How to ensure control and security when moving to SaaS/cloud applications

Stéphane Hurtaud
Partner
Information & Technology Risk
Deloitte

Laurent de la Vaissière
Directeur
Information & Technology Risk
Deloitte

Security concerns are still one of the major barriers to mass adoption of cloud computing

Cloud computing is one of the hottest trends in the IT industry today. Referred to as 'a game-changer' in analysts' articles, cloud technology gives organisations the opportunity to enhance collaboration, agility, scaling and availability while providing them with some exceptional levers for cost reduction through optimised and efficient computing.

Although most organisations have already adopted cloud computing or are in the process of moving to cloud solutions, others are still reluctant to take the plunge. A Deloitte survey on cloud adoption in Europe[1] revealed that for a panel of CIOs who have not yet adopted cloud computing, the main inhibitors are the following:

- Insufficient data security and risk of data availability
- Open compliance and legal issues
- The risk of losing governance or control over data

Another recent survey revealed that 78% of IT managers considered that the lack of trust in security was the biggest barrier to the adoption of cloud technologies.

Security concerns are driven by the perception that holding data in a third-party data centre means compromising security, control and access. Indeed, many organisations are highly concerned by security breaches that could result in their data being lost or stolen, reputation damaged, or worse, a security breach that would allow competitors to gain access to highly sensitive information. Consolidating huge amounts of data within large public clouds is also perceived as creating a massive point of failure in the event of a communication breakdown (impairing data availability) or espionage activities such as the recent PRISM programme revelations (a clandestine mass electronic surveillance data mining programme created by the NSA - US National Security Agency).

In this context, organisations are seeking reassurance regarding the ability of cloud computing to provide an effectively secure controlled environment and thus ensuring that moving applications and information into cloud computing services is safe.

[1] *Deloitte - Cloud Adoption Study - Cloud computing is gaining momentum – October 2011*
https://www.deloitte.com/assets/Dcom-Global/Local%20Assets/Documents/TMT/dttl_tmt_CloudAdoption%20SurveyDeloitte_CIONet.pdf

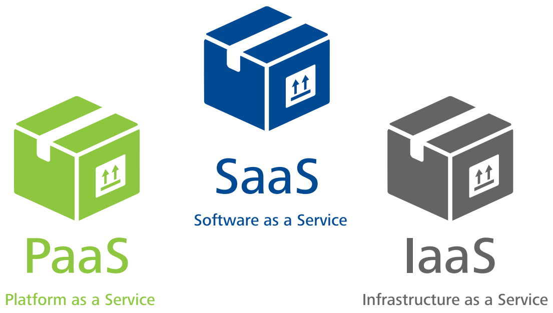
There is no single security approach that fits for all forms of cloud computing

There are actually several forms of cloud computing. Each offers different characteristics, varying degrees of flexibility, different collaborative opportunities and, of course, different risks. As a consequence, it is fundamental to understand each form and each deployment model with their respective characteristics, in order to accurately assess the risk and the security landscape surrounding cloud computing services. The three fundamental cloud computing classifications are often referred to as the 'SPI model', where SPI refers to Software, Platform and Infrastructure (as a Service), respectively.

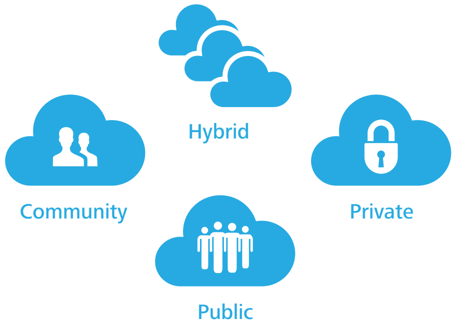
Regardless of the service model utilised (SaaS, PaaS or IaaS), there are four deployment models for cloud services:

- Public cloud: the cloud infrastructure is made available to the general public or a large industry group and is owned by an organisation selling cloud services
- Private cloud: the cloud infrastructure is operated solely for a single organisation. It may be managed by the organisation itself or by a third party and may be located on-premises or off-premises
- Community cloud: the cloud infrastructure is shared by several organisations and supports a specific community that has shared concerns
- Hybrid cloud: the cloud infrastructure is a combination of two or more clouds (private, community or public)

Delivery Models



Deployment Models



With so many different cloud deployment options including public vs. private deployments, internal vs. external hosting and various hybrid permutations, no single security approach and no list of security controls can cover all circumstances. Each combination of deployments and hosting options carries its own risk considerations, including threats, ability to respond and jurisdictional requirements. For example, the 'private cloud/off-premises' combination is protected from mixed use, but carries risks that could lead third-party providers to access confidential data.

As a consequence, when an organisation considers moving to cloud computing technology and Software as a Service (SaaS), a risk-based approach has to be adopted in order to determine (i) the deployment model and hosting option best suited to the organisation's risk tolerance and then (ii) the detailed security control requirements that will have to be implemented in the context of the selected deployment model.

Adopt a risk-based approach for identifying which deployment models fit with your risk tolerance

When moving to cloud computing technology and SaaS, an organisation should adopt a risk-based approach to evaluate initial cloud risks and to identify the most suitable cloud deployment models:

- Identify the asset for the cloud deployment: the first step in evaluating risk for the cloud is to determine exactly which data or applications are being considered.
- Evaluate the asset: this step consists in determining how important the data or application is to the organisation. Essentially, it means assessing confidentiality, integrity and availability requirements for the assets and how the risk changes if all or part of the asset is handled in the cloud. At least, a rough assessment has to be carried out by asking the following questions:
  - Are there any sensitive data that should not be placed into the cloud (at this time)? For example, should client names, private asset information, health information, personal data, etc. be placed in the cloud? What regulatory restrictions exist (e.g. CSSF requirements on IT outsourcing for financial institutions in Luxembourg)? Any of these items could be deal breakers that prevent the use of cloud resources.
  - Are there any applications that provide a competitive advantage (which would be lost) if a 'generic' version of that application was provided in the cloud? While there is certainly the allure of using cloud applications for many tasks (e.g. customer relationship management) consideration should be given to how those cloud applications would interface with on-premise applications that are a source of competitive advantage.

- Map the asset to potential cloud deployment models: once an organisation has an understanding of the asset's importance, the next step consists is determining which deployment models the organisation is comfortable with.
  Just as a critical application might be too important or critical to move to a public provider, there might be no reason to select a private and in-premises deployment model including extensive security controls to host low-value data and non-critical applications. Before looking at potential providers, an organisation should know if it can accept the risks implicit to the various models: private, public, community or hybrid as well as hosting scenarios: internal, external or combined.
- Evaluate potential deployment models and cloud providers: in this step, the focus is on the degree of control the organisation will have at each layer to implement risk mitigation, as well as any other specific requirements.

Once all these steps have been completed, the organisation should be able to understand the importance of what is considered for moving to the cloud, what the risk tolerance is, and which combinations of deployment models are acceptable. This should give sufficient terms of reference to determine the required control framework that will have to be implemented and negotiated with the cloud provider.

Determine security control requirements adapted to your specific cloud deployment options

Numerous Information Security standards and compliance frameworks are well established and have matured over the last decade - ISO/IEC 27002, NIST SP 800-53 or PCI DSS, to name a few. Standardised security controls frameworks specific to cloud computing have also been defined, the most established being the cloud controls matrix from the Cloud Security Alliance[2].
These control frameworks offer the advantage of providing an exhaustive inventory of all possible security requirements that could apply to cloud computing, but on the other hand, not all cloud models and all deployment options need every possible security control.
Once again, a risk-based approach has to be deployed by the cloud subscriber in order to 'pick and choose' relevant security requirements based on (i) the specific risks inherent in its cloud model and deployment options and (ii) the potential exposure specific to its case.

Organisations will undoubtedly face complexities and challenges when it comes to (i) identifying risks inherent in their specific cloud deployment options and (ii) determining roles and responsibilities between the cloud subscriber and cloud provider. Fortunately, some cloud computing risk assessment frameworks exist, thanks to public and governmental initiatives (e.g. 'Cloud Computing - Benefits, risks and recommendations for information security' from ENISA[3]) as well as private initiatives (e.g. Deloitte's Cloud Computing Risk Intelligence Toolbox).

Cloud computing is one of the hottest trends in the IT industry today

[2] *Cloud Security Alliance (CSA) is a not-for-profit organisation with a mission to 'promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing'. Deloitte is a corporate member of CSA*

[3] *The European Network and Information Security Agency (ENISA) is an agency of the European Union created in 2004 by EU Regulation No. 460/2004. The objective of ENISA is to improve network and information security in the European Union*

The following is an example of control requirements (including responsibilities between the cloud subscriber and the cloud provider) identified for an organisation moving to SaaS:

Security Components	Security requirements (not exhaustive – for illustrative purpose)	
	Cloud subscriber	Cloud provider
IDENTITY AND ACCESS MANAGEMENT (IAM)	• Select an IAM solution based on current and anticipated access control requirements • Secure authorisation and mature role-based access control life cycles	• Drive access control solutions that align with customer contract requirements and in support of several regulatory requirements for customers • Least privileged access enabled and followed
CYBER THREAT	• Revise patch and vulnerability assessment policies and standards based on risks • Develop mature security assessments and standards for vendor management	• Establish security monitoring processes in conjunction with vulnerability management program • Implement encryption • Establish application-level code reviews, stringent software development life cycle processes, and provide notification of changes
PRIVACY	• Revise privacy statements and programmes to adjust to the geographic challenges of cloud computing • Define privacy practices and processes	• Develop processes for handling sensitive/privacy-related data with defined acceptable use and data protection processes and standards • Reporting process for unauthorised access
SECURITY OPERATIONS	• Create explicit security operations policies and standards for cloud computing • Consider a policy-based approach for consistently consuming cloud services	• Establish a Security Operation Center (SOC) • Define assessment, reporting and response capabilities • Consider a policy-based approach for consistently managing cloud systems
REGULATORY	• Select a cloud provider/vendor that can support your regulatory requirements • Build a vendor oversight programme to monitor/measure compliance to contract requirements	• Utilise a rationalised security framework based on multiple regulatory requirements to establish controls and processes
RESILIENCY AND AVAILABILITY	• Redefine enterprise continuity of operation policies and standards for data replication and backup • Re-establish availability metrics and standards	• Define processes for replication, failover and reconstitution of services related to disruptions • Reassess availability commitments and confirm testing results for compliance with SLAs
APPLICATION DEVELOPMENT	• Use release and change management policies	• Establish application-level code reviews, stringent SDLC processes, and provide notification of changes and release management • Offer self-service change acceptance processes
ENTERPRISE RESOURCE PLANNING (ERP)	• Establish security policies and standards for ERP management and acceptable data usage • Define acceptable use of modules and databases	• Establish security zones, data protection and access-provisioning processes • Offer strong authentication with single sign-on capabilities based on customer roles

Negotiate security requirements with the cloud provider and define your compliance assurance approach

The lower down the stack the cloud provider stops, the more security the cloud subscriber is tactically responsible for implementing and managing. In other words, in a SaaS model the cloud provider is responsible for implementing and managing most of the required controls. In this context, security controls as well as privacy and compliance are all issues to be dealt with legally in contracts. Like any procurement, selecting a cloud provider involves verifying that the business needs and security requirements are fully addressed in the contractual arrangements.

The cloud subscriber has at its disposal a growing number of mitigation strategies in order to reach an acceptable level of assurance regarding the cloud provider's compliance with agreed security requirements:

- **Contractual protection:** organisations should look to contractual protection to ensure vendors adhere to acceptable practices, as well as manage planned and unplanned terminations.
- **Security audits:** it is increasingly possible to perform security audits of cloud providers to ensure the providers' security policies align with those of the organisations. These audits can involve on-site visits and remote testing and may leverage independent third parties.
- **Security certifications:** providers are increasingly certifying their control environments, using Service Organisation Control reports (i.e. ISAE 3402 reports) or ISO/IEC 27001 security management certifications issued by independent third parties.
- **Leverage standards:** the cloud industry is pushing for standards, with initiatives such as the Cloud Security Alliance. However, consensus remains to be built among the major providers.

Cloud computing: a threat to security but also an opportunity

As explained earlier in this article, the strongest resistance to the adoption of cloud computing relates to data security and risk of data availability. However, compared with in-house data centres, cloud computing is not necessarily less secure. In some cases, it typically improves security because cloud providers are able to devote huge resources to security that many cloud subscribers cannot afford if they have to do it by themselves. All kinds of security measures such as hardware, software, human resources and management costs are cheaper when implemented on a large scale.

With respect to data availability, most cloud providers replicate users' data in multiple locations. This increases data redundancy and protection from system failures and provides a level of disaster recovery. In addition, a cloud provider always has the ability to dynamically reallocate security resources for filtering, traffic shaping or encryption in order to increase support for defensive measures (e.g. against distributed denial-of-service attacks).

As a conclusion, when moving to SaaS/cloud applications, organisations must take due care to ensure that any inherent risks are appropriately mitigated as well as try to benefit from cloud advantages in order to improve security controls and lower costs.

> There is no single security approach that fits for all forms of cloud computing