Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence,
Civil Protection and Sport DDPS

National Cyber Security Centre NCSC
Analysis and Prevention

2 May 2025

Technology brief: Cloud computing and cybersecurity

1 Introduction and background

'The cloud' or 'cloud computing' is often described as a paradigm shift, i.e. something new that operates according to a different set of rules. As a result, discussing cybersecurity in the context of cloud solutions can be challenging. This is evident in many projects, such as deciding whether to use cloud services or enhancing the security of existing cloud-based solutions.

This document aims to equip IT managers and decision-makers in businesses, authorities, and educational institutions with the foundational knowledge required to navigate this situation more effectively. The first section provides an in-depth exploration of the concept of 'the cloud', clarifying its meaning, the reasons behind the wide variation in cloud solutions, and the cybersecurity challenges of using cloud-based services. It also argues that cloud computing is not a new paradigm, but rather a way of outsourcing IT.

The second section builds on this by outlining a concrete approach that decision-makers can use to assess and select (cloud) service providers.

This document does not aim to present specific cybersecurity solution architectures based on cloud services. This work takes place after the decision has been made to adopt a cloud service or procure a cloud-based solution, during the planning and development of the system.

1.1 History

The history of cloud computing is fascinating and dates back further than many realise. As early as the 1950s, IBM started exploring the concept of distributing data and tasks across multiple computers. Then, in the 1960s, John McCarthy – a pioneer in computer science – proposed that computing power and applications could be provided like public utilities. These early ideas formed the basis of what we now know as cloud computing.

In the 1970s, Intel launched the first microprocessors, paving the way for the development of personal computers. The 1980s saw the introduction of PCs and the rise of the client–server model, which enabled organisations to offer IT services to users via internal networks. As the internet became more widespread in the 1990s, companies such as Amazon and Google started to lay the foundations for modern cloud services. The term 'cloud computing' emerged in the 2000s when, in 2006, Amazon Web Services (AWS) started offering scalable IT resources over the internet. In the 2010s, cloud services became more sophisticated and diverse, with major players such as Microsoft, Google and IBM entering the market.

As cloud computing grew in popularity, security concerns became more prevalent. Organisations began to worry about the security of their data stored in the cloud, since they

no longer had complete control over the underlying infrastructure. Concerns about compliance with data protection regulations were also growing.

In the 2010s, a wide range of cloud security solutions emerged. These solutions aimed to strengthen trust in cloud computing by offering features such as data encryption, access control and monitoring.

1.2 Cloud computing

The meaning of the terms 'cloud' and 'cloud computing' has broadened significantly in recent years and become somewhat blurred – partly due to the terms' use in marketing. In order to have a meaningful conversation about cybersecurity in the cloud, we first need to define what is meant by 'the cloud'. In addition, any discussion of security must take into account the specific cloud services being used. Many of the terms used in cloud computing may sound familiar, but are often poorly defined. To provide clarity, the following sections offer an overview and clear definitions of key cloud computing concepts – including cloud service models (IaaS, PaaS and SaaS) and deployment types (private, public and hybrid clouds).

With any type of cloud service, customers must relinquish at least some degree of physical control over their data and services to a third party. This means cloud providers are always in a supplier relationship with their customers.

To avoid any misunderstandings, this technology brief will try to avoid vague phrases such as 'in the cloud' or 'moving to the cloud'. Instead, the following terms are used:

- **Cloud provider**: A company that offers (and operates) cloud services.
- **Cloud services and solutions**: Services and solutions that meet the defining characteristics of cloud computing (see 1.2.1).
- **Cloud computing**: The umbrella term covering all cloud services.

1.2.1 Core characteristics

Cloud computing is a model that provides access to IT resources and services via a network. Instead of purchasing and maintaining their own hardware and software, organisations and private individuals can rent these resources from a cloud provider and use them as needed.

The following five core characteristics are taken from the definition of cloud computing [1] by the US National Institute of Standards and Technology (NIST) and are widely recognised and accepted.

- **On-demand self-service**: Users can access the required cloud services at any time, preferably via a self-service portal or application program interface (API), without needing manual intervention from the cloud provider.[1]
- **Resource pooling**: The provider’s network, storage, and processing resources are pooled and dynamically allocated to multiple users, enabling efficient use of these resources.
- **Rapid scalability**: Resources can be scaled quickly and automatically to respond to changing needs.
- **Measurability**: Resource usage is continuously monitored and measured, allowing for transparent billing and optimisation.

[1] In larger companies and in the Federal Administration, this characteristic is not always available when services are being procured for the first time. While the cloud provider may offer a self-service portal, procurement processes do not always permit its use.

- **Access via the internet**: Cloud accounts can be managed online.[2] There is a distinction between the management environment (the network used to operate and administer services) and the system environment (the environment in which systems such as servers run and data is stored). The system environment does not have to be accessible via the internet.

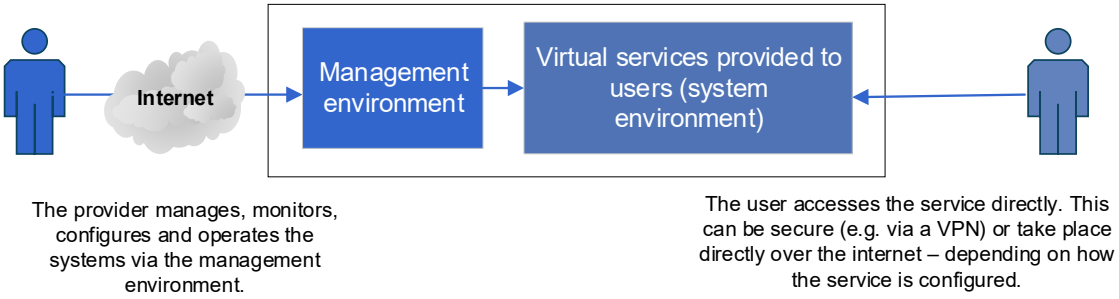

Figure1: Use case diagram – Management and system environments in cloud services

A public cloud service is only considered as such if the provider fulfils (at least) these five core characteristics.[3]

1.2.2 Services

Cloud services differ in terms of the type of service provided – and these can, of course, be combined:

1. Data storage: The main service is storing data.
2. Computing power: The main service is providing processing capacity.
3. Network: The main service is making data available efficiently over the internet, enabling fast access regardless of geographical location.

1.2.3 Cloud service models

In cloud computing, there are several cloud service models that give the customer more or less control over how they use the services. This also leads to different expectations regarding the responsibilities of the cloud provider versus the customer. The three main cloud service models are:

- **Infrastructure-as-a-Service (IaaS)**: The cloud provider supplies basic IT resources, such as computing power, storage, and networking. Customers can configure virtual networks, servers, and storage themselves. With IaaS, the infrastructure is operated by third parties under contract. Customers are responsible for running servers, databases, applications and other services.
- **Platform-as-a-Service (PaaS)**: The cloud provider offers a platform on which applications can be developed, deployed, and operated. With PaaS, the platform is operated by third parties under contract. Customers are responsible for running their own applications.

[2] The NIST definition refers only to 'broad network access' and does not mention management access specifically. However, with cloud services, it is typically the management access that is available via the internet. Whether the virtual resources supplied by the cloud provider are also accessible via the internet is up to the customer. More on this in section 1.2.4.

[3] Another characteristic often associated with cloud services is the use of modern development and operational methods, as well as task automation. However, this is not unique to cloud services and is more indicative of a modern working approach as opposed to a traditional one.

- **Software-as-a-Service (SaaS)**: The cloud provider enables access to software applications over the internet without the need for local installation. In this model, software solutions are operated by third parties under contract.

In addition to these three basic models, there are also hybrid forms. M365, for example, provides familiar Office applications as a SaaS solution and also includes a management, authentication and deployment/development platform for custom applications (PowerTools).

Although SaaS is considered part of cloud computing, this distinction is less relevant to organisations purchasing a SaaS solution in terms of cybersecurity and resilience. In this case, customers need not concern themselves with the technical aspects of cloud technologies per se, but rather with managing IT suppliers and handling IT outsourcing.[4]

1.2.4 Deployment types

Cloud services can be categorised into three deployment types:

- **Public cloud**: Access to the management environment used to administer cloud services is provided via the public internet. The infrastructure is shared by multiple customers (also called 'tenants'). Each customer can use and modify their own data, and decide who has access to it. The system environment is only publicly accessible if the customer explicitly allows it.
- **Private cloud**: Cloud services are provided for a closed group of organisations, offering greater control. This is typically achieved by running the services on dedicated hardware for the organisation. This can be either on-premises ('on prem', i.e. at the organisation's own premises) or hosted by the cloud provider. As a rule, the management environment is not accessible from the internet.[5] If the hardware is hosted by the cloud provider, access to the management environment is provided via a secure connection.[6]
- **Hybrid cloud**: This deployment type combines public and private cloud environments, taking advantage of both deployment types. This approach can be applied to an organisation's overall infrastructure – for example, one server might run in a private environment and another in a public one.

[4] This naturally includes questions around data backup and ensuring business continuity in the event of a provider outage.

[5] While the term public cloud is relatively well defined and generally understood correctly, the same is not true for private cloud. Many providers – unhelpfully – use the term simply to refer to environments hosted on their own servers, rather than using the services of a large provider such as Amazon, Google or Microsoft. From the perspective of the National Cyber Security Centre (NCSC), a cloud environment can only be considered private if access to the management interface is restricted.

[6] Technologies such as leased lines, direct peering, SD-WAN, VPN, and explicitly enforced access restrictions (often referred to as conditional access), as well as other similar solutions, are all possible.

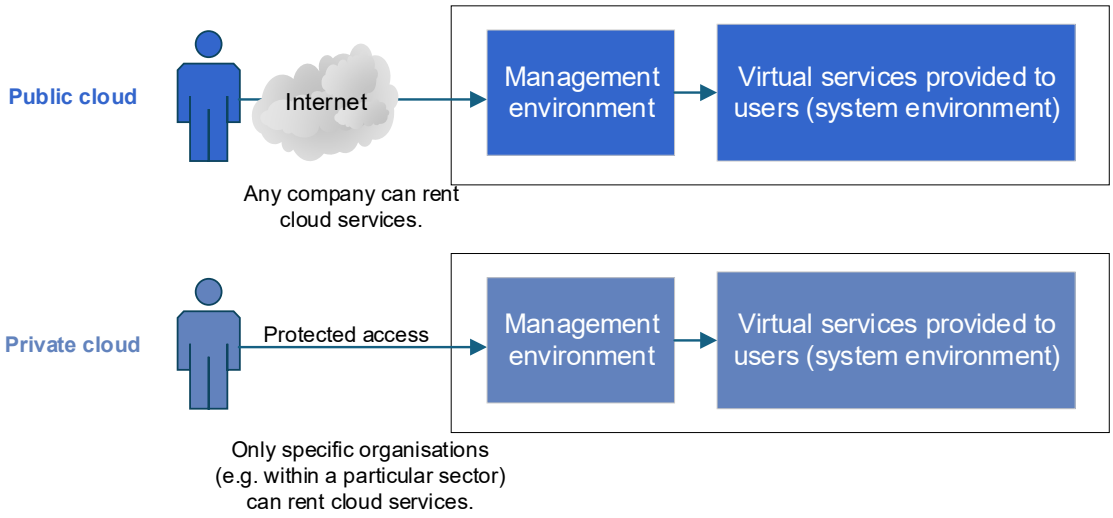

Figure 2: A distinction is made between public and private clouds from both a technical perspective and the point of view of the National Cyber Security Centre.

It is not always possible to clearly determine whether a public or private environment is being used, since hybrid forms are also possible. For this reason, deployment types play only a secondary role in determining the suitability of a cloud service. From a cybersecurity perspective, the key issue is reducing the attack surface, which is already more limited in a private environment.

1.2.5 Not all clouds are the same

As discussed above, not all clouds are the same. The following table provides examples to illustrate this. The decision to use services from a cloud provider should be made in the context of the intended applications. Therefore, it is not a matter of deciding in favour of or against cloud services in general, but rather of assessing whether a specific cloud service is the right choice for the target architecture of a project or organisation.[7]

Cloud service models	Services	Deployment type	Example
Infrastructure-as-a-Service (IaaS)	Data storage	Public cloud	Configurable online storage solutions such as Amazon S3, Google Bucket or Azure Blob
	Data storage	Private cloud	Configurable and scalable on-prem storage solutions such as NetApp SAN
	Computing power	Public cloud	Virtual servers such as Amazon EC2, Azure VM or Google Compute Engine
	Network	Public cloud	Network solutions such as AWS NAT Gateway, Azure WAF or Google Cloud Firewall
Platform-as-a-Service (PaaS)	Computing power	Public cloud	Kubernetes services such as Amazon EKS, Azure AKS, Google GKE; or serverless services such as AWS Lambda or Azure Functions
	Network	Public cloud	Minimally configurable network services such as Google Cloud Armor for DDoS protection
	All	Public cloud	Application development and runtime

[7] This perspective clarifies the term 'cloud' as a paradigm shift for IT services.

			platforms such as Microsoft Power Tools or Google AppSheet
Software-as-a-Service (SaaS)	Computing power	Public cloud	Grid computing or services such as AWS Quantum Computing Service
	Data storage	Public cloud	Online storage services such as Dropbox, Google Drive or Microsoft OneDrive
	All	Public cloud	Applications such as Microsoft 365, SAP S/4HANA, ChatGPT, DeepL or Miro

Table 1: Examples of various cloud services.

1.3 Cybersecurity when using cloud services

In addition to being a matter of supplier management, the use of cloud services presents a number of broader challenges due to the characteristics of cloud computing and its service and deployment types:

- With cloud solutions, data is no longer under the sole control of the organisation. If there are issues with network connectivity or the service provider, access to information and services may be temporarily, or even permanently, lost.
- Solutions are now available for the cryptographic protection of data stored and transmitted between customers and the cloud provider. However, the major challenge is the cryptographic protection of data that is being processed (i.e. located in the processor). This is an active area of research (e.g. 'fully homomorphic encryption': a type of encryption that allows encrypted data to be processed without first being decrypted). As no practical solution currently exists, efforts are being made to achieve a similar result using specialised hardware (confidential computing).
- Key management is another major concern, as cloud services typically handle decryption and therefore manage the keys themselves. Solutions in which encryption and decryption take place on the client side are rare.[8] Combined with resource pooling, this means that if an attacker gains access to the key infrastructure, they could potentially access data from many customers.[9]
- In traditional network architectures, the management area is isolated and accessible only through secure interfaces, networks, or terminals. With public cloud services, however, access is typically open to anyone with the right credentials – if these credentials (for example, an API key) are stolen, misconfigured, or if vulnerabilities are found in the cloud service, the entire infrastructure may be at risk. This presents an additional challenge, as unauthorised users may also be able to delete or alter logs and backups, especially if they are stored in the same cloud account.
- Misconfigurations can also lead to the unintended exposure of data stored in the cloud. This makes monitoring and the ability to respond quickly essential, particularly compared to environments that are not exposed to the internet. This kind of monitoring (often referred to as 'observability') is fundamentally more complex and demanding in cloud environments.
- While not a direct security issue, cost is also an important consideration. Security solutions in the cloud usually incur extra costs that often increase in line with the number of users. For larger organisations, this can mean that cloud services are more expensive than maintaining their own infrastructure. And for smaller

[8] Also called Hold Your Own Key (HYOK).

[9] For example Storm-0588's attack on the Microsoft environment: https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/

organisations with tight budgets, this may result in necessary security measures being overlooked.

2 Cybersecurity considerations when using cloud services

Since cloud computing usually involves outsourcing IT, it is important to carefully assess and select suppliers, subcontractors and providers to ensure secure operations. These decisions form the first phase of the implementation process. The second phase involves planning, developing and deploying the cloud solution. The third phase involves integrating cloud services into the organisation's ongoing supplier management process.[10]

We identify three key steps for the decision-making stage (phase one), which are outlined in more detail in the following sections:

1. Check that the cloud provider can meet the legal requirements (see section 2.1).
2. Check that the technical and organisational requirements for secure and resilient operation can be met (see section 2.2).
3. Based on the outcome of the above checks, and considering key factors such as availability, the impact of data loss and your organisation's IT capabilities, assess whether using a cloud service is the right choice (see the questions in section 2.3).

2.1 Legal requirements

The legal requirements depend on the legal status and location of the cloud provider, as well as the type of data being processed. The following points should be reviewed, and, depending on the organisation, additional sector-specific requirements or guidelines may also need to be considered.

1. If an organisation transfers data to a cloud provider for processing and/or storage, a **contract** must be in place between the parties that defines their respective rights and obligations.[11] The organisation must assess whether legal or contractual confidentiality obligations, such as professional or official secrecy, could prevent such a contract. If so, the organisation must ensure that the cloud provider is capable of fulfilling these confidentiality obligations through prior due diligence. The provider must strictly regulate and control employee access to the systems. In the case of data subject to professional or official secrecy, only explicitly authorised personnel may access such data.[12]
2. If personal data is transferred to the cloud provider for processing and/or storage, a **data processing agreement** (**DPA)**) must be concluded. Under the relevant data protection laws, the organisation remains the controller while the cloud provider acts as the processor. The cloud provider may only process data on behalf of the organisation if it does so in a manner that the organisation itself would be permitted to, and provided that no legal or contractual confidentiality obligations prohibit the outsourcing of data processing. Organisations must, in particular, ensure that the cloud provider can guarantee data security.
3. If processing personal data could pose a high risk to the personal or fundamental rights of the people concerned, the organisation must assess whether a **data protection impact assessment** needs to be carried out in advance, in accordance with applicable data protection legislation.

[10] See also: Cybersecurity in the supply chain
National Cyber Security Centre NCSC (2024) [2].

[11] See also: Supplier Agreement: Best Practices in [2].

[12] Art. 320 and Art. 321 of the Swiss Criminal Code (SCC)

4. Personal data may be transferred to a cloud provider **abroad** if the country in question guarantees adequate data protection.[13] If this is not the case, the transfer is still permitted – but only if appropriate safeguards are in place. These could include international agreements, special contractual clauses, guarantees from a federal authority, standard contractual clauses approved by the Federal Data Protection and Information Commissioner (FDPIC) or binding internal data protection rules.

2.2 Technical and organisational requirements

Cloud service customers must plan for the possibility of the service becoming unavailable (point A), while also trusting that the provider implements the agreed technical and organisational safeguards. Building this trust requires transparency on the part of the provider (points B to E). All requirements are described in such a way that customers can assess them independently, without having to rely solely on the provider's assurances:

A. **Contingency planning and offline backups:** As part of contingency planning, organisations should be able to export and save their data from the cloud service. This export should also be stored offline as a backup (providing protection against ransomware). There should also be an exit strategy in place to ensure that switching providers is possible at any time without data loss.[14]

B. **Transparency of security measures:** The cloud provider must document how it implements basic security measures to protect data in a transparent manner. These include:

    1. Data transmission between the organisation and the cloud provider must always be encrypted (using up-to-date protocols, such as the latest version of TLS, a VPN or an encrypted SD-WAN).
    2. The provider must offer access control mechanisms on a need-to-know basis, and every access request must be authenticated. Authentication must, by default, use multi-factor authentication (MFA). Granting access to employees, partners, suppliers or customers of the organisation must be easy and intuitive.[15]
    3. Access to cloud services and cloud-based applications, including management access, must be monitored and protected against denial-of-service (DoS) attacks (e.g. flooding the application with requests) and brute-force login attempts (e.g. rapidly testing large numbers of login combinations).
    4. Key management must be documented and comply with current best practices.
    5. Because misconfigurations can quickly lead to data exposure on the internet, there must be a service in place that can detect, alert on, and ideally automatically fix configuration errors.

C. **Access transparency**: Administrators in the organisation must be able to monitor and track all access to and processing of data. This also applies to access by the cloud provider's suppliers and partners. All access and processing activities must be logged, and ideally included in offline backups, so that traceability is not lost in the event of a compromise at the cloud provider.

D. **Product security**: The cloud provider must clearly disclose the methods used to ensure the secure development of its cloud services.

[13] See the list of countries here: https://www.fedlex.admin.ch/eli/cc/2022/568/en#annex_1

[14] For example, you might plan a switch to another provider in advance, but only carry it out if the need actually arises.

[15] If access rights are difficult to manage, errors will quickly occur, so a simple, user-friendly interface is essential.

E. **Incident and vulnerability reporting**: The provider must have a process in place to ensure that any relevant incidents or vulnerabilities are reported to the customer in good time. The cloud provider must publicly release patches and updates to its services and provide a way to report security-related incidents and vulnerabilities.[16]

2.3 Key questions for assessing the use of cloud services

These questions are intended to support decision-making regarding the use of cloud services, highlighting potential risks that must be addressed. This section does not cover detailed solution architectures to be implemented after this decision.

Question 1 – *Requirements*: Can the legal, organisational, or technical requirements be met (see sections 2.1 and 2.2)?

If the cloud solution doesn't meet the legal requirements, it must be ruled out.

Caution is advised if the technical or organisational requirements cannot be met, for example because data cannot be exported (which would prevent proper contingency planning) or because the provider does not offer the minimum required security features or lacks transparency in its security documentation. These risks must be carefully considered, as the basic conditions for trusting the provider are not in place. In particular, when processing personal data, this would mean that the required level of data security could not be guaranteed.

If none of the assessed cloud solutions can meet these requirements, a solution based on the organisation's own infrastructure (on-premises or hosted) should be preferred.

Question 2 – *Continuous availability*: Does the cloud solution need to be available at all times to keep our operations running?

This is an important question because a key characteristic of cloud services is that access depends on internet availability. For example, if a patient information system is provided via the internet but must be continuously available, alternative solutions must be in place in case the cloud infrastructure becomes unavailable. A stable and uninterrupted internet connection must also be ensured.

Question 3 – *Data loss*: How serious would the consequences of data loss be?

If data loss would have serious consequences for the organisation itself or for individuals whose data is being processed (e.g. court records), the organisation must be able to create an offline backup of the data.

If unauthorised access to or publication of this data would have serious consequences (e.g. a breach of confidentiality), the use of cloud solutions is not recommended, as uncertainty remains about who may be able to access the data. However, if the organisation still plans to use a cloud service, the data must be strongly encrypted and this risk must be explicitly addressed during the design and development of the system.

Question 4 – *Organisational (IT) capabilities*: Are we able to implement the necessary internal security measures?

If capabilities are limited, outsourcing to a cloud provider can be risky. Using cloud services (particularly IaaS solutions) requires a higher level of IT maturity, since operating and monitoring these solutions is more complex than managing systems in-house. For SaaS solutions, however, the key issue is having a viable contingency plan in case the cloud provider becomes unavailable. This kind of contingency planning could also be handled by another IT outsourcing partner – but doing so increases costs and the workload of supplier management, and this should be carefully weighed against the benefits.

[16] This can be implemented via a publicly accessible *security.txt* file, as defined in RFC 9116.

3 References

[1] Mell, P.; Grance, T. *The NIST Definition of Cloud Computing - NIST SP 800-145* National Institute of Standards and Technology (2011), accessed 2 May 2025, https://csrc.nist.gov/publications/detail/sp/800-145/final

[2] *Cybersecurity in the supply chain* National Cyber Security Centre NCSC (2024), accessed on 2 May 2025, https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-unternehmen/aktuelle-themen/lieferkette.html