanctioned ones.

   At this point reassess the current level of legal and regulatory compliance with regards to enterprise data in the cloud, and initiate a compliance project to update the existing governance structure to include management of the cloud specific risks.

PwC's Cloud Management Lifecycle



4. **Control**: Exert the fullest control on scoped cloud services.
5. **Collaborate**: Build guidelines and a governance structure for managing existing / adding new cloud services.
6. **Communicate**: Establish fact-based communications to internal and external stakeholders.

What's next?

The consumer culture driving IT consumption is a modern enterprise reality which is here to stay. With the burgeoning popularity of cloud services, the risks presented by unsanctioned IT grow exponentially. These risks should not be overlooked or underestimated.

Organisations that are 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 to build a sustainable model, they will be better positioned to implement agile, workable solutions that adhere to recognised standards and controls – both within and beyond the traditional technology perimeter.

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

Belgium

Steven Ackx
Ghent
+32 9 268 81 86
steven.ackx@be.pwc.com

Chris Kappler
Ghent
+32 2 710 41 76
chris.kappler@be.pwc.com

Finland

Timo Takalo
Helsinki
+358 (0) 50 383 7786
timo.takalo@fi.pwc.com

Germany

Markus Vehlow
Frankfurt
+49 160 7139416
markus.vehlow@de.pwc.com

Netherlands

Bram van Tiel
Amsterdam
+31 (0)88 792 53 88
bram.van.tiel@nl.pwc.com

Lolke Reinstra
Amsterdam
+31 (0)88 792 50 90
lolke.reinstra@nl.pwc.com

Sweden

Martin Allen
Stockholm
+46 725 849380
martin.allen@se.pwc.com

United Kingdom

Pritesh Patel
London
+44 (0) 7711 194575
pritesh.patel@uk.pwc.com

Hakan Gokalp
London
+ 44 (0) 7810 751806
hakan.gokalp@uk.pwc.com

www.pwc.com