Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

Public | the way we see it

Trends in Cloud Computing

Secure Journey to the Cloud - a Matter of Control

People matter, results count.

Trends in Cloud Computing

Secure Journey to the Cloud - a Matter of Control

February 2012

The introduction of cloud computing marks a crucial transformation

Everything will change in the years ahead in the field of ICT-based operational management. Civil servants will no longer have computers under their desks, customer-facing counters in government offices will become superfluous or be digitized, data centers will be merged and ICT departments of public authorities and executive agencies will be fully or partly abolished. At the same time, increasing amounts of data stored by public authorities will be made available to citizens and businesses for reuse. Influenced by social media developments, citizens and businesses will demand that the government provides its services through the same channels. This must all take place in a government-guaranteed secure environment.

It is high time for a fresh look at the organization and use of ICT in and by public authorities; and an associated security policy. The necessity of the latter, is clearly demonstrated by the recent developments relating to WikiLeaks and particularly the successful denial-of-service attacks on the websites of various public authorities. Cloud suppliers could have thwarted these attacks if cloud computing had already been implemented.

Cloud computing can only be successfully adopted if traffic can flow securely along the digital highway. Security is, therefore, often a key area of concern in discussions on cloud computing. It is essential that security is well organized in the interest of society as a whole. The question is what actions the government should take in the field of security to guarantee the proper introduction of cloud computing. This paper on the theme of "Secure Journey to the Cloud - a Matter of Control," provides an answer to this question for politicians, administrators, and others dealing with or responsible for implementing cloud solutions in the public sector.

Contents

1 Cloud computing - an irreversible trend

Cloud computing in its various forms

Cloud computing allows smart use of the potential offered by the Internet. Both businesses and public authorities view it as a useful and unstoppable development in information and communication technology (ICT), which modernizes and improves services and operational management. Implementations will succeed only if data, data security and data traffic via the Internet are handled in a careful and well-managed way from day one.

Cloud computing differs conceptually from existing ICT arrangements. A key difference is that users do not have to store information on data carriers such as PCs and USB sticks. That is a major advantage. Surveys reveal that business-sensitive information is held insecurely on hard drives in over 60 percent of workstations and laptops. Business sensitive information is also held in unencrypted form on 66 percent of all USB sticks (www.cloudworks.nu/uploads/cloudworks05.pdf, November 2010).

Cloud computing takes various forms. The best known are social media. Social apps (cloud-based applications) such as Hyves, LinkedIn, and Facebook are used daily by millions of people around the world. Users now store data not on their own PC but somewhere in the cloud. Another example is the increasing use of thin-client computers. These are computers with very limited storage and processing capacity. They provide access to applications and remote storage via a (web) browser. A thin client is, therefore, nothing more than an information viewer that seeks to connect to the World Wide Web. You read your email, download videos or use word-processing applications directly on the Internet. A third concrete example of the impact of cloud computing is the reduction in the number of data centers, as cloud computing enables server capacity to be used more efficiently and only when it is really necessary.

What are the benefits of cloud computing?

Cloud solutions offer innumerable benefits:

- **Joined-up government**
  Government services are increasingly being provided via the Internet, which acts as a virtualized counter for public services. In this way public authorities can be contacted seven days a week, 24 hours a day. Citizens and businesses increasingly expect that. They are also less concerned about the way in which authorities organize themselves behind the computer screen. Whether for a tax return, a licence or benefit application, the customer expects the authority to know who he is and link up the relevant files, thereby keeping the number of transactions to a minimum. This is all possible using the cloud as the basic framework. After all the government services have been interlinked, the next step in the modernization of service provision is the enrichment of the available information via social media, and communication via social media by public authorities, citizens, and businesses.

- **Lower costs/less ICT investment in the workplace**
  Unwieldy computers under or on desks will be replaced by a tiny box that manages traffic via the Internet. The benefits are lower costs in the investment and operational phases for hardware, and licences which are no longer required in the workplace but which can be accessed via the cloud. Also fewer ICT personnel are required on the shop floor to keep computers running. The savings on workplace facilities alone are considerable. For example, the US Federal Government is aiming to achieve savings of more than 60 percent on licence costs for the use of email (source: CIO.gov). The range of tried-and-tested applications and services available in the cloud is growing daily, including for the support of operational management functions (personnel, information, organization, finance, computerization, communication, and accommodation). This substantially reduces the time required to implement new ICT systems. They are no longer built or purchased, but are selected and paid for on a per-use basis on the Internet.

- **Consistent supplier management**
  The introduction of cloud computing enables us to purchase and use ICT resources in a more coordinated and consistent manner. ICT decisions are currently taken across multiple levels and departments within governments. The relationship with business is changing. Public authorities can greatly reduce the number of commercial relationships by signing contracts with partners on the basis of a one-stop-shop model,

using ICT hardware and software, to a large extent, remotely. This model helps governments to concentrate on their core tasks.

- **Consolidation of data centers**
  Data center consolidation significantly reduces costs. The government uses more cloud-based services, and so less capacity is required than in the current situation. It also means ICT can be used more sustainably. The average utilization in cloud solutions is between 60 percent and 70 percent. In on-premise data centers it is still between 10 percent and 15 percent.

- **Economies of scale and security**
  The economies of scale offered by cloud computing allow security and privacy to be managed more effectively than at present. At first sight that may seem illogical, but just think for a moment about the current security situation. Standalone computers in the workplace are often inadequately secured. All kinds of things can happen while they are unattended: for example, data can be read, USB sticks can be copied, and intruders can manipulate software to spy on data or can install viruses. What about passwords? And is it possible to detect data breaches in local data storage? With cloud computing, data does not have to be stored on a data carrier or local PC, and problems such as those described above are prevented. Security, including data encryption, is managed centrally for all users. But even within the cloud environment there is human input, so checks and balances must be set up to keep the risks of human error to a minimum.

Cloud computing requires consistent management

The secure and efficient implementation of cloud computing solutions by ministries and local authorities requires a consistent approach under the overall 'direction' of the central government. The management rules must be clear to prevent everyone reinventing and implementing their own cloud wheel. Security requirements must be supported by all government institutions, otherwise all the benefits will be negated; and chaos and complexity will merely increase. As an illustration, suppose that company X supplies cloud services to 500 government institutions. Those 500 government institutions cannot carry out their own separate annual audits of the solvency, security compliance, privacy, and data controls of company X.

Hence there must be centralized management on several fronts:

- a single client, a uniform schedule of requirements from a demand-focused organization on the basis of consensus among all layers of government;
- a uniform ICT architecture, policy and organization for departments, local authorities, and executive agencies;
- specification of and compliance with available and open standards;
- accessibility of basic registers for use in cloud solutions for government and business;
- establishment and management of the government "App Store" providing cloud solutions;
- international developments/regulations (EU and elsewhere);
- a consistent and effective security policy and clear service level agreements (SLAs) between the government and suppliers of cloud products and services.

The next part of this report deals in greater depth with security policy, the context, risks, and available cloud services. The aim is to provide guidelines for worry-free use of the cloud. In short, a restrictive set of boundary conditions must be established and enforced for public authorities. Ensuring continuity of service is of prime importance. Some people also view this as an integral part of "security".

2 Worry-free use of the cloud

What policy can be formulated?

Cloud computing naturally poses many ICT-related challenges which require constant attention. Many companies (IBM, Microsoft, Intel, among others) have conducted research into the concerns frequently raised by senior business and ICT management. Overall, this research has highlighted the three biggest concerns as follows:

1. security and privacy of data in the cloud (44 percent);
2. availability of cloud services for business processes (41 percent);
3. integration with other services (39 percent).

Proper security arrangements are therefore a top priority!

Why the fear of security issues in the cloud?

Security is seen as the biggest concern. Why? Because the cloud appears to be somewhat "hazy" in terms of security, and the way in which security should be set up to promote business initiatives and comply with regulations. This is mainly because we can no longer point to the room, server or tape that contains our information. Many people instinctively believe that if they can see and touch something they have more control over it. You could liken it to somebody who travels by motorcycle (the least safe means of transport) to the airport in order to board an aircraft (the second safest means of transport). For most people, the fear of an accident when flying is many times greater than when riding a motorcycle, whereas the statistics show precisely the opposite. That is because on a motorcycle you retain control. Whereas in an aircraft you do not.

Now, back to security in the organization: has there ever been an assessment of the current level of security in the organization's own data center or that of the outsourcing partner? They may have an SAS 70 statement and an ISO 27000 certificate, but what do these actually cover and what are the actual risks?

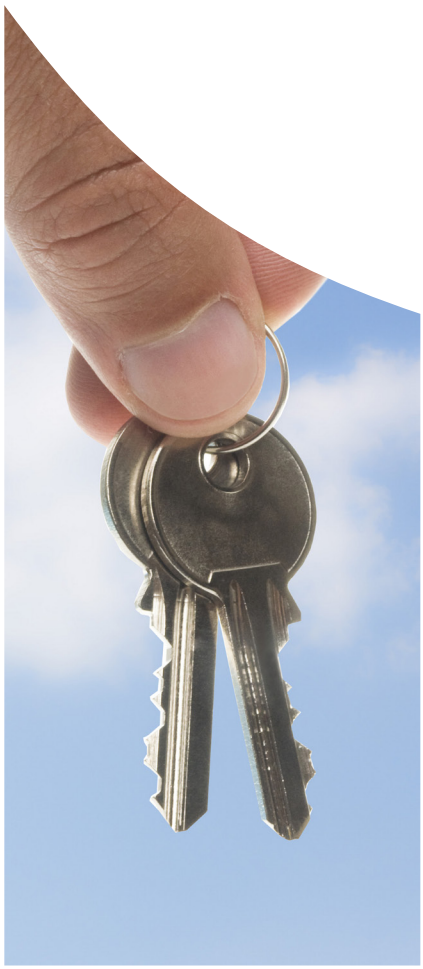
How well secured is your data at present? Do you know who sweeps the server room floor in the evenings after work? Is everything securely under lock and key, both physically and digitally? Cloud architectures require additions and modifications for use in the cloud.

Risk management

The fears surrounding this new cloud phenomenon are understandable, but cloud services can help improve the current level of information security. Increasing numbers of parties are becoming involved; and, as stated previously, human failings are always a possibility. Risks must therefore be managed. The following five points are of great importance in risk management:

1. inventory of information of importance for the government;
2. inventory of possible threats with regard to that information;
3. determining the probability of threats materializing;
4. determining the impact of a materialized threat;
5. determining measures to protect/minimize the impact.

Security is one of the possible measures resulting from point 5.



Towards a new security approach for the cloud

Risk management means striking a balance between opportunities in operational management and financial factors or regulations. It is about enabling flexible services, not limiting new initiatives.
If the government wants to use the cloud successfully without worries, then it needs to develop policy differently with regard to security and control under the influence of changes resulting from economies of scale and standardization. The basic principle is actually very simple. At present, decisions on security matters in many countries are still taken independently at many different points in government. With the introduction of cloud computing, this must take place in a coordinated and coherent way. A central government CIO, for example in the Netherlands, could have a prominent role to play in setting the framework in this regard.

It must also be possible to open up cloud services on the basis of standard protocols, so that information can easily be reused within the government. After all, care must be taken to avoid recreating information silos, this time in the cloud.
A possible means of worry-free migration to the cloud could involve the government developing a migration strategy in which less sensitive ICT services with lower security requirements are examined first. Subsequent levels will then only be tackled if there are adequate results with known learning effects.

Shift of responsibility

When ICT services are moved to the cloud, the government also ceases to be responsible for the implementation of part of the services. It no longer matters to the government how these services are structured in terms of hardware and software, although the government does retain responsibility for functionality, including security requirements. These must be set out in clear SLAs. The central government CIO must specify the framework for this. The government must maintain overall control of the standards that will be used to secure the information. There are various reasons for this:

- the government must prevent the formation of cloud silos, which cannot communicate with each other;
- the government must prevent cloud suppliers setting up their own authentication and authorization systems independently of each other;
- the government must maintain overall control of any encryption used, and in particular the management of keys among cloud suppliers;
- the government must enter into agreements on how cloud suppliers will communicate securely with each other;
- the government must ensure that cloud suppliers fulfil their agreements by monitoring them comprehensively across all suppliers.

Conclusion

Governments should develop a government-wide process and ICT architecture that makes optimum use of the possibilities afforded by modern cloud facilities. They must also draw up and implement measures to maintain the architecture (both within the government and extending to cloud suppliers).

3 The context of cloud security

What are the risks?

The apparent new risks resulting from the use of cloud services appear further-reaching than the security risks associated with conventional client-server infrastructures, such as the risk of loss or theft incurred when physically transporting information on laptops, USB sticks or paper files. Such transportation is no longer necessary when using the cloud, as secure information can be accessed from any location.

The main risks when using cloud services are:

- **Unavailability**
  Whatever the cause, data managed by a cloud service provider would be less readily available than data stored within the organization. If a government organization takes no steps to guarantee the reliability of the cloud, services may become unavailable. That will result in a failure of business processes. An interesting example concerns the recent developments surrounding WikiLeaks. This organization had stored a large number of documents with an American cloud provider. Despite the use of the "safe harbour" model (a model in which the rules and laws of the data owner's country apply rather than those of the US), the US Government was nevertheless able to pull the plug on the organization.

- **Data leaks**
  You do not know who, other than your own employees, has access to your data. After all, it is outside the field of vision and boundaries of your organization. There is a risk that without sufficient access security your data will also be used by criminals or by the administrators of the cloud service. The impact of this type of data leak depends on the type of data stored in the cloud. As far as is known, the recorded cases have always involved an error by a system administrator, for example forgetting to change the default password, thereby allowing other users in those organizations to abuse their access permission. This type of data leak cannot, however, be attributed to the concept of the cloud provider.

- **Privacy breaches**
  Almost all government organizations handle privacy-sensitive data. This type of data must not fall into the wrong hands. Privacy also has to do with the type of information stored and the length of the permitted storage time. These aspects are not specific to the cloud, but it is advantageous to know where privacy-sensitive information is stored in the cloud. The privacy laws applying in Europe differ from those applying elsewhere. Most cloud providers can currently guarantee that information will remain within the EU. It is expected that a number of cloud providers will go a step further, and even give country guarantees. This will depend on the spread of the various cloud data centers and their economic feasibility. In the case of both examples, these guarantees must be legally and technically watertight.

- **Compliance issues**
  Compliance with internal and - more importantly - external regulations sometimes means that organizations need to know the physical location in which their data is stored. Depending on the type of regulation, there may be a requirement to know, for example, precisely who has access to what data, who has carried out particular modifications, etc. Cloud services do not always incorporate functionality to provide clients with such information. Additional logging tools and access controls will be necessary when using cloud services for that type of compliance. It should be stated that a number of suppliers in the cloud are already providing such services.

- **Integration across multiple organizations**
  When government organizations begin transferring services to the cloud, the cloud services must be able to communicate with services still running in the organization's own data centers. They must also be able to integrate with partners in the logistics service chain. Two types of risk are significant. Firstly, on the basis of standards, the cloud service must be able to communicate with other services within and outside the boundaries of the client organization. Secondly, the service must be able to secure this communication to satisfy the requirements of the government organization.

4 The concept of cloud security

Which security aspects have to be fulfilled?

What must government organizations do for a reliable transfer to the cloud based on acceptable risks? They must fulfil a number of basic security aspects, the principles of which are described below.

Protection

A user's information and access rights must be protected against abuse by unauthorized users and intruders. Due to the fact that information and applications are based in the cloud, security measures such as door locks or uniformed security personnel no longer work. The storage, transmission, and use of information must be digitally protected. This can be done using technologies such as PGP, SSL, FTPS, and HTTPS. However, cloud providers choose to go further. Most supplement the existing security measures with specific measures to dispel the cloud user's fears and unfamiliarity with cloud data centers. Data in cloud environments must be protected to an even greater extent than in your own operating environment. Government bodies must of course decide for themselves whether a cloud provider is using sufficient security techniques in the data center. This requires the government to have specific expertise.

The transmission part requires separate attention, addressing aspects such as virtual intrusion (penetration tests have been found to be very useful), theft or compromising of data during transmission (stealing a copy), interception, and sending forged messages. The data center is ultimately just part of the assets and aspects requiring protection.

Privacy

Privacy measures protect personal information in such a way that others cannot access it. Various identity and access management systems support cloud services with a wide range of privacy and security measures. These include low security level with password-based authentication, to high security level with attribute-based authentication systems. The latter systems use state-of-the-art privacy-supporting certificates. Efficient process organization is also important in the event that the authorities raise any questions. For example, what does the provider do if a public prosecutor asks for data? How can the government demonstrate to its citizens and businesses that the provisions of the relevant laws will be upheld?

Recoverability

Data stored in the cloud is subjected to regular integrity tests to guarantee its recoverability. Most cloud service providers replicate data three of four times instead of making real backups. This means they can recover from disk crashes and major disasters. However, most service providers do not guarantee the backup and recovery of data which is "accidentally" deleted by the end-users themselves. A government body must therefore make or arrange its own backups, for example by taking snapshots and downloading and storing these on its own premises or with another cloud provider. Another problem is that data in clouds can be stored indefinitely. Depending on the type of data and the applicable legislation, this may not be permitted. Service providers only process and store data. So, they may have insufficient knowledge of statutory retention periods or mandatory clearances. Public authorities have an important role to play in this regard. Cloud providers can guarantee that information has actually been destroyed, but the owner of the data needs to ensure that the destruction has been initiated. ITIL formulated an appropriate set of processes some years ago for incident and problem management, backup, and recovery. The government must enforce those requirements and have them guaranteed by a TMP. In an SLA, all conditions such as retention time, minimum performance, and storage size can be recorded in a standardized way and verified subsequently by means of standard reports.

Access and reliability

Access to information and the processing of data items must comply with the privileges granted to the user requesting access. Unauthorized access must be prevented. Every user claiming a unique identity when gaining access to data will be subject to a process to investigate whether he is indeed the authentic owner of the claimed identity. After verification, the user may only carry out those actions for which he has been granted permission. Cloud providers have set up facilities for this. There are even providers who offer the possibility, for example, of linking such facilities to an active directory of their customers. An active directory of this kind establishes the authenticity and access rights. These are then managed exclusively by the client organization. The advantage of this is that such information is recorded in only one place and can be used both by the internal information systems and externally by the cloud provider. The authentication and authorization data constitute an application/information system in

their own right. That system must therefore also meet the specified requirements. These concern authentication and authorization for people who are or are not given formal access to the data. Safeguards against unauthorized (criminal or terrorist) access are not yet covered.

Connectivity

Managing the process of access to cloud services through identity authentication and authorization is critical, but there are also other steps once connected to the network. Extract network security may be needed beyond SSL, TLS secure messaging and data transport layers to ensure the actual security of this network.
With the growing public telecommunications infrastructure such as the Internet to connect to cloud services, and the potential for company networks and external non-company networks to be involved in cloud service use, this raises issues of connection security both for mobile employees, and external users outside the company firewall environment. Choices of private networks and the use of technologies such as Virtual Private Networks (VPN) and Virtual Wide Area Networks (VWAN) are increasingly necessary parts of a secure network strategy to underpin the desire for more freedom and mobility. Using secure networks enables remote user access management while enabling encryption of data as a layer to prevent disclosure to unauthorized users.

Yet the virtual private network is also seeing other new cloud consumption models that are reversing previous trends of centralized systems and network management. Bring Your Own Device (BYOD) connectivity and Voice over IP (VoIP) seek to empower users by managing identity and security "on the fly" or dynamically in place of traditional directory control activity. Certification and policy control of applications and data from devices is managed through the federated security of multiple devices outside the corporate firewall. Access is through device policy control, enabling new cloud service models of apps stores and new content delivery channels. The advent of cloud broker services has led to the emergence of a Bring Your Own Policy (BYOP) concept where companies not only have multiple devices, but also control the policies that enable devices to be approved, audited and controlled remotely.
These network topology choices also affect the "last mile logistics" of connecting a user device to the information technology service, whether it be cloud or non-cloud hosted. Connectivity can be fixed-line, or IP address-enabled and delivered through a wireless connection. It also is a key enabler in the idea of hybrid cloud, where data and applications movements between different clouds and host environments can be achieved securely. The security of networks is an essential strategic architecture choice in cloud computing which affects the access, mobility and usage of cloud-enabled business and users.

Accountability and controllability

A full log must be maintained for accountability in respect of data operations. This must record all actions carried out within a user session to allow controllability. What precisely has to be logged must be agreed within your organization. This is technically feasible, but (comparable to the storage and logging of telecom data) can be very expensive. Most cloud providers offer logging and monitoring tools, although some are rather rudimentary. Market participants are responding to this by offering additional logging and monitoring tools.

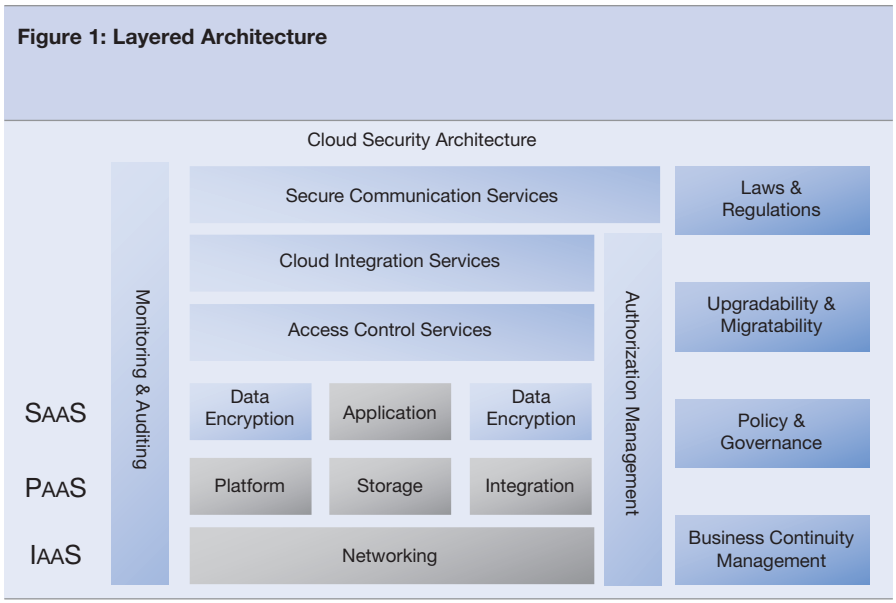
Integrity and irrefutability

Cloud providers must ensure that the integrity of data is protected and that it cannot be modified, duplicated or deleted without authorization, just as in the client's own ICT organization. The long-term irrefutability of digitally signed data is an important aspect of PKI-related standards in clouds. Cloud providers use various mechanisms among themselves to deal with routine events. These could include the expiry of a public-key certificate and the expiry of a time-dependent trusted-authority certificate.

Compliance with regulations

Legal, regulatory, and contractual requirements must be defined for all parts of the information system. Monitoring activities must be planned and laid down in advance in joint consultation between the parties concerned. It is also necessary to conduct regular independent reviews and assessments. Cloud providers must comply with all internal and external regulations, laws, contracts, policy and mandatory standards. Many public cloud providers use the compliance and legislative frameworks of the country in which the respective cloud data center is located. Government organizations can adopt these frameworks or outsource them to a cloud provider that complies with the necessary legal frameworks. This could be an additional task for the government audit service that can opt to keep it in-house or have it outsourced.

Figure 1: Layered Architecture



Insurable

The risks relating to the system must be controlled. Few parties other than the cloud service providers themselves currently offer such financial insurance for cloud services.

Migratable and upgradable

A migration path must exist that is feasible, controllable, and acceptable to users in order to move from an old to a new cloud provider or to a subsequent version. The cloud infrastructure must be easily upgradable to new releases of hardware and software. This may pose a problem for the use of some business functionality, as some business functions are currently available from only one cloud provider. The growth of the cloud market should mean that technology to support every possible business process will become available from multiple sources; and open up the possibility of migration from one cloud service provider to another. In the first place, energy will be focused on migrating from conventional to cloud-oriented ICT services. This will take a number of years. The first migration must also incorporate an exit strategy (back to conventional services), otherwise there may be a feeling of being on a "one-way street", which will be unsettling.

What architecture model can be used?

Cloud security services can be implemented in layers. Figure 1 shows how the various security layers for cloud computing are positioned relative to each other. It is important that the familiar cloud computing variants of Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) are all aligned: these include associated services. The main message in figure 1, from a security architecture perspective, is the distribution of responsibilities. Depending on the type of cloud service in the model, there is a further responsibility relating to management and security aspects. Of course, it is also necessary to fulfill the interoperability of cloud services.

In the case of IaaS, for processing power or storage capacity for example, the service provider may be required to store the data within a country or region, for example in the EU or the Netherlands. This is to comply with legislation on data storage.

In the case of PaaS, the exposure is changed for example for in-house applications or purchased packages, which were initially behind a firewall but which now operate on the cloud infrastructure. Anyone with an Internet connection can now access them. Therefore, more attention needs to be paid to whether the access to data via the application or directly to the database is properly secured. PaaS gives a third party the possibility of hosting its own software on a particular platform made available by a provider (perhaps a standard application with adjustable parameters). Some providers may also handle the application management tasks.

In the case of SaaS, there are other matters of importance. Each SaaS supplier must be able to fulfil the compliance rules applicable to government institutions.

In each cloud service (IaaS, PaaS or SaaS) the compliance, management, and security aspects must be assessed. A gap analysis can be carried out showing what is required and what is present. It is also possible to determine how these characteristics relate to the insurance and protection requirements of the respective information components. This answers the question of which data and which functionality can be accommodated in which location.

5 Cloud security services

What cloud services are available on the market?

Figure 1 identifies the main security services in the different layers of cloud environments. These services and their operation within the cloud environment are described below.

Data encryption services

Most people believe that the cloud services in the market provide a lower level of security than their own data center. The question is whether this is an accurate observation. In many cases the cloud service provider will have a higher level of security than most data centers and outsourcing providers. There are two possible reasons for this. First, cloud service providers take a standardized, general approach to security. Moreover, they simply cannot afford to lose customers as a result of deficient security. A single newspaper report about a serious data leak could mean the end of a cloud provider, particularly if it involves data that government institutions are legally required to keep under surveillance. Cloud providers are therefore focused on information security from day one. It is their most important priority.

How do you know your provider has implemented the right level of security measures? If there is insufficient control of the system in which the data is stored, it is necessary to ensure that the security of the data itself is controlled. By using data encryption and retaining control of encryption key management, organizations can take full advantage of cloud computing. They need have no concern about whether their data is stored somewhere in their own country or abroad. It is also necessary to look at the security of the connections: this is a specialist area that must be addressed separately.

Authorization management services

Authorization management services ensure that the right user accounts with the right information are available in the relevant systems. If that is not properly implemented, access control will be a mere illusion. All accounts, including administrative accounts, must always be related to individuals in order to prevent abuse. The first step is, therefore, to manage the entire life cycle of accounts related to individuals (employees, partners, customers, etc.). This must include the functional accounts (for example, administrators) that are linked to these identities at any given time. Identity and authorization management is liable to be a complex matter within the organization.

Outside the boundaries of the organization, however, such as in ecosystems, supply-chain channels or cloud services, identity and authorization management is essential for operational management. Applications can be moved to the cloud, but control of authorizations must remain within the client organization. This does not mean, however, that the actual identity and authorization management cannot be carried out in the cloud; on the contrary, Identity-as-a-Service can be very useful in the outsourcing of identity management and the facilitation of a model such as e-Recognition as implemented in the Netherlands, which enables users to log into various government institutions through their own account. Always be aware that combining cloud services and

cloud security services in the same cloud will only be effective if the cloud service provider can effectively guarantee functional separation.

Access control services

Authorization management may then be a requirement, but if access control measures fail to operate effectively, your data will be unprotected without your being aware of it. If the access control is too tight, however, operational management may be impeded. Access control measures must ensure a balance between practicability and security, and must be based on the relevant risks. Another important aspect is the integration of access control measures in your data center, your outsourcing partner's data center and the cloud applications used. Single sign-on (SSO) across the boundaries of the organization and relationships of trust between organizations are essential for the successful use of cloud services.

Cloud integration services

People generally speak of "the" cloud. However, it is unlikely that there will be a single cloud containing all the organization's applications. Some office applications may be obtained from Google, for example, whereas the CRM is with Salesforce.com. The security services may in turn be supplied by a dedicated security provider. This not only means that all employees must have access to all these services from any location, but also that cloud services must have access to each other's network for specific services. Consideration must also be given to where brokers and other generic ICT services will be accommodated, such as the enterprise service bus (ESB) or print servers. At present, we appear to be creating the same islands or 'stove pipes' that we have been trying to get away from in our own data centers in the last ten years. All these services must be integrated in a secure and controllable way. The cloud services must communicate with standard protocols for web services in order to achieve genuinely secure cloud integration.

Communication security services

Cloud services - and hence data belonging to citizens and businesses - may be located anywhere and transmitted frequently via the Internet. During transmission, the data must be secured by standard protocols. Encryption is also an option, but it is too complex to store all data in encrypted form. It will probably only be necessary to store business- or privacy-sensitive data in encrypted form. The rest must nevertheless be protected during transmission via the Internet. This can be achieved by means of standard protocols such as SSL/TLS. Network traffic can be protected by PKI based protocols. Even more important than traffic to end-users is traffic between service providers. This must also be encrypted, but you will probably not own the keys used, which means you will incur a risk when services of different service providers are integrated. You must at least ensure that this risk is known. You can discuss ways of mitigating this risk with your service provider.

Monitoring and auditing services

If security levels are not being measured, it will be difficult to assess the status and quality of these security levels. It is important to have access to monitoring and auditing services,

either in-house or with a cloud service provider, where all the information from the client data center, the outsourcing provider, and the cloud services provider will be gathered for further processing. This solution must be able to receive log files from all systems in order to process security warnings from all systems.

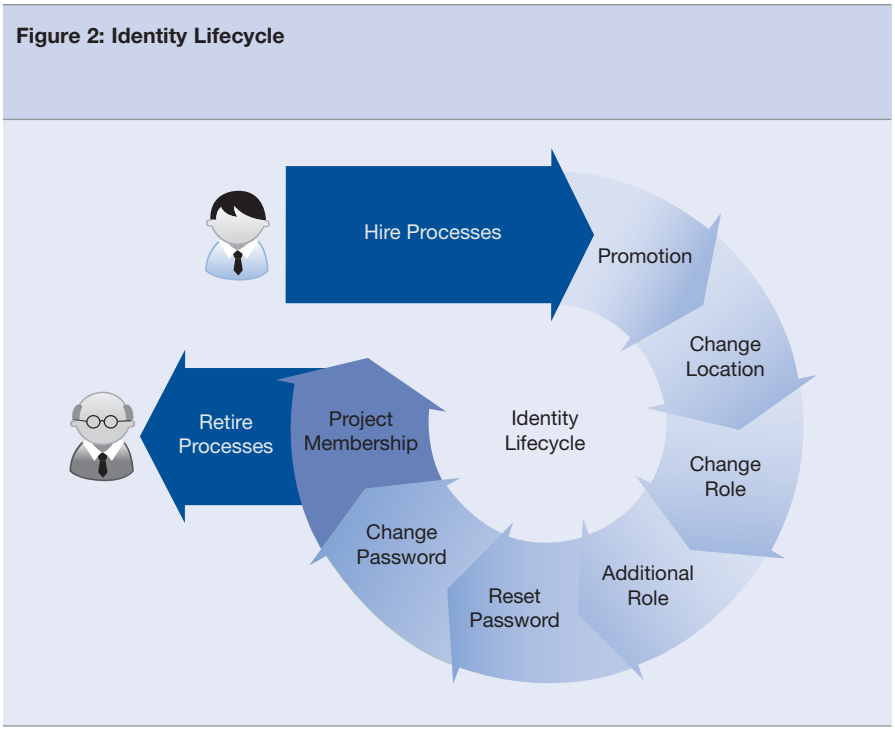
This is a labor-intensive process requiring people with very specific skills to analyse the results. It is, therefore, advisable to also use this service in the cloud, with all other cloud and non-cloud services being connected.

Business continuity service

Business continuity management (BCM) is an important area of attention for all government organizations. The drawing up of detailed emergency plans for unforeseen disasters, such as denial-of-service attacks on government websites, is essential nowadays. In the ICT sector, that means backups of business critical data must be available at different locations.

Cloud service providers such as Google, Microsoft, and Amazon are very useful in this regard. They promise 99.9 percent uptime and their services release organizations from the burden of creating and maintaining a backup infrastructure and recovery facilities. BCM incorporates various complementary elements, such as disaster recovery, business recovery, business resumption, contingency planning, and crisis management. However, disaster recovery alone is not sufficient. A mechanism must exist to recover this data automatically even if small quantities of data or specific documents are deleted, accidentally or otherwise.

Figure 2: Identity Lifecycle



The business continuity service must at least perform the following:

- identify threats and the associated potential business impact;
- determine the requirements for business continuity and recovery;
- assess the current possibilities;
- design, implement, and test a business continuity plan based on business objectives.

www.nl.capgemini.com/expertise/publicaties/a-secure-start-in-cloud-computing.

6 Conclusions and recommendations

Cloud computing in its various forms

Cloud computing is an important trend in the field of information provision and related ICT. It turns computer processing power and data storage into a utility for collective use, as has long been the case of gas, water, and electricity. The rise of cloud computing has been particularly strong, is set to continue, and is irreversible. In view of the advantages for government organizations, cloud computing should also be trusted and supported within the public sector, both at central and local government levels and within executive agencies.

The actions required in order to migrate securely and carefully to the cloud can be summarized as follows:

1. formulating a clear security policy including security requirements;
2. organizing the management among the government organizations and market participants concerned;
3. acquiring the required expertise in the field of cloud computing and demand management;
4. international coordination for the exchange of knowledge and experience.

It is important that all government institutions cooperate consistently with each other. Security requirements must be supported by all government institutions. Otherwise all the benefits will be negated and, chaos will result. Overall management of the formulation and implementation of the security policy must be guaranteed.

The public services provided by the government, with ICT as an enabler, extend beyond the boundaries of ministries and local governments. This applies particularly to the use of applications offered by cloud computing.

The authority to decide on and implement cloud computing models must therefore cut across departmental boundaries. Cloud computing is too complex and too generic to assess risks, develop security concepts, and select services individually in each government body. The security requirements should be translated into a clear SLA. Every government institution must nevertheless carry out an additional risk analysis to ascertain whether all generic risks also apply to them, and whether they need to be supplemented with specific risk areas and additional measures.

Cooperation is important. The challenges involved in adopting cloud services, and the scale of the potential risks and benefits demand that risk assessments, security frameworks and service selections be elaborated on a pan-governmental basis.

Governments must also align their security and privacy policy regulations to the new reality, coordinate them effectively with those of the other EU member states, and test them against those of non-EU states. That will prevent unauthorized reading of data and breaches of privacy rules.

About Capgemini

With around 120,000 people in 40 countries, Capgemini is one of the world's foremost providers of consulting, technology and outsourcing services. The Group reported 2011 global revenues of EUR 9.7 billion. Together with its clients, Capgemini creates and delivers business and technology solutions that fit their needs and drive the results they want.

A deeply multicultural organization, Capgemini has developed its own way of working, the Collaborative Business Experience™, and draws on Rightshore®, its worldwide delivery model.

Learn more about us at
www.capgemini.com

Contact

Zsolt Szabo: zsolt.szabo@capgemini.com
Hans F. Scholten: hans.scholten@capgemini.com
Pieter Hörchner: pieter.hörchner@capgemini.com
Mark Skilton: mark.skilton@capgemini.com
Email: publicsector.global@capgemini.com

IN/1B-052.11a

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

www.capgemini.com