Cloud Adoption Assessment

Vincent Damen RE CISA

Many organizations struggle in deciding whether or not to adopt cloud computing. Cloud computing offers major benefits, but also poses serious security risks. To make an informed decision, organizations can conduct their own assessments of any particular cloud service. This includes building a framework tailored to the specific organization and its security requirements in order to structure the assessment. The results of the assessment will determine whether the organization has sufficient information to make an informed decision on cloud adoption. This article explores a method of setting up such a framework and conducting a cloud adoption assessment.

V. Damen RE CISA
is manager at KPMG Advisory N.V.
damen.vincent@kpmg.nl

Introduction

The cloud market has been maturing and growing at such a rapid pace that few organizations can choose to ignore it. According to Gartner, by 2016 most of what organizations spend on new IT will be for cloud services and cloud computing ([Gart1]). Additionally, Gartner indicates that the cloud-based security services market was worth $2.1 billion in 2013, rising to $3.1 billion in 2015 ([Gart2]). With a rapidly growing market and a myriad of security concerns, organizations have a lot of questions and need informed advice when adopting cloud computing.

The current cloud-boom poses its own specific opportunities and challenges. A few years ago it seemed that organizations would not even consider moving to the cloud due to security concerns. However, due to significant improvements in cloud security, organizations are not only considering cloud services but are actively pursuing adoption strategies. The reasons for adopting cloud services vary, but two main factors stand out above all: one is flexibility and the other is cost savings. Cloud computing seems to progress on a lot of fronts where traditional IT is considered too limited, complex and costly. However, organizations are also worried about the risks that surround the cloud. The decision-making process is often inhibited by fear, uncertainty and doubt, together with the perceived risks surrounding cloud computing.

This article will explore a method for how organisations can perform their own assessment of the cloud services, thus enabling them to make an informed decision on cloud adoption.

Cloud computing benefits and risks

Generally speaking, a wide range of different cloud services are readily available for nearly immediate use. These services can range from a single piece of online storage to a fully fledged Customer Relationship Management (CRM) system. The inherent nearly instant delivery of cloud services creates a flexible environment, enabling businesses to react quickly to changes in their organizational or customer landscape. It also erases nearly all hardware investments (buying software licenses, paying to maintain data centers, funding long (and costly) implementation projects) as well as eliminates the human resources costs in supporting the “nuts and bolts” of IT. Additionally, the Cloud Service Provider (CSP) makes sure that the service

acquired is kept current, is online 24/7 and is available from practically anywhere in the world. The possibilities are limitless and the price tag for this flexibility is, in most cases, lower than that of traditional IT ([Chun11]).

Capital Expenditures (CapEx) are almost nonexistent when adopting cloud computing. An organization will shift its CapEx to an Operational Expenditure (OpEx) model, which forces the reevaluation of existing IT investments and spending. CSPs charge for the services delivered, but do not require an organization to pay for setting up the underlying infrastructure. The CSP pays for the infrastructure set-up and maintenance that supports the cloud service functionality. Additionally, if a service is no longer needed it can be terminated, without the organization having to rid itself of obsolete IT equipment. Compared to traditional IT, the benefits of cloud computing are easily recognizable and paint an attractive picture of a cheap and very usable technology.

The fact is, however, that many organizations are apprehensive because there is not a lot of transparency about what's going on behind the CSP's closed doors. What is actually happening behind the cloud service that has just been implemented, and where does my data go? Who is actually managing the infrastructure, and do they have access to my data? Is my data even stored in this country? This discussion on cloud security focuses on the maturity and quality level of security controls put in place by the CSP. In the days of traditional IT, a customer could rely on relevant assurance reports, such as the International Standard on Assurance Engagements (ISAE) 3402, to provide the requisite assurance. An alternative could be to have an agreement establishing a right to an audit, and perhaps a right to conduct the audit or assessment. The problem is that the assurance reports we currently have do not always answer the relevant questions regarding cloud computing, while we have pressing needs for insight into the safety of data, the implementation of the correct controls and the way information is treated, be it in the cloud or elsewhere.

Security standards

In order to be confident that our provider's services are secure, we traditionally have a few options:

1. We can either trust the provider based on the contracts and underlying Service Level Agreements (SLA);
2. We can ask the provider to agree to grant us access to their premises, information and systems, in order to perform our own audits and assessments; or,
3. The provider can provide us with an assurance report compiled by an independent third party who did a security assessment. Examples of these types of reports include the ISAE 3402 (type 1 and 2), ISO/IEC 27001/2, PCI DSS, and so on.

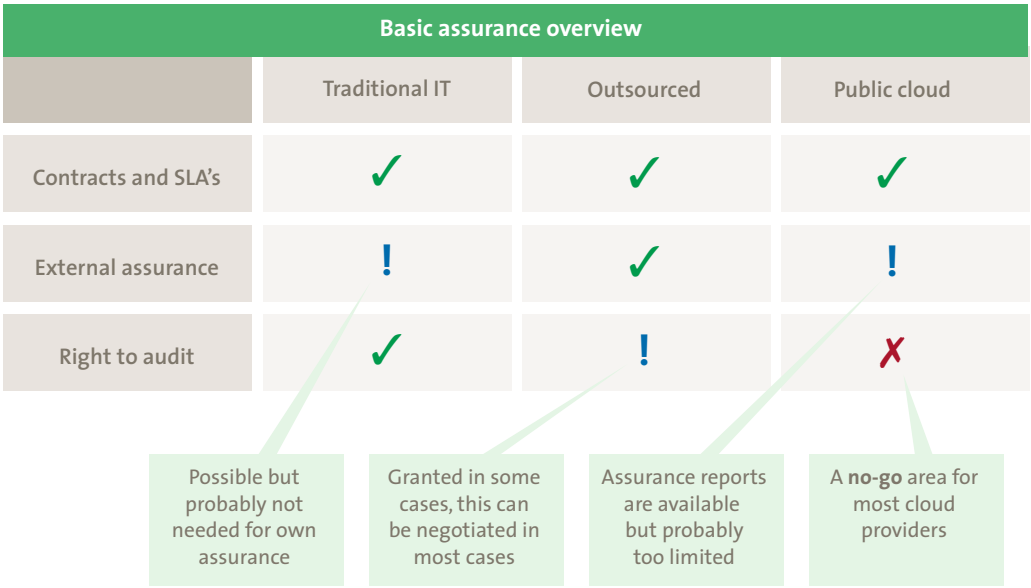

Figure 1.

Now, the chances of an organization relying solely on contracts and underlying SLAs are slim. A commercial contract probably does not provide sufficient detail as to the way the service is set up and managed. It probably doesn't specify how security is handled by the provider. The chances of a CSP opening up their doors to a prospective client to perform an assessment onsite are even lower. There are not many examples where a right to audit has been exercised successfully with a CSP ([Chun11]). Not only is there but a slim chance of gaining a right to audit, the organization would need exceptionally capable technical auditors to assesses a cloud architecture that could be (and probably is) very different from traditional IT.

This basically leaves an organization few options, apart from trusting the opinion of an independent third party that has carried out a security assessment.

Gaps

However, traditional assurance reports and security frameworks do not fully cover the relevant aspects of cloud computing. The ever-popular ISO 27001/2 controls, for example, do not cover the specific cloud risks related to topics such as privacy or multi tenancy. Also, while not covering all elements of cloud computing, there are many standards and certifications to choose from. Listed below is just a small selection of standards, certifications and other information-security tools and reports an organization may encounter when dealing with CSPs:

- The Statement on Standards for Attestation Engagements Number 16 (SSAE 16), including the Service Organizations Control 1, 2 and 3 (SOC1, SOC2, SOC3), types I or II;
- The Payment Card Industry Data Security Standard (PCI DSS);
- The American National Standards Institute /Telecommunications Industry Association Telecommunications Infrastructure Standard for Data Centers (ANSI/TIA-942);
- Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM); and
- Code of practice for information security controls for cloud computing services (ISO/IEC 27017).

The problem with these various standards is that they have each been developed with a specific purpose in mind. The PCI DSS was created to secure the transmission and storage of credit card data. The number of controls dealing with system availability in this standard is therefore lower than other standards. The ANSI/TIA-942 has been developed to set minimum requirements for telecommunications infrastructure of datacenters and computer rooms. This means that most of these controls deal with ensuring the availability of computer equipment but, for example, do not include controls dealing with logical access control.

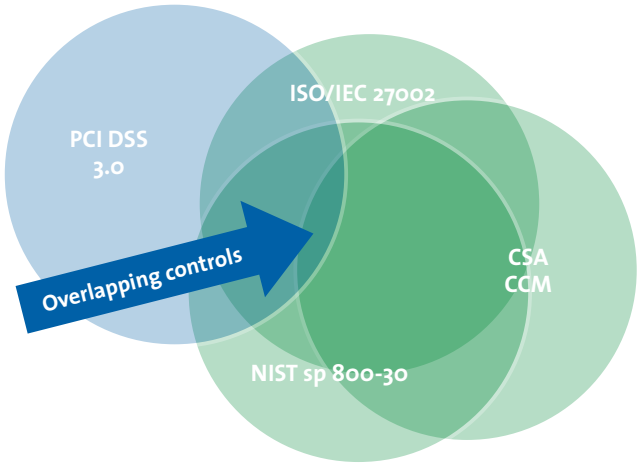

Figure 2.

Overlap

To make matters worse, the different standards overlap. Certain controls may exist in almost all information security standards. A good example is the mechanism to synchronize the clocks on related computer systems:

- System clocks should be automatically synchronized with an accurate time source. Determining when events took place is of paramount importance for properly logging audit trails (§10.10.6, ISO/IEC 27002);
- Internal Information System clocks should be synchronized on an organization-defined frequency using an authoritative time source (§AU-8(1), NIST SP 800-53);
- Using time-synchronization technology, synchronize all critical-system clocks and times, and ensure that the following is implemented for acquiring, distributing, and storing time (Requirement 10.4, PCI DSS 3.0).

As we can see, the different controls basically have the same purpose: make sure that your clocks are on time and are synchronized correctly.

This poses a problem for a potential CSP customer. How many certifications and audit reports does a CSP need in order to provide sufficient insight into security for a customer organization? How can an organization be sure that the different standards create full coverage to serve their needs with minimal overlap? A possible solution is custom tailoring the reporting based on the information and tools at hand, by creating an assessment of the organization's own security framework.

Adoption assessment

In order to obtain at least some kind of confidence that an organization is making the right decision regarding information security when adopting a cloud service, the organization can conduct its own assessment based upon relevant industry standards plus all information the CSP is able to provide. Ultimately the decision to either adopt or reject the proposed cloud service is based on weighing this available information. An assessment based on a framework tailored for the specific organization and situation will help to provide this in a structured manner. Setting up a custom framework forces an organization to systematically review what they should protect, what the risks are and what controls are deemed necessary to mitigate these risks. Once this is structured as a set of controls in a framework, the organization can focus on getting the right answers from the CSP.

As we have seen, there is a multitude of standards, controls and frameworks that the organization may adopt as a starting point. We also saw that almost all standards are "purpose built". Of course an organization could start with a blank slate and start adding the biggest risks they need to mitigate first. However, having a basic predetermined set of cloud risks and vulnerabilities certainly helps in structuring the process. As a starting point, it would be wise to pick a standard that is "purpose built" for the cloud. Examples are the ISO/IEC 27017, NIST sp 800-14 or the ENISA cloud computing risk assessment.

In this example we take the ENISA cloud computing risk assessment as a basis for creating a framework and doing our own assessment. The European Union Agency for Network and Information Security (ENISA) has conducted a risk assessment on the cloud computing business model and technologies. ([ENISA09]). The ENISA report is an independent analysis that outlines some of the information security benefits and key security vulnerabilities of cloud computing. It is not considered a full standard but more of a guideline to help organizations assess the risks involved in cloud computing. The 24 ENISA vulnerabilities contained in this report have become the preferred basis for assessments by financial institutions in the Netherlands seeking to obtain the approval of the Dutch National Bank (DNB) for cloud adoption ([DNB13]).

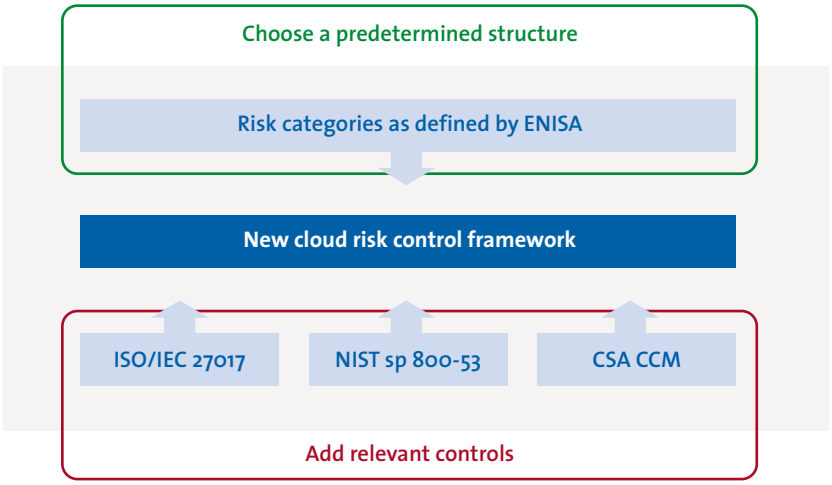

Figure 3.

Building a framework

To build the framework we will select the relevant controls from various standards in order to sufficiently mitigate all 24 ENISA vulnerabilities. Sometimes one control will be enough, but in other cases we will need more than one. The ENISA Vulnerability number 8, "Resources exhaustion," which deals with the CSP failing to deliver the requested services due to a lack of resources, can be taken as an example. Here we have a very broad "cloud" risk that should be addressed before implementing a cloud service. The vulnerability can of course be mitigated in advance by making sure that a CSP has all correct controls in place. The definition of correct controls depends on the type of organization, the service and the CSP we are dealing with.

Luckily we have a multitude of industry standards that provide controls we can use. For example, the following control could be used:

1. **Multi Tenancy Capacity Management** – "The CSP will establish and implement policies, procedures and mechanisms to ensure enough capacity is available, taking peaks in usage and multi tenancy into account."

This is control number 11.4.1 taken from the ISO/IEC 27017, and can be used to cover the risk of resource exhaustion. What we want to see is a manner of evidence from the CSP that they have established and implemented the aforementioned policies, procedures and mechanisms. The method of obtaining and assessing this proof will be discussed further down in this article. Another example of a mapping could be the next ENISA vulnerability number 9, "Isolation failure," which deals with the CSP failing to separate the cloud services provided to different customer organizations. A mapping could be:

1. **CSA CCM [IVS-09]** – Multi-tenant organizationally owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users.
2. **NIST 800-53 rev 4 [SC-7] – BOUNDARY PROTECTION** – The information system:

a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;
b. Implements sub networks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and
c. Connects to external networks or information systems only through managed interfaces comprising a boundary.

This way an organization can develop a risk control framework based on broad vulnerabilities enhanced with controls from multiple industry standards and frameworks. The framework thus provides a selection of controls taken from the relevant industry standards that fit the situation and organizational needs.

Assessment method

The assessment can only analyze the data that is available. If an organization does not have a right to conduct an audit, the information available will mostly consist of oral and written items. Because of this we are limited in conducting an assessment that only tests the related controls in design (TOD). A test of effectiveness (TOE), where we assess the effectiveness of the controls, is not possible at this stage.

The goal will be to gather as much information as possible that can serve as evidence for the set of controls in our framework. The CSP will probably be happy to provide its customers with information that is already publicly available. Some CSPs such as Microsoft have even developed whole web pages dedicated to answering security and compliance questions for potential customers. An example is the Office 365 Trust Center ([MS14]), which holds a lot of information that can be used as a foundation for the selected controls in your framework.

If the publicly available information does not satisfy the need for information, schedule a meeting with the CSP. Make it clear that, as a potential customer, you need more detailed information and would like to discuss the specifics of your framework. Be prepared to share your framework with the CSP, and ask if they are willing to go over the various controls with you and answer your questions. Once you have created a dialogue with the CSP and have shared your framework with them, you can discuss what additional information they might be willing to share. Perhaps the CSP is willing to give you insight into one or more of their assurance reports. As more and more customers are asking the same questions regarding security, the CSPs are becoming more open about their procedures and implemented controls. If assurance reports are provided, you should analyze the scope of these assurance reports and see where their controls overlap the ones in your framework. Where an overlap exists, and the control was reported to be functioning without deviations, you have the most compelling evidence available.

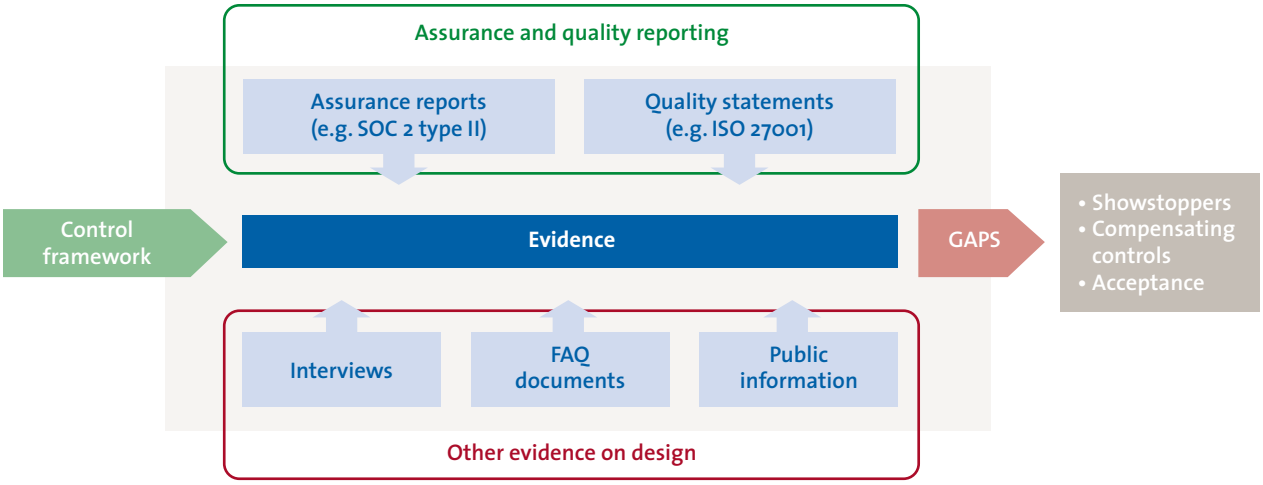

Figure 4.

In order to get the most out of an assessment of the CSP, have an experienced auditor or security assessor perform the assessment. Considering whether the presented evidence is enough to fully satisfy the security insight needed is more akin to performing an audit than anything else. When the assessment is finished and the organization is left with controls that remain "unanswered," we have a gap. And if the vulnerabilities selected have been classified based on their importance to the organization, it can be easy to spot the show stoppers for cloud adoption.

To give an example: the CSP did not provide any information on protection against Distributed Denial of Service (DDoS) attacks, while this vulnerability was classified as a high risk for the organization. If the CSP remains unable to provide this information, it is more likely the offered cloud service will be rejected (depending on the organization's risk appetite). When all controls have been sufficiently answered, cloud service adoption is a more likely option. In practice, you will be left with a mix of unanswered, partially answered and fully answered controls. For some of these gaps you might be able to implement compensating controls yourself. If not, consider accepting the risk. The decision for cloud adoption will then be based on the risk appetite of the organization. Of course, this has always been the case, but the difference now is that the decision can be made based on a structured set of available information, specifically tailored to the assurance needs of the organization.

Lessons learned and conclusion

In assisting an organization to set up its own framework to assess cloud adoption, we have learned a great deal. The following items are the lessons learned while setting up the framework and conducting the assessment with the CSP:

- In order for the framework to be effective, an organization should take care to be very precise in mapping controls. It is easy to become redundant in your control set due to the amount of overlap between the different standards. Gaps are also easily created, because some cloud vulnerabilities do not have standard controls (privacy and legal aspects are hard ones).
- Make sure you include the controls from the "big standards," such as ISO 27001/2, and show you are taking these into account when the framework and assessment is questioned later on. It facilitates future audits and assessments because, when a cloud service is adopted, you can easily translate back to the then-current standard.
- If possible, include the controls from your own internal control framework or use this as a basis. This will save time if an internal audit department wishes to assess an implemented cloud service in the future. The mapping to the internal controls will be easier and more direct.
- Determine the classification of your vulnerabilities in advance. ENISA has already categorized the various vulnerabilities, but don't be afraid to tailor this classification to your own organizational needs. This makes the future decision making process a lot easier, since you have already determined which vulnerabilities must be mitigated before adopting the cloud service.
- Remember this is not a formal audit but a first assessment, in order to gather enough insight for the decision-making process. Almost no CSP is able to mitigate all vulnerabilities or provide a prospective client with all information, but the framework allows you to make a very informed decision.

Although it appears to be a daunting task, most organizations already know what they really need to secure. They also know that not moving to the cloud is becoming an increasingly less viable option. Conducting an assessment as to whether to adopt or reject cloud services will definitely support the company's decision-making process.

About the author

V. Damen RE CISA is manager at KPMG Advisory N.V., specializing in audits and advisory regarding information security, risk management and cloud computing. He also provides guest lectures on information security at the Vrije University Amsterdam (VU), the University of Amsterdam (UA), Delft University of Technology (TUD) and is a trainer on information security at the Institute for International Research (IIR.nl).

Literature

[Gart1] Gartner, "Cloud Computing Will Become the Bulk of New IT Spend by 2016." Press release 2013/10.

[Gart2] Gartner, "Cloud-Based Security Services Market to Reach $2.1 Billion in 2013." Press release October 31, 2013/10.

[Chun11] Drs. W.S. Chung RE, "Assurance in the Cloud." *Compact* 2011/0.

[ENISA09] ENISA, "Cloud Computing Benefits, Risks and Recommendations for Information Security." 2009/11.

[DNB13] DNB, "Sjabloon risicoanalyse cloud computing." Press release, 2013/06.

[MS14] Microsoft, "Office 365 Trust Center." Website, 2014/03.