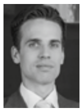
A Journey into the Clouds

How SaaS Adoption Changes the World of Contracting

Pieter de Meijer RE CISSP CISA and Olga Kulikova MSc CCSK

Software as a Service (SaaS) solutions have been around for years and organizations are starting to move on a larger scale to business software through the SaaS model. Based on a business case at one of the largest global organizations we provide insight into what the impact of adopting SaaS is on the procurement process. More specifically we will present an approach on how various functions can and should work together to ensure SaaS contracting is done in a compliant and secure manner.



P.R. de Meijer RE CISSP CISA
is a senior manager at KPMG.
demeijer.pieter@kpmg.nl

O. Kulikova MSc CCSK
is a senior consultant at KPMG.
kulikova.olga@kpmg.nl

The Old Days of Contracting IT Solutions No Longer Suffice

Once upon a time the world of IT contracting followed a clear process. A business analyst was assigned to identify the business needs and requirements and the IT department would function as a bridge between the business and IT vendors. IT vendors were more than pleased to build whatever was needed; the sky was the limit. The business was in a strong position to negotiate, often playing off the potential vendors against each other who were standing in line to win the project. Custom-made solutions or customized standard solutions where the standard. This approach to contracting also came with a price as custom solutions tend to be more expensive than standard solutions (assuming a solution is delivered to the business). Pricing of the solution seemed straightforward since during the contract phase the license fee was negotiated by the Procurement team and was agreed for a longer period. Scaling down the license fee, however, appeared to be more challenging as time went by.

Naturally, the above description is somewhat exaggerated. We do however believe that there is truth in this approach and that this has resulted in increased business attention for SaaS solutions.

Business Users Start to Believe in SaaS Solutions

The business case we are using, a globally operating company similar to other companies across various industries, quickly recognized the benefits of using SaaS. SaaS is one of the cloud computing deployment models (in addition to IaaS and PaaS), in which various third-party vendors develop applications and make them available to customers over the Internet. SaaS solutions are typically offered through a subscription based model in a multi-tenant environment.

There could be different reasons for turning to SaaS; companies themselves often mention cost savings, while users primarily recognize faster innovation, greater business agility and improved collaboration. What users often find as a benefit, for example frequent and unnoticeable automatic software updates, becomes a headache for organizations that traditionally used to dictate times and scopes of updates to their software. Another example would be collaboration capabilities of certain SaaS solutions that can provide additional insights into companies by analyzing all the information and data that SaaS users can store and share within applications. While being an excellent information sharing and analysis platform for end users,

Valuable time is spent on low risk and low value contracts

collaboration SaaS increases the risks of information being "over-shared" – either by end users themselves, or by the SaaS provider that analyses the data in the first place.

The rise of cloud computing in the consumer domain (think about such players as MS Office 365, Salesforce, Workday) has raised user expectation about the types of services that IT departments deliver and the speed of delivery. An employee's legitimate desire to start using these tools to improve the quality of their work will often be backed up by a solid business case explaining how the company can benefit from the new SaaS service. Yet, many organizations are still unable to keep up with these expectations, citing various reasons ranging from loss of control over organizational data to different legal jurisdictions for data origin, storage and processing. As a result, deployment of SaaS services is being delayed or rejected, and individual employees and departments choose to bring cloud services into the organization by themselves, circumventing the IT department. This situation is often described by a well-known term in the IT world – Shadow IT.

In order to gain an understanding of the degree of cloud Shadow IT used at the company, meaning the exact number of cloud applications being used by company employees and the associated business risks, a cloud discovery scan was performed by using software from a Cloud Access Security Broker (CASB). The analysis revealed that the actual number of cloud services in use was 5 to 10 times higher than the company estimated. The results served as an additional driver to start developing high-level Information Security requirements and guidance in adopting cloud solutions.

Business Drives the Need for a Redesign of the Procurement Process

The company in our business case predicted a significant growth in SaaS usage in the coming years – this trend is also supported by their "Cloud First" strategy. This triggered a new initiative within the company of reviewing the older process of contracting and procuring IT services. The old process that was followed by Procurement for onboarding IT solutions was not optimally designed to allow for an efficient and effective way of contracting cloud solutions, more specifically:

- The process lacked speed (with the average time to contract being 90 days) and agility to deal with the growing demand of SaaS requests from the business.
- Information Security, Legal and Regulatory risks were not properly reflected in the procurement process.
- The process aimed at contracting SaaS solutions on the company's own terms and conditions (T&Cs), whereas the SaaS concept assumes a standard offering with standard (supplier) terms and conditions and limited opportunities for negotiation. The company would notice how many SaaS vendors reject the company's contractual clauses and instead propose their standard T&Cs.

Together, these issues have often led to the situation where a substantial amount of valuable time and expense was being spent on low risk and low commercial value contracts. As supported by audit opinions, there was a clear need to improve the company's capability to introduce SaaS in the business.

Shadow IT is Increasing the Need for SaaS Orchestration

In the cloud world, shadow IT is any software that employees acquire directly from cloud service providers, circumventing the internal IT department and not following approved processes to deploy IT services. This can potentially reduce the organization's level of security and result in the following risks for the business:

- *Data Risks.* Valuable business data may reside in cloud environments that are not secured and controlled by the organization's data governance standards. This can result in sensitive data being shared with unwanted parties or accessed, modified or removed by unauthorized users;
- *Compliance Risks.* Business or privacy-sensitive data may be transferred or stored in locations with different laws and regulations, which can result in regulatory and security non-compliance incidents;
- *Assurance Risks.* There are many different assurance standards regarding cloud computing. However, there is currently no unified standard and many cloud service providers do not share enough information and do not allow customers to conduct audits. This creates challenges on obtaining assurance on data and processes.

To mitigate the risk of cloud-based shadow IT organizations need to stay aware of the full scope of cloud services in use by their employees, which nowadays can be done with the help of next generation firewalls and cloud access security brokers (CASBs).

While Taking a Conscious Risk Based Decision

To address the growing issue with SaaS contracting and procurement, the Procurement team, together with a multi-functional team of specialists, has developed a new uniform SaaS Contracting process for the company. The key idea was to not only renew the overall process during a procedure writing exercise, but also to support it with a practical implementation. This would translate later in the project into a tool that we refer to in this article as the Cloud Adoption Tool.

The company in our business case wanted to enable the acceptance of the Terms & Conditions (T&Cs) of SaaS Providers, as this accelerates execution of SaaS contracts. They would accept T&Cs when specific contract requirements are known, verified and met. As such, the company needed to know when adding a side letter or using a company contract is the only way to mitigate the residual risk of adopting a SaaS solution.

Renewed Procurement Process for SaaS Solutions

The purpose of the new SaaS procurement process was to provide staff with guidance in selecting an appropriate contracting method for a SaaS solution and to provide the requirements that need to be validated in the terms & conditions of the SaaS vendor, demanded as an attachment to the vendor's T&Cs, or included in the company specific contract (if such an option would be possible with a cloud vendor). Furthermore, the risks could be deemed to be too large and therefore reject a SaaS proposal irrespective of the contractual approach.

With our support, the company came up with an improved process that focuses on integration between the business (through the representative for the business request), Information Security (through the inclusion of the data oriented risk assessments), Legal, Compliance and Procurement. Key here for Procurement would be to rely and reuse as many existing assessments performed by the different functions as possible, instead of designing a completely new assessment. In other words; Procurement staff should not take over any of the responsibilities of the other functions involved, but rather rely on the work already done by those functions.

Summarized, the process included the following steps:

- defining the starting triggers and the input for the process;
- performing the analysis and segmentation;
- performing the requirements checks based on the segmentation outcomes;
- performing any required follow-up actions and signing the contract.

Detailed guidance and responsibilities have been assigned for the above steps. Supporting their execution would be the key purpose of the CIRA tool.

Cloud Adoption Tool

The Cloud Adoption Tool is aimed at consolidating various requirements from different risk assessments within the company, such as a Business Impact Assessment and Legal assessments that will determine a certain profile (or segmentation) for a particular SaaS case. The segmentation will then suggest the contracting approach when moving the company's information assets to the cloud and a concrete set of contractual requirements to be demanded from a cloud provider prior to signing the contract. These requirements are to be checked against a supplier's T&Cs, or to be included in a side letter or the company's own specific contract.

It is important to highlight the following key features:

- The Tool identifies information security, legal and regulatory risks, as well as details of the SaaS solution in the early stages of the procurement process.
- The Tool supports an enhanced segmentation model to help determine the contract profile:
  - Operational contract, when the company accepts the supplier's T&Cs.
  - Tactical contract, when the company accepts the supplier's T&Cs and requires the signing of a side letter in addition.
  - Strategic contract, when the company wants to sign a company-specific contract.
- The Tool is based on Subject Matter Expert (SME) support and sign off. Each SME has provided advice to the Tool and supports its aims. This is a, not to be underestimated, necessity. With the approach developed, SMEs that would normally be consulted in a procurement process have now given their consent for pre-defined scenarios assuming the requirements are met in the Supplier T&Cs.

Figure 1 represents, at a high level, the SaaS procurement process and results of the Tool.

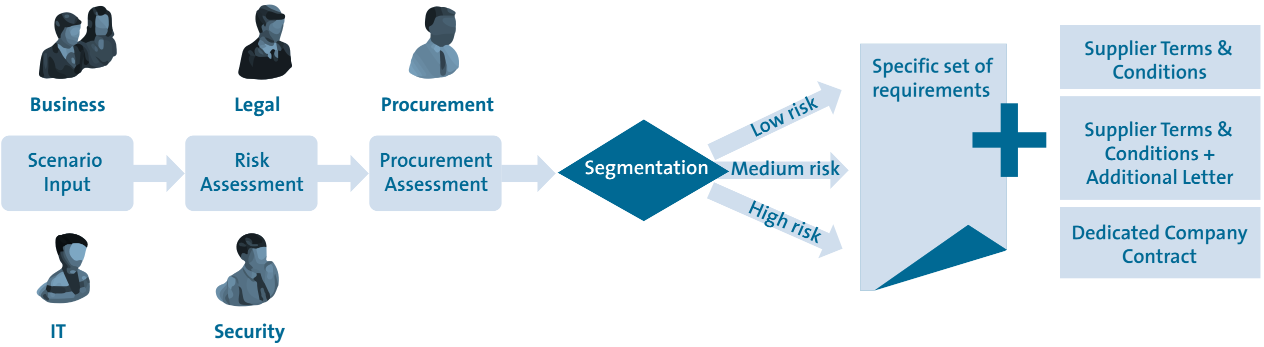

Business
Legal
Procurement
Scenario Input
Risk Assessment
Procurement Assessment
Segmentation
Low risk
Medium risk
High risk
IT
Security
Specific set of requirements
Supplier Terms & Conditions
Supplier Terms & Conditions + Additional Letter
Dedicated Company Contract

Figure 1. **Simplified representation of Cloud Adoption Tool.**

In one of the largest global companies, which serves as our business case, changing such a fundamental process and way of thinking requires more than a tool. Key elements during the release of the Tool include, amongst others:

- engaged and informed key stakeholders and support obtained from senior executive within the company;
- prepared guidance and manuals;
- issued communications;
- training provided to the Procurement staff on the SaaS contracting process;
- an initial trial period of six months;
- SMEs engaged to review the design, implementation and "run & maintain" phases of the revised process.

In a World That Continuously Matures and Evolves

The world has not stopped revolving. SaaS vendors recognize the increased demand from potential professional clients for insight into how their solution is provided. This has resulted in a growth in (specific) certification programs and security products, as well as actual assurance products such as SOC 1 and SOC 2 reports. SaaS vendors no longer suffice with "being in control", but are required to actually "show control" as well. The first movers, such as our business case, might cause frustration with the SaaS vendors. Typically, the smaller players are not used to difficult questions around security and compliance, whereas the larger players start to employ security officers with high commercial skills to sell the security of the solution. We do believe that the SaaS market is slowly evolving as well and is moving to a state of maturity when it comes to security and compliancy. However, we should be aware of SaaS vendors that try to benefit through dodgy certifications and "audit reports". But this is not limited to the SaaS market and has been around in security for a long time (e.g. through cheap ISO 27k certificates).

Where the SaaS vendor evolves, the IT department cannot remain behind. IT teams can experience this as a struggle; how to stay relevant in a model where the business can directly procure an IT solution? Especially where SaaS solutions are used in a professional environment, e.g. to support a business process, the IT department needs to step in and ensure the SaaS solution is properly embedded in its portfolio. Eventually, users will go to the IT Helpdesk if they cannot log in to the SaaS application, or when an interface with a "legacy" system no longer functions. And when the user query concerns shadow IT, then the user might not even realize this; to him it is all IT. It is important that in the fast moving SaaS world, the IT department is capable of quickly adding a SaaS solution to its portfolio. A clear view on architectural principles and minimum requirements is necessary for this. In fact, this should also be a part of the overall contracting model: it is not only about security or compliancy risks, it is also about the ability to support and operationalize the SaaS solution. This is actually one of the next steps identified in the business case we used as the basis for this article and this truly combines all relevant functions and teams involved in procuring, implementing and supporting an IT solution. Which happens to be SaaS ...

Where Did This Journey Take Us and Where to Go Next?

The straightforward process supported by the Cloud Adoption Tool makes it a simple and consistent process for procuring SaaS solutions where relevant risks are identi-

Problems faced	Problems solved
Time to contract too long	Reduced contract cycle time from 90 to 30 days empowering the Procurement frontline (operational buyers dealing with vendors) to be more commercial
Non-compliance with Legal, Regulatory and Compliance requirements	Clear identification of risks prior to contracting and identification of which requirements are in/out of scope for a specific project
Lack of ownership of issues to manage risks	Can assign correct ownership by identifying the relevant risks
No clear governance	Clear about how to handle SaaS requests and who should be involved
Limited visibility of SaaS contracts inventory	Can provide better oversight on SaaS contracts being placed by the Group

Table 1. **Cloud contracting process resolved problems.**

fied early in the procurement stage and that triggers an appropriate contracting approach to reflect the degree of risk.

After running the process and the Cloud Adoption Tool for around 9 months the company is currently evaluating the overall process to continue building on its strengths and address weaknesses. Initially designed to be a simple and straightforward tool that can align different parties within the company (such as Procurement, IT, business partners, Legal, and various subject matter experts) on steps and requirements for SaaS onboarding, it seemed to achieve this goal. During the evaluation workshop it has been noted by various stakeholders that the Tool:

- helps to *understand business needs* in procuring a particular SaaS solution (scope of use, demand, requirements);
- *simplifies and speeds up the contracting process* by enabling preparation of a custom, fit for purpose contract to source SaaS or entering into a contract on the supplier's terms;
- *increases compliance* by identifying the actions required prior to signing the contract and verifying that all key stakeholders are involved in the process;
- *streamlines communication* between stakeholders that use the same process and forms from the Tool.

Table 1 provides a summary of problems resolved with introduction of the process and tooling at the company.

The SaaS contracting process has so far been focused on risks from various angles. Next steps could include the integration of other specialist areas or functions. Where the Tool in its current form provides requirements to check the Terms & Conditions of the SaaS vendor, in a next phase the Tool could also provide requirements to check the actual solution:

- IT Architecture to provide requirements for the design of the SaaS solution;
- the Service and Support function to provide requirements for bringing the SaaS solution into its support processes;
- business representatives to provide requirements for actual functionalities that need to be provided by the SaaS solution.

Overall, the approach developed together with the company in our business case, has shown to be relevant and add value, while taking a risk based approach. What is learned from this case should serve as food for thought in any organization that deals with an increasing push for SaaS solutions while dealing with traditional (risk) functions.

About the Authors

P.R. de Meijer RE CISSP CISA is a senior manager at KPMG Cyber and has extensive experience in Information Security and Compliance. Furthermore, he is an experienced IT Auditor. He has worked in various organizations advising how to structurally improve an organizations' ability to keep their information safe and secure.

O. Kulikova MSc CCSK is a senior consultant at KPMG Cyber. She has experience with advisory engagements related to Cloud Security, Identity and Access Management, Information Risk Management, and Cyber Defense. She is certified for Cloud Security Knowledge (CCSK) by the Cloud Security Alliance (CSA).