Security and the cloud

Guidelines for navigating the path to secure cloud adoption

Many organizations recognize the benefits of adopting cloud services, but many have stalled or failed to progress to implementation, due to poor planning and inadequate analysis of the security challenges associated with the cloud.

Furthermore, cloud providers are often unable to clearly articulate the level of security protection offered, leaving potential adopters confused about where the responsibility for basic security controls exists.

The purpose of this paper is to discuss the security controls that organizations should consider prior to adopting cloud- based services. Security can help to control the risks of cloud, while enabling the organization to reap the rewards associated with it. In this paper, we outline the steps required for a secure and logical progression toward cloud service adoption.

The journey to secure cloud adoption

1. Understand your business strategy

The cloud presents a variety of business benefits, from speed of service establishment to reduced cost of design and delivery; however, it does not provide a one-size-fits-all solution and presents some risks which are different to traditional IT systems, as well as some that are common.

Before you consider the cloud, you need to understand your business strategy and goals for using this resource. How will it be incorporated into your other IT services? What value will the cloud provide to the business? What is the value and criticality of the services, applications and data that you plan to host in the cloud? And, most importantly, what level of risk are you prepared to accept for the services, applications and data to be delivered from the cloud? Organizations must carefully consider and articulate what the business reasons are for moving to the cloud, before building the strategy to get there.

A sound understanding of the business drivers for cloud adoption is the first step in creating a high-level cloud road map. To ensure informed decision making when selecting the services to be delivered in the cloud, IT needs to be aligned to and support the strategic business vision and organizational goals. Understanding your business strategy also helps you begin to define the base level security controls you expect from your Cloud Service Provider (CSP) and any additional security controls the organization may need to meet the business requirements enabling cloud adoption.

2. Determining the assets to be migrated to the cloud

Knowing and understanding which information assets your organization plans to move in to the cloud is critical, because this will define the impact on the business if those assets are unavailable, lost, stolen or disclosed without proper authorization. An organization must evaluate the information or process and determine the value and importance to the business, so that they can ensure the appropriate security controls are in place to protect the information.

For processes or applications that could be migrated to the cloud, organizations should develop an understanding of whether or not these are critical to the business. By this, we mean that if the process or application cannot be accessed, how significant the impact on the business would be. Interdependencies between business processes should also be considered.

Business criticality:

This includes intellectual property, formulas, patents, blueprints, trade secrets or any information that the organization is highly dependent on.

Sensitive information:

This includes data such as personally identifiable or financial information such as bank account or credit card data.

The table below highlights the potential business impact on information assets that should be taken into account:

Business impact

Type	Unavailability	Loss	Theft	Disclosure
Information	• Disruption of business operations. • Lack of resources to maintain business as usual.	• Disruption of business operations. • Required activation of backup restore procedures (DRP). • Financial loss associated with recovery efforts. • Impact of legal implications should a breach occur.	• Business competitive disadvantage. • Significant reputational damage.	• Damage to the organization's reputation or image. • Possibility of regulatory sanctions or fines. • Financial impact.
Process / Application	• Disruption of business operations. • Lack of resources, skills or understanding to maintain business as usual.		• Greater risk or threat of more selective attacks to information	

Figure 1: Significance of the impact on the business if the process or application cannot be accessed

Cloud service and deployment models

A variety of cloud service and deployment models exist, and organizations must ensure they carefully consider the benefits and limitations of each. Informed decisions can then be made about the right route to follow to adopt cloud services.

Cloud service models
Three main cloud service models exist, each requiring a different level of involvement from the CSP:

- **Infrastructure as a Service (IaaS)**
  IaaS provides a complete IT infrastructure delivered as a service. Users pay for the computing power consumed over time and the service includes applications, hardware, storage etc. IaaS provides a computing model that is relatively easy and cost effective to set up and that can expand across all areas of IT in response to business demands.
- **Platforms as a Service (PaaS)**
  PaaS provides infrastructures and platforms on which cloud users deploy their own applications. It enables companies to develop applications using the resources of a third-party cloud provider, thereby reducing the cost of application development and enabling development costs to be more easily attributed to specific application projects.
- **Software as a Service (SaaS)**
  SaaS is the delivery of an application via a third-party application service provider. This enables organizations to pay for these enterprise applications as an operational expenditure rather than capital investment in hardware, operating systems and application licenses, and storage and data centre costs.
- **Cloud deployment models**
  Sometimes referred to as cloud structures, the following main cloud deployment models exist:
- **Private cloud**
  The infrastructure is used only by one company and can be deployed on the company's site or is delivered by a cloud provider using dedicated infrastructure.
- **Public cloud**
  The infrastructure is available to the general public or a large industry group and is provided and hosted by the cloud provider.
- **Hybrid cloud**
  The infrastructure is composed of both public and private cloud structures and may move between these according to performance demands, the time of day, or specific events requiring unusual computing demands.
- **Community cloud**
  There is an option for like-minded organizations to share infrastructure in a community cloud. This enables organizations of a similar nature – e.g. government or banking – to leverage savings similar to public cloud. This includes initiatives such as G-Cloud, which is used for government departments only.

Security considerations

Security of the CSP
A key requirement of choosing the services to be delivered by a CSP relates to your risk appetite and the security controls you need in place to support that risk. You need to determine whether the security controls offered by the CSP support your business risks or whether additional security controls must be incorporated – either by the provider, or implemented by your organization as part of the deployment. A formalized and consistent approach should be taken to conduct a CSP security assessment, which includes a review of essentials such as:

- security governance
- privacy considerations
- compliance
- legal
- multi-tenancy
- incident management
- service termination

Security governance
Security governance is vital to ensuring the effective management and mitigation of information security risk, both for organizations considering cloud adoption and the CSPs delivering the service. Both should have documented a clearly defined and aligned governance framework to ensure information security is managed appropriately throughout the service lifecycle. Without adequate governance in place, organizations and CSPs will not be aware of the specific security requirements necessary to mitigate any risks associated with infrastructure, applications or data used in the cloud. The following questions at a minimum need to be answered:

- Who is accountable for ensuring the security of confidential or sensitive information stored in the cloud?
- How will security be managed throughout the full supply chain – including for third parties that have access to confidential or sensitive information?
- Has the business engaged with cloud-based services in an attempt to implement new solutions quickly and cheaply, but without engaging either the corporate IT department or security team, bypassing security controls and creating unknown risks as a result?

Privacy considerations
Personally identifiable and sensitive information is often stored in the cloud and is usually considered the most valuable by hackers. Managing the protection of such data in the cloud is more complicated than it is in the standard on-premise IT system. Two main challenges are:

- loss of control over information
- reliance on the CSP

If sensitive corporate information is to be stored within the cloud, the organization must consider additional controls to appropriately protect it. Controls to consider as a minimum are:

- Data sovereignty requirements and where the data will reside.
- Data encryption.
- Two-factor authentication.
- Privileged identity management controls.

Compliance
Due to the number of potential unknown elements associated with the cloud, such as who can access the information or which security controls have been implemented, the adoption of cloud services can increase and complicate the challenge of compliance with standards such ISO or PCI DSS certification.
To enable secure cloud adoption, the organization must outline how the controls needed to meet compliance standards are met by the cloud service, and be able to demonstrate ongoing risk management in support of those controls.

Legal
Due to the nature of the cloud, laws, regulations and other mandates may exist that limit or prevent certain types of information or business functions from being moved to the cloud. Organizations must take time to consider the legal aspects associated with cloud adoption and seek appropriate counsel to identify any applicable legal requirements that must be addressed. Laws impose information security requirements on organizations, and organizations that adopt cloud services may face a variety of challenges if these requirements are not considered and addressed in advance.

Examples include:

- The location where the CSP stores an organization's data may have legal implications, due to cross-boundary issues with regulations such as data protection legislation.
- Lack of understanding of which data protection acts apply to the information a company puts in the cloud.
- Information ownership and control issues such as: Who owns the data in the cloud? Can the CSP use the data for its own purposes, or sell the data on? What happens if the CSP goes bankrupt?
- Some national laws grant the government the right to access any data held by companies registered in that country.
- Are contracts, cloud service agreements and SLAs well defined and do they cover exactly which security standards the CSP should implement, rights to audit and liabilities in the event of a data breach?
- If the CSP has to provide evidence to law enforcement authorities, how does that impact your sensitive corporate information or systems?

Multi-tenancy and isolation failure
Multi-tenancy cloud services can deliver a variety of business benefits, including cost savings and easy scalability. However, there are a number of factors that should be considered prior to adopting this type of cloud service:

- Your information may be being stored on the same physical servers or databases that are used to deliver services to a competitor.
- Are the services you are sharing infrastructure with attracting additional attention from potential hackers or experiencing increased denial of service attempts?
- Are sufficient controls in place to safeguard against the potential for human error, or to restrict access to customer data?
- How does the CSP store client data? Is all the data stored on one database, or are different databases used and protected by separate encryption keys?

Security incident management
Given the number of high-profile security breaches in recent years – including Target, Amazon and Sony – it is clear that it is not a question of whether an organization will have a security incident, it is more a case of when and how it will occur. Weaknesses or gaps in security controls within the cloud can lead to a myriad of problems, from security incidents not being discovered, to reputational damage or loss of revenue.

Organizations must ensure they are prepared and have a plan in place for how they will manage such incidents while minimizing damage to the organization. Effective security incident management requires a proactive approach to avoid common issues such as lack of defined roles, responsibilities and accountability of those involved in managing incidents, gaps existing in the incident handling process, or under resourced staff with insufficient training.

Terminating cloud services
Any organization that transfers services or data to a CSP must consider how it will exit from the service. To achieve this,

there must be a well-defined exit strategy in place to protect against scenarios such as the CSP going bankrupt. This is an area which many companies overlook, and which could lead to serious business disruptions or complicated legal disputes. Consideration should be given to:

- Data retention for legal purposes such as litigation e-discovery or preservation as evidence upon law enforcement request.
- How and when will data be returned upon contract termination?
- How long after termination will the CSP delete a client's data, possibly rendering it irrecoverable?
- When a customer terminates the contract, what obligations does the CSP have to assist with the transition?
- What assurance is there that once a CPS deletes client data, it cannot be recovered?

Security in the public cloud is a partnership between cloud provider and customer

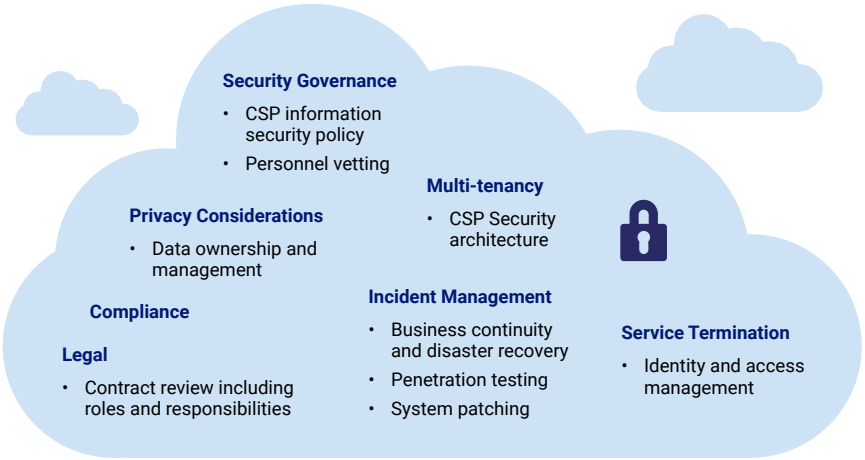

Figure 2: Security of the Cloud Service Provider – a formal and consistent approach should be used to conduct a CSP security assessment, which includes a review of the elements below. This will determine whether the security controls offered by the CSP support your business risks or if additional security controls must be incorporated.

Working with NTT: answering cloud security concerns to deliver real business benefits

Our customers ask us for independent advice on moving to the cloud and choosing the right cloud partner for the business. Faced with a demand for cloud adoption to increase the agility of its supply chain and enhance collaboration with its extensive network of partners, one global manufacturing customer needed a secure way to adopt multiple cloud-based services. We worked with the customer to create cloud adoption checklists and risk assessments with a specific focus on data, increased cloud solution architecture focus and assessed the cloud-readiness of internal applications, as well as increasing virtualization as a step toward cloud.

The customer's CTO valued our help in understanding the increased need for due diligence. Understanding what data the organization had and its location was essential to balance privacy and performance in the cloud.

Outsourcing is now an accepted model for numerous business activities, but cloud computing requires significant trust between customer and CSP. Security is rightly a major concern, but you, rather than your CSP, should be defining service levels – and any service should be an extension of your current security policy, maintaining existing levels of confidentiality, integrity and availability.

Disclaimer: The work described in this whitepaper was performed while the company was known as NTT Security.


NTT