Royal HOLLOWAY SERIES 2012

How a Cloud Service Provider Can Offer Adequate Security to its Customers

What security assurances can cloud service providers give their customers? This article examines whether current security standards are adequate for cloud-specific risks and suggests ways organisations can reduce their risks in the cloud.

BY ROBERT FARRUGIA AND GERAINT PRICE

TechTarget

Royal Holloway University of London

How a Cloud Service Provider Can Offer Adequate Security to its Customers

A RECENT UK SURVEY carried out by CompTIA has discovered that 18% of SMEs already use the services of a cloud provider. In addition, it was revealed that a further 30% are planning to use them over the next 12 months. Other surveys carried out in various parts of the world uncover similar trends. In the coming months, many Information Security and IT managers will be faced with a number of decisions related to the choice of a Cloud Service Provider (CSP) for their organisations.

This article provides insight to the assurance that is being provided by CSPs through certification of compliance with internationally recognized security standards. After setting the scene, we take a high-level look at cloud-specific risks from a customer's point of view.

Next we evaluate whether the current security standards are adequate for providing assurance that the cloud-specific risks have been mitigated. We will also describe the components that one would ideally find in a standard that provides such assurance. Finally we look at some recommendations that should be followed when moving the organisation's information and processes from the traditional in-house infrastructure to that of the cloud.

SETTING THE SCENE

Whether we like it or not, cloud computing is changing the way we look at the IT environment. Due to its distinct characteristics, we may be in a situation where the current information security standards are not applicable to the security risks of cloud environments. This article questions whether such standards can provide an easy and transparent mechanism whereby a

customer of a cloud service provider (CSP) can be assured that the cloud-specific risks are being adequately managed. In order to achieve this objective, three tasks have to be carried out. Firstly, identification and selection of the main risks associated with the cloud environment. Secondly, analysis of how each standard and framework mitigates the risks that have been identified. Lastly, but not least, understanding the certification compliance mechanisms of the standards and frameworks.

CLOUD-SPECIFIC RISKS

First of all, we start by identifying the risks specifically pertaining to the cloud. Some recommended documents that are really useful for this are the ENISA 2009 report, *Benefits, Risks and Recommendations for Information Security* and the work carried out by the Cloud Security Alliance. The top risks are summarised in **TABLE 1**.

ANALYSING THE STANDARDS AND FRAMEWORKS

Having identified the cloud-specific risks we now consider what level of assurance is provided by the currently available security standards in relation to such risks.

There are a number of security standards and frameworks that are being used by CSPs with a view to providing assurance to their customers on the security being employed. We consider six which are used predominantly by the top CSPs or are frequently mentioned by security experts and consultants. They are ISO 27001 / 27002, Trust Services Framework, Payment Card Industry Data Security Standard (PCI DSS), Cloud Controls Matrix (CCM), ISACA's Cloud Assurance Program (CCMAP) and the Statement on Auditing Standards (SAS) No.70.

The main standards used for assurance in the cloud are:

- **ISO 27001 / 27002,**
- **Trust Services Framework,**
- **Payment Card Industry Data Security Standard (PCI DSS),**
- **Cloud Controls Matrix (CCM),**
- **ISACA's Cloud Assurance Program (CCMAP), and**
- **Statement on Auditing Standards (SAS) No.70.**

How do they mitigate the identified cloud-specific risks? We need to understand how the controls from each standard mitigate the risks identified. Let us look at an example to illustrate this: how does PCI DSS mitigate risk 1? This is the risk that at a point

(Continued on page 5)

TABLE 1.
Top Risks for Information Security

RISK	DESCRIPTION
Risk 1.	At a point in time, the CSP encounters a **lack of availability of sufficient (technical) resources** due to incorrect statistical capacity planning or inadequate infrastructural investment or inadequate functionality to limit the usage of its pool of resources.
Risk 2.	Customers are not able to access their systems due to the interruption of the Internet service, since within the cloud there is a **dependency on the Internet**.
Risk 3.	**Data is intercepted whilst being transferred** between the cloud and the customer or within cloud infrastructure itself.
Risk 4.	The CSP has **insecure storage of data**.
Risk 5.	**Data is not effectively deleted** within the CSP's system.
Risk 6.	**Management of hardening procedures** is ineffective, resulting in an insecure cloud.
Risk 7.	The CSP operates **inadequate cryptographic management** procedures.
Risk 8.	The CSP operates an **unreliable service engine**.
Risk 9.	**Failure of the isolation mechanism** within the cloud infrastructure.
Risk 10.	The CSP offers its customers an **unreliable management interface**.
Risk 11.	**Malicious activities**, within the internal network, **by customers of the same cloud**.
Risk 12.	A CSP **employee(s) carries out malicious activity** on the customers' data and systems.
Risk 13.	The cloud is not adequately protected against a **distributed denial of service** attack.
Risk 14.	Customers are paying more than they should, resulting in **economic denial of service**.
Risk 15.	Customers are **dependent on their CSPs**.
Risk 16.	Customers **lose governance** on a number of security requirements.
Risk 17.	**Loss (by customers) is incurred due to activities carried out by another customer** who is on the same cloud.
Risk 18.	Customers **cannot always achieve compliance to international standards** due to the complexities of the cloud or because the CSP is not compliant with such standards.
Risk 19.	The **CSP terminates its services**.
Risk 20.	As a result of the **acquisition of a CSP**, non-binding security agreements between the original CSP and its customers are jeopardized.
Risk 21.	The deterioration or unavailability of the CSP's services as a result of **supply chain failure**.
Risk 22.	The CSP is **non-compliant with legal requirements**.
Risk 23.	The CSP **changes its location to a relatively unsafe jurisdiction**.
Risk 24.	**Subpoenas for one cloud customer may adversely impact all CSP operations**.
Risk 25.	**Licensing agreements** which do not cater for the complexities found within the cloud have an **adverse financial impact on the customer**.
Risk 26.	The CSP **does not comply with customer's requirements relating to data protection law**.
Risk 27.	The CSP **does not provide all the privacy rights** required by the customers.
Risk 28.	Customers may **lose intellectual property** for the data that they store on the cloud.

(Continued from page 3)

in time the CSP will not have sufficient technological resources (such as working memory or processing power) available. The problem can emerge if there has been inadequate infrastructural investment or if the CSP architecture has inadequate functionality to control the usage of its pool of resources. The only PCI DSS controls which may help in mitigating such risk are found within the incident response section. Amongst other things, those controls highlight the importance of having a disaster recovery and continuity plan. On close inspection, they are clearly not sufficient: PCI DSS does not include controls related to capacity planning, capacity monitoring and resource capping which would be appropriate to mitigate this risk. As a result, PCI DSS does not mitigate this risk. This analytical method can be used to assess how and whether each standard mitigates the various cloud-specific risks.

ASSURANCE PROVIDED BY SECURITY STANDARDS WITHIN CLOUD COMPUTING

In addition, one also has to understand the certification compliance mechanisms of every selected standard and framework. This is to ensure that such mechanisms provide a straightforward and transparent method for the customer to be confident that risks are being managed effectively.

Analysis reveals that **none** of the selected standards and frameworks is adequate for providing assurance that all the risks pertinent to the cloud have been addressed. Here are some examples where these standards failed to provide mitigation for specific risks:

- **The jurisdiction from where a CSP operates has an effect on the level of service provision that is being offered to the customers.** This is because the laws and regulations of certain countries provide more assurance on the security of data, which in turn gives an improved level of comfort to the customers. Certain jurisdictions are more respected than others, mostly because some of them offer strict enforcement of high level requirements and also because of political stability. Before moving to the cloud, one must make sure that the service is being provided from a 'safe' jurisdiction. Nevertheless there is always a risk of the CSP changing its location and moving its operations to a relatively 'unsafe' jurisdiction. This situation would adversely affect the security of the cloud's operation and that of its customers. When moving to the cloud, ideally, customers are assured that their CSP would not shift

operations to a less safe jurisdiction. None of the six standards provides an adequate level of assurance on this. For instance, having an ISO 27001 certificate does not provide assurance that this risk is managed in any way.

- **Another risk that customers face is CSP dependency.** This is a result of customers not being able to migrate from one CSP to another or to their own IT environment. It may arise from a lack of standard technologies and open frameworks or arrangements between CSPs to facilitate such requests. Another factor is that even though certain CSPs provide migration features, it is very expensive and thus financially infeasible. ISO 27001, PCI DSS and Trust Services Framework do not provide adequate assurance that such a risk has been mitigated. On the other hand, CMM and CCMAP partially mitigate the risk as they are specifically designed for the cloud.

- **As a result of business decisions, a CSP may opt to sell its cloud to another party.** The risk here (risk 20) is that of jeopardising non-binding security agreements between the original CSP and its customers. For instance, the customer may require some security controls which are not in the agreement between him and the CSP, although the CSP would have still agreed to provide such security features. As a result of the acquisition the continued provision of such security controls may be at risk. An acquisition may have other impacts on the customers depending on who is buying the cloud. Examples of such impacts may include the deterioration of the reputation of the CSP itself, loss of employee loyalty etc. Controls within CCMAP specifically provide assurance that security requirements are detailed in the service level agreements (SLAs) and contracts between the CSPs and individual customers. As a result, this risk is considered mitigated. On the other hand, controls found within other standards and frameworks do not appear adequate in providing assurance against such risk and should be graded as either partially mitigating this risk or not mitigating it at all.

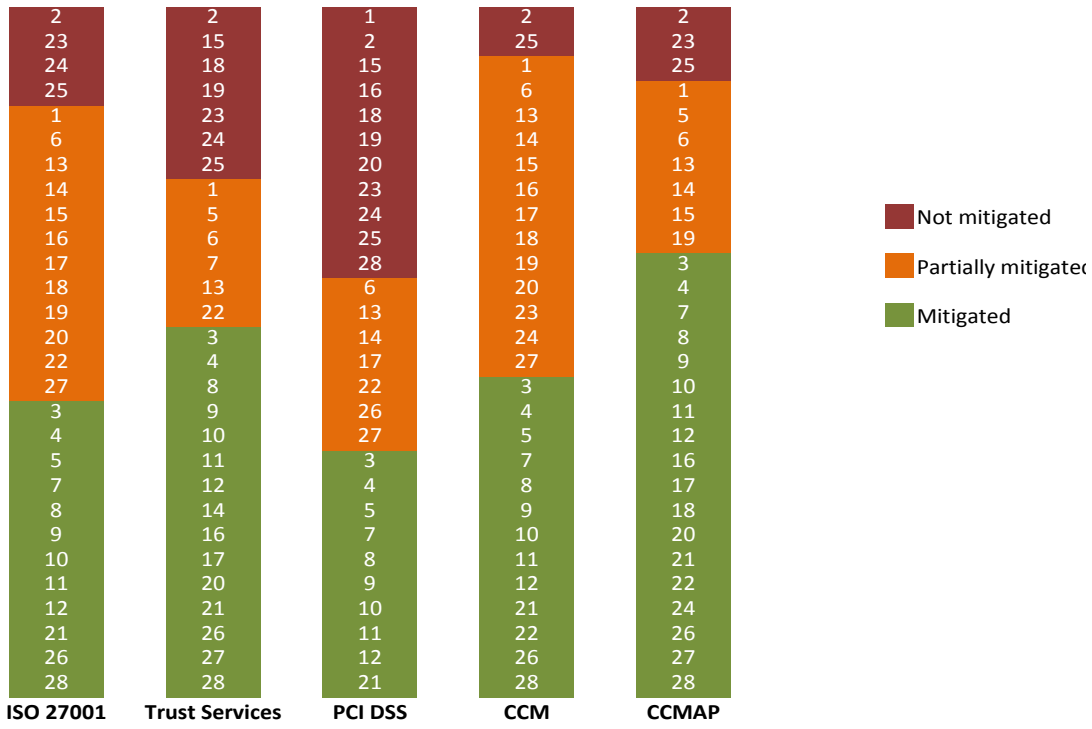
- **PCI DSS was not the only standard that does not adequately manage the risk described in the previous section—that the CSP will not have sufficient technological resources.** Trust Services, ISO 27001/2, CMM and CCMAP all have a number of controls, such as disaster recovery plans, capacity management and monthly monitoring to ensure availability of the systems. Although this provides some level of assurance

on the management of this risk, it is not enough. This is mainly because none of these standards/frameworks cater for capacity capping, an important concept for ensuring that customers do not request more resources than those available on the Cloud.

FIGURE 1 provides a summary of the full analysis. The risks highlighted in green are the ones that can be mitigated by applying controls that are found within the named standard. The risks in orange are those that can be partially mitigated by applying the controls found within the standard and the ones in red are those that cannot be mitigated by applying any of its controls.

Even though none of the standards has been identified as adequately managing all the cloud specific risks, some of the standards did indeed mitigate quite a substantial number of them. These were mainly the Cloud Controls Matrix (CCM) and ISACA's Cloud Assurance Program (CCMAP). Unfortunately, unlike the Trust Services Framework, PCI DSS and ISO 27001, the CCM and CCMAP standards are still being fine tuned and are not yet internationally recognised.

FIGURE 1.
Full Analysis of Risks



Wider analysis also takes into consideration other features and characteristics of the standards and frameworks. For instance, a disadvantage of CCM and CCMAP is that they do not offer customers an easy and transparent certification mechanism to provide assurance that risks are being appropriately managed. Another disadvantage identified in SAS 70 is that it does not include any specific security controls. Therefore, the controls in scope for an SAS 70 audit of one CSP will differ from the controls found in another SAS 70 audit carried out for a different service provider. As a result each customer would need to obtain a copy of the SAS 70 report relating to that particular CSP, and analyse what is being protected and how this protection is achieved before being able to conclude if the risks are being mitigated adequately.

Other than SAS 70, all the analysed standards include controls which reduce the cloud risks to some degree. Some standards provide controls which are more detailed than others. For instance, the control descriptions of the Trust Services Framework and PCI DSS are very detailed, especially when compared to those in ISO 27002 within which some of the controls may be deemed subjective. Therefore, if, for instance, a customer comes across a Trust Service Framework certificate and has comfort in the level of assurance that this framework provides, the customer does not need to look further into how the controls have been interpreted and implemented. On the other hand, the ISO 27002 requirements may have to be investigated further to understand exactly how these requirements have been interpreted in relation to the cloud risks.

A CLOUD-SPECIFIC STANDARD

In the preceding, we have claimed that none of the standards fits our requirements. Let us for a moment consider a hypothetical situation and try to come up with the ingredients that a cloud-specific standard should have. Based on the information described in the previous sections, ideally such a standard should:

- **include** only specific criteria such as those found in the Trust Services Framework and PCI DSS and should be cloud-specific such as the controls described within the CCMAP;
- **be seen** only as a minimum requirement. Hence a risk based approach with continuous improvement (such that offered by ISO 27001) should be included;

- **provide** a mechanism where a reputable third party can certify the security within the organisation. This should result in a report which would be available to existing customers and prospective ones; and

- **include** key performance indicators which are publicly available in order that customers can compare the security levels between different CSPs.

For such a standard to be successful and achieve its goals, it needs to be embraced by the information security community, marketed accordingly and supported by all the stakeholders including the CSPs.

This level of security assurance may introduce extra costs, but certified security should result in a competitive advantage and thus attract more customers. Moreover, due to economies of scale, this added cost would not be so high when spread across a number of customers.

When talking about a cloud-specific standard, one must bear in mind that security does not have a '*One-size-fits-all*' solution and such a standard may not be sufficient for all security requirements that one can imagine. For instance, a CSP offering services to insurance agencies may need to comply with different security requirements from one offering services to hospitals. The former would focus more on confidentiality aspects whilst for hospitals, availability usually comes first. Most probably a cloud-specific standard would not provide assurance on the highest level of security in terms of confidentiality, integrity and availability. The standard would not even cater for all applicable laws and regulations that govern various countries and industries. A CSP that has attained a recognised certification of compliance to a cloud specific standard could only provide its customers assurance that the generic risks specifically pertaining to the cloud environment are being adequately managed.

THE WAY FORWARD

Regrettably the Cloud Specific Standard described above has not yet been developed. Nevertheless, one can still carry out a number of tasks to manage the risks for an organisation. Daniel Gardner, author of the book *The Science of Fear*, affirms that human beings owe their existence to fear because it is fear itself that keeps us alive. He analyses the fact that without fear we would not be able to recognise and carry out justified actions regarding the risks surrounding us.

Fear is essential for understanding the environment around us. However,

this fear does not need to be inflated since unreasonable and unjustifiable fear may have a negative effect. Hence the importance of risk management which can play an important role in the identification and management of the risks found within a cloud and thus help in providing a secure cloud to the customers.

The above analysis of the importance of risk management leads us to the critical fact that we need to understand the value of our information and assess what are the risks of moving such information and processes to a CSP.

High profile CSPs such as Amazon, Google, Microsoft and Salesforce provide documentation to inform existing and potential customers of the security employed within their organisations. In reality, it is not always transparent or easy to get assurance that these controls are actually being effectively implemented. Nevertheless, looking carefully at this information is always a good start. One could also do some research to investigate whether there were any incidents that were made public and whether such incidents were adequately managed. Further, it is also valuable to obtain an independent third party opinion and perhaps discuss the views of the CSPs' current and past customers who are making, or have made, use of the services of the selected CSPs. Next, organisations could also take responsibility for managing some of the identified risks, such as backing up their services via a different CSP. Finally, it seems advisable that a shift to the cloud should be gradual. If possible, at first one should transfer only low risk information.

Cloud computing is a reality and over time most organisations will transfer part or all of their information and processes to this new environment. It is important that such a shift is managed through a risk based approach. Decisions should not be taken on one's perception but should be analysed objectively. Understanding what assurance is provided by the certifications attained by the CSPs and how such certifications affect the management of our organisation's risks is the key to taking an informed decision on how and whether to make the shift. ■

ABOUT THE AUTHORS:

Robert Farrugia is a manager within the IT Advisory KPMG team in Malta, specialising in information security and IT assurance. He has recently played a central role in engagements relating to ISO 27001 implementation, the development and coordination of an information security awareness programme, business continuity and disaster recovery planning, business process mapping and IT outsourcing.

Geraint Price is a lecturer in information security at Royal Holloway. His research interests include secure protocols, public key infrastructures, denial of service attacks and resilient security.