Emerging from the shadows

Why business ownership is the answer to managing the risk of Shadow IT

Shadow IT **might sound threatening to some people, as if it originates from a thrilling detective novel. In an organizational context, this term simply means IT applications and services that employees use to perform their daily activities and that are not approved or supported by the IT department. With recent developments where many people have to work from home, employees are reaching out to Shadow IT even more. Although these applications can be genuinely valuable and help employees with innovation, collaboration and productivity, they can also open the door to unwanted security and compliance risks. In this article, we take a look at the challenges presented by Shadow IT, and the methods to manage them, so that the risks do not outweigh the benefits.**

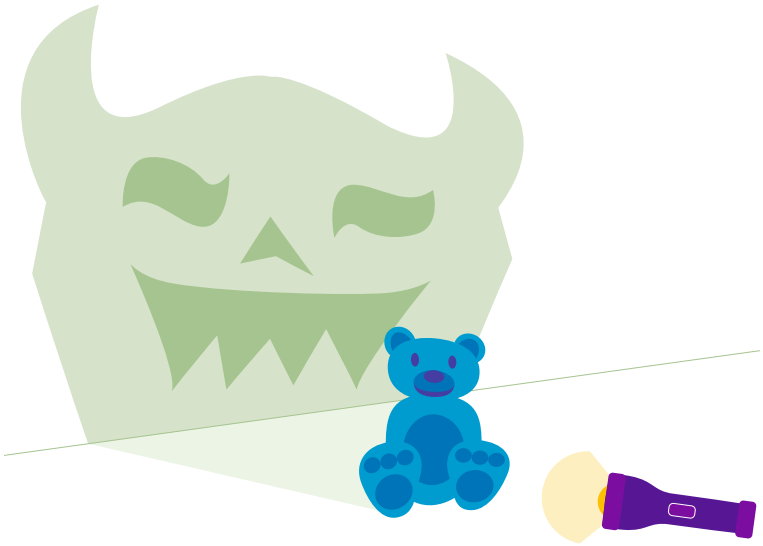
Olga Kulikova MSc
is Manager at KPMG Cyber.
kulikova.olga@kpmg.nl

Ramya Iyer MSc
is Senior Consultant at KPMG Cyber.
iyer.ramya@kpmg.nl

THE SHIFTING CHALLENGES OF SHADOW IT

As bandwidth and processing power have grown, software companies have invested heavily in cloud-based software and applications. Recent research ([Syma19]) suggests that companies largely underestimate the number of third-party applications being used in their organization – with the actual amount of apps in use being almost 4 times higher on average. Some of these applications have been immensely valuable, bringing about digital transformation by speeding up processes, saving costs, and helping people to innovate. They can also point to any software needs: for example, if its employees are signing up for a cloud-based resource management tool, it may show that the company's existing offerings are not up to the job. However, these applications may bring certain risks and challenges if not managed properly, as outlined below.

1. *Data leaks and data integrity issues*
   Data is the main factor to be considered when it comes to the use of unsanctioned or unknown applications to store or process enterprise data. When less secure applications are used, there's a high risk of potential confidential information falling into the wrong hands. Also, the usage of too many Shadow IT services with data stored across all of them does not benefit the organizational IT portfolio and reduces the value and integrity of data.
2. *Compliance and regulatory requirements*
   Legislations such as GDPR, or local regulations for data export, have raised the level of scrutiny and massively increased the penalties for data breaches, especially around personal data. Business or privacy-sensitive data may be transferred or stored in locations with different laws and regulations, possibly resulting in regulatory and non-compliance incidents. There is also a risk of not being compliant with software licensing or contracts if employees agree to the terms and conditions of certain software without understanding its implications or involving the right legal authority.
3. *Assurance and audit*
   In an ideal scenario, IT or risk departments could simply run regular audits to identify and either accredit or prohibit specific applications. Practically, it's an impossible task. It is not unusual for large organizations to run thousands of Shadow IT applications. Yet the IT and risk departments that are trying to reduce this amount, and understand the usage and associated risks, can only handle a few hundred applications per year at best.
4. *Ongoing and unknown costs*
   Shadow IT can be expensive, too. When businesses don't know which applications are already in use, they often end up using the wrong services, or overpaying for licenses and subscription costs. For instance, multiple departments could be using unsanctioned applications to perform their day to day activities. As the usage of these applications occurs under the radar, the organization cannot take advantage of competitive rates, assess security requirements, or request maintenance and support services directly from the application provider that would benefit them.
5. *Increased administrative burdens*
   Why can't corporate IT departments simply solve the problem by banning the use of these applications? They can, but doing so eliminates any productivity gains that the business may be getting, and probably damages employee engagement in the process. Worse still, employees may look for alternative tools that are not on the prohibited list, but may in fact be even riskier.



SOLUTION: CONVERTING SHADOW IT TO BUSINESS MANAGED IT

We propose the following way forward – to give business users ownership of Shadow IT risk and involve them in the risk management process, instead of leaving it entirely up to IT or risk departments. Applications and services that are known to an organization and have successfully passed the risk management process, are called Business Managed IT. According to [Gart16], Business Managed IT addresses the needs of both IT and the business in "selecting, acquiring, developing, integrating, deploying and managing information technology assets".

Research ([Harv19]) states that almost two-thirds of organizations (64%) allow Business Managed IT investment, and one in ten actively encourage it. They also found out that organizations that actively encourage Business Managed IT are much more likely to be significantly better than their competitors in a

number of areas, including customer experience, time to market for new products (52% more likely), and employee experience (38% more likely). [Forr18] noted that the majority of the digital risk management stakeholders are information security (50%), threat intelligence (26%) or IT (15%) and are encouraged engaging other teams that use the applications to set the Business Managed IT strategy.

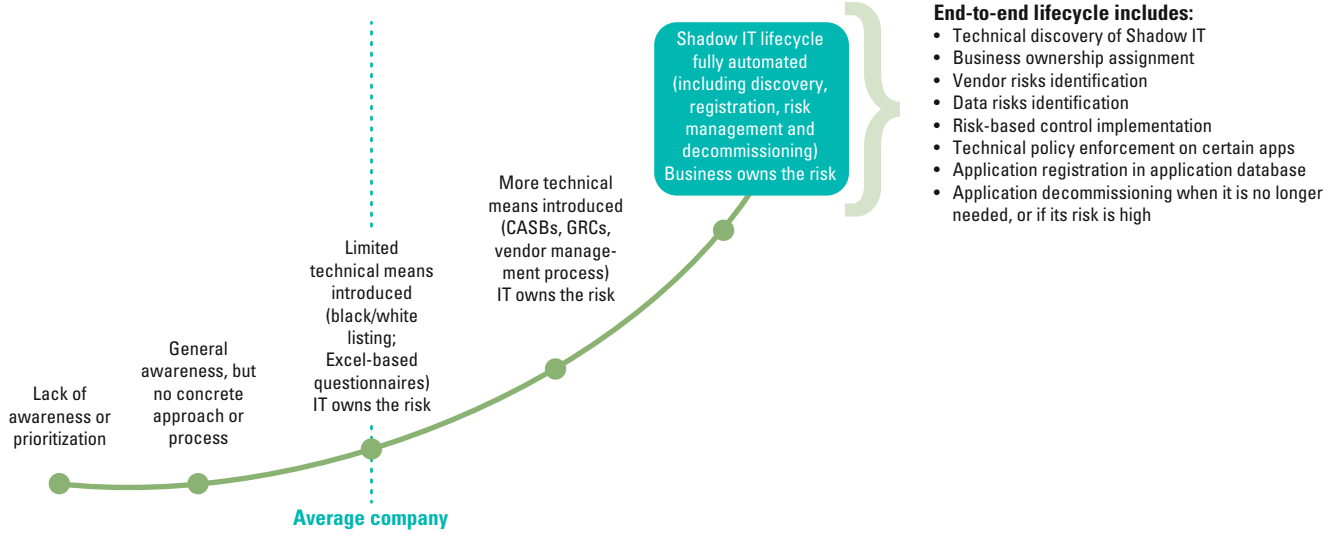
We see many organizations taking small steps towards Business Managed IT as a strategy within in the Netherlands and the EU. Companies are increasingly aware of Shadow IT and some of them are already busy discovering, filtering, registering, and risk assessing Shadow IT apps. According to [Kuli16], most of these activities are typically performed manually with some help of automation – typically for blacklisting or whitelisting the apps or running Shadow IT discovery with Cloud Access Security Brokers (CASBs). The actual Shadow IT registration and risk management processes are usually done manually by IT or risk departments using lengthy risk questionnaires. The result is low throughput, resulting in businesses often waiting months or even years before the applications and services they want get the right internal approval.

We believe the future proof model will be more sustainable when the business becomes the actual owner of Shadow IT apps, including the process of their registration, risk management, and risk mitigation. Actual risk questionnaires should be simplified to focus on what's really important in identifying actual risk and the required mitigating measures. This way, the business can try a new risk role while not being tech-savvy, and IT and risk departments can start focusing on cases where their involvement is really required – for example situations with high-risk apps, where a certain application is better to be run centrally by IT, and not owned by the business. For the lower risk scenarios, business ownership means that apps and services are available without long delays.

Give business users ownership of Shadow IT risks and involve them in the risk management process

Business Managed IT is a strategy and "mind-set", and the results can be achieved in multiple ways. We encourage organizations to follow what businesses are already doing in their daily work – digitization, automation, analysis – which in the case of Shadow IT risk management means automating the risk management processes with the help of dedicated software. As shown in the maturity graph in Figure 1, not all companies are at this stage – some are still heavily dependent on manual work to run the required processes.

Figure 1. Maturity of Shadow IT risk management.



SETTING THE GROUNDWORK FOR BUSINESS MANAGED IT

Business Managed IT is an attractive approach but getting the business involved in IT is a new paradigm and should be introduced with care. Implementation requires cultural change and proper communication. The following five steps can help organizations get started:

1. Define Shadow IT risk ownership by the business and discuss it at a senior level to ensure their support and buy-in.
2. Set a policy and target operating model for business ownership of Shadow IT, clearly specifying what such ownership means. How will the business work with IT? When will IT and/or the risk department get involved? What are the escalation chains in case there are any delays or uncertainties in risk management process?
3. Secure involvement of change and communications departments. Focus on increasing business awareness with regard to the upcoming changes. Involve people who are skilled at organizational change management rather than relying on IT or risk experts.
4. Tackle the Shadow IT monster one step at a time. First, initiate a pilot. Then, deploy the new model with one – ideally more mature – department or operating unit to learn lessons that can be applied during further rollout.
5. Monitor and adjust. Work closely with the business during the roll-out period. Questions and feedback from the business are good as it helps improve the approach – silence is a bad indicator.

An organization's journey

The organization: A global group of energy and petrochemicals companies with 86,000 employees in 70 countries.

The challenge: The organization required a significant improvement in their risk management practices around Shadow IT, driven by the vast amount of known Shadow IT applications, the larger unknown services, and audit findings around security and privacy of data stored in such services. At the start of the engagement, the organization didn't have polices or procedures that outlined how employees should use such applications and services, or how the IT and risk management teams could have insight into and control over this usage.

The approach:

1. Shadow IT policies and procedures were created and approved by senior IT and risk stakeholders.
2. Business ownership of Shadow IT apps was defined.
3. The responsibilities of IT and risk management departments changed to monitoring only, with their involvement required only for high risk cases.
4. Change & communication teams were established to enable the change across the organization. Multiple trainings, videos, train the trainer and other learning materials were created to educate business users about new ways of working.
5. Pilots and a hyper care period with handholding sessions were used to support any questions during the initial rollout.
6. The organizations used KPMG's SaaS software built on top of Microsoft Azure Cloud to run the newly established process for Shadow IT. The software, connected to the organization's application database, enabled the business to perform risk assessments of identified Shadow IT services, discover relevant risks, and automate the deployment and monitoring of controls. It also provided integrated risk insights to the IT and risk departments.

The value delivered:
Business users conducted over 4,000 risk assessments of Shadow IT applications in one year by completing a simple questionnaire. These assessments resulted in 1000 applications being decommissioned (due to the unacceptable risk exposure for the company, or applications deemed not anymore relevant) and specific controls being deployed based on risks identified through the assessments. Business users appreciated the central database of apps and associated risk ratings that was created as part of this process, which allowed users to look up available apps prior to purchasing anything extra. Businesses reached out more frequently to the IT and risk management departments with thoughtful questions, indicting their increased awareness and ownership of Shadow IT risks.

Business risk ownership and accountability adds an important layer of protection

VALUABLE BENEFITS BEYOND RISK MANAGEMENT

Effective risk management is even more challenging for large international enterprises in today's context of digital transformation and evolving regulation. Organizations should assess and utilize its risk appetite and, accordingly, allow the business to continue using applications if they are deemed low risk or if there are sufficient mitigating controls in place. When an application poses a high risk, then a decision whether to discontinue its usage or to invest in remediation should be made with involvement of IT or risk management teams.

Business risk ownership and accountability adds an important layer of protection against data breaches and immediately strengthens and facilitates compliance. More importantly, IT becomes an enabler, rather than a department that is viewed as blocking the progress.

To support business ownership of IT and applications, more mature organizations can use automated technologies such as CASBs and the KPMG DRP to automate most of the critical BMIT workflows, such as Shadow IT applications discovery, application portfolio management, organization-specific risk assessments, control implementation, and monitoring and reporting.

For organizations that are still in the beginning of their journey to risk mitigate Shadow IT, an immediate automation of Business Managed IT workflows might be a step too far. In such cases, it is important to start adopting the mind-set of business ownership of IT risk through improved and simplified risk policies as well as business enablement programs, as this is the very first step for long-term business enablement, security and privacy of critical organizational data.

References

[Forr18] The Forrester New Wave (2018). Digital Risk Protection, Q3 2018, 2.

[Gart16] Gartner (2016). Gartner's Top 10 Security Predictions. Retrieved from: https://www.gartner.com/smarterwithgartner/top-10-security-predictions-2016/

[Harv19] Harvey Nash / KPMG CIO Survey (2019). A Changing Perspective. Retrieved from: https://home.kpmg/xx/en/home/insights/2019/06/harvey-nash-kpmg-cio-survey-2019.html

[Kuli16] Kulikova, O (2016). Cloud access security monitoring: to broker or not to broker? Understanding CASBS. *Compact* 2016/3. Retrieved from: https://www.compact.nl/articles/cloud-access-security-monitoring-to-broker-or-not-to-broker/

[Syma19] Symantec (2019). Cloud Security Threat Report. Retrieved from: https://www.symantec.com/security-center/cloud-security-threat-report

About the authors

Olga Kulikova MSc is Manager at KPMG Cyber and Product Manager at Digital Risk Platform (DRP). She helps KPMG clients with their information risk management, cloud transformation, identity and access management (IAM) and IT assurance programs. Her passion is helping companies realize value in their large-scale transformation and innovation programs without introducing security and privacy risks. Olga is a Certified Cloud Security professional (CCSP) by (ISC)2.

Ramya Iyer MSc is Senior Consultant at KPMG Cyber. She has a background in Risk Management and has helped organizations in defining and improving their cyber strategy through cyber security assessments, identity and access management, data access governance, unstructured data management, and data protection initiatives.