Federal Office
for Information Security

White Paper

Security Recommendations for Cloud Computing Providers

(Minimum information security requirements)

www.bsi.bund.de

Contents

Preamble 3

The BSI Serving the Public 5

1 Introduction 7
- 1.1 Motivation 7
- 1.2 Objectives 8
- 1.3 Target audience 9
- 1.4 Method of application 9
- 1.5 Defining the scope of the BSI security recommendations 10

2 Cloud Computing basics 12
- 2.1 What is Cloud Computing? 12
- 2.2 How does a public cloud differ from a private cloud? 14
- 2.3 Which different service models are available in Cloud Computing? 15
- 2.4 How does Cloud Computing differ from traditional IT outsourcing? 16
- 2.5 Strategic planning of Cloud Computing services by users 17

3 Security management by the provider 19

4 Security architecture 23
- 4.1 Data centre security 23
- 4.2 Server security 25
- 4.3 Network security 27
- 4.4 Application and platform security 29
- 4.5 Data security 32
- 4.6 Encryption and key management 34

5 ID and rights management 36

6 Control options for users 39

7 Monitoring and security incident management 40

8 Business continuity management 43

9 Portability and interoperability 46

10 Security testing and Audit 48

11 Requirements of personnel 50

12 Drawing up agreements 53
12.1 Transparency 53
12.2 Service level agreements (SLA) 55

13 Data protection and compliance 57
13.1 Data protection 57
13.2 Compliance 59

14 Prospects 62

15 Glossary 64

16 References 66

17 Acknowledgements 68

Preamble

Minimised risk in Cloud Computing

Cloud Computing has the long-term potential to change the way information technology is provided and used. But information security is a key factor if IT services from the cloud are to be used reliably. To create a sustainable basis in terms of security in Cloud Computing, in September 2010 the German Federal Office for Information Security (*German abbreviation* BSI) promoted an exchange of practical experience. The providers of relevant solutions, their users and security experts were invited to debate the white paper published by the BSI which defined the minimum requirements for information security in Cloud Computing.

It is not only the traditional attack scenarios that are relevant to cloud systems. There are also specific characteristics, such as the fact that multiple users share a common IT infrastructure. The dynamic sharing of the IT service across multiple locations also represents a particular challenge.

The sector's many responses to this BSI initiative showed that the strategy of having a joint, practical discussion between providers and users was a correct one – the white paper was generally well received by those involved in the market. This is evidenced by the many queries and numerous constructive comments. The outcomes from that discussion have now been documented in this paper.

The BSI, working with those involved, aims to develop reasonable, adequate security requirements for Cloud Computing to ensure that information, applications and systems are protected. We have come much closer to realising this

goal. The minimum requirements described below are scalable in terms of availability and confidentiality. They provide a methodological starting point, from which other issues can be integrated and then adjusted to changing circumstances on an ongoing basis. Furthermore, they are a good basis for debates at international level. International standards are the certification basis for interoperability and information security. It is only this basis that will enable users to acquire a complete, reliable picture of the various cloud offerings available. As the next step we are planning to incorporate Cloud Computing into the BSI's IT-Grundschutz (*basic protection*) approach.

It is only when the relevant services are provided with a high degree of security that the potential in cloud solutions – such as flexibility, efficiency, reduced costs and the provision and use of information technology – will really be able to be exploited .

I hope you find your reading extremely rewarding.

Michael Hange

The BSI Serving the Public

The Federal Office for Information Security (BSI), based in Bonn, was founded on January 1st 1991 and forms part of the Federal Ministry of the Interior.

With, currently, around 500 employees and a budget of 62 million Euros, the BSI is an independent, neutral body that deals with all issues relating to IT security in the information society.

As the central IT security provider for the federal government, the BSI operates on behalf of the government, works in partnership with the commercial sector, and provides information to the public.

Through its work on basic IT security, the BSI, as the national IT security authority, is responsible for our society and is, therefore, a key pillar of domestic security in Germany.

The BSI's objective is that information and communication technology can be used securely in our society. IT security should be taken seriously and implemented responsibly. The security issues involved in IT systems and applications should be dealt with up-front, at the development stage.

The BSI aims its services at users and manufacturers of information technology. The target group includes public authorities at the national, state and district levels, private users and companies.

This white paper on Cloud Computing provides a compact overview of the main organisational, personnel, infrastructural and technical information security measures for Cloud Computing providers.

1 Introduction

1.1 Motivation

Cloud Computing is currently one of the hottest topics in information technology (IT). However, it is not so much that the term 'Cloud Computing' represents a host of new technologies, but rather that these technologies are combined and effectively upgraded so that they enable new IT services and new business models.

With Cloud Computing, as with many new technologies and services, information security and data protection issues are intensely debated, and examined far more critically than is the case with offerings that have been around for a while. Many surveys and studies reveal that potential customers have concerns about information security and data protection which stand in the way of a wider deployment. The required trust still needs to be developed if cloud offerings are to be taken advantage of.

For this reason, the BSI has drawn up recommendations for secure Cloud Computing which are primarily aimed at cloud service providers (CSP). These CSPs have the means and the obligation to adequately implement information security. They may use this white paper as a guideline for implementing security measures. Cloud users, for their part, who are affected by these recommendations can ask the CSPs whether they have been implemented. However, the initial step for any cloud customer should be to clarify what protection their own data and applications require. This will largely determine whether, and upon which underlying conditions, business-related data and applications may be stored in the cloud.

The white paper provides an overview of the main Cloud Computing areas in which security should be implemented. Not all the points listed are equally relevant to all cloud services. For example, since the threat profile differs in

some areas for private and public clouds, different security measures must sometimes be taken.

This document does not only examine cloud-specific issues, but also examines underlying information security requirements, since these form the basis on which all cloud services are to rest. The recommendations have been kept largely abstract, with no detailed instructions on their implementation being provided. Doing so would be beyond the remit of the document and would not allow for the diversity of cloud offerings. Assessing the security of any particular offering, therefore, must also be undertaken on a case-by-case basis.

1.2 Objectives

Though IT services from the cloud are becoming increasingly in demand around the world, almost every survey and study shows that there are also many concerns which discourage users away from using Cloud Computing services. A lack of faith in the security of the services provided is frequently cited as being one of the main barriers. As the central information security service provider for the federal government in Germany, the BSI feels it is important that it is actively involved in shaping the development phase for cloud services.

The primary objective of this white paper is to provide a basis for discussion between CSPs and cloud customers. As a further aim, the paper intends to provide the basis for working out, based on this discussion, specific recommendations as to how companies and public bodies can make cloud services secure. The white paper is the first step towards creating standards based on which the security of Cloud Computing platforms can be verified. The requirements formulated in this paper will continue to be debated and, where necessary, revised, and further details will be worked out. However, the aim is not to make the guidelines more specific. They are to retain their current depth, and any further additions and details on the subject of Cloud Computing will be fed into IT-Grundschutz, for example in the form of IT-Grundschutz modules or “short informations“. There are plans to develop IT-Grundschutz modules for both us-

ing and providing cloud services. The BSI 100-2 standard for integrating cloud issues into the IT-Grundschutz methodology needs to be adjusted, particularly in the area of modelling complex, virtualised information networks.

1.3 Target audience

The white paper is aimed at IT professionals involved in providing or using cloud services. Issues of information security will be mentioned in passing and we assume a basic understanding of information security at the technical, infrastructural, personnel and organisation levels.

The recommendations are primarily aimed at CSPs providing these services to companies and public bodies, and at professional users. They are not aimed directly at private users who use specific cloud services, but they may help guide such users on security issues.

1.4 Method of application

The points listed below show, at an abstract level, which security measures a CSP should implement. Both a structured process and an effective system for managing information security are prerequisites if an adequate level of security is to be achieved and maintained in a company or public body. Relevant norms, such as ISO 27001 and the BSI 100-2 standard on the IT-Grundschutz methodology, describe how a functioning system of managing information security can be built and what it should include. For Cloud Computing services to be protected, the threats that are specific to Cloud Computing also need to be analysed, and appropriate security measures must be identified and implemented.

Each CSP must, therefore, produce a risk analysis identifying the current and relevant threats to the services they operate, which impacts they might have and how the identified risks are to be dealt with, for example through specific security measures. To a lesser degree, cloud users also need to assess the risks that may arise for them by storing data or running applications in the

cloud. The security recommendations presented in this white paper constitute a framework for addressing the Cloud Computing areas that the BSI feels are critical.

When a CSP is considering the risk factors, they usually face the challenge of not knowing in advance the value or the protection requirement of the customer's data. One solution would be to offer a high or very high protection level for all customers and their data. Experience shows, however, that this is too expensive for data with a normal protection requirement. CSPs should address the issue of information security with their customers at an early stage. Information security is one of the main decision-making criteria that customers have when selecting cloud service providers and specific cloud services. So CSPs should demonstrate to their customers how well they are set up in terms of information security. This includes showing their customers which security measures are a standard part of their offerings and are available as options, but they also need to point out to customers which security measures they themselves need to take.

1.5 Defining the scope of the BSI security recommendations

The focus of this document is on security issues in the cloud-based processing of information with a normal to high protection requirement, e.g. confidential company and personal data worthy of protection. The specifying of the protection requirement is based on the protection requirement categories as defined in IT-Grundschutz (see BSI standard 100-2 [1]). This document does not explicitly examine the protecting of data that has been rated as national classified information.

Being the core values that need to be protected, confidentiality and availability are the priorities when drawing up these guidelines. Therefore the security recommendations are divided into availability and confidentiality, while integrity as a core value is not given specific consideration.

The security recommendations provided are assigned to three categories:

- **Category B** (=basic requirement) includes those requirements which are basic for all cloud service providers.
- **Category C+** (=high confidentiality) includes additional requirements where data with a high protection requirement in terms of confidentiality is to be processed.
- **Category A+** (=high availability) includes additional requirements where services with a high protection requirement in terms of availability are to be considered.

In the tables that provide an overview of the security requirements in the various areas, there are also arrows showing how the BSI rates the threat level in each area for private and public clouds. A right-pointing arrow (⇨) indicates an average threat level, while an upward-pointing arrow (⬀) indicates a high threat level.

All the requirements listed apply to IaaS, PaaS and SaaS unless otherwise indicated.

Given the dynamic developments in the area of Cloud Computing, the security recommendations listed below will also need to be regularly reviewed and adjusted, and additional requirements may need to be added. Updated versions of this white paper will be published on the BSI's web server www.bsi.bund.de.

2 Cloud Computing basics

2.1 What is Cloud Computing?

No definition of the term 'Cloud Computing' has yet succeeded in becoming universally acceptable. Definitions are often used in publications and presentations that are extremely similar to each other while nonetheless differing. One definition that is frequently drawn upon by experts is that of the USA's National Institute of Standards and Technology (NIST) [2], which is also used by ENISA [3]:

"Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Under the NIST definition, the five characteristics of a cloud service are listed below:

- On-demand self service: Resources (e.g. server time, storage) are provisioned unilaterally without interacting with the service provider.
- Broad network access: The services are available over the network, accessed through standard mechanisms and not tied to a particular client.
- Resource pooling: The provider's resources are pooled to serve multiple consumers (multi-tenant model). The users do not know where the resources are located but they may be able to contractually specify the storage location, e.g. the region, country or data centre.
- Rapid elasticity: The services can be rapidly and elastically provisioned, in some cases even automatically. To the consumer, therefore, the resources appear to be unlimited.

- Measured services: Use of resources can be measured and monitored and similarly provided to the cloud users in a measured way.

This definition reflects the vision of Cloud Computing although the individual points should not be viewed in too dogmatic a manner. For example, in the case of private clouds, there may be no requirement at all for ubiquitous availability.

According to the Cloud Security Alliance (CSA), Cloud Computing also has the following characteristics – in addition to the elasticity and self service referred to above [4]:

- Service oriented architecture (SOA) is one of the basic requirements for Cloud Computing. The cloud services are usually provided via a so-called REST API.
- In a cloud environment, multiple users share common resources which therefore need to be multi-tenant.
- The only resources paid for are those actually been used (Pay per Use model), with flat rate models also being an option.

Definition of terminology

In order to have a standard basis for all future work related to Cloud Computing, the BSI has drawn up this definition for the term "Cloud Computing":

> *Cloud Computing refers to the dynamic provisioning, use and invoicing of IT services, based on demand, via a network. These services are only made available and used via defined technical interfaces and protocols. The range of services provided under Cloud Computing covers the entire information technology spectrum and includes infrastructure (e.g. processing power, storage), platforms and software.*

In this document, the term "Cloud Computing" will be used in this way, and the characteristics listed by the NIST and CSA should always be kept in mind.

Thus, simple web applications are not usually Cloud Computing, though manufacturers' marketing departments often refer to them as such.

2.2 How does a public cloud differ from a private cloud?

NIST distinguishes four deployment models:

- In a **private cloud** the cloud infrastructure is only run for one institution. It may be organised and managed by the institution itself or by a third party, and it may be located in the institution's own data centre or in that of a different institution.
- The term **public cloud** is used if the services can be used by the commonality or by a large group, for example an entire industrial sector, and if they are supplied by one provider.
- In a **community cloud** the infrastructure is shared by multiple institutions having similar interests. This type of cloud can be run by one of these institutions or a third party.
- If multiple cloud infrastructures, each of which is independent in itself, are commonly used via standardised interfaces, this is referred to as a **hybrid cloud**.

The definitions referred to above do not, however, cover all cloud offering variants resulting in further definitions, such as "virtual private cloud", etc.

Whereas in the case of a private cloud where the provider and user are, in principle, identical, the user has complete control over the services used, in a public cloud the user hands over control to the Cloud Computing provider.

From this point onwards, this document distinguishes only between private clouds and public clouds which, under the definition above, represent the full range of cloud deployment models. With any model that lies "between" these two extremes, there is a need to ask whether the threats, e.g. from jointly used infrastructures, resemble those of a private cloud or a public cloud.

2.3 Which different service models are available in Cloud Computing?

Essentially, a distinction may be drawn between three different categories of service model:

1. **Infrastructure as a Service (IaaS)**
   With IaaS, IT resources such as processing power, data storage and networks are available as a service. A cloud customer buys these virtualised and, to a large degree, standardised services and adds their own services on top for internal or external use. For example, a cloud customer can rent server time, working memory and data storage and have an operating system run on top with applications of their own choice.

2. **Platform as a Service (PaaS)**
   A PaaS provider provides a complete infrastructure and, on the platform, provides the customer with standardised interfaces to be used by the customer's services. For example, the platform can provide multi-tenancy, scalability, access controls, database accesses, etc. as a service. The customer has no access to the underlying layers (operating system, hardware), but can run their own applications on the platform, for which the CSP will usually provide its own tools.

3. **Software as a Service (SaaS)**
   Any provision of applications that meet the Cloud Computing criteria falls into this category. No limits are set here on the range of offerings. Examples are applications for contact data management, financial accounting, text processing and collaboration.

The term "as a Service" is also used for many other offerings, such as 'Security as a Service', 'BP as a Service' (Business Process) and 'Storage as a Service', so that one often speaks of "XaaS", i.e. "something as a service". Most of these offerings can at least roughly be assigned to one of the categories above.

The service models also differ in terms of the customer's influence over the security of the services provided. In the case of IaaS the customer has total con-

trol of the IT system, from the operating system upwards, since everything is operated within their area of responsibility. With PaaS the customer only has control over their applications running on the platform, while with SaaS they hand over almost all control to the CSP.

2.4 How does Cloud Computing differ from traditional IT outsourcing?

With outsourcing, an institution's work, production or business processes are wholly or partly handed over to external service providers. This is an established part of modern organisational strategies. Classic IT outsourcing is usually set up in such a way that all of the infrastructure hired is used exclusively by one customer (single tenant architecture), even though outsourcing providers normally have multiple customers. Outsourcing agreements are also usually signed for lengthy time-scales.

The use of cloud services is similar in many ways to classic outsourcing, but there are certain differences which need to be taken into account:

- For financial reasons, multiple users in a cloud share a common infrastructure.
- Cloud services are dynamic, so they can be scaled upwards and downwards far more quickly. Thus cloud-based offerings can be adjusted to the customer's actual needs more swiftly.
- The managing of services that are used from the cloud is usually done via a web interface by the cloud user themselves. Thus, the user can automatically tailor the services used to suit their needs.
- The technologies used in Cloud Computing enable the IT service to be dynamically shared across multiple locations which may be geographically very dispersed (both nationally and internationally).
- The customer can easily administer the services used and their resources via web or other suitable interfaces, and little interaction with the provider is required.

2.5 Strategic planning of Cloud Computing services by users

Before business-critical data or applications are outsourced to the cloud, a cloud strategy needs to be defined in which the main underlying principles are clarified. For this purpose, there should always be a specific security analysis for the data or applications that are to be outsourced. The cloud strategy should define, for example, what the IT structure looks like (e.g. in the case of IaaS), how existing IT systems or business processes can be delimited and separated, what all the underlying operational and legal parameters look like, and what the protection requirement is for the data or applications that are to be outsourced.

In fact, CSPs have typically tailored their offerings to particular types of information and applications. In so doing, however, they are faced with the challenge of not knowing the specific protection requirement for their customer's data. They might offer a high or very high level of protection for all their customer data, but this would be too expensive for data with a normal protection requirement.

To be able to offer every cloud customer a service that is persuasive in both functional and financial terms for customers from different sectors, CSPs should bring up the subject of data security at an early stage with their cloud customers. CSPs should tell their customers which security measures are included as standard with their offerings, which can be procured as a supplement, and which security measures the customer is responsible for himself. This also helps to avoid misunderstandings. For example, the CSP often has to bear enormous losses caused by incidents such as losing data even though it was the cloud customer that failed to ensure their data was sufficiently secure, because they opted for a level of protection that was too low or accepted a risk that was too high.

For this reason it is also vital for the CSP that the cloud customer understands the protection requirement for the outsourced data or applications and that they are clear about the protection level being offered. In this way, the CSP

can also bring the customer's attention to any potential security benefits which may arise from using cloud services.

Therefore the user must first work out the basic issues relating to security during the process of making the strategic decision, as to whether – and in which form – a cloud service is to be deployed. This applies to both public and private clouds, and equally to IaaS, PaaS and SaaS.

This process includes the following steps:

- Analysing the structure of the IT systems (e.g. with IaaS) and applications in order to enable a delimitation and to identify all the interfaces
- Specifying the protection requirement for data, applications and IT systems
- Dividing up the data, applications, systems and cloud services into protection requirement categories
- Clarifying the underlying operational and legal framework
- Defining the specific security requirements for CSPs

In this way, the cloud customer can decide which security level they require and must request it for their cloud services.

3 Security management by the provider

Figure 1 shows a reference architecture that roughly shows the components common to many Cloud Computing platforms. This reference architecture is used as a basis for discussing the guidelines that follow. The reference architecture shown takes into account the ideas in similar reference architectures, such as those used by NIST [5], IBM [6] and the Cloud Computing Use Cases Group [7].

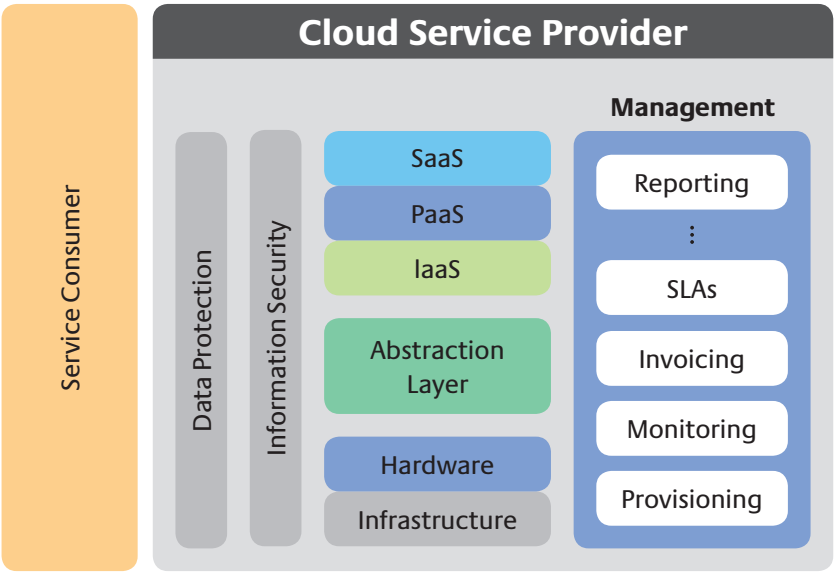

Figure 1: Reference architecture for Cloud Computing platforms

A close look at the underlying reference architecture reveals that a provider needs to address a large number of tasks in order to provide cloud services. The tasks typical to a public CSP include:

- Providing a catalogue of services which describes the services being offered,
- Provisioning and de-provisioning resources such as virtual machines, load balancers, virtual data storages, IP and MAC addresses, and
- Invoicing for the services used in a way that the customer can clearly understand.

Another key task is to monitor the services provided to be able to comply with the guaranteed service quality. This monitoring is a continuing process. Any faults or failures in resources, e.g. virtualisation servers, virtual machines, load balancers, etc. need to be detected quickly so that appropriate countermeasures can be taken as rapidly as possible. Besides security management, other tasks that are usually part of a CSP's repertoire are:

- Patch and change management
- Configuration management
- Network management
- System management
- Application management
- Reporting

The complexity and number of the above tasks require a structured approach. To this extent, each CSP should deploy standard procedural models such as ITIL and COBIT which can be used as guides when implementing IT processes.

Trusting the CSP and their offerings is currently cited as a key motivator when users are asked why they decide for or against cloud offerings. Trust is based on the assessment as to whether a provider has covered all the risks, both those in the data security area and in areas such as data protection, technology and the law – sufficiently, adequately and sustainably.

The CSP having an efficient information security management system (ISMS) is an essential basic, if Cloud Computing is to be reliable and secure. The BSI recommends that ISO 27001/2 or, preferably, the BSI standard 100-2 on the IT-Grundschutz methodology (which covers ISO 27001/2) should be used as guides to setting up and running an ISMS.

Key parts of an ISMS are a functioning information security organisation and an information security concept as tools for managing the implementation of the security strategy. A CSP should use the security organisation chart to give their customers the names of suitable contact persons able to answer the customer's security questions. Information security is a process and, therefore, should be constantly further developed in line with the PDCA (Plan-Do-Check-Act) cycle.

It is a good idea for CSPs to get their information security management system certified so that they can provide evidence that they provide sufficient security even when there is a high level of protection required in terms of confidentiality and availability. CSPs should preferably be certified in compliance with ISO 27001 based on IT-Grundschutz, ISO 27001 or other established standard.

Note:

Here and in the following, the security recommendations listed are firstly subdivided according to whether they are aimed at private or public clouds, and secondly assigned to one of three categories. In this context

- B stands for basic requirement (aimed at all cloud service providers),
- C+ (=Confidentiality high) covers additional requirements for areas with a high confidentiality protection requirement,
- A+ (=Availability high) covers additional requirements for areas with a high availability protection requirement.

A right-pointing arrow (⇨) represents an average threat level, and an up-pointing arrow (⬀) an elevated threat level for private or public clouds.

Security Management for Providers	Private ⇨			Public ⇨		
	B	C+	A+	B	C+	A+
Defined procedural model for all IT processes (e.g. as per ITIL, COBIT)	✓			✓		
Implementing a recognised information security management system (e.g. by BSI standard 100-2 (IT-Grundschutz), ISO 27001)	✓			✓		
Sustainably implementing an information security concept for the cloud	✓			✓		
Evidence of adequate information security (certification)		✓	✓		✓	✓
CSP has an adequate organisational structure for information security (including named contact persons to answer customers' security questions)	✓			✓		

4 Security architecture

If a Cloud Computing platform is to be made operationally secure, all the issues potentially posing a threat to the confidentiality, integrity and availability of the data stored there needs to be examined. Besides a well-structured procedural model for all IT processes, it is important that a security architecture be set up to protect resources (employees, infrastructure, networks, IT systems, applications, data, etc.) and that the customer is securely isolated. A robust separation of customers at every level in the Cloud Computing stack (application, servers, networks, storage, etc.) is a fundamental requirement that each Cloud Computing platform should meet. This requirement applies equally both to public and private clouds. The issues described below should be examined when setting up a solid security architecture for Cloud Computing.

4.1 Data centre security

Data centres form the technical basis for Cloud Computing. To this extent, it is important that every CSP ensures their systems are secure in compliance with the current state the technology. This includes permanent monitoring of access, for example using video monitoring systems, movement sensors, alarm systems and trained security personnel. Any provision components which are essential for operations, for example the power supply, air-conditioning and Internet connection, should be designed to be redundant.

Modern fire protection precautions also need to be taken, and tested on a regular basis. Overall, a data centre should form a security area that affords adequate protection against both damage by the elements, e.g. caused by storms and flooding, and against unauthorised entry. If a customer requires a particularly high level of availability for their services, the CSP should also reserve capacities in backup or redundant data centres which can compensate for another data centre failing. The data centres should be located far enough away from each other geographically so that a controllable damage event, e.g. fire, explo-

sion, road, rail, water or air accidents and natural disasters with a limited impact such as flooding does not simultaneously affect both the data centre originally being used and the one containing the backup capacities.

In the SaaS area, many providers do not operate their own infrastructure. If this is the case, the requirements set out here must be met by the subcontractor used by the SaaS provider, i.e. in this case the data centre operator.

Data Centre Security	Private ⇨			Public ⇨		
	B	C+	A+	B	C+	A+
Designing all the key supply components (power, air-conditioning in the computer centre, internet connection, wiring, etc.) to be redundant	✓			✓		
Monitor access: access control system, video monitoring systems, movement sensors, security personnel, alarm systems, etc.	✓			✓		
Two-factor authentication for access to the data centre	✓			✓		
Fire protection: fire alarm system, fire early detection system, suitable fire extinguishers, regular fire drills	✓			✓		
Robust infrastructure that provides adequate resistance to damage by the elements and unauthorised entry	✓			✓		
Redundant data centres that are, at least, far enough away from one another that a controllable damage event does not simultaneously affect the data centre originally used and the one containing the backup capacities			✓			✓

4.2 Server security

The servers represent the environment for performing the processes and their computations. For this reason the operating systems deployed on the servers should be hardened to the extent that they offer the smallest possible area to attack. To achieve this, when the basic installation is being undertaken, only the necessary software packages should be added and any superfluous programs and services should be disabled or, better, uninstalled. Standard measures to protect IT systems, such as host firewalls, host-based intrusion detection systems, etc. should be implemented and regular integrity reviews run on important system files. Host-based intrusion detection systems are characterised by the fact that they are run on the IT system to be monitored. They are typically deployed to detect attacks made at the application or operating system level. Examples of such attacks are policy violations by users, failed login attempts and malware such as Trojan horses.

The technical basis for providing and using cloud services reliably and securely are provided by a broadband connection, standardised and widely-used transmission protocols, a service-oriented architecture and, above all, virtualisation.

Providers deploy different hypervisors for server virtualisation. The hypervisor is the central component of server virtualisation controlling access to shared resources. With a few exceptions, no attacks on the hypervisor have yet appeared in the wild [8] - they have only been described in theoretical terms or as proof-of-concept. Should an attack succeed, however, the consequences are devastating. The hypervisor can be attacked, for example, by manipulating CPU registers that control the virtualisation functions. Errors in implementing the resources provided by the hypervisor to the virtual machines (VMs) can also cause the hypervisor to be compromised. To this extent, CSPs who deploy server virtualisation should revert to certified, hardened hypervisors. The recommendations that manufacturers publish on configuring virtualisation servers securely should be used when hardening hypervisors. Certification should be

based on the globally accepted “Common Criteria for Information Technology Security Evaluation”, known as the Common Criteria for short. The depth of testing that should be achieved in the certification process is evaluation assurance level EAL 4 at least.

In the case of offerings in the “IaaS compute” form, virtual machines are provided to the customer, e.g. via a web interface. In terms of making the virtual machines secure, it is helpful if the provider gives their customer guidelines on hardening the virtual machines. The customer should also be able to upload their own images for the virtual machines or to purchase quality-assured images from the provider.

PaaS or SaaS providers using server virtualisation, such as Microsoft with the Windows Azure platform, should also guarantee the security of the guest operating systems.

Server Security	Private ⇨			Public ⇗		
	B	C+	A+	B	C+	A+
Technical measures to protect the host (host firewalls, regular integrity checks, host-based intrusion detection systems)	✓			✓		
A secure basic configuration for the host (e.g. deploying hardened operating systems, disabling unnecessary services, etc.)	✓			✓		
Customers having the option to use their own images for virtual machines or use the provider's quality-assured images (with IaaS only)	✓			✓		
Secure default configuration for the guest operating system using hardened operating systems, disabling unnecessary services, etc. (with PaaS/SaaS only)	✓			✓		
Deploying certified hypervisors (Common Criteria EAL 4 at least)		✓	✓		✓	✓

4.3 Network security

In the past, Cloud Computing platforms have often been misused either by placing malware there which is then used to send spam, or their processing power has been exploited to crack passwords using brute force attacks or to hide command and control servers (C&C servers) used to control botnets. To prevent these and similar attacks as well as the misuse of resources, each CSP should take effective security measures to defend against network-based attacks. As well as the usual IT security measures such as anti-virus protection, Trojan detection, spam protection, firewalls, Application Layer Gateway and IDS/IPS systems, particular care should be taken to encrypt all communication between the CSP and the customer and between the provider's sites. If a third party provider is required to deliver the services, the communication with them also needs to be encrypted.

Because of the concentration of resources in centralised data centres, an attack which is a particular threat to public Cloud Computing platforms is the Distributed Denial of Service (DDoS) attack. According to a report by Arbor Networks, a provider of security solutions, DDoS attacks (such as the DNS Amplification/Reflection Attack) can now achieve enormous bit rates (over 100 Gbps) [9]. A standard backbone is designed for a far lower data rate. As a result, many CSPs can hardly defend against DDoS attacks using high data rates. This can have serious consequences for both the victim themselves and other connected customers. Against this background, each public CSP should undertake suitable measures to defend against DDoS attacks. Owing to the fact that many CSPs can scarcely protect themselves against DDoS attacks using high data rates, the option exists to buy these mitigation services from larger Internet service providers (ISPs) and regulate their use in agreements. Measures should also be implemented to detect internal DDoS attacks by cloud customers on other cloud customers.

The incorrect configuring of a system is frequently the reason for successful attacks. As Cloud Computing platforms consist of many different components,

the overall configuration is very complex. Changing a configuration parameter for one component (e.g. virtualisation server) can, when interacting with other components (e. g. network or storage) lead to security vulnerabilities, faulty functions and/or failures. For this reason, the components deployed need to be securely and carefully configured. All CSPs should also ensure that their networks are suitably segmented, preventing any faults from spreading freely. In this context the option exists to define and set up different security zones within the provider's network, based on the protection requirement. Examples include:

- Security zone for managing the cloud
- Security zone for the live migration, if server virtualisation is being used
- Security zone for the storage network
- With IaaS, customer to have their own security zones for the virtual machines

The CSP's management network should be isolated from the data network.

If the cloud infrastructure or cloud services are being administered remotely, this needs to be accomplished via a secure communication channel (e.g. SSH, TLS/SSL, IPSec, VPN).

If a service consumer has particularly high availability requirements in terms of the services they are drawing down, the CSP's sites should be networked on a mutually redundant basis.

Network Security	Private ⇨			Public ⇗		
	B	C+	A+	B	C+	A+
Security measures against malware (anti-virus, Trojan detection, anti-spam, etc.)	✓			✓		
Security measures against network-based attacks (IPS/IDS systems, firewall, Application Layer Gateway, etc.)		✓	✓	✓		
DDoS mitigation (protection against DDoS attacks)			✓	✓		
Suitable network segmentation (isolate the management network from the data network)	✓			✓		
Secure configuration of all components in the cloud architecture	✓			✓		
Remote administration via a secure communication channel (e. g. SSH, TLS/SSL, IPSec, VPN)	✓			✓		
Encrypted communication between Cloud Computing provider and Cloud Computing user (e. g. TLS/SSL)	✓			✓		
Encrypted communication between Cloud Computing locations	✓			✓		
Encrypted communication with third party providers where these are required for the provider's own offering	✓			✓		
Redundant networking of the cloud data centres			✓			✓

4.4 Application and platform security

In the case of offerings in the PaaS area, customers no longer have to worry specifically about database accesses, scalability, access controls, etc., as the platform provides these functionalities for them. Due to the fact that the customers use the platform's core functionalities to develop their own software, they can only succeed in developing software securely, if the entire software stack on the platform is developed and upgraded professionally and securely. CSPs typically deploy not just a large number of different software components, but they also continue to upgrade them in order to be able to optimally provide their customers with the services in the runtime environ-

ment. When developing software, all CSPs must have established security as a fixed component in the software development life cycle process (SDLC process). Security issues need to be addressed at each phase of the software development process, and programs and modules may only be deployed if they have been properly tested and approved by the CSP's security manager.

While software developed by the customer requires a secure basis (to be provided by the CSP), security issues also need to be considered in this respect. It is recommended that the CSP provides appropriate user guidelines for customers to create secure applications so that the programs the customer develops themselves fulfill certain minimum requirements in terms of security, documentation and quality. This is not only helpful for the customers but also emphasises the provider's expertise and reduces the danger of security vulnerabilities in customer software impacting on other customers.

If the CSP also calls in other suppliers to provide the platform's services, these requirements apply equally to them. Alongside code reviews, automated review tools should also be deployed and vulnerability tests run. Automated review tools can, for example, detect common programming errors such as infinite loops and null pointer exceptions. Where there is a higher level of protection requirement, the CSP should also automatically check the code the customers have developed themselves for vulnerabilities.

With PaaS, multiple customers share a common platform to run software. The customers' applications need to have guaranteed secure isolation, for example by using sandboxing technologies. Strict isolation of customer areas helps, for example, to prevent one application from unauthorised accessing another application's data.

As the cloud communication is fundamentally based purely on web technologies, e.g. web interfaces for cloud users and application administrators, application frameworks such as Java and .NET, communication via HTTP(S), the security of cloud applications against attacks at the application level takes on

even more importance than is the case with traditional web applications. Therefore all CSPs should ensure that they comply with the principles of secure software development as specified in the Open Web Application Security Project when producing the applications designed against the main security risks for web applications (OWASP Top 10) [10].

It is still important to have a well-integrated, effective patch and change management system so that operating faults are avoided and security vulnerabilities are minimised and can quickly be resolved. For quality assurance and in order to be able to detect errors and prevent future errors, each patch and each change should be adequately tested and their effectiveness evaluated before they are implemented.

Application and Platform Security	Private ⇨			Public ⇗		
	B	C+	A+	B	C+	A+
Security must be a basic component of the software development life cycle process (reviews, automated tests, vulnerability tests, etc.)	✓			✓		
Securely isolated applications (PaaS)	✓			✓		
The web applications provided comply with minimum security standards (e.g. the principles of secure software development as per OWASP)	✓			✓		
Guidelines for customers to create secure applications (PaaS)	✓			✓		
Automated checking of customer applications for application vulnerabilities, particularly before going live (PaaS)		✓	✓		✓	✓
Patch and change management (patches, updates and service packs deployed swiftly) and release management	✓			✓		
Ensuring that patches are compatible on test systems before adopting them in production	✓			✓		

4.5 Data security

The data life cycle comprises its generation, data storage, data usage, data distribution and data destruction. Each CSP should support all these phases in the data life cycle with appropriate security mechanisms.

A number of storage technologies, e.g. NAS, SAN, Object Storage, etc., are used to store data. Common to all these storage technologies is the fact that many customers share a common data storage. In this type of constellation, a secure separation of customer data is essential and should, therefore, be guaranteed.

With SaaS, for example, customer data is usually stored in a common table. The distinction between customers is then achieved using a so-called tenant ID. If the web application (shared application) is insecurely programmed, a customer could possibly use an SQL injection to gain unauthorised access to another customer's data, and delete or manipulate it. To prevent this, appropriate security measures must be implemented.

As with traditional IT, in Cloud Computing data losses are a threat that must be taken seriously. To avoid data losses, each CSP should do regular data backups based on a data security plan. Technical defects, incorrect parametrisation, obsolescent media, inadequate data media administration and non-compliance with regulations stipulated in a data security plan can result in an inability to reinstall backups and reconstruct the data inventory. So there is a need to sporadically check whether the data backups created to restore lost data can be re-used. Depending on the length of time between backing up the data and restoring the data due to data loss or some other incident, the most recent data modifications may be lost. So a CSP should immediately notify its customers if data backups need to be restored, and in particular indicate the status of the backup. The backing up of data (scope, save intervals, save times, storage duration, etc.) should be transparent and auditable for the customers.

It may also be useful to the customer if cloud providers provide them with the option of backing up data themselves.

Because of the underlying multi-tenant architecture, customer data can often only be deleted permanently – i.e. fully and reliably – at the request of a service consumer, for example when a contractual relationship ends, after a certain period of time. The SLAs should make this period clear. When the specified time-scale has elapsed, all the customer data must then be fully and reliably deleted from each storage media. To delete data selectively, care must be taken to delete not only the current version but all previous versions, including temporary files and file fragments.

Therefore all CSPs should have an effective procedure for securely deleting or destroying data and data media. customers should ensure that their agreement specifies at which time and in which manner the CSP must completely delete or destroy their data or data media.

Data Security	Private ⇨			Public ⇗		
	B	C+	A+	B	C+	A+
Defining and implementing data security in the life cycle of the customer data	✓			✓		
Securely isolating the customer's data (e.g. virtual storage areas, tagging, etc.)	✓			✓		
Regular data backups, with customers being able to audit their basic parameters (scope, save intervals, save times and storage duration)	✓			✓		
Data must be fully and reliably deleted at the customer's request	✓			✓		

4.6 Encryption and key management

To be able to store, process and transport sensitive data securely, suitable cryptographic methods and products should be used. The management of cryptographic keys in Cloud Computing environments is complex, and there are currently no appropriate tools for key management. For this reason, most providers do not encrypt data categorised as 'at rest'. With "IaaS storage" offerings, however, the customer has the option of encrypting their data themselves prior to storage. In this way, they retain complete control over the cryptographic keys and also obviously need to deal with key management.

If the provider encrypts the data, suitable security measures should be implemented at each phase in a cryptographic key's life cycle to ensure that keys are generated, stored, shared, used and destroyed on the basis of confidentiality, integrity and authenticity. As highly complex factors need to be considered when using cryptographic methods, each CSP should draw up a cryptography strategy. If customers are to know which tasks the CSP is taking on with respect to cryptography, and which issues they themselves need to consider, it is a good idea if providers provide customers with an overview of the cryptographic mechanisms and methods used.

The following key management best practices should be implemented:

- Keys should be generated in a secure environment and using suitable key generators.
- Where possible, cryptographic keys should be used for one purpose only.
- In general, keys should never be stored in the system in a clear form, but always encrypted. Furthermore, the storage should always be redundantly backed up and restorable, to avoid losing a key.
- The keys must be distributed securely (on the basis of confidentiality, integrity and authenticity).
- The cloud's administrators should have no access to customers' keys.

- Keys should be changed regularly. The keys used should be regularly checked to ensure they are current.
- Access to key management functions should require a separate authentication.
- The keys should be archived securely.
- Keys that are no longer required (e.g. keys whose validity duration has elapsed) should be deleted or destroyed in a secure manner.

Adequate cryptography skills are required for reliable key management. For this reason, CSP personnel who are responsible for key management must be identified and trained.

Key Management	Private ⇨			Public ⇗		
	B	C+	A+	B	C+	A+
Implementing key management best practices	✓			✓		
providing customers with access to a crypto overview		✓			✓	

5 ID and rights management

Identity and authorisations management is a major part of access control. A CSP should make these secure using suitable organisational, personnel and technical measures. For this reason all Cloud Computing platforms should support identity management. The basis for this support can be either that a service provider supplies the customer with an ID management system themselves, or that they supply interfaces to external identity providers. For both models, service providers with or without an integral ID management system, the issues of authentication and authorisation which need to be mapped in Cloud Computing platforms will be examined more closely below.

Authentication

In Cloud Computing, hardware, software and services are used by many users. The role of identity and authorisations management is to ensure that only authorised persons may use the IT resources. Access to all the IT systems or services must be made secure by identifying and authenticating the users or IT systems seeking access. For security-critical application areas, strong authentication should be used, i.e. two-factor authentication as is normal, for example, in online banking. Any network access should, in principle, be made secure by strong authentication. These strict requirements apply particularly to the CSP's staff. They, too, should only gain access to the IT resources being administered via strong authentication, i.e. for example via a hardware-based authentication system using chip cards or USB sticks or via one-time passwords that can also be generated by hardware devices. This is absolutely indispensable for access via the Internet. If a CSP administrator accesses the CSP systems from a secured company network via a VPN for which they have already had to authenticate themselves with two factors, then in this case a second two-factor authentication can be dispensed with.

Where security requirements for the services provided are high, service users too can only be given access to the services after a strong (e.g. two-factor) authentication, if the access to the service used ensues directly via the Internet. If a customer accesses the cloud services for which they must authenticate themselves with two factors via a VPN from the secured company network, no additional two-factor authentication to use the cloud services is necessarily required.

In the case of encrypted communication between a CSP and service consumers, as specified in Section 4.3, access to the services can be restricted to particular IP addresses or domains in order to increase security.

Another issue playing a key role in Cloud Computing is the federation of identities when authenticating corporate customers, when providing single sign-on (SSO) solutions and the sharing of identity attributes between the service provider and the identity providers. In the corporate environment, SAML or WS Federation are widely used, with SAML being far more popular. The alternative to SAML and WS Federation is a SSO solution that is deployed via a secured VPN tunnel. The widely used SAML standard is often used in versions 1.1 and 2.0. Where possible, SAML 2.0 should be supported because various proprietary upgrades have been integrated into this standard, enabling the addressing of a broad base of deployment scenarios.

Authorisation

The rights management system must ensure that each role may only see the data (including meta-data) required to achieve the task. The access control should be role-based and the roles and authorisations set up should be reviewed regularly. In general, the least privilege model should be used, with users and CSP administrators only possessing the rights that they require to achieve their tasks. Particular attention should be directed here towards privileged users. If the role is that of a CSP administrator, it should be possible to demonstrate that the only data viewed was that which was required for the task.

The rights management system should also be capable of fully documenting and monitoring data exports and imports from and to the CSP. Lastly, any particularly critical administration activities, such as installing patches, should only be performed on the four-eye principle.

ID and Rights Management	Private ⇨			Public ⇗		
	B	C+	A+	B	C+	A+
Strong authentication (two factor authentication) for the CSP's administrators	✓			✓		
Role-based access control and regular reviews of roles and rights	✓			✓		
Least Privilege Model (users and CSP administrators should only possess those rights required to perform their task)	✓			✓		
Four-eye principle for critical administration activities		✓	✓		✓	✓
Strong authentication (e.g. two factor authentication) for cloud customers		✓			✓	

6 Control options for users

With public Cloud Computing, the customer is strongly dependent on their cloud provider – after all, they can no longer directly access any hardware or software and they depend on the availability of the services running in the "cloud". To this extent, the customer should have the capability to monitor the availability of the services they use, e.g. via a web interface or API. Numerous CSPs already practise this. In many cases the customers can display the status of the services they use on a web page belonging to the CSP. Customers can also use additional services that can be reserved through the CSP or third-party providers' tools, to obtain a wide range of monitoring data about the performance of the services used, such as CPU utilisation, network utilisation, throughput, latency and average transaction time.

Customers should also ensure that they are able to monitor the service quality specified in their agreement. The CSP ought to provide suitable interfaces for this purpose.

Control Options for Users	Private ⇨			Public ⇨		
	B	C+	A+	B	C+	A+
Customers must be able to monitor measurable parameters as agreed in the SLA	✓			✓		

7 Monitoring and security incident management

An extensive monitoring capability is essential if the operational security of a Cloud Computing platform is to be assessed. Besides monitoring performance in complying with the SLAs and also for invoicing purposes, security monitoring is also important in a cloud environment. To sustain information security in operation, it is necessary to plan and practise the handling of attacks and security incidents in advance. Cloud services should be extensively monitored round the clock (24/7), and staff should be held in reserve to respond promptly to attacks and security incidents. If so regulated in the SLA (e.g. where there is a high availability requirement for the cloud services), the customers should also be able to contact the CSP's security incident handling and troubleshooting team round the clock.

For administration to be auditable, all administrative activities should be logged. In this way, the CSP can provide their customer with evidence of when and which changes have been made to the service, and by whom.

To identify attacks, log files (e.g. showing system statuses, failed authentication attempts, etc.) and other data sources relating to security, e.g. analyses by system monitoring tools (IDS, IPS, integrity checkers, etc. see Section 4.3) should be used and correlated. Where a customer has a high requirement for protecting the confidentiality of their information, other tools can, if necessary (e.g. for data leakage protection) be deployed to control the data flow to the network and/or to terminals. These should detect or even intervene, if confidential data is sent via insecure routes or falls into the wrong hands. This type of tool checks, for example, whether particular data has been sent by email, data sharing or via Internet use, or whether it should be burned on a CD or copied to a USB stick. Since confidential or personal data can sometimes be viewed using this type of tool, their use must be carefully planned and agreed between the CSP and customer.

If the CSP detects attacks on the Cloud Computing platform, they should respond promptly and adequately and take appropriate counter-measures. Because of the multi-tenant architecture, particular attention should also be paid to internal attacks by cloud users on other cloud users when planning attack detection measures. It is also important to assess messages about new vulnerabilities in the IT components deployed, and to review whether open vulnerabilities can be exploited.

With public Cloud Computing, the customer has a priori only a limited view of the log files. Here, customers should be able to access some of the log files via an external interface, e.g. those showing failed authentication attempts. To this extent it is important that the CSP responds promptly to security incidents and notifies customers about potential impacts that may affect their services.

Another important point is that the CSP should offer the customer the option of storing the relevant log files in a audit-compliant form.

Besides providing rapid information, the CSP should provide the customer with all the log files relevant to them in a suitable format. There is the option here of providing them in a format which is suitable for machine processing so that the customer can, if they require, integrate them into a Security Incident and Event Management (SIEM) tool.

Monitoring and Security Incident Management	Private ⇨			Public ⇨		
	B	C+	A+	B	C+	A+
24/7 extensive monitoring of the cloud services and prompt responses to attacks and security incidents	✓			✓		
Recording and analysing data sources (e.g. system status, failed authentication attempts, etc.)	✓			✓		
24/7 contactable security incident handling and troubleshooting team with the authority to act			✓			✓
CSP obligations to notify the customer about security incidents or provide information about security incidents potentially affecting the customer	n/a			✓		
CSP provision of relevant log data in a suitable form	✓			✓		
Logging and monitoring of administrator activities	✓			✓		

8 Business continuity management

Preventive protection against potential threats is a key task when considering security measures. However, experience shows that despite the best precautions, serious incidents and disasters cannot be entirely prevented. And it is often unexpected events which bring the greatest risk, e.g.:

- When a Hanover substation failed in October 2008, cash machines, statement printers and online banking in around 150 financial institutions across Germany became unusable.
- In January 2009, faulty maintenance work in a data centre resulted in rail tickets throughout Germany being unable to be printed out for several hours. The trains suffered substantial delays or were unable to run at all, and customers in many locations complained that they were unable to get adequate information from the transport company concerned.
- In April 2010, an eruption of the Eyjafjalla volcano in Iceland brought air traffic to an almost complete standstill for days in Europe which led many companies to fear production disruptions due to delayed deliveries.

What all these examples have in common is the fact that what appeared to be merely local events had unanticipated, widespread impacts and caused substantial damage in other sectors. However, when one looks more closely at these and similar incidents, it can be repeatedly seen that there were deficiencies in the way the organisations affected had prepared for such events. There was a lack of rules regarding responsibilities and an absence of backup capabilities, crisis communications were inadequate, contingency plans were out of date or non-existent – the list of potential defects could go on and on.

To be armed against such incidents, and to be capable of responding adequately to emergency situations, all CSPs should, therefore, have a functioning business continuity management system based on established standards such

as BS 25999 and BSI standard 100-4 [11]. This involves developing appropriate organisational structures and plans that enable a rapid response when emergencies occur and a quick resumption of at least the crucial business processes.

One of the most important up-front tasks is to prioritise which of the services and business processes being run should be restarted first. To do this, the CSP needs to determine their availability requirements and clearly explain the consequences to their customers, because the priorities and the restart times that are set have financial impacts on both sides. Dividing the cloud services into restart categories can be a good idea here.

Building on this, contingency plans and measures should be developed and implemented which enable effective crisis management and the rapid resumption of the critical business processes as specified in the prioritisation.

To verify the efficacy of measures in the business continuity management area, each CSP should carry out regular tests and emergency exercises. These will not only check that the crisis management strategies and plans work, can be implemented and are auditable, but staff too will acquire the necessary practice in dealing with exceptional situations. As tests and exercises can be very time-consuming, careful thought has to be given as to which types of check are useful for which purpose. Any plan that is drawn up should describe which tests and exercises are scheduled. The main aims of exercises are to uncover any inconsistencies in the crisis plans or defects in the planning and implementing of crisis measures, and to provide training in effective, smooth workflows in the event of an emergency. Typical exercises might be:

- Function tests (e.g. on power units, air-conditioning systems, central servers),
- Carrying out fire drills,
- Restarting individual resources or business processes after a failure,

- Evacuating an office building and moving to a backup location, and
- Closing down one data centre and starting up a backup data centre.

Where processes have a high protection requirement in terms of availability, the CSP should provide evidence that their business continuity management is based on a recognised standard, e.g. BS 25999 or BSI standard 100-4 and that their crisis organisation and crisis strategy (comprising the two main components, i.e. the crisis prevention plan and the emergency manual) are effective and efficient.

Business Continuity Management	Private ⇨			Public ⇨		
	B	C+	A+	B	C+	A+
The cloud provider must set up and operate a business continuity management system	✓			✓		
The CSP must make the prioritising of the restart for the cloud services provided transparent to their customers			✓			✓
Regular business continuity management exercises (e.g. in the closing down of a Cloud Computing location)			✓			✓
The CSP should provide evidence that their business continuity management system is based on an internationally recognised standard such as BS 25999 or BSI standard 100-4 (e.g. using a contigency planning concept and a business continuity handbook)			✓			✓

9 Portability and interoperability

Interoperability in Cloud Computing platforms refers to the capability of having two or more independent Cloud Computing platforms working together, without a need for specific agreements between the platforms. The use of common standards is the basis for this.

Portability and platform independence, on the other hand, refer to the cloud service property of being capable of running on different Cloud Computing platforms.

In the case of data, portability means that it can be exported from one cloud service and imported to another service. In the case of SaaS offerings, the customer acquires the right to use a software service. Since the customer normally relies on the fact that this service is delivered based on the agreement signed, this creates a bond with the cloud service provider. To prevent a so-called vendor lock-in, i.e. a dependency on the provider which is difficult to break, it is important that the customer's data and applications remain portable. For this reason, the portability of the data must be guaranteed as part of an exit agreement with ensured formats and the retention of all logical relations. If, for example, the data is migrated to another CSP, costs might be incurred which the cloud service provider should explain to their customers.

At the current time, no platform independence between different CSPs can be guaranteed. Platforms such as Force.com from Salesforce (uses the APEX programming language, a subset of Java), SAP Business byDesign, Microsoft Azure (.NET, PHP; Ruby, Python or Java) and Google App Engine (Python, Java) provide customers with a number of functionalities for developing SaaS applications. Where a service consumer creates their own services based on a PaaS service, they have to choose one of the available platforms. For example, it is not currently possible to use a Microsoft Azure database service via a cloud serv-

ice developed on Google App Engine. A service developed on one platform can currently not normally be ported without a great deal of work. In such cases, a new cloud service often needs to be developed.

In the case of offerings in the IaaS Compute form, VMs can be made portable by using OVF (Open Virtualization Format). OVF is a platform-independent standard for packaging and distributing virtual appliances [12]. Currently, however, almost all virtual machine providers use their own formats, which makes it difficult for service consumers to switch provider. In the case of Amazon, for example, both the API for managing the cloud services and the format of the virtual images are proprietary. In general, it would be welcome if the service providers supported OVF.

There are now a number of industry standards for reducing interoperability and portability problems that can be used in the Cloud Computing area, some of which are already being used. These include the Open Cloud Computing Interface (OCCI) of the Open Grid Forum [13], the vCloud API from VMware [14] and the OVF format referred to above. Another way for service providers to improve interoperability and portability is to reproduce existing, manufacturer-specific interfaces, as was for example done with the Amazon web services interface for Eucalyptus open source software. To ensure interoperability, Cloud Computing providers should use standardised or open interfaces (API and protocols).

Portability and Interoperability	Private ⇨			Public ⇗		
	B	C+	A+	B	C+	A+
Exit agreement with assured formats and retention of all logical relations and specifying any associated costs (SaaS)	✓			✓		
Standardised or open interfaces (API and protocols)	✓			✓		

10 Security testing and Audit

A vital part of any successful information security management system are regular reviews of the established security measures and data security processes. Cloud service providers must regularly review the IT security status of their business processes, services and platforms, as well as improving and upgrading them on an ongoing basis. There is the option of having an independent third party carry out regular reviews and tests in order to avoid blindness to one's own professional shortcomings, and provide cloud users with the evidence of such tests.

Based on an information security review (IS review), statements can be made about the effective implementation of security measures and their currency, completeness and adequacy and hence about the current information security status. The IS review is therefore a tool for identifying, achieving and maintaining an adequate level of security within an institution.

The key requirement for CSPs in terms of testing and certifying security has different facets:

- The results of tests that CSPs carry out themselves should be published in a suitable form.
- The customers have a justifiable interest in carrying out their own security tests or having them carried out on their behalf by a third party.

If a CSP uses a subcontractor to deliver their services, this does not free them from the obligation of reviewing the security of such services, because the CSP is responsible to their customers for the overall security of their offering and cannot delegate this to subcontractors. In cases such as these, the CSP should ask their subcontractor for the required evidence resulting from all the necessary security tests. In general, the security tests carried out should be documented in such a way that they can be passed on to their

customers where required, both by the CSP themselves and their subcontractors.

Regular security reviews must be carried out in the case of both public and private cloud services. However, it is typically easier for operators to pass the results of security reviews, e.g. penetration tests, on to users in the case of private clouds, because the users are all within one common institution.

To review the effectiveness of existing technical measures, penetration tests are a suitable tried and tested method. They are used to assess in advance the probabilities of success of a deliberate attack on an information domain or an individual IT system, to derive the necessary supplementary security measures from this, and to review the effectiveness of security measures already been taken. CSPs should carry out regular penetration tests on the networks, systems and applications they run.

In general, all types of security test should be carried out by individuals with suitable skills. These should not, however, have been involved in drawing up the strategies and plans being tested, in order to avoid conflicts and business blindness. The testers and auditors should be as independent and neutral as possible.

Security Testing and Evidence	Private ⇨			Public ⇗		
	B	C+	A+	B	C+	A+
Cloud service providers should regularly notify cloud users about security measures, changes to the IT security management system, security incidents, the results of IS reviews and penetration tests	✓			✓		
Regular penetration tests	✓			✓		
Regular penetration tests at subcontractors	✓			✓		
Regular, independent security reviews		✓	✓		✓	✓
Regular, independent security reviews at subcontractors		✓	✓		✓	✓

11 Requirements of personnel

Responsibility for information security lies directly with those individuals who are handling the information concerned. It is therefore essential that the staff working for CSPs have been adequately inducted and trained in all the techniques used and in information security and data protection. Individuals who have security-related tasks, such as administrators and employees with access to financially-related or confidential information must be trustworthy and reliable.

Trustworthy staff

The ways in which the trustworthiness of new or third party staff can be verified are very restricted by law, both in Germany and in many other countries. On top of which, the results are often rather meaningless, as is the case with police certificates of good conduct. The principle remains, however, that before the CSP takes on new or external staff, a check should be run to see

- whether they have adequate references, e.g. from other, similar lines of work, and
- that the applicant CV which has been submitted is complete and relevant.

It is also a good idea to get confirmation of any academic or professional qualifications, for example by sending a request to the university or previous employers or customers. The data protection laws should always be complied with when checking on the individual.

If a CSP uses external staff who have access to internal applications and data, similar checks should be carried out as for in-house personnel. When contracts are being drawn up with external providers, they should specify which party is to carry out these checks and how deep they should go.

Issuing tasks and the roles thereby required should be structured in such a way that operational and controlling functions are issued to different people in order to minimise or completely eliminate conflicts of interest amongst them. Attention should also be paid to conflicts of interest that may arise, if an employee holds different roles that either give the person wide-ranging rights or are mutually exclusive. Moreover, employees' tasks should not be affected by conflicts of interest external to the authority or company, for example, by previous positions or other obligations. A role-based rights management system which only permits access to the data and systems required to perform the tasks concerned offers the necessary organisational and technical support here.

In particular, all those people with access to customer data should have their attention drawn to their obligations when handling it. Attention should also be paid to the selection of staff and their skill levels in subcontractor companies.

Staff must not only receive instruction on the existing regulations and guidelines on information security, on data protection and on dealing with customer data, but they must also be obliged to comply with them.

Training

Many new technologies and IT components are being used in Cloud Computing. The innovation and update cycles are therefore extremely short in this sector, and for this reason, CSPs should provide their employees with regular training enabling them to master all the technologies, components and functionalities being used. The staff should also understand and be familiar with all the security implications relating to these technologies. This particularly applies to the group of people involved in developing and operating cloud services.

Because faulty configurations in a Cloud Computing environment can have serious consequences for the resources provided there, the requirements on administrators are accordingly greater. It is therefore important for the admin-

istrators to have adequate knowledge of the products deployed and their underlying technologies, so that they can avoid problems arising from their own actions, identify and resolve technical problems at an early stage, and make optimal use of the functions and security features of the technologies the Cloud Computing is based on – in particular, they should be capable of assessing the consequences of configuration changes.

To ensure that administrators are also kept informed of the latest security risks associated with Cloud Computing and of the latest developments in the dynamic data centre area, the CSP should ensure that they receive regular training.

All of the CSP's staff should also be sensitised on an continuing basis to general data security and data protection issues.

Requirements of the Staff	Private ⇨			Public ⇨		
	B	C+	A+	B	C+	A+
Trustworthy staff	✓			✓		
Education of the cloud service provider's staff (regular training)	✓			✓		
Raise awareness among cloud service provider employees on information security and data protection issues	✓			✓		
Employees obliged to adhere to regulations on information security, data protection, adequate handling of customer data	✓			✓		

12 Drawing up agreements

The precise details involved in the use of cloud services should be clearly regulated. This includes describing the required services i.e. service level agreements, and clarifying such points as contact persons, response times, IT connection, service monitoring, the nature of security precautions, dealing with customer data and passing information to third parties.

12.1 Transparency

Only when the CSP can convincingly demonstrate to their customers how and on which basic conditions they operate, will the customers develop the necessary trust in the CSP beyond the technical measures that the CSP is taking. Public cloud providers, in particular, are obliged to give the customer the information required.

Initially, cloud service providers should present their contractual and business conditions in a way that can be clearly understood. Above all, it should be transparent which interventions the cloud service provider or third parties are permitted to make in the customer's data and procedures. The basic contract also includes Service Level Agreements (SLAs) which regulate, for example, the scope of the services provided, availability requirements, response times, processing power, the storage space available and support.

Cloud service providers must make clear to their customers at which locations (i.e. which countries and regions) the data is to be stored and processed. In this context, the issue is less the geographical distance, than the question as to what kind of impact the choice of location can have on the services provided and the data stored. Another key point is how the locations concerned are made secure and how third party access to the customer data is regulated.

Depending on the location of the CSP's data centres, different legal situations need to be taken into account. In some countries, for example, crypto-

graphic methods may not be used without approval. This can result in a situation where the CSP may in fact use encryption but may have to provide state agencies with access. CSPs should, therefore, tell their customers which local regulations might impact on the confidentiality, integrity or availability of the customer data.

CSPs should also make it clear what their legal and ownership situation is. Only in this way can customers judge whether a CSP is a suitable business partner.

If, for example, a CSP belongs to a company in competition with a cloud customer, this could lead to conflicts of interest, and finally to the customer or the CSP terminating the existing agreements. So it can be important to know to whom the CSP belongs and how decision-making is structured in the CSP. Not all legal statuses permit such statements, however, because the ownership structure in companies quoted on the stock exchange can change and only large shareholders are obliged to publish their holdings.

In all cases the CSP should exempt the customer from legal disputes relating to licence fees or patent disputes when using the service.

Many SaaS providers do not operate their own infrastructure but use PaaS or IaaS offerings from other CSPs. In these cases the subcontractors crucial in delivering the cloud services must also be disclosed to customers, who should be given the necessary information.

If there is any substantial change to any of the above items, the CSP should notify their customers in a suitable way.

If specific cloud services can only be used if the customers install programs provided by the CSP beforehand (e. g. browser plug-ins with SaaS), then customers must be informed of this before contracts are signed. The CSP should also indicate to customers any security risks that might arise from using them, and any security measures that the customer should take.

Transparency	Private ⇨			Public ⇗		
	B	C+	A+	B	C+	A+
Disclosure of the cloud service provider's locations (country, region) where the customer data will be stored and processed	✓			✓		
Disclosure of the cloud service provider's sub-contractors who are vital for providing the cloud services	✓			✓		
Transparency as to which interventions the cloud service provider or third parties are allowed in the customer's data and processes	✓			✓		
Providing regular information about changes (e.g. new or discontinued functions, new subcontractors, other SLA related issues)	✓			✓		
Transparency as to which software the cloud service provider will install onto the customer's systems and the security requirements / risks resulting from this	✓			✓		
Transparency on governmental intervention or viewing rights, on any legally definable third party rights to view data and on any obligations that the cloud service provider has to check stored data at any potential location	n/a				✓	✓
The cloud service provider to explain their legal and ownership structure and decision-making powers	n/a				✓	✓

12.2 Service level agreements (SLA)

A service level agreement (SLA) contractually specifies the services that the CSP will deliver, whereby it usually focusses on the functional and legal issues involved. SLAs usually consist of general and quantitative descriptions of services. The CSP is only committed to deliver the functionalities agreed in the SLAs. If specific values are given for individual issues, these should also be measurable, e.g. availability requirements. The CSP must allow their customers the possibility to verify compliance with the agreed values or have them verified. The CSP may, for example, provide their customers with access to these service parameters via special interfaces.

Also important are rulings on the place of jurisdiction, the applicable law and the language of the agreement. Property rights and copyrights to data, systems, software and interfaces must thereby be stated.

The SLA should also specify security-related content. For example, the CSP may undertake to implement particular security measures (e. g. use an intrusion prevention system). Even though the user may not be able to verify this immediately, indicating security measures creates trust in the CSP. Non-disclosure agreements should also be contractually agreed. This may also be done in an additional security SLA.

If a CSP uses a subcontractor to deliver the services provided (e.g., if an SaaS provider uses a third party IaaS), the CSP can themselves generate trust by showing the cloud users the relevant declarations on data security and service quality from the SLAs with the third party providers.

If a business is outsourced or the CSP becomes insolvent, the customer should still be able to access their data, and the confidentiality of the data and availability of the applications and data must continue to be guaranteed. In this context, German insolvency law contains regulations to be complied with in order to guarantee this. If the CSP is not subject to German law, the relevant regulations must be explained to the customer.

When an order comes to an end, Cloud Computing providers should be obliged to hand over all the customer data they have, including backups, and to delete all of the customer's stored data.

Service Level Agreement (SLA)	Private ⇨			Public ⇗		
	B	C+	A+	B	C+	A+
Defined security services clearly highlighted by Security SLA or in the SLA	✓			✓		
Ensuring operation or provision of data if the cloud service provider becomes insolvent, observing confidentiality undertakings and data protection requirements		✓	✓		✓	✓

13 Data protection and compliance

13.1 Data protection[1]

If personal data is gathered, processed or used in the cloud, its protection must be guaranteed in compliance with data protection laws.

A feature of Cloud Computing is the cloud user transferring data to the cloud provider. Where the data is (also) personal, in the context of data protection law this transfer is a case of transmitting personal data or of processing personal data on behalf of others, which is not to be classified as transmission. The legal classification of the transfer depends on the legitimacy of the transfer under data protection law and on its contractual legal form.

In the case of a data transfer from the cloud user to the cloud provider, the cloud user cedes all of their legal responsibility for data protection to the cloud provider. In principle, they also then lose the option of exercising any influence over the handling of the data they have transmitted. However, at the civil law level, depending on how the agreement has been drawn up, a different assignment of liability may be possible, namely that part of the liability remains with the cloud user. The cloud user must check up front, whether this type of solution is in their interests.

The transmission requires a legal basis under data protection law. Where the cloud user is not working for a public authority, the options for this are either the consent of the individual concerned or a balancing of interests as specified in Article 28 Para. 1 Clause 2 BDSG (German Data Protection Act), providing no area-specific law (e. g. Article 97 Para. 1 German Telecommunications Act) applies. If the cloud user is completely outsourcing parts or all of their data processing, the content channel would often be impractical since, where con-

1 The "Data Protection" section was drawn up with the involvement of the BfDI (Federal Commissioner for Data Protection and Information Freedom)

sent is not given or subsequently withdrawn, outsourcing would not be permitted (any longer) because of an absence of any legal basis. In the case of a balancing of interests under Article 28 Para. 1 Clause 2 BDSG, outsourcing to the cloud is not permitted if this is required to protect the legitimate interests of the individual concerned and there are no grounds for assuming that those interests of the individual concerned which merit protection outweigh exclusion from the outsourcing. Whether these conditions apply needs to be examined in each individual case. It will primarily depend on the recipient of the transmission (the Cloud Computing provider) having the same level of data protection as the cloud user, the individual concerned being able to assert their rights vis-a-vis the provider in a simple manner, and there being a certainty that the provider will only process and use the data for the purposes specified.

Where personal data is being processed on behalf of others, the legal responsibility for data protection remains unreservedly with the cloud user – as the controller. Under data protection law, the cloud user retains complete control of the data. In principle, processing personal data on behalf of others is not tied to any other material requirements; however a number of formal requirements need to be implemented. Processing personal data on behalf of others requires a written agreement which should include at least those points listed in Article 11 Para. 2 BDSG. As the processor (contractor), the Cloud Computing provider is subject to the instructions of the cloud user and is not permitted to make their own decisions about processing and using the data. The controller should assure themselves that the processor's technical and organisational measures are being complied with before data processing commences and at regular intervals thereafter. This need not necessarily be done through on-site checks, but rather by independent bodies.

There may only be recourse to the privilege of processing personal data on behalf of others, if the Cloud Computing provider is based within the EU or countries in the European Economic Area (EEA) and the data is also being processed there (Article 3 Para. 8 BDSG). Where data is being processed in other

countries, the requirements for data transmission should be met and the Cloud Computing provider should have an adequate level of data protection. Where the EU Commission has not certified an adequate level of data protection for individual countries as a whole (e.g. as in the case of Switzerland, Canada and Argentina), various measures might be considered, each of which are covered by Article 4c BDSG.

13.2 Compliance

Besides the legal data protection requirements, the cloud service provider should comply with the other legal provisions requested by the cloud user. This presupposes that the cloud user has notified the Cloud Computing provider of their specific legal requirements to be fulfilled so that the provider can decide whether they can in fact fulfil them or, alternatively, the provider explains specifically which legal requirements they will fulfil. The user can then decide whether this meets their needs. Purely as examples, we would mention requirements under the German Telecommunications Act (TKG), the Fiscal Code (AO) when processing data relating to tax laws, the Commercial Code (HGB) when processing data relating to accounting data, and the Penal Code (StGB) in case duties of confidentiality are affected.

Data Protection and Compliance	Private ⇨			Public ⇗		
	B	C+	A+	B	C+	A+
Guaranteeing data protection under German law	✓			✓		
Compliance with the data protection guidelines and laws to which the cloud user is subject	✓			✓		
When transmitting data: legal basis for the transmission: ▪ Article 28 Para. 1 Clause 1 No. 2 BDSG ▪ Consent	✓			✓		

Data Protection and Compliance	Private ⇨			Public ⇗		
	B	C+	A+	B	C+	A+
When processing personal data on behalf of others: written agreement between cloud user and cloud provider as specified in Article 11 Para. 2 BDSG with minimum content as per Article 11 Para. 2 Clause 2 BDSG, incl.: ▪ Describing the object and duration of the order ▪ Describing precisely the gathering, processing and use of personal data ▪ Specifying technical and organisational measures: ▪ Specifying the exact location where personal data is processed by the cloud provider, including the technical and organisational processing environment ▪ Handling the requests of those concerned as relating to the correcting, locking and deleting of personal data ▪ Compliance with Article 11 Para. 4 BDSG ▪ Identifying or forbidding any subcontracting relationships ▪ The cloud user's monitoring rights ▪ The cloud user's rights to give instructions ▪ Returning or deleting data when the order ends	✓			✓		
On transmission and processing data on behalf of others: storing and processing personal data ▪ Within the EU member states or a EEA signatory country or ▪ Outside the EU or a EEA signatory country, if an adequate level of data protection can be guaranteed e.g. via: – An EU Commission decision – Signatory to the Safe Harbor Agreement (USA) – Standard EU contract clauses – Permission from the supervisory authority	✓			✓		

Data Protection and Compliance	Private ⇨			Public ⇗		
	B	C+	A+	B	C+	A+
No involvement of a subcontractor who is unable to guarantee that personal data will be processed under the conditions indicated above	✓			✓		
When processing data on behalf of others, customers have the right to monitor that their personal data is being processed in compliance with data security law via ▪ Onsite checks or ▪ Reports by an independent expert	✓			✓		
When processing data on behalf of others: the supervisory authority responsible for the cloud user has monitoring rights	✓			✓		
When processing data on behalf of others: the cloud user has the right to give instructions to the cloud provider	✓			✓		
The provider should comply with any laws which the cloud user feels are relevant	✓			✓		

14 Prospects

Cloud Computing promises great flexibility in reserving, using and decommissioning resources depending on current requirements. A high levels of savings is also anticipated in the area of IT systems which would otherwise need to be reserved, maintained and renewed at the local level. If the promised flexibility is to become reality, there is a great need to standardise the services offered by Cloud Computing and the related interfaces. This will enable customers to invariably procure the latest technologies. Another advantage of Cloud Computing is the ubiquitous availability of business applications (depending on the cloud model), a key issue in the increasing mobility of employees.

Facing these potential benefits are a number of challenges which need to be resolved before business data or applications are outsourced to a public cloud. The reason for this with public Cloud Computing is that data and applications are outsourced away from the premises, the institution itself losing direct control of them. A large number of legal and contractual guidelines and rules, such as data protection requirements, also need to be taken into consideration if business-critical or personal data, for example, is to be outsourced to a public cloud. With public Cloud Computing, moreover, unknown users share a common infrastructure. This increases the risk that core information security parameters might be violated. Moreover, data and applications are being used via the Internet so that any failure in the Internet connection will render access impossible.

To be able to exploit the potential benefits of Cloud Computing while retaining control over the IT infrastructure, many users turn to their own virtualised data centres (private clouds) to provision services. But private clouds as well involve a number of threats which need to be protected against. A private cloud may also be highly complex, depending on its implementation. Due to the number of configuration settings and mutually influencing parameters, many security problems can also occur here, e.g. through data loss, unauthor-

ised data access, reduced availability and even services failing. Cloud providers make a number of interfaces available to access their services. If these interfaces are insecurely programmed, an attacker may exploit vulnerabilities in order to access data without permission. Managing cloud platforms also presents a major challenge for both public and private clouds due to the complexity and dynamism of the underlying processes.

However, these challenges can be overcome if appropriate infrastructural, organisational, personnel and technical measures are implemented to protect the services being provided. In particular, measures to securely and reliably separate customers in a cloud need to be implemented alongside traditional IT security measures.

This BSI white paper on Cloud Computing, as well as such works as the Cloud Security Alliance [4], the ENISA [3] and the NIST [2] provide important bases for achieving this.

Because of its anticipated technical and financial potential, Cloud Computing will probably do well in the marketplace, but only if providers succeed in clarifying customers' queries about information security and data protection. However, as Cloud Computing offerings become more popular, they also become more attractive to attackers because of the concentration of many business-critical resources in central data centres and the required standardisation of components and interfaces. So in the long term there will be a need to draw up and establish international data security standards which can be used as the basis for testing and certifying Cloud Computing platforms. Therefore a key task in the coming years will be to draw up and establish international data security standards in the Cloud Computing sector which can be used as the basis for certifying the security of Cloud Computing providers. Only through having internationally recognised certification for Cloud Computing providers and their services will an adequate level of trust be generated on the part of the customer.

15 Glossary

Labels in the tables:

The security recommendations shown in the tables have been divided into three categories.

B	Basic requirement, security recommendations in this category are directed at all cloud service providers
A+	Availability high, security recommendations, including additional requirements for areas with a requirement for a high level of availability
C+	Confidentiality high, security recommendations, including additional requirements for areas with a requirement for a high level of confidentiality protection

The threat level which led to these security recommendations is also indicated:

⇨	Average threat level
⇗	Increased threat level

Abbreviations / Terms	Definitions
Bot	Malware on a client which is used to develop remotely controllable computing networks (botnets)
BSI	Federal Office for Information Security
COBIT	Control Objectives for Information and Related Technology, methods for controlling risks that can occur by using IT to support business-related workflows
CSA	Cloud Security Alliance
CSP	Cloud service provider

DDoS	Distributed denial-of-service, a coordinated attack on IT availability e.g. by using a large number of attacking systems
IaaS	Infrastructure as a service, provisioning of IT resources e.g. processing power, data storage or networks as a service
IDS	Intrusion detection system
IPS	Intrusion prevention system
ISO 27001	International norm ISO/IEC 27001 “Information technology – Security techniques – Information security management systems – Requirements” (ISMS)
ITIL	IT Infrastructure Library, a collection of works on the subject of IT service management from the perspective of an IT service provider
NAS	Network Attached Storage, a storage architecture variant
OVF	Open Virtualization Format, a platform-independent standard for packaging and distributing virtual appliances
SAN	Storage Area Network, a storage architecture variant
PCI DSS	Payment Card Industry Data Security Standard, testing regulations for secure credit card transactions
PaaS	Platform as a Service, the provision of a complete runtime and development environment as a service
SaaS	Software as a Service, the provision of IT applications as a service
SAML	Security Assertion Markup Language, an XML framework for sharing authentication data
SOA	Service-oriented architecture, an approach for implementing distributed systems in order to use IT to efficiently help institutions to run their business processes
VM	Virtual machine
VPN	Virtual private network

16 References

[1] Federal Office for Information Security (BSI), IT-Grundschutz Methodology, BSI standard 100-2, Version 2.0, May 2008

http://www.bsi.bund.de/grundschutz

[2] Wayne Jansen, Timothy Grance, Guidelines on Security and Privacy in Public Cloud Computing, NIST, Draft Special Publication 800-144, January 2011

http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf

[3] ENISA, Cloud Computing: Benefits, Risks and Recommendations for information Security, November 2009

http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport

[4] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, December 2009

http://www.cloudsecurityalliance.org/csaguide.pdf

[5] Dr. Fang Liu, Jin Tong, Dr. JianMa, NIST Cloud Computing Reference Architecture, Version 1.0, March 2011

http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/ReferenceArchitectureTaxonomy/NIST_CC_Reference_Architecture_v1_March_30_2011.pdf

[6] Mahesh Dodani: "Architected" Cloud Solutions Revealed, in Journal of Object Technology, vol. 9, no. 2, pages 27 – 36, March – April 2010

http://www.jot.fm/issues/issue_2010_03/column3/

[7] Whitepaper Cloud Computing Use Cases Version 3.0, produced by the Cloud Computing Use Case Discussion Group, February 2010

http://opencloudmanifesto.org/cloud_computing_use_cases_whitepaper-3_0.pdf

[8] Webhost hack wipes out data for 100,000 sites, The Register, June 2009

http://www.theregister.co.uk/2009/06/08/webhost_attack/

[9] Worldwide Infrastructure Security Report, Arbor networks, 2010

http://www.arbornetworks.com/dmdocuments/ISR2010_EN.pdf

[10] OWASP Top 10 - 2010 The Ten Most Critical Web Application Security Risks

http://www.owasp.org/images/0/0f/OWASP_T10_-_2010_rc1.pdf

OWASP Application Security Principles

http://www.owasp.org/index.php/Category:Principle

[11] Federal Office for Information Security (BSI) BSI Standard 100-4 on Business Continuity Management, 2009

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1004.pdf?__blob=publicationFile

[12] Open Virtualization Format Specification, February 2009 http://www.dmtf.org/standards/published_documents/DSP0243_1.0.0.pdf

[13] Open Cloud Computing Interface - Core & Models, January 2010

http://www.ggf.org/Public_Comment_Docs/Documents/2010-01/occi-core.pdf

[14] vCloud API Programming Guide, vCloud API 1.0, 2010

http://communities.vmware.com/servlet/JiveServlet/downloadBody/12463-102-2-14932/vCloud_API_Guide.pdf

17 Acknowledgements

With the aim of addressing the subject of information security in Cloud Computing and supporting users and providers, on 28th September 2010 the Federal Office for Information Security (BSI) published as a draft discussion the white paper “Minimum Requirements for Cloud Computing Providers”, and invited comments. The white paper was positively received and constructive comments were offered. Thank you to everyone who has helped to improve the white paper by making suggestions, providing constructive criticism and suggesting improvements.

We also wish to thank the following experts and institutions, who with their input, assistance with quality assurance and useful debates, helped enormously to draw up and improve this work:

- Bayerische Landesbank, Sven-Torsten Gigler
- Federal Commissioner for Data Protection and Information Freedom (BfDI), Sven Hermerschmidt
- BITKOM e.V., on behalf of the members of BITKOM’s Security department, Lutz Neugebauer
- Cyber-Ark Software Ltd., Jochen Koehler
- EMC, Klaus Böttcher, Wolfgang Reh
- Eurocloud Deutschland_eco e.V., Andreas Weiss
- Google, Robin Williamson, John Collins, Thorsten Koch
- ITDZ Berlin, Kai Osterhage
- Microsoft, Gerold Hübner
- ORACLE Deutschland B.V.& Co. KG, Lutz Kahlenberg
- Pironet NDH, Dr. Clemens Plieth
- RSA, Alexander Hoffmann, Thomas Köhler

- SAP AG
- Siemens, Dr. Bernd Grobauer, Steffen Fries
- Symantec, Ilias Chantzos, Zoltán Précsényi
- ToolBox Solution GmbH, Tillmann Basien
- TÜV Informationstechnik GmbH (TÜViT), Adrian Altrhein
- VMware, Stephan Bohnengel
- VZM GmbH, Werner Metterhausen

We would also like to express our gratitude to those members of the BSI who produced this document:

Alex Didier Essoh, Dr. Clemens Doubrava, Isabel Münch.

The following BSI members also provided important inputs and contributed to the debate:

Horst Flätgen, Dr. Hartmut Isselhorst, Andreas Könen, Dirk Reinermann, Dr. Stefanie Fischer-Dieskau, Thomas Caspers, Oliver Zendel, Holger Schildt, Dr. Dörte Rappe, Thomas Borsch.

Publisher and Editorial Staff:
Federal Office for Information Security
Section 114, Security Management and IT-Grundschutz
P.O. Box 20 03 63
53133 Bonn

Phone: +49 (0) 22899 9582 - 5369
Fax: +49 (0) 22899 9582 - 5400

Internet: www.bsi.bund.de/grundschutz
E-Mail: grundschutz@bsi.bund.de

Article Number: BSI-Bro11/314e

Printed by:
Druckpartner Moser Druck + Verlag GmbH
53359 Rheinbach
www.dpmoser.de