Federal Office
for Information Security

Secure use of cloud services

Step by step from the strategy to the expiration of the contract

Federal Office for Information Security
Post Box 20 03 63
D-53133 Bonn
Phone: +49 22899 9582-666
E-Mail: cloudsecurity@bsi.bund.de
Internet: https://www.bsi.bund.de/EN/Cloud

Table of Contents

Introduction

Cloud computing is no longer just hype, cloud computing has become reality. And it fundamentally changes the way in which IT services are provided and used. This document presupposes that the potential cloud user has dealt with cloud computing and sees the potential of using it in the own organisation.

This publication serves as an aid to organisations, as companies and government agencies are referred to collectively in this document, on the path to the secure use of cloud services. It is applicable

- to **each deployment model** (private cloud, community cloud, public cloud, hybrid cloud [03]),
- to **each service model** (infrastructure as a service (IaaS), platform as a service (PaaS), software as a service (SaaS) or other models (XaaS)) and
- to **normal and high protection requirements** [04].

It describes the path through all phases: from the strategy to the termination of use of a cloud service. This description is based on the IT-Grundschutz module "Cloud usage" which, in turn, is based on the IT-Grundschutz methodology [4]. This document, however, is complete in itself so that specific detailed knowledge of IT-Grundschutz and its methods is not required to be able to understand and apply it.

BSI defined a level for security requirements in the Cloud Computing Compliance Controls Catalogue C5 that should be met by all cloud service provider in combination with the required verification. This is included in the present version of the document.

IT-Grundschutz: Baustein B 1.17 Cloud-Nutzung [04]
BSI Cloud Computing Compliance Controls Catalogue C5 [02]

Here, the following target groups are addressed:

- Persons responsible and employees in cloud usage project groups
- IT security officers
- Responsible IT persons
- Decision-makers (management)

The path to secure cloud usage described in this document can and should be adapted depending on the type and scope of the cloud service.

What is a secure cloud?

The BSI is often asked what a secure cloud would be. The reply is often unsatisfactory for the questioner, as they desire more specific statements. If we apply the question by analogy to a car, the reason for this is clear.

Assuming that a popular standard-size car is considered to be a safe car: Why are various different assistance systems installed in top-class model to increase safety? Would racers use a standard-size model to drive on the racing track? Definitely not, since neither they nor the car would be likely to survive an accident at a speed of 180 km/h. For high-ranking politicians or business representatives, a standard-size car would not be a safe car either. Questions concerning bulletproof window panes, fire-extinguishing and oxygen equipment inside the car etc. would have to be answered in the negative. Single people and families also have different requirements regarding the safety of the car.

When buying cars, a certain safety level is assigned to car categories (small cars, standard-size cars, SUVs) or car brands.

Furthermore, there are legal regulations (e.g. for air bags) which, however, only define lower limits. Crash test results and the experiences of others complete our picture with regard to safety. And, all things considered, money plays an important role, as safety will also have to be financed and not everything which is desirable can also be implemented.

This means: Just as there is no one and only safe car for all situations, there is no one and only secure cloud for all purposes. Like for a car, for the cloud you also have to ask for which purposes it is to be used in each case. For the respective purposes, suitable security safeguards can be found.

However, the security requirements are not use either if the provider does not comply with the security targets and regulations during operation.

Therefore, the goal is:

Secure cloud computing and not a secure cloud, as there is no secure cloud.

1 Threats when using cloud services

With regard to the topic of information security, it must be clarified which information and processes have to be protected and which threats fended off. This also applies to cloud computing without any restrictions. The confidentiality, integrity and availability of information must be protected – these are the so-called basic values of information security.

Users of a cloud service are exposed to (external) threats to the cloud infrastructure and when introducing and using the cloud.

1.1 Threats for the cloud infrastructure and the cloud service

The infrastructure and the cloud services of the cloud provider must be protected by the latter against the following threats

- Data loss and/or leakage of information
- Manipulation of different users in the shared cloud infrastructure up to attacks from the cloud.
- Failure of the Internet or network connection, making it impossible to access data and/or applications.
- Denial-of-service attacks on cloud providers, which will certainly increase.
- Errors in the cloud administration which may cause significant security problems (service failure, loss of data, etc.) due to the very high complexity. Small errors or accidents may have substantial impacts in a cloud infrastructure (not only on security).

1.2 Threats when using cloud services

The cloud user is exposed to the following threats in particular:

- Identity theft and/or misuse of accounts
- Loss of control for data and applications control
- Violation of applicable specifications and policies (e.g. data protection requirements)
- Security of the end-points with which the cloud services are used.
- Data can be intercepted on the network and spied out (in case of poor or lack of encryption).

The non-profit organisation Cloud Security Alliance (CSA) issues an annually updated list of the most important threats [05].

Chapter 4 of the report of the ENISA (European Union Agency for Network and Information Security) “Cloud computing – Benefits, risks and information security” (Rev. B, December 2012) provides a good overview of risks related to cloud computing, going beyond merely referring to attacks [06].

1.3 Threats when introducing and using the cloud

The threats mentioned above arise if the cloud service is offered and used. On the path to the cloud too, further dangers are lurking for cloud users.

- There is no cloud strategy and the goals which are to be achieved by means of cloud computing are thus neither clear nor can they be verified.
- Critical elements in the introduction process were overlooked due to poor planning and the intended cloud project fails.

- The cloud service is defined too vaguely, leading to differences with the cloud provider with regard to the service quality. As a result of this, the cloud user is either provided with inadequate service quality or expensive subsequent improvements become necessary.
- A strong will to use cloud computing in any case results in illusory assumptions and "beautified" costs/benefits analyses. Ultimately, this results in financial losses.
- The path to the cloud can be very difficult and it is overlooked that the path out of the cloud must also be taken into account. Otherwise, there is a high level of dependency on the cloud provider, which may be a financial disadvantage.
- With the term "flexibility", cloud providers refer to the capacities made available within a service. Other wishes of the cloud users often cannot be fulfilled and their own possibilities of intervention are very limited.
- Cloud providers themselves often obtain services (e.g. administration or backup of data) from subcontractors. Thus, for example personal data may leak in an unauthorised manner (which might be penalised with a fine) or a security certificate may be jeopardised by this, because an auditor cannot audit this subcontractor.
- Emergency? What emergency? The cloud is always there and this is why the cloud user does not have a business continuity plan.

2 Secure paths to the cloud

The risk that a cloud project fails is increased substantially without a structured approach. In some cases, cloud services introduced ad hoc can be used successfully, but this is rather the exception. Planning and evaluation, however, must not become so extensive that the goal – i.e. using cloud services and the benefits arising from this – cannot be achieved.

In order to reach a sustainable and economic decision, the goals related to the intended cloud service must be clear. On the part of the cloud user, however, there is also a need for flexibility: both in terms of functionality and security. Not all wishes and requirements will be realised, as cloud offers are highly standardised in most cases. When evaluating cloud services, it must be clarified to what extent an offered service differs from the user's own goals. This is the only way to follow alternative paths if necessary.

The recommendations given below can and should be adapted to the respective, specific situation. This applies to the scope and documentation, where applicable, but not to the essential content which remains valid for all cloud projects.

2.1 It all starts with the cloud strategy

Irrespective of the size of the cloud project, it is necessary to be familiar with the essential requirements and boundary conditions and, based on them, to develop directions for action. Otherwise, the project is already in difficulty right from the beginning.

Using a project team

The management places the following assignment with a project team in which decision-makers for the IT strategy and for the corporate strategy are represented:

- Description and documentation of the initial situation and the desired benefit
- Definition of the subject under examination: which service, which service model and which deployment model. At this point, some aspects can still be open or weighed explicitly against each other.

Caution:

- It does not make much sense to make specifications that are too concrete, such as examining a specific service of a provider, in this project step. The aim is to find a service which meets the organisation's own requirements as well as possible.
- The project team carrying out the examination needs sufficient resources and time, otherwise the quality of the project is at risk!

Feasibility study

The project team prepares a feasibility study the scope and implementation of which should be based on the planned cloud service. The following aspects should be addressed:

- Examination of the **legal framework conditions** (e.g. data protection, classified information, regulatory authorities) and the company's or government agency's own policies (compliance). Which type of data should be processed in the cloud? May the data be stored in a cloud? Are there restrictions regarding the storage or processing location (e.g. due to access to the information by third parties, espionage)? Do restrictions result from this with respect to the deployment model (public cloud, community cloud, private cloud or hybrid cloud)?
- Is the IT of the company or government agency **mature enough** to be able to use cloud services? When using IaaS on a larger scale, the following questions must be asked: Can the services concerned be virtualised? Can they be standardised? Only when these prerequisites have been met can IaaS be used successfully.

- Outsourcing services always results in **internal adaptations**. If they cannot be realised, the cloud service examined cannot be used. Example: A cloud service requires a high bandwidth and redundant Internet access, which is not the case in rural areas with an available connection of only 6 Mbit/s.

It can now be defined more specifically which **service** and which **deployment model** can be used and are to be examined further in the next step.

Risk assessment/analysis

The classification (protection requirements) of the information to be processed is of key importance for defining the requirements for a cloud service. The classification should have at least three categories, with the damage which the loss, change or non-availability of the information would entail being the measure for the classification. It is important to distinguish between confidentiality, integrity and availability.

Information security is always based on a risk management process, the core of which is the risk analysis. This is what each organisation must think about. While the risks can be described generally, the impacts may vary greatly in occurrence of damage.

In this rough risk analysis, at least the following threats should be taken into consideration:

- Access to the data by the cloud provider
- Access options by government agencies due to the (even foreign) jurisdiction applicable to the cloud provider
- Non-availability of data and services
- Compromising of the authentication
- Loss of data
- Data manipulation

This analysis already sets out areas in which special security safeguards must be taken and/or in which risks arise that cannot be addressed. There is no such thing as secure cloud computing by external cloud providers for all possible applications.

Costs/benefits assessment

When the aspects mentioned above have been clarified, the costs and benefits are assessed roughly by taking at least the following aspects into account:

- Usage costs of the service
- Internal administration work
- Training of employees and administrators
- If necessary, new IT or new network connection
- Costs of the adaptation of processes
- Costs of the migration
- Internal savings

If this assessment is carried out properly and realistically, it provides a first impression of whether a cloud service could pay off. The results are summarised and present to the decision-makers. They decide on the progress of the project.

IT-Grundschutz: M 2.534 Erstellung einer Cloud-Nutzungs-Strategie [04]

2.2 Security requirements (security policy)

If the management has, on the basis of the feasibility study, the risk analysis and the costs/benefits assessment, opted for further advancing the use of a cloud service, specific implementation steps are presented below.

In addition to the functional requirements which are not the priority subject matter of this document, the requirements for the information security and availability of the cloud service must be described. These requirements not only include those to be fulfilled by the cloud provider, but also those to be met by the user's own organisation.

The first rough risk analysis serves as the framework, which is now refined further. In addition, the risk or security analysis (hopefully) already existing in the organisation should be used. Moreover, requirements arising from the legal framework conditions must be taken into account.

If you have not yet drawn up your own security requirements, you will have difficulties in telling the cloud provider specifically what you expect from them. Thus, the planned usage of cloud services may be an impetus to also think about the information security of the existing IT and the availability of the business processes carried out with them. Demanding a "secure" and "permanently available" cloud from the cloud provider without imposing specific requirements can only go wrong: Either the security level is not sufficient or the offered solution is too expensive.

The security requirements of BSI Cloud Computing Compliance Controls Catalogue C5 shall be requested as a minimum level. But performing a risk analysis is still necessary.

Here, the **classification of information** is referred to again, without which appropriate requirements for information security and availability cannot be drawn up.

The approach shown below can be applied to determine the security requirements.

Simplified plan

Drawing up a simplified plan in which all (groups) of persons and/or roles, communication connections, IT systems and business processes involved in the planned cloud usage are described; both on the part of the organisation using the cloud (services) and (symbolically) on the part of the cloud provider.

- Organisation using the cloud (services)
  - Groups of persons
    - Normal users
    - Privileged users (usually administrators) who control the usage of the cloud service on the part of their own company
    - Other users with special rights, such as the accounting department for accounting purposes
  - Communication connections
    - Internet connection(s) of the organisation using the cloud (services) or also the communication connection in a closed network
  - IT systems on the part of the organisation using the cloud (services)
    - Interface systems
    - Network components (routers, firewalls, virtual private network (VPN) gateways, ...)
    - Terminals for using the service
    - Terminals for the service administration

    - Business processes (in government agencies, business processes are usually considered to be the specialised tasks of the respective organisational units)
- Cloud providers
    - Groups of persons
        - Administrators
        - Other employees of the provider
    - Communication connections
        - Internet connection(s) of the provider or also the communication connection in a closed network
    - IT systems
        - Interface systems which offer a web interface or a web service
        - Network components (as above and, additionally, load balancers)
        - Administration IT
        - Databases

Attack vectors

Working out where and over which paths information could be accessed in an unauthorised manner or the service prevented from being delivered or used. The most important attack vectors include:

- Authentication to the cloud service is forged
- Authentication procedure to the cloud service is too insecure
- Backdoors in the authentication (e.g. standard user and password)
- Incorrect implementation of the interface (e.g. web application prone to injection attacks)
- End-point-security at the user's premises
- Access to information by cloud provider personnel (administrators in particular) or external employees
    - Encrypted data is decrypted for processing
    - Access to backed up or archived data (also snapshots of virtual machines)
- Eavesdropping on the communication (encrypted communication, Transport Layer Security (TLS) 1.2, VPN)
- Direct access to IT systems and network components which are not patched and/or not hardened.

Based on the attack vectors compiled, requirements are formulated which do not yet have to, but can be of a technical nature (example: the computer centre must be connected redundantly to the Internet).

Determining the security policy

In the security policy, the most important attack vectors are listed and security requirements formulated. The choice of security safeguards is still open unless there are already reasons in this phase to choose them.

If the security requirements are so high that they cannot be met when using a cloud, the cloud usage process should be stopped at this stage.

If the security requirements cannot be achieved with a public cloud solution, the project must be shelved upon consultation with the decision-makers or it must be examined whether it is possible to use a community cloud or a private cloud as an alternative.

IT-Grundschutz: M 2.535 Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung [04]

Risikoanalyse auf der Basis von IT-Grundschutz (BSI-Standard 100-3) [04]

IT-Grundschutz: Gefährdungskatalog G 0 „Elementare Gefährdungen“ [04]

BSI Cloud Computing Compliance Controls Catalogue C5 [02]

BSI Sicherheitsprofile SaaS Teil 2: Bedrohungs- und Risikoanalyse (durchgeführt für drei verschiedene Cloud-Dienste) [03]

2.3 Definition of services/interfaces/fields of responsibility

Writing down definitions is an arduous task, but without making such detailed specifications, major problems might occur at a later stage of the process.

2.3.1 Definition of services

The cloud user documents what the service should offer and not what the user is probably offered by cloud provider. Adaptations can still be made subsequently, but defining the user's own requirements to be fulfilled by the service is of key importance for choosing a suitable service and provider.

Having performed the steps described above composes a picture of how the service should be designed and which security requirements have to be imposed. The definition of the service is primarily of a functional nature, but functional deficits also bear security risks. (Example: Necessary functions made available by the provider are still in the beta phase, but are discontinued at a later stage. This could mean that the entire project fails.)

The competent department and IT department must collaborate in defining the services, whereby weighted specifications might already be used at this stage (“must have” – “nice to have”). Service templates according to the Information Technology Infrastructure Library (ITIL) can provide assistance in structuring and formulating the service:

- Service abbreviation and service name
- Brief description
- Category
- Sub- and/or secondary services
- Versions
- Technical parameters
- Service-parameters/service level agreements (SLAs)
- SLA measurement
- Validity of the service (period of time)
- Service delivery
- Cost determination methods
- Price/invoicing
- Contact person(s) for the service
- Authorised and requesting parties
- Prerequisites

2.3.2 Definition of interfaces

Cloud services are used via interfaces. If misunderstandings and errors arise when defining the interfaces, this may have serious effects on functionality and security. The following aspects need to be considered in this regard:

- Generic description of the interface on the part of the user including information about protocols and/or software used.
- Description of the authentication means of the user's own user and rights management which are to be used for the cloud service. (Recommendation: 2-factor authentication for cloud services that are accessed via the Internet).

2.3.3 Fields of responsibility

The demarcation of the fields of responsibility between the cloud user and cloud provider is very important with regard to the interfaces in particular. This is the only way to establish a structured and solution-oriented approach in the event of problems and this is only successful when the definitions are complete and clear. In the contracts, reporting and escalation routes with regard to troubleshooting and handling problems must be described (see chapter 2.6.3).

IT-Grundschutz: M 2.536 Service-Definition für Cloud-Dienste durch den Anwender [04]

2.4 Planning the usage with foresight

Up to this step, no cloud provider has been chosen yet, but the planning of the migration and operation should now be addressed. Even before specific offers are invited, it should be examined how the cloud service can be used permanently in a secure manner and whether there are possible obstacles to the migration. This rough planning can already be done even if the service has not yet been defined clearly. At this point, costs and/or time delays which may prevent cloud services from being used successfully can still arise.

2.4.1 Migration plan

For the planning of the migration, a migration concept is essential. In this concept, the aspects to be taken into account when introducing the cloud service are listed. If the new service replaces an already existing service, data migration, availability, authorisations and the administration model must be adjusted. If no previous service is used, the migration is easier; however, administration and the authorisation management must be extended.

Cloud services are almost always integrated into other processes and this aspect has to be taken into consideration in terms of the migration. Furthermore, it must be prepared to what extent existing process descriptions have to be adjusted and how much time has to be planned for training etc.

How can it be verified that a migration has been successful? For this purpose, test and transfer procedures which not only cover functional, but also security-relevant aspects must be defined. In the case of larger cloud projects, a service provider who plans and carries out the migration can be engaged. In this case, it is obvious that prescribed criteria which have to be complied with by the service provider must be in place.

IT-Grundschutz: M 2.537 Planung der sicheren Migration zu einem Cloud Service [04]

2.4.2 Planning the usage

The time between the decision in favour of a cloud service and its introduction should be as short as possible. Therefore, it must be considered in advance which changes result from using the cloud service for

the existing IT. As was the case with the migration, some essential aspects should already have been analysed even if the cloud provider has not been chosen yet.

Important aspects to be taken into account when planning the usage include:

- Adaptation of the interface systems such as load balancers, proxys, routers, security gateways and federation systems.
- Analysis of whether the existing interface systems are interoperable with the cloud service or/and whether new interface systems are required which may also have a longer delivery time.
- Calculation of the network load and checking if the existing (network) performance is sufficient (example: Streaming office applications as cloud services results in much higher data volumes than for a local software installation).
- The administration model as well as the user and authorisation model must be adapted to the cloud service.

If the data is to be stored not only in the cloud, but also on your own systems within the organisation, it must be clarified whether sufficient storage capacity is available and whether it can also be used as backup for the cloud service.

IT-Grundschutz: M 2.538 Planung der sicheren Einbindung von Cloud Services [04]

2.5 Security concept

In the security concept, all security-relevant aspects of the IT are written down. It is the central document with which an organisation defines its information security.

Actually, such a concept should be available in each organisation for the existing IT, but it might be referred to differently. It is used to document the necessary security safeguards and must be revised (fundamentally) for cloud usage. As an aid, the IT-Grundschutz of the BSI can be used.

Both the cloud user and the cloud provider (and, if necessary, also the network provider) require a security concept. The provider should allow the cloud user to inspect the concept upon request.

In the security concept for cloud use, the special threat scenario resulting from the service being rendered as a cloud service should also be described. In this respect, the following points in particular should be taken into account:

- Premature or compulsory termination of contract
- The lack of portability of data (especially in the case of software as a service), applications (especially in the case of platform as a service) and systems (especially in the case of infrastructure as a service) if the cloud service chosen deviates from established standards.
- Dependency on a cloud service provider due to not having the possibility to change provider (vendor lock-in)
- Using proprietary data formats can endanger the integrity of the information and make it difficult to change the provider.
- Cloud infrastructure being used jointly by several organisations
- Poor knowledge of the storage location of information
- Usually high mobility of information
- Unauthorised access to information, for example by administrators of the cloud service provider

Possible security safeguards to be taken against these threats:

- Specifications regarding the secure administration of the cloud service (for example two-person rule for certain particularly critical administrative activities such as the copying of individual databases or systems)
- Specifications regarding business processes and security management processes (interfaces for example for the change, incident, security incident and risk management)
- Rules regarding the monitoring of the rendering of services and reporting
- Encryption of the information for storage and transmission
- Granting and withdrawal of authorisations
- Data backups being carried out both by the cloud provider and by the cloud user

The best way of testing the provider's security concept is to perform audits. They can be carried out by the cloud user or independent third parties. This must be communicated clearly, contractually agreed upon and performed together with the cloud provider.

IT-Grundschutz: M 2.539 Erstellung eines IT-Sicherheitskonzeptes für die Cloud-Nutzung [04]

IT-Grundschutz-Vorgehensweise (BSI Standard 100-2 Kap. 4) [04]

Webkurs IT-Grundschutz: Sicherheitskonzept [04]

IT-Grundschutz: M 2.195 Erstellung eines Sicherheitskonzepts [04]

2.6 Selection of the cloud provider

The cloud strategy has been accepted, the desired cloud service described well and the security concept drawn up: The next step is to select a suitable provider.

A shortlist of providers was probably available prior to the cloud process. Nevertheless, it is important that the organisation's own requirements are first also summarised for security. The service description and the security requirements can now be incorporated in a requirements specification or a service description.

A possible selection includes:

Attestation according to BSI Cloud Computing Compliance Controls Catalogue [02]

ISO 27001 on basis of IT-Grundschutz [04]

ISO/IEC 27001: Information security management [13]

ECSA – EuroCloud Star Audit, Certification for Cloud Services [14]

Cloud Security Alliance: Open Certification Framework (CSA) Security, Test & Assurance Registry (STAR): STAR Self Assessment, STAR Certification, STAR Attestation, C-STAR Assessment [15]

ISO 22301: Societal security – Business continuity management systems – Requirements [16]

Data protection certificates, e.g. EuroPriSe of ULD [17]

Attestation according to AICPA SOC 1, SOC 2, SOC 3 or ISAE 3402 (or other comparable standards). Successor of SSAE 16 (Statements on Standards for Attestation Engagements) and SAS70 (Statement on Auditing Standards) No. 70, Service Organizations [18]

IDW-Standards (Institut der deutschen Wirtschaftsprüfer) [19]

If there are rules for the awarding of contracts, they must be observed (example: To government agencies, the Regulation on the Award of Public Contracts) applies.

The security concept (see chapter 2.5) should already make clear which security requirements have to be met by the cloud provider and whether they have to demonstrate proof of this by means of certificates.

In case of certificates and attestations, it must be verified whether the scope of certification includes the entire cloud service offered and what the main message of the certificate is.

IT-Grundschutz: M 2.540 Sorgfältige Auswahl eines Cloud-Diensteanbieters [04]

To review the suitability of a provider, the following criteria should be taken into consideration:

- Reputation (verifiable references)
- Rankings or evaluation matrices of organisations (which are as independent as possible)
- Is cloud computing the provider's core business? If this is not the case, it might be possible that the cloud service is discontinued quickly or taken over by another provider.
- What access by the service provider or third parties is allowed or possible?
- At which sites is the information processed and stored?
- What is the applicable law of a contract and which legal framework conditions apply to the provider?
- Information of the subcontractors on the rendering of the service in order to be able to assess dependencies of the cloud provider

An audit report with an attestation based on BSI Cloud Computing Compliance Controls Catalogue C5 offers answers to many of the mentioned topics above. C5 should therefore be ask for. A public accountant testifies the compliance with the security requirements and the correctness of the surrounding parameters for transparency of the cloud service (e.g. real locations of data processing, sub-contractors). Included are information on the qualification of the audit team (existence or relevant certification of the team members). The cloud customer should evaluate the audit report based on the indications given in C5.

Espionage:

Since Edward Snowden's revelations by means of which the extent and possibilities of government monitoring came to light, espionage as a threat substantially became the focus of attention. To cloud computing, the possibilities of law enforcement authorities to force cloud provider to hand over data of their customers without informing them about this and be allowed to make a statement about this at all are particularly relevant. This fosters mistrust, less against the provider themselves, but against the legal framework in which the information is processed in the cloud or in which the headquarters of the cloud provider are.

Since 2011, the BSI has already requested that cloud providers have to disclose which possibilities of intervention government agencies or other third parties have with respect to customer data. This is a difficult undertaking in case of global clouds in which the data is distributed across all continents. Therefore, a cloud provider providing sufficient clarity in this respect should rather be chosen.

2.6.1 Service description

In the cloud provider's offer, the services offered must be described in a sufficiently clear manner; otherwise, the aspects have to be clarified in writing. (Example: Does the description, in addition to information on the availability, also cover information as to which definition is used to calculate it?)

2.6.2 Costs/benefits analysis

In case of suitability and following the evaluation of the offers, a detailed costs/benefits analysis must be performed. It must also include costs for migration, adaptations, training and maintaining operations. This analysis should also consider costs which incurred when terminating the contractual relationship with the

cloud provider. Here, the cases “Migration to another provider” and “Insourcing” should be considered separately.

If the conclusion that the cloud service offered does not meet the economic expectations or the costs do not correspond to the possibilities has to be drawn at this point, the project is stopped at this stage.

2.6.3 Contract with the cloud provider

The cloud providers’ offers also always include contractual elements (general terms and conditions (GTC)). They must be checked as to whether they can be borne by the cloud user.

Cloud computing contracts are usually not as complex as outsourcing contracts. Nevertheless, they require a lot of time and attention.

The contract must at least contain the elements listed below:

- Place where the service is rendered
- Subcontractors
- Compliance with the security requirements preferably at least those of BSI Cloud Computing Compliance Controls Catalogue C5
- Infrastructure of the cloud service provider and personnel
- Communication channels and contact persons
- Rules regarding processes, workflows, and areas of responsibility
- Where applicable, special regulations in case of security incidents or business interruptions at the cloud provider’s premises (e.g. access to log files)
- Termination of contract and deletion of data
- Contingency planning
- Rules regarding general legal conditions
- Change management
- Checks
- Contractual penalties in case of non-fulfilment
- Questions of liability

Financial penalties can be agreed upon; enforcing them, however, could turn out to be difficult. In most cases, the cloud provider offers credits for future services. Enforcing the cloud provider’s liability for the damage occurred is to be aimed for, but it is very difficult to assert these claims.

If necessary, it must be specified how the licensing of the software used is handled.

Cloud computing is based on standardisation to ensure that many customers can use the offers and the “economy of scale” comes into effect. Accordingly, the service level agreements (SLAs) and operational level agreements (OLAs) are fixed and cannot be negotiated. This is often OK for the functions offered. The security needs and requirements differ from customer to customer – not least because the information processed by the cloud service has a different value depending on the customer.

Nevertheless, it should preferably be insisted that the organisation’s own security objectives be complied with. In professional environments, it is possible to negotiate an SLA, whereas it is not possible to do this as a private customer in most cases.

For an agreement about the security requirements it is useful to stipulate at least the compliance to BSI Cloud Computing Compliance Controls Catalogue C5 with the cloud provider. Additionally, an agreement

for a regular submission of the C5 audit reports. In the contract design references to the relation between cloud provider, cloud customer and public accountant should be noted (e.g. reporting on remediation of defects).

In principal audit rights for the cloud customer can be stipulated that may also be used for issues of information security. In certain cases this could be mandatory due to regulation or according to the risk management of the cloud customer. If audit rights are necessary for the cloud customer it should be paid attention to stipulate them clearly and comprehensively. The same applies to the reporting of security incidents and risk reports.

In any case the cloud customer is responsible to meet the respective regulations. This must be considered before signing a contract with the cloud provider.

Further documentation for contractual arrangements:

I T-Grundschutz: M 2.541 Vertragsgestaltung mit dem Cloud-Diensteanbieter [04]

Kompetenzzentrum Trusted Cloud: Leitfaden – Vertragsgestaltung beim Cloud Computing [Guide – Contractual arrangements for cloud computing] [07]

BITKOM: Leitfaden Cloud Computing [Cloud computing guide], chapter 4 [01]

On license management:

Kompetenzzentrum Trusted Cloud: Arbeitspapier – Lizenzierungsbedarf beim Cloud Computing [08]

2.7 Migration and operation

The migration to a cloud service is carried out in several stages with test and pilot operations. The simple usability of cloud services must not obscure the fact that not only the IT, but also the organisation with its processes has to be adapted and must run smoothly. This must be tested in any case. In case of larger adaptations, it is recommended to run a pilot phase in which a part of the users uses the cloud service first.

The continuous, secure operation of the cloud service includes to check the provision of services. Close contact with the cloud provider is essential. Particular attention should be paid to the following aspects:

- Regular updating of the documentations and policies
- Regular checks include amongst other things:
  - Ensuring proper administration
  - Regular checks of the rendering of services (according to the SLA)
  - Regular service reviews together with the cloud provider
  - Security certificates by the cloud provider
  - Backing up data properly
  - Compliance with the processes planned and agreed upon
  - Audits, security checks, penetration tests or analyses of vulnerabilities
- Regular coordination talks with the cloud provider
- Planning and implementation of exercises and tests

IT-Grundschutz: M 2.542 Sichere Migration zu einem Cloud Service [04]

IT-Grundschutz: M 2.543 Aufrechterhaltung der Informationssicherheit im laufenden Cloud-Nutzungs-Betrieb [04]

IT-Grundschutz: M 2.544 Auditierung bei Cloud-Nutzung [04]

2.8 Termination of cloud usage

There are several reasons for terminating the usage of a cloud service: Switching to another cloud provider, no more use for the cloud service or insourcing. Depending on the cloud service, this can be very complex. Irrespective of this, the following aspects should be taken into account:

- All necessary data must be transmitted or otherwise handed over to the cloud user.
- All data of the cloud user must be deleted securely at the cloud provider.
- It is recommended to contractually agree upon a transitional period in which the cloud provider is still available for queries and support and/or the data is not deleted yet.

IT-Grundschutz M 2.307 Geordnete Beendigung eines Outsourcing- oder Cloud-Nutzungs-Verhältnisses [04]

2.9 Data protection/compliance

If personal data is collected, processed or used in the cloud, protection of the personal data must ensured in accordance with the data protection regulations.

In addition to the data protection requirements, the cloud user must comply with the required legal regulations (compliance). These regulations may be requirements such as of the Telecommunications Act (TKG), the General Tax Code (AO) when tax data is processed, the Commercial Code (HGB) when data relevant to accounting is processed and the Criminal Code (StGB).

In all cases, the cloud user (usually) remains responsible for the data when processing such data in a cloud and they have to ensure that the data at the cloud provider is handled according to these regulations and laws.

EuroCloud Leitfaden Recht, Datenschutz & Compliance [10]

Trusted Cloud: Datenschutzprofil TCDP (Trusted Cloud Data Protection Profile) [11]

Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises: Orientierungshilfe Cloud Computing [09]

ISO/IEC 27018:2014, Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors [12]

3 Summary

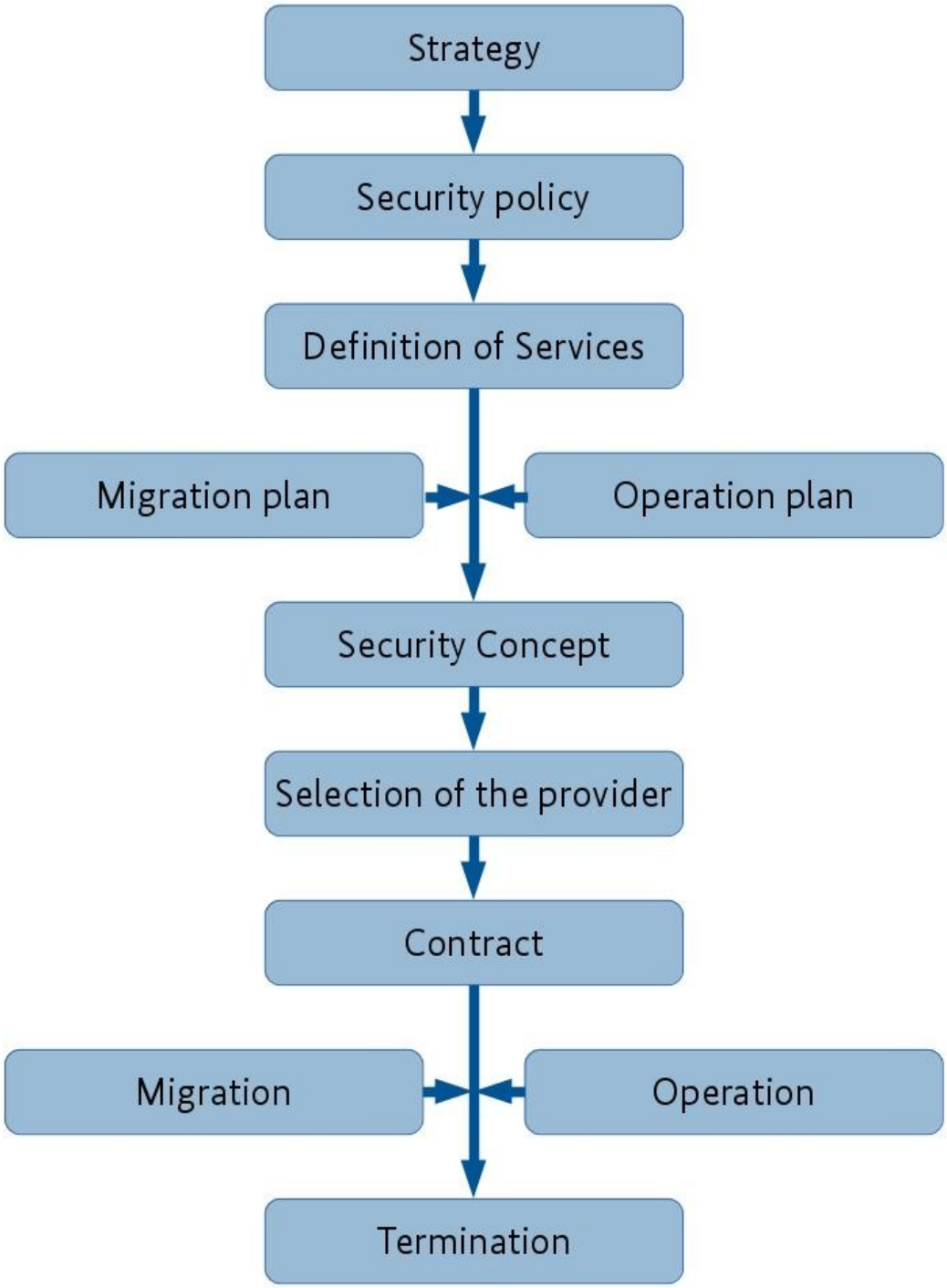
Cloud services offer new possibilities and promise cost savings which are met in many cases. The chances and risks of cloud usage as well as the effective costs must be identified objectively and reasonably, assessed soberly and weighed up intelligently. Any other approach results in conditions which can no longer be controlled.

Making use of cloud computing is a strategic decision and this decision cannot be made on the work level. This is where cloud services are needed, but only the management of companies or the management of government agencies have the option to introduce cloud services efficiently and securely. It is not a "one-click job", as sometimes suggested by advertisements. Even if it is not so complex from a technical point of view, it always remains an organisational effort. In this respect, an (adapted) process from the initial planning to the introduction is necessary.

Because the greatest risk in the case of cloud computing is: "For they know not what they do!"

4 Appendix

4.1 Schematic overview of a secure cloud usage process



4.2 Reference Documentation

[01] BITKOM: Leitfaden: Cloud Computing – Evolution in der Technik, Revolution im Business (October 2009) (in German only) https://www.bitkom.org/Publikationen/2009/Leitfaden/Leitfaden-Cloud-Computing/090921-BITKOM-Leitfaden-CloudComputing-Web.pdf

[02] Bundesamt für Sicherheit in der Informationstechnik: Cloud Computing Compliance Controls Catalogue (C5) (February 2016) https://www.bsi.bund.de/EN/C5

[03] Bundesamt für Sicherheit in der Informationstechnik: Sicherheitsprofil SaaS (2014) (in German only) https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Sicherheitsprofile/sicherheitsprofil_saas_node.html

[04] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz (in German only) https://www.bsi.bund.de/grundschutz

[05] Cloud Security Alliance (CSA): Top Threats https://www.cloudsecurityalliance.org/topthreats

[06] European Union Agency for Network and Information Security (ENISA): Cloud Computing Risk Assessment https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment/at_download/fullReport

[07] Kompetenzzentrum Trusted Cloud: Leitfaden – Vertragsgestaltung beim Cloud Computing (in German only) https://www.trusted-cloud.de/sites/default/files/media/article/downloads/ap_3_vertragsleitfaden.pdf

[08] Kompetenzzentrum Trusted Cloud: Arbeitspapier – Lizenzierungsbedarf beim Cloud Computing, (in German only) https://www.trusted-cloud.de/sites/default/files/media/article/downloads/arbpap_2_lizensierungsbedarf_0.pdf

[09] Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises: Technische und organisatorische Anforderungen an die Trennung von automatisierten Verfahren bei der Benutzung einer gemeinsamen IT-Infrastruktur – Orientierungshilfe Mandantenfähigkeit (Version 1.0, October 2012) (in German only) https://www.bfdi.bund.de/DE/Infothek/Orientierungshilfen/Artikel/OHCloudComputing.pdf

[10] EuroCloud Deutschland_eco e.V: Leitfaden Recht, Datenschutz & Compliance (in German only) https://www.eurocloud.de/wp-content/blogs.dir/5/files/eurocloud-leitfaden_rdc.pdf

[11] Kompetenzzentrum Trusted Cloud:: Zertifizierung nach dem Trusted Cloud Data Protection Pofile (in German only) http://www.tcdp.de/data/pdf/TCDP-1-0.pdf

[12] International Organization for Standardization (ISO): ISO/IEC 27018:2014, Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors https://www.iso.org/iso/catalogue_detail.htm?csnumber=61498

[13] International Organization for Standardization (ISO): ISO/IEC 27001:2013, Information technology – Security techniques – Information security manage-ment systems – Requirements https://www.iso.org/iso/home/standards/management-standards/iso27001.htm

[14] ECSA (EuroCloud StarAudit): Certification for Cloud Services https://staraudit.org/

[15] Cloud Securty Alliance: Open Certification Framework https://www.cloudsecurityalliance.org/research/ocf

[16] International Organization for Standardization (ISO): ISO 22301:2012, Societal security – Business continuity management systems – Requirements https://www.iso.org/iso/catalogue_detail?csnumber=50038

[17] Unabhängigen Landeszentrum für Datenschutz (Schleswig-Holstein): Datenschutzzertifikat EuroPriSe https://www.european-privacy-seal.eu

[18] American Institute of Certified Public Accountants (AICPA): Standards: SSAE 16 (Statements on Standards for Attestation Engagements), SOC 1 (Service Organization Controls), SOC 2, SOC 3, https://www.aicpa.org

[19] Institut der deutschen Wirtschaftsprüfer: IDW-Standards https://www.idw.de/the-idw