National Cyber Security Centre
Ministry of Justice and Security

5 recommendations for securely purchasing cloud services

Factsheet FS-2020-06 | version 1.0 | 16 October 2020

Many organisations are either considering or in the process of purchasing cloud services. Cloud services can serve as a major functional addition for organisations, although this does require balanced measures to be taken during their purchase. In practice, organisations regularly fail to purchase cloud services securely, leading to uncontrollable risks. Many of these risks can be mitigated subsequent to the purchase. However some measures are only effective if taken in advance. The NCSC-NL recommends only purchasing cloud services after five measures have been taken, by conducting or ensuring: (1) risk analysis, (2) configuration and monitoring, (3) an exit strategy, (4) functional management and (5) audit access.

Background

Public cloud services are popular, with people, but also increasingly with organisations. Major cloud service providers, such as Microsoft and Amazon, offer cloud variants for an increasing number of commonly used applications. These cloudservices offer greater scalability and may also help to cut costs. As a result, many organisations are considering emigrating functionality from on-premise environments to cloud environments, or are already in the process of doing so.

In this factsheet, 'public cloud services' are understood to include IaaS, PaaS and SaaS. Examples are Amazon EC2 (laaS), Microsoft Windows Azure (PaaS) and Microsoft Office 365 (SaaS). The recommendations described pertain to all types of cloud services.

What is the situation?

Cloud services offer many attractive functionalities compared to on-premise environments. In order to use these services as securely as possible, their purchase needs to be well-considered. In practiceorganisations make insecure purchases. For example, if employees are unaware of the sensitivity of the data they are working with, there is a risk of sensitive data unintentionally being stored in cloud environments. If in such a case no additional measures are taken, the organisation will be running an increased risk of security incidents such as data breaches or laws being infringed. Employees often also fail to establish which tasks a cloud service provider does and does not perform. They forget to contract out responsibilities such as backup, monitoring and authorisation management, which can later lead to major problems.

Target audience

Employees involved in cloud purchasing

The following parties have contributed to this factsheet

- Government Chief Information Officer
- Conclusion
- DNB
- Netherlands National Communications Security Agency
 (General Intelligence and Security Service)
- Schuberg Philis
- Strategic Suppliers Management Microsoft Google AWS Dutch government

Such a situation is the result of organisations not adhering to existing rules – not the lack of rules. There are multiple guidelines, standards and assessment frameworks[1] concerning outsourcing risks related to cloud services. In practice, organisations regularly fail to adopt these, or only do so in part. There are various reasons for this. Implementing all sorts of measures can make the outsourcing more expensive, for example. In addition, specific knowledge of cloud services is required in order to securely purchase and use such services.

What are the risks?

When an organisation outsources functionality (e.g. storage or processing) to cloud service providers in insufficiently secure fashion, this creates risks. Some of these risks can be mitigated by taking measures after the fact. Yet some measures will only be effective if they are taken in advance.

Most cloud service providers offer options for effective authorisation and access management. If purchasing organisations avail themselves of these to an insufficient extent, it could easily be the case that many employees have complete access to all data. This can have major consequences, for example for an organisation's ability to adhere to relevant legislation and regulations. If logging and monitoring is not adequate, it might subsequently prove impossible to determine who accessed which data; the only possible conclusion is that no one knows what happened to the data in the interim.

Many cloud services are easy to implement, yet may prove difficult to leave, since the service provider of course has an interest in keeping customers on board. This risk is referred to as 'vendor lock-in'. If you fail to include the option of easily leaving the service in contractual terms, you will no longer have this option after the fact. In that case, a migration process can end up being very complex or expensive.

When organisations purchase cloud services, they often fail to make agreements with the service provider on the application of standards and access to audit information. Such agreements are nearly impossible to make at a later juncture. This creates the risk that an organisation lacks insight into the security level of the cloud service provider. It might be the case that, as a result, an organisation will not be adhering to legislation and regulations (such as the General Data Protection Regulation), and is unable to manage risks.

What does the NCSC-NL recommends?

The NCSC-NL recommends mitigating the risks of cloud purchasing by taking the measures outlined below in advance. These measures mitigate the risks that will be nearly impossible to mitigate once an agreement has been concluded.

The listed measures are primarily organisational, administrative and legal in nature. It makes a great difference for such aspects in particular, whether or not you address them in advance. During the selection stage, you can establish which suppliers allow you to suitably implement these measures, and when negotiating the contract, you can lay down certain provisions from a legal perspective. Once an agreement has been concluded, it is often difficult, if not impossible, to implement these measures. This applies less strictly to technical measures. Although early

[1] Examples of organisations that have issued guidelines and frameworks are CISPE, ENISA, SANS, CSA, DHPA and the Dutch government. Examples of frameworks are ISO 27010, CSA, SOC2, C5 and G-CLOUD.

application will also lead to a higher security level where technical measures are concerned, in the event of a hasty purchase, these can often be addressed after the fact.

This list of measures is not exhaustive. First, there are many other measures you can take in order to securely outsource to the cloud. Second, your organisation may have additional interests and security needs when functionality is outsourced to a cloud services provider. The NCSC-NL therefore advises using existing purchasing standards and guidelines for cloud purchasing, based on risk management and legislation and regulations. This will allow you to effectively manage the risks of cloud outsourcing, including after the initial purchase.

The NCSC-NL has published a cloud experience document describing how the NCSC-NL itself deals with safeguarding its interests when outsourcing to the cloud[2].

Action perspective

Make someone in your organisation responsible for the cloud service being purchased and have them conduct a risk analysis.

For each cloud service, conduct a risk analysis with regard to privacy, compliance, security and financing. Outsourcing to cloud service providers creates both advantages and new risks.

The risk analysis will allow you to decide what data you will migrate to the cloud service. Operate under the assumption that the cloud service provider will be able to access the data. There are multiple assessment frameworks that can help you decide what data you should to migrate to a cloud service. Also involve professionals with knowledge of cloud services, such as security architects, in the risk analysis.

Outsourcing to a cloud service provider also entails risks related to privacy and compliance. Many organisations choose to outsource due to the convenience it entails, but should incidents occur, supervisory authorities and the public will hold you responsible. Modern legislation and regulations often consider you responsible to at least some extent for the data processing you outsource.

More information on conducting a risk analysis can be found in the NCSC-NL factsheet entitled Risk management: the value of information as point of departures[3]. The NCSC-NL can assist organisations from its target group in conducting risk analyses.

When conducting a risk analysis, you should also outline a cloud assessment, which sets out the requirements that a cloud service being purchased should meet. Verify regularly – annually for example – whether the cloud services you are purchasing still meet the requirements. This is necessary due to the fact that the nature of your cloud service or of the way you use it may change over time.

Clearly allocate responsibilities related to configuration between the cloud service provider and your organisation, and establish monitoring.

Security incidents in cloud environments are often the result of misconfiguration on the user side; for example, if functional managers fail to shield data storage sufficiently, this could lead to data breaches. Due to the open nature of many cloud services, stored information

[2] See https://www.ncsc.nl/actueel/nieuws/2020/juni/11/clouddiensten. (only in Dutch)

[3] See https://english.ncsc.nl/publications/factsheets/2020/september/15/factsheet-risk-management-the-value-of-information-as-point-of-departure.

could even end up being accessible to any internet user. This means that it is necessary to adopt suitable configuration processes of the service in question, prior to migrating data to cloud services.

Organisations that outsource remain primarily responsible for a secure configuration, so describe in the configuration process who is managing configurations and how you will be detecting misconfigurations. Cloud service providers regularly offer scanning tools to check customer configurations. In addition, in your contract, you can agree with a cloud service provider that you would like a third party to check the configuration with a penetration test. Such tests allow you to detect misconfigurations prior to migrating your data to the cloud service.

Determine your exit strategy and include this in the contract.

You may one day decide that you no longer wish to use a cloud service. In that case, you will want to migrate your data, preferably with as few additional costs involved as possible. To that end, make agreements in the service contract on options for migrating your data elsewhere. If the data's specific format is important for you, also include this in the service contract. Organisations often choose to have their applications deeply integrated into the cloud services they use. Decide in advance whether you want to integrate applications. One risk is that migrating to another cloud service becomes difficult or impossible. Would this pose a major risk to your organisation? In that case, select software that can operate independently from a platform as far as possible.

There are standards and service providers that can help you switch cloud service providers. SWIPO (Switching Providers and Porting Data)[4], for example, is a European initiative that has developed codes of conduct for switching between cloud service providers more easily. Cloud service providers can commit to these codes of conduct in order to show their customers that they can migrate their data with ease.

Align your functional management with the cloud service, and take suitable measures for authentication and authorisation.

Although using a cloud service may have security advantages, it also enables new types of misuse to take place. For example, not using a strict access policy in a cloud environment, can leads to data breaches. This could, for instance, mean that all employees have access to all the information and functionalities.

Introduce highly specific access management when you implement a cloud service, such as RBAC-based or ABAC-based identity and access management[5]. Create a policy describing who has access to which data and functionalities in the cloud service. As part of this policy, restrict the access of accounts to a minimum by default, and grant increased rights on a temporary basis. Request your functional managers to apply this policy and to monitor it.

The previous recommendation can be implemented in various ways. For example, you could use two-factor authentication for all the accounts. Or you can grant access to data and functionalities only when necessary. This is also referred as ‘least privilege’. If you would like to use your own resources for identity and access management, arrange for this in the contract. Your functional managers can apply and monitor these measures, which could also entail doing so with special software for cloud environments for this purpose. Cloud service

[4] See https://swipo.eu/.

[5] RBAC stands for Role-based access control, ABAC stands for Attribute-based access control.

providers can, for example, provide various automated tools that will test settings in light of the security policy.

Reach agreements to gain effective audit information about your cloud service provider.

Reach an agreement with your cloud service provider on how you can use audits to gain insight into the quality of the service on offer. In nearly all cases, independent audit access is restricted or impossible. In that case, you will be dependent on third-party audits. The reports made by these parties can provide a certain degree of certainty, referred to as the *assurance level*.

If you include this in the contract, it will often be possible to provide input when your cloud service provider has a third party conduct an audit. This could mean having the issues that are paramount to your organisation addressed specifically. Ensure that you are able to provide such questions and process the resulting reports, for example in a specialised process.

Before conducting these conversations, you will have to be clear on which norms and standards are important to your organisation. You will often be able to reach agreements with a cloud service provider on popular standards such as DPA, SOC2 or ISO 27017. The same applies to the location where your data is processed and stored. Various framework agreements have been concluded with cloud service providers for Dutch government organisations. Such framework agreements could help your organisation in concluding an agreement with one of these cloud service providers.

Publication
National Cyber Security Centre (NCSC)
Postbox 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

More information
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

October 2020