Federal Office
for Information Security

# Cloud Computing Compliance Criteria Catalogue – C5:2020

# Preface by the President

In recent years, the BSI's C5 requirements catalogue has developed into a leading force that drives and supports cyber security in one of the most important fields of digitisation: cloud computing. For digitisation to succeed, it is of great importance that cloud services have a proven and generally accepted level of security.

When I was appointed to the BSI in 2016, I was responsible for the adoption of the first C5 requirements catalogue. It was one of the first things I did, and I noticed that the BSI was breaking new ground in this area. The BSI has defined security objectives but has left open how they will be achieved. The BSI does not carry out C5 audits, rather it is auditors who have added cloud security aspects to their existing audit portfolio with C5. It is difficult to standardise concrete individual measures in different cloud architectures, but it is possible to agree on common security objectives which have found their way into the C5. Such audits cannot be carried out by a national authority alone, or at least not easily. Since cloud services are usually provided globally, audits are carried out by internationally reliable partners.

The international success story of C5 shows that the decisions made at that time were correct. Many national and international Cloud Service Providers, both small and large, have now received a C5 audit certificate, and many cloud customers outside the public sector are asking for the certificates to assess the security of the cloud services used. Furthermore, C5 certificates are used and accepted as verification in regulated areas such as banking and insurance. As a result, the BSI has earned itself an important role as a shaper of information security in digitisation in the cloud area, which is accepted and appreciated worldwide.

When the BSI announced that it would be revising the C5 at the beginning of 2019, it also inquired about the experience of Cloud Service Providers, customers and auditors. The response was incredibly positive. Many different groups, associations and even competing vendors and auditors participated in joint workshops led by BSI, sharing their experiences and making constructive suggestions for improving the C5. I would like to take this opportunity to thank them all!

The result is impressive. Besides countless updates and improvements, I would like to highlight the following:

1. The new C5 implements the general requirements of the EU Cybersecurity Act (EUCA). This European regulation describes requirements for IT products and services that are certified according to an EUCA-compliant procedure. These requirements have been incorporated into the C5:2020 and are summarised in the new domain of product security.

2. The interfaces between Cloud Service Providers and cloud users plays an important role in the secure use of cloud services. The C5:2020 introduces "corresponding criteria" that the cloud customer must meet at the interfaces to the cloud service in order to play its part in the shared responsibility for security.

This further extends the role of C5 as a foundation for cloud security for providers, customers and auditors. As such, it will continue to serve as a good example of how information security can be shaped in the digital age.

# Table of Contents

# 1 Introduction

# 1 Introduction

## 1.1 Preliminary remarks

As the federal cyber security authority, the Federal Office for Information Security (BSI) shapes information security in digitisation through prevention, detection and reaction for government, business and society. Digitisation can only be successful if users can develop confidence in (new) technologies and use them safely and securely for their benefit.

The use of cloud computing has increased steadily in recent years and has become an established standard for the service and delivery model of IT services. Cloud computing is based on a high degree of standardisation of hardware and software, as well as the services based on it, the details of which are usually not known to the customer. As a result, the Cloud Service Providers must establish a particularly high level of trust.

In 2016, the BSI published this criteria catalogue for assessing the information security of cloud services in order to establish this trust. Established standards for information security (e.g. ISO/IEC 27001 and the Cloud Controls Matrix of the Cloud Security Alliance) formed the basis for the criteria and made it possible for auditors to carry out audits in accordance with international audit standards.

With the first revision of the contents of the criteria catalogue, the BSI aims to take account of developments in this environment. The BSI has also initiated dialogue with providers of cloud computing services, customers, auditors and regulators in order to take up their suggestions. The following aspects represent the main changes compared to the previous version of this criteria catalogue:

- Change or extension of the criteria regarding new concepts, i.e. “DevOps” as the convergence of the development and operation of IT systems;
- Extension of the criteria for the provision of cloud services to include product-specific aspects of information security. These are derived from the European Cybersecurity Act;
- Extension of the criteria for the provision of cloud services to include aspects relating to the cloud provider’s handling of enquiries from government agencies.
- Inclusion of corresponding criteria for cloud customers. These show where cloud customers need to develop their own measures to ensure the security of the cloud service.
- Additional guidance and information to better understand and continuously audit the criteria; and,
- Extension of the existing audit engagement type ‘attestation engagement’ with the option for a ‘direct engagement’.

The name was changed from “Controls Catalogue” to “Criteria Catalogue”. This was in response to the fact that Cloud Service Providers rarely transferred the controls set out in the Controls Catalogue directly into their service-related internal control systems. Instead, the controls contained in the Cloud Service Providers’ service-related internal control system were tested to see whether they provided the same level as the level of the controls set out in the Controls Catalogue. Hence, they already provided criteria for a control system, which is now reflected by the renaming. The English name was also changed to “Cloud Computing Compliance Criteria Catalogue”; therefore, the abbreviation “C5” was retained.

The structure and content of this criteria catalogue are presented in Section 2. Guidance on demonstrating conformity with this criteria catalogue is provided in Section 3. The criteria for independent audits can be found in Sections 4 and 5.

The criteria in this criteria catalogue are applicable to periods ending on or after February 15, 2021. Cloud Service Providers can apply the criteria earlier than this date.

### 1.2 Definitions

For the purposes of this criteria catalogue, the following definitions apply, derived from the BSI's IT-Grundschutz-Kompendium and the international standard ISO/IEC 17788:2014 (Information Technology – Cloud Computing – Overview and Vocabulary):

**Assets:** In this criteria catalogue, this term is used synonymously with the term "system components" (cf. below).

**Authenticity:** Feature of information in which changes can be uniquely assigned to an originator.

**Availability:** The accessibility of information, services, and functions of an IT system, IT applications or IT networks as intended.

**Cloud Computing:** Approach for the dynamic provision, use and billing of IT services via a network, adapted to demand. These services are offered and used exclusively via defined technical interfaces and protocols.

**Cloud service:** Information technology service offered as part of cloud computing. This includes infrastructure (e.g. computing power, storage space), platforms and software.

**Cloud Service Provider:** Natural or legal person providing a cloud service.

**Confidentiality:** The ability of information to be made available or disclosed only to authorised persons, entities and processes in a permissible manner.

**Cloud customer:** Natural or legal person who has a business relationship with the Cloud Service Provider for the purpose of using the cloud service.

**Hardware-objects:** Physical and virtual infrastructure resources (e.g. servers, storage systems, network components), as well as end point devices if the Cloud Service Provider has determined in a risk assessment that these could endanger the information security of the cloud service in the event of loss or unauthorised access (e.g. mobile devices used as security tokens for authentication).

**Information Security:** Protection of the information the Cloud Service Provider's customers processed, stored or transmitted in the cloud service with respect to the protection objectives of confidentiality, integrity, availability and authenticity.

**Integrity:** The ability of information to be complete, accurate (correct, undamaged) and protected from manipulation and unintentional or erroneous alteration.

**Protection needs:** Sufficient and adequate level of information security for the Cloud Service Provider's customers with respect to the information processed, stored or transmitted in the cloud service.

**System components:** The objects required for the information security of the cloud service during the creation, processing, storage, transmission, deletion or destruction of information in the Cloud Service Provider's area of responsibility, e.g. firewalls, load balancers, web servers, application servers and database servers.

Furthermore, the following definitions apply, based on the International Standard on Assurance Engagements (ISAE) 3000 (Revised) "Assurance Engagements Other than Audits or Reviews of Historical Financial Information" and ISAE 3402 "Assurance Reports on Controls at a Service Organization".

**Attestation engagement:** An audit engagement under which the auditor verifies that the written statement is free from material misstatement.

**C5 criteria:** The criteria applied to assess the information security of the cloud service and defined in this catalogue of criteria (cf. Section 5).

**Control:** Process-integrated or process-independent measure to reduce the likelihood of events occurring or to detect events that have occurred in order to maintain the information security of the cloud service.

**Direct engagement:** An audit engagement in which the practitioner (auditor) audits the cloud service as the underlying subject matter against the C5 criteria and presents the resulting subject matter information as part of its reporting.

**Material misstatement:** deficiencies in the statement, e.g.:

- Information does not indicate that controls are not suitably designed, not implemented or not operating effectively to meet the C5 criteria with reasonable assurance;

- Information is false or missing that may be individually or collectively relevant to the Cloud Service Provider's customers in order to assess the information security of the cloud service; or

- Information includes inappropriate generalisations or unbalanced and distorting representations that may mislead the Cloud Service Provider's customers.

**Service Organisation's System:** The principles, procedures and measures applied by the legal representatives (management) of the Cloud Service Provider towards the organisational and technical implementation of management decisions to ensure the effectiveness and efficiency of business activities, the information security of the Cloud Service and compliance with the legal and other regulations applicable to the Cloud Service Provider.

**Written statement:** Assertions on the description of the service organisation's system for the provision of the Cloud Service and on the suitability of the design and, where relevant, operating effectiveness of the controls to meet the C5 criteria prepared by the legal representatives of the Cloud Service Provider.

# 2 Structure and Content of the Criteria

# 2 Structure and Content of the Criteria

## 2.1 Structure

This criteria catalogue contains 17 objectives regarding the information security of cloud services. Each objective is broken down into the criteria required to achieve the objective (cf. Section 2.2).

The criteria are divided into basic criteria and additional criteria (C5 criteria).

According to the BSI, the basic criteria reflect the minimum level of information security that a cloud service must offer when cloud customers use it to process information that has a normal need for protection. The basic criteria define the minimum scope of an audit according to this criteria catalogue. Nevertheless, it is up to the cloud customers to assess for their individual use case to what extent the basic criteria adequately reflect the protection needs of their information. For cloud customers whose information has a higher need for protection, the additional criteria provide a starting point for conducting this assessment. Cloud Service Providers may include the additional criteria in an audit in addition to the basic criteria to address customers with higher protection needs.

Chapter 5 contains the following elements in addition to the basic criteria, additional criteria and supplementary information:

- Notes on Continuous Auditing:
  The C5 criteria include guidance on how Cloud Service Providers can take actions towards continuous monitoring, including independent third-party audits, by automating their procedures and measures. This guidance should enable Cloud Service Providers to assess the general feasibility and effort implications of a continuous third-party audit.
- Complementary Customer Criteria:
  Maintaining the information security of a cloud service is not the sole responsibility of the Cloud Service Provider. Customers must also comply with the obligations to cooperate in their area of responsibility. In the case of cloud services for infrastructure, customers are typically responsible for bringing in security updates for the operating system they are using, whereas this responsibility typically lies with the Cloud Service Provider when using a cloud service for software.
  Selected C5 criteria contain complementary customer criteria where potential cooperation obligations exist. However, this is not an exhaustive list that is generally valid for all cloud services. Rather, the complementary customer criteria provide the following support:
  - The criteria support Cloud Service Providers with identifying those C5 criteria that typically require corresponding controls on the cloud customer's side which must be set up together with the controls of the Cloud Service Provider in order to meet the C5 criteria (cf. Section 3.4.4.1);
  - The criteria support auditors with assessing the system description regarding the appropriateness of the information provided about the complementary controls; and,
  - The criteria support cloud customers in better understanding the information provided about the complementary controls in the system description and where to set up such controls.

Providing details about the controls in place at the Cloud Service Provider establishes confidence in the information security of a cloud service. Potential customers should consider the information on the general conditions of the cloud service (e.g. the Cloud Service Provider's place of jurisdiction or contractual agreements on availability and troubleshooting) in addition to the transparency regarding the C5 criteria (cf. Section 2.2). According to the BSI, potential customers of a cloud service must know this information in order to assess its suitability for their respective use case.

## 2.2 Content of the C5 Criteria

The C5 criteria are subdivided into 17 areas based on the description of the objectives of the measures in ISO/IEC 27001:2013 Annex A (cf. Table 1).

| No. | Area (identifier) | Objective |
|---|---|---|
| 1 | Organisation of Information Security (OIS)<br>5.1 on page 35 | Plan, implement, maintain and continuously improve the information security framework within the organisation. |
| 2 | Security Policies and Instructions (SP)<br>5.2 on page 39 | Provide policies and instructions regarding security requirements and to support business requirements. |
| 3 | Personnel (HR)<br>5.3 on page 42 | Ensure that employees understand their responsibilities, are aware of their responsibilities regarding information security, and that the organisation's assets are protected in the event of changes in responsibilities or termination. |
| 4 | Asset Management (AM)<br>5.4 on page 46 | Identify the organisation's own assets and ensure an appropriate level of protection throughout their lifecycle. |
| 5 | Physical Security (PS)<br>5.5 on page 51 | Prevent unauthorised physical access and protect against theft, damage, loss and outage of operations. |
| 6 | Operations (OPS)<br>5.6 on page 58 | Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures. |
| 7 | Identity and Access Management (IDM)<br>5.7 on page 72 | Secure the authorisation and authentication of users of the Cloud Service Provider (typically privileged users) to prevent unauthorised access. |
| 8 | Cryptography and Key Management (CRY)<br>5.8 on page 79 | Ensure appropriate and effective use of cryptography to protect the confidentiality, authenticity or integrity of information. |
| 9 | Communication Security (COS)<br>5.9 on page 82 | Ensure the protection of information in networks and the corresponding information processing systems. |
| 10 | Portability and Interoperability (PI)<br>5.10 on page 86 | Enable the ability to access the cloud service via other cloud services or IT systems of the cloud customers, to obtain the stored data at the end of the contractual relationship and to securely delete it from the Cloud Service Provider. |

| No. | Area (identifier) | Objective |
|---|---|---|
| 11 | Procurement, Development and Modification of Information Systems (DEV)<br>5.11 on page 89 | Ensure information security in the development cycle of cloud service system components. |
| 12 | Control and Monitoring of Service Providers and Suppliers (SSO)<br>5.12 on page 95 | Ensure the protection of information that service providers or suppliers of the Cloud Service Provider (subservice provider) can access and monitor the agreed services and security requirements. |
| 13 | Security Incident Management (SIM)<br>5.13 on page 100 | Ensure a consistent and comprehensive approach to the capturing, evaluation, communication and handling of security incidents. |
| 14 | Business Continuity Management (BCM)<br>5.14 on page 103 | Plan, implement, maintain and test procedures and measures for business continuity and emergency management. |
| 15 | Compliance (COM)<br>5.15 on page 106 | Avoid non-compliance with legal, regulatory, self-imposed or contractual information security and compliance requirements. |
| 16 | Dealing with investigation requests from government agencies (INQ)<br>5.16 on page 109 | Ensure appropriate handling of government investigation requests for legal review, information to cloud customers, and limitation of access to or disclosure of data. |
| 17 | Product Safety and Security (PSS)<br>5.17 on page 111 | Provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers, appropriate mechanisms for troubleshooting and logging, as well as authentication and authorisation of users of cloud customers. |

Table 1: Areas of the criteria catalogue with assigned objectives

## 2.3 Underlying Standards and Publications

Requirements of nationally and internationally established standards and publications form the foundation of the C5 criteria. The level of detail usually goes beyond these standards and publications in order to achieve a high level of transparency about the principles, procedures and measures of the Cloud Service Providers.

Requirements from the following standards and publications have been taken into account during the development of this criteria catalogue:

- ISO/IEC 27001:2013 – Information security management systems – Requirements
- ISO/IEC 27002:2016 – IT security procedures – Guidelines for information security measures
- ISO/IEC 27017:2015 – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- BSI – IT-Grundschutz-Kompendium, 2nd Edition 2019

- CSA (Cloud Security Alliance, a non-profit organisation for the dissemination of security standards in cloud computing) – Cloud Controls Matrix 3.0.1 (CSA CCM)

- AICPA (American Institute of Certified Public Accountants) – Trust Services Criteria 2017 (TSC)

- ANSSI (Agence nationale de la sécurité des systèmes d'information, National Cybersecurity Agency of France) – Providers of cloud computing services v. 3.1 (SecNumCloud)

- IDW (Institut der Wirtschaftsprüfer, the German Institute of Certified Public Accountants) RS FAIT 5 – Statement on Financial Reporting: "Principles of Orderly Accounting for the Outsourcing of Financial Reporting-Related Services including Cloud Computing", as at November 4, 2015

Cloud Service Providers who already base their policies, procedures and measures on one or more of these standards and publications can map them to the C5 criteria to assess compliance.

Reference tables of the BSI support the mapping and are available on its website (https://www.bsi.bund.de/EN/C5). Cloud Service Providers should consider the tables as aids when assessing compliance. Notwithstanding the information contained in the reference tables, Cloud Service Providers must determine to what extent existing principles, procedures and measures meet the C5 criteria on a case-by-case basis (cf. Section 3.4.6).

# 3 Providing Conformity through Independent Audits

# 3 Providing Conformity through Independent Audits

### 3.1 Introduction

Cloud Service Providers and cloud customers can use the C5 criteria set out in this criteria catalogue. While Cloud Service Providers can align their policies, procedures and measures with the C5 criteria, cloud customers will have the objective to verify whether the Cloud Service Provider meets these criteria. However, a self-assessment for each individual customer would not be efficient for Cloud Service Providers and would not provide enough assurance for customers. In addition, if a customer requests this information from several providers, a standard set of information will not be available making it difficult for a customer to compare the information provided by the different providers. According to the BSI, an audit by an independent third party who issues a report for the Cloud Service Provider according to international audit standards, made available to existing and potential customers, is an appropriate and economic solution.

For this reason, the BSI sets out below its view of the requirements for proof of conformity and reporting to the Cloud Service Provider and its customers.

The cloud customer should consider compliance with the criteria set out in this criteria catalogue as an integral part of engaging a Cloud Service Provider. Further, the cloud customer should agree this in the contract with the Cloud Service Provider. In particular, this applies if the Cloud Service Provider has to fulfil the additional criteria. Furthermore, the potential cloud customer should not base its decision only on an existing, up-to-date reporting (regardless of whether it refers to the basic or additional criteria) according to this criteria catalogue but should request the audit report regularly and evaluate it for their individual use case.

The BSI is not involved in any part of the audit or reporting. The auditor carries out the audit independently of instructions from the BSI and is engaged by the Cloud Service Provider, not the cloud customer.

### 3.2 Audit Standards to be Applied

Nationally and internationally established standards form the foundation for the design of the C5 criteria and the requirements for proving conformity.

Specifically, the International Standard on Assurance Engagements (ISAE) 3000 (Revised) “Assurance Engagements Other than Audits or Reviews of Historical Financial Information”, the German Audit Standard (PS) 860 “IT-Prüfung außerhalb der Abschlussprüfung” of the Institut der Wirtschaftsprüfer (IDW), which is in line with ISAE 3000 (Revised), or other national equivalents to ISAE 3000 (Revised). Auditors should consider one of these standards or national equivalent as a basis for audit planning, execution and reporting.

Auditors should consider further audit standards for individual questions of audit execution and reporting. These include ISAE 3402 “Assurance Reports on Controls at a Service Organization”, the German IDW PS 951 n.F. „Die Prüfung des internen Kontrollsystems bei Dienstleistungsunternehmen”, which is in line with ISAE 3402, or other national equivalents to ISAE 3402. Requirements for the contents of the description of the service organisation’s system, which is part of the audit report, were derived from these standards (cf. Section 3.4.4.1).

In addition, the audit standard AT-C section 105 “Concepts Common to All Attestation Engagements” and AT-C section 205 “Examination

Engagements" of AICPA, the American Institute of Certified Public Accountants, have been taken into account. These standards supplement ISAE 3402 and IDW PS 951 especially with requirements for the consideration of subservice organisations.

### 3.3 Connection to Other Audits

Nationally and internationally established standards form the foundation for the design of the C5 criteria (cf. Section 2.3). If the Cloud Service Provider uses the references to established standards and publications, the provider has already considered the corresponding principles, procedures and measures in its operations.

These principles, procedures and measures typically also form the basis for additional audits, which the Cloud Service Provider may already have carried out by independent auditors. In this context, especially audits according to ISAE 3402/ SOC 1 or SOC 2 should be mentioned. In these cases, it makes sense to combine these audits with an audit according to this criteria catalogue in terms of organisation and time. This enables auditors and Cloud Service Providers to use records in parallel for reporting according to ISAE 3402 and/ or SOC 2, as well as for reporting according to this criteria catalogue.

In cases of the Cloud Service Provider obtaining certificates (e.g. ISO/IEC 27001, ISO 22301), it is also possible to combine the relevant audits as far as possible. The reference table defined in a separate accompanying document to this criteria catalogue can be used for this purpose.

When assessing the coverage of C5 criteria by results obtained during other audits, particular consideration shall be given to the nature of the audit and compared with the 'reasonable assurance' required for an attestation engagement or a direct engagement (cf. Section 3.4.1). For example, results from ISO certification audits are to be assessed differently from those obtained from an ISAE 3000 audit.

In the reference tables, the C5 criteria are mapped to the criteria defined in other standards. It should be noted that a mapping initially only reflects the thematic relationship between the criteria. In addition, it is indicated to what extent the C5 criteria reflect the level of information security articulated by the mapped criteria according to the BSI.

The tables are only an aid to understand the extent to which the C5 criteria overlap with the criteria defined in other standards. As such, it is not possible to conclude the actual coverage of the C5 criteria by policies, procedures and measures implemented by a Cloud Service Provider solely from the mapping given in the reference tables. This applies even if the established policies, procedures and measures have already been audited against one or more of the standards contained in the reference table. According to the BSI, it must always be assessed individually and specifically to what extent the policies, procedures and measures set up by a Cloud Service Provider actually cover the C5 criteria.

The mere reference to the criteria defined in other standards to which the C5 criteria are mapped in the reference tables is not enough.

This does not affect further possibilities for the auditor to use the results of third parties within the auditors responsibility.

### 3.4 Supplementary Requirements of the BSI

The following sections outline the application of the above-mentioned audit standards.

#### 3.4.1 Audit Engagement

Proof of conformity is always to be provided using the audit standard ISAE 3000 (Revised).

The ISAE 3000 (Revised) audit standard distinguishes between audit engagements with "reasonable assurance" and audit engagements with "limited assurance". According to the BSI, auditors should perform reasonable assurance audits to provide conformity with this criteria catalogue.

A distinction is also made between “attestation engagements” and “direct engagements”. Both variants are suitable for proving conformity with this criteria catalogue.

In addition, audits may be carried out regarding the suitability of the design or the operating effectiveness. According to the BSI, an operating effectiveness audit is necessary in order to provide an appropriate opinion on the Cloud Service Provider’s controls to meet the C5 criteria defined in this criteria catalogue. Audit engagements on the suitability of the design should only be carried out in the case of an initial engagement according to this criteria catalogue. As such, audit engagements on the suitability of the design only are not to be recurring.

### 3.4.2 Criteria to be Applied

#### 3.4.2.1 Criteria for Information Security of the Cloud Service

According to the BSI, the basic criteria reflect the minimum level of information security that a cloud service must offer when cloud customers use it to process information that has a normal need for protection. The basic criteria define the minimum scope of an audit according to this criteria catalogue. Nevertheless, it is up to the cloud customers to assess for their individual use case to what extent the basic criteria adequately reflect the protection needs of their information. For cloud customers whose information has a higher need for protection, the additional criteria can provide a starting point for conducting this assessment. Cloud Service Providers may include the additional criteria in an audit in addition to the basic criteria to address customers with higher protection needs.

The Cloud Service Provider must explain in the description of the system if individual basic or additional criteria are not applicable due to the nature and design of the cloud service or the principles, procedures and measures of the Cloud Service Provider. Based on the information provided by the Cloud Service Provider, the auditor must assess to what extent the C5 criteria are not applicable, and if applicable whether they are fully applicable or partially fulfilled. The Cloud Service Provider must explain in the description of the system if individual basic or additional criteria are not applicable due to the nature and design of the cloud service or the principles, procedures and measures of the Cloud Service Provider. Based on the information provided by the Cloud Service Provider, the auditor must assess to what extent the C5 criteria are not applicable, and if applicable whether they are fully or partially fulfilled.

The applicable C5 criteria are to be presented in the audit report’s section containing the C5 criteria, controls, test procedures and results.

#### 3.4.2.2 Further Criteria for Transparency and Reporting

Further criteria define the information on the general conditions of the cloud service (cf. Section 4) as well as the requirements concerning the system description and written statement (cf. Section 3.4.4.1; this Section also provides guidance for the handling of the general conditions in a direct engagement). These further criteria serve to inform customers about the information security of the cloud service supporting them with assessing its suitability for their individual use case. The further criteria also ensure the comparability of the reporting in order to make it easier for customers to compare several Cloud Service Providers or cloud services for which a C5 report has been issued.

### 3.4.3 Subject Matter and Objective of the Audit

#### 3.4.3.1 Attestation Engagement

The subject of an attestation engagement is the description of the Cloud Service Provider’s service-related system of internal control to meet the C5 criteria prepared by the Cloud Service Provider (“description”). The audit is based on a written statement by the Cloud Service Provider's management about the suitability of the design of controls to meet the applicable C5 criteria as at a specified date (type 1 report) and, if mandated, the operating effectiveness of the controls throughout a specified period (type 2 report).

The objective of the audit is to enable the auditor to provide an opinion with reasonable assurance as to whether:

- the description fairly presents the Cloud Service Provider's service-related system of internal control to meet the C5 criteria as at a specified date (type 1 report) or throughout a specified period (type 2 report) and includes the minimum content as set forth in Section 3.4.4.1 this criteria catalogue;
- the controls stated in the description were suitable designed and implemented to meet the applicable C5 criteria as at a specified date (type 1 report) or throughout a specified period (type 2 report); and
- where mandated (type 2 report), the controls stated in the description operated effectively throughout a specified period.

According to the BSI, Cloud Service Providers who already have a system description can reuse it in audits according to this criteria catalogue. However, an existing system description that meets the requirements of another standard must be adapted to this criteria catalogue, as necessary.

#### 3.4.3.2 Direct Engagement

In a direct engagement, the auditor takes stock of the principles, procedures and measures applied by the Cloud Service Provider for the cloud service.

In contrast to an attestation engagement, the Cloud Service Provider does not provide a description. Identifying the relevant parts of the service-related internal control system takes place during the execution of the engagement. This typically requires the auditor to interview the Cloud Service Provider's subject matter experts and review relevant records and documents.

The objective of the audit is to enable the auditor to provide an opinion with reasonable assurance as to whether

- the principles, procedures and measures applied by the Cloud Service Provider were suitable designed and implemented to meet the applicable C5 criteria as at a specified date; and,
- where mandated, the principles, procedures and measures applied operated effectively throughout a specified period.

According to the BSI, the direct engagement is particularly suitable for Cloud Service Providers who have not yet documented their service-related internal control system completely or in enough detail in a system description.

### 3.4.4 Requirements for the Description and the Written Statement

#### 3.4.4.1 Description

For an attestation engagement, the Cloud Service Provider's service-related system of internal control to meet the C5 criteria shall include the following minimum content in order to provide customers with sufficient transparency about the information security of the cloud service:

- Name, type and scope of cloud services provided;
- Description of the system components for providing the cloud service;
- Information on the general conditions of the cloud service in accordance with the criteria in Section 5 this criteria catalogue, which enable potential customers of the Cloud Service Provider to assess its suitability for their use case;
- Applicable C5 criteria;

- Policies, procedures and measures, including the controls implemented to provide (develop and operate) the cloud services with respect to the applicable C5 criteria;

- Dealing with significant events and conditions that represent exceptions to normal operation, such as security incidents or the failure of system components;

- Complementary customer controls assumed in the design of the Cloud Service Provider's controls; and

- Functions and services with respect to the applicable C5 criteria provided by subservice organisations, including the type and scope of such functions and services, the location of processing and storage of data, the complexity and uniqueness of the functions and services as well as the resulting dependency of the Cloud Service Provider, (if carve-out method is applied) complementary controls assumed in the design of the Cloud Service Provider's controls, and the availability of audit reports according to the criteria in this criteria catalogue.

When auditing operating effectiveness (type 2 reporting), the following minimum contents shall be added to the system description:

- Details on significant changes to the policies, procedures and measures, including the controls, to govern the provisioning (development and operation) of the Cloud Services with respect to the applicable C5 Criteria, that have been implemented during the period under review;

- Details on significant events and conditions that are exceptions to normal operation, that have occurred throughout the specified period and have resulted in:

  - contractual agreements regarding the availability of the Cloud Service not being fulfilled, or

  - unauthorised third parties having gained access to the data of cloud customers stored in the cloud service, or

  - the integrity of the data stored in the cloud service was compromised and the protective measures put in place (e.g. data backup) were not effective,

  as well as the measures initiated by the Cloud Service Provider to prevent such events and conditions in the future.

An incident is typically significant when it affects multiple cloud customers and the Cloud Service Provider informs the affected parties or the public. The information about the incidents and the protection measures put in place should be as transparent as possible, without revealing vulnerability or potential points of attack. Furthermore, the reporting must not jeopardise the confidentiality of information concerning individual cloud customers and should therefore not contain a detailed description of individual incidents.

The description shall not omit or distort any information relevant to the fulfilment of the applicable C5 criteria. This does not mean that all aspects of the service-related internal control system that can be considered important from the point of view of individual customers of the Cloud Service Provider should be presented. It should be noted that the description is intended to achieve an appropriate level of transparency for a broad range of customers and that some of the processes can be customised.

In the case of a direct engagement, the auditor shall present the above-mentioned minimum content in all material aspects as part of the audit report so that the intended customers can obtain an appropriate understanding of the information security of the cloud service, including the principles, procedures and measures applied. This includes sufficient information on the general conditions of the cloud service (cf. Section 4).

#### 3.4.4.2 Written Statement

In the written statement, management of the Cloud Service Provider confirms that:

- the description fairly presents the Cloud Service Provider's service-related system of internal control to meet the C5 criteria as at a specified date (type 1 report) or throughout a specified period (type 2 report) and includes the minimum content as set forth in Section 3.4.4.1 this criteria catalogue;
- the controls stated in the description were suitably designed and implemented to meet the applicable C5 criteria as at a specified date (type 1 report) or throughout a specified period (type 2 report); and,
- where mandated (type 2 report), the controls stated in the description operated effectively throughout a specified period.

### 3.4.5 Consideration of Subservice Organisations

If necessary, the Cloud Service Provider will outsource parts of its business processes for the provision of the cloud service to other service providers (use of subservice organisations). The Cloud Service Provider describes this in its description and the auditor takes this into consideration as specified in the audit standards ISAE 3402. The standard distinguishes for an attestation engagement between the "inclusive method" and the "carve-out method":

- **Inclusive method:** In the case of the inclusive method, the service-related internal control system of the subservice organisations is also included in the description and is in scope of the audit. Therefore, the auditor also assesses the subservice organisation's controls regarding the suitability of the design and, if mandated, their operating effectiveness. In this respect, the inclusive method provides a report on the audit of the service-related internal control system at the Cloud Service Provider and its subcontractors.
- **Carve-out method:** This method merely describes the services provided by the subservice organisation in accordance with the minimum contents of the description (cf. Section 3.4.4.1). The controls of the subcontractor are not presented. Instead, the service provider's description presents those controls that are designed and implemented to monitor the operating effectiveness of the controls at the subservice organisation. This criteria catalogue contains corresponding criteria in the area "Control and Monitoring of Service Providers and Suppliers".

The Cloud Service Provider shall select the method to be used at its own discretion and state it accordingly in the description (cf. Section 3.4.4.1 on Minimum Contents of the System Description).

For the purposes of this criteria catalogue, a service organisation is a subservice organisation if the following two characteristics apply:

- The services provided by the service organisation are likely to be relevant to customers' understanding of the applicable C5 criteria.
- Complementary controls at the service organisation are required in combination with the controls of the Cloud Service Provider, to meet the applicable C5 criteria with reasonable assurance.

If the Cloud Service Provider's controls, including its controls to monitor the effectiveness of the service organisation's controls, meet the applicable C5 criteria with reasonable assurance, it is not a subservice organisation within the meaning of this criteria catalogue.

If the cloud service is provided in data centres operated by third parties, it is to be generally assumed that the characteristics noted above apply and that a subservice organisation relationship within the meaning of this criteria catalogue exists, in particular regarding the area of "Physical Security". The same applies, for example, to "Operations" if software is provided using the infrastructure or platform of another Cloud Service Provider. The criterion of relevance for the user, as well as the requirement of complementary controls, typically does not apply, for example, to business relationships of the Cloud Service Provider with cleaning companies or advertising agencies.

In the case of a direct engagement, the above remarks shall be applied mutatis mutandis.

### 3.4.6 Assessing the Fulfilment of Criteria at an Attestation Engagement

If the Cloud Service Provider already performs audits in accordance with other standards and publications, it is possible that the controls presented in the description may be optimally aligned with the criteria of these standards and publications, but that their description does not fully meet all elements of the C5 criteria to which they are assigned.

If the Cloud Service Provider can provide evidence of additional controls not previously stated in the description, but in place for non-covered elements of the C5 criteria, the Cloud Service Provider shall include these controls in the description or adjust the existing control descriptions and present these changes in an appropriate form.

An adjustment of the description may be waived if the descriptions of the auditor's test procedures clearly state how the elements of the C5 criteria not covered by the control description were audited. Such test procedures shall be marked in an appropriate form (e.g. “Further test procedure for assessing full coverage of the C5 criterion”).

This applies mutatis mutandis to a direct engagement.

### 3.4.7 Deviation Handling

Deviation handling is regulated in the audit standards. In assessing whether applicable C5 criteria are not met due to identified deviations and whether the opinion needs to be qualified, the auditor must consider the following procedures:

- Inquiry of management of the Cloud Service Provider regarding their assessment of the cause of the identified deviation;

- Assessment of the Cloud Service Provider's handling of the identified deviation;

- Assessment whether comparable deviations have been identified by the Cloud Service Provider's monitoring processes and what measures have been taken as a result; and,

- Verification whether compensating controls are in place and effective to address the risks arising from the deviation in such a way that the C5 criterion is met with reasonable assurance. This concerns, for example, the assessment of alternative organisational and technical approaches of the Cloud Service Provider to meet the applicable C5 criteria, which have not been considered in the design of the criteria set out in this criteria catalogue.

Irrespective of the assessment as to whether a deviation leads to a qualified opinion, further information should be presented in the audit report. This information is intended to enable report recipients to assess whether the Cloud Service Provider is taking appropriate actions to handle errors and optimise its policies, procedures and actions. The following additional information from the Cloud Service Provider shall be included in the audit report:

- If the deviation was detected by the Cloud Service Provider itself, when and in the course of which measures the deviation was detected.

- If the deviation was already stated in a report of a previous audit, an indication should be given of when and by what means the deviation was detected, together with a separate indication that the detection occurred in a previous audit period. This requires that the auditor has access to prior reports from the Cloud Service Provider. In case of doubt, the auditor shall have the inspection of these reports separately assured in his engagement letter.

- The measures to be taken to remedy the deviation in the future and when these measures are likely to be completed or effectively implemented.

This additional information is not subject of the audit, and, accordingly, the auditor does not express an opinion thereon. For example, the information may be provided in a separately marked section of the Description or in the optional section "5. Other Information Provided by the Cloud Service Provider" (cf. the following section).

### 3.4.8 Reporting

The reporting on an attestation engagement is based on the requirements of ISAE 3402. In the case of a direct engagement, these are applied mutatis mutandis. Details are given in the following section.

The report on an attestation engagement includes the following elements:

1. Independent auditor's report
   a. Scope and C5 version
   b. Cloud Service Provider's responsibility
   c. Independence and quality control of the auditor/auditing firm (including information on compliance with qualification requirements (cf. Section 3.4.9)
   d. Auditor‘s responsibility
   e. Inherent limitations
   f. Audit Opinion
   g. Intended users and purpose
   h. General terms of the engagement
2. Written statement by the Cloud Service Provider's management responsible for the cloud service(s).
3. Description of the Cloud Service Provider's service-related system of internal control to meet the C5 criteria.
4. Presentation of the applicable C5 criteria, the associated controls (part of the description), test procedures performed and the individual test results of the auditor.
5. Optional: Other information provided by the Cloud Service Provider (this information is not subject of the audit, and, accordingly, the auditor does not express an opinion thereon).

In case of a direct engagement, the components 2 'Written statement' and 3 'Description' are omitted. Nevertheless, the minimum contents of the description mentioned in Section 3.4.4.1 shall be presented in all material respects in the audit report so that the intended customers can obtain an appropriate understanding of the information security of the cloud service, including the principles, procedures and measures applied. This includes sufficient information on the general conditions of the cloud service (cf. Section 4). Such information shall be provided in a separate section, e.g. "Description of the cloud service and the policies, procedures and measures applied by the Cloud Service Provider".

The test procedures performed shall be described for both suitability of design (type 1 report) and operating effectiveness (type 2 report) engagements.

### 3.4.9 Qualification of the Auditor

According to ISAE 3000 (Revised), the auditor must determine before accepting an engagement that the professional duties (for auditors in Germany § 43 WPO, German Law regulating the Profession of Wirtschaftsprüfer: Wirtschaftsprüferordnung), including the duty of independence, are complied with. Based on the auditor's knowledge of the subject matter, the auditor shall assess whether the members of the audit team entrusted with the engagement have the necessary competency and understanding of the industry as well as capabilities to perform the audit and whether sufficient experience with the relevant formal requirements is available or can be obtained.

According to the BSI, audits based on this criteria catalogue place special requirements on the qualification of the auditor and the members of the audit team. From the BSI's point of view, the following aspects on professional qualifications and professional experience are suitable indications that these special requirements are met.

Therefore, the following aspects are to be fulfilled by those members of the audit team who, according to the International Standard on Quality Control (ISQC) 1 "Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance and Related Services Engagements" or the German IDW quality assurance standard "Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis" (IDW QS 1) or other national equivalents of ISQC 1, supervision the execution and review the results of the engagement (including evaluation of the work performed, review of the documentation and the planned reporting):

- 3 years relevant professional experience with IT audits in a public audit firm

or one of the following professional examinations/certifications:

- Information Systems Audit and Control Association (ISACA) – Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM) or Certified in Risk and Information Systems Control (CRISC)
- ISO/IEC 27001 Lead Auditor or BSI certified ISO 27001 Auditor for audits based on BSI IT-Grundschutz
- Cloud Security Alliance (CSA) – Certificate of Cloud Security Knowledge (CCSK)
- $(ISC)^2$ – Certified Cloud Security Professional (CCSP)

At the client's request, the auditor shall provide appropriate evidence that the audit team meets the qualification requirements.

Compliance with the qualification requirements shall be confirmed in the section "Independence and quality control of the auditor/auditing firm" of the independent auditor's report.

### 3.4.10 Information on Limitation of Liability

According to the BSI, information on liability regulations is important information for the report recipient.

The regulations on the auditor's liability – in the case of audits outside the scope of statutory reserved duties – are fundamentally based on civil law requirements and can be specified by contractual agreement. A liability agreement can be made individually or by using pre-formulated contractual conditions.

In this context, a reference to a liability agreement must be made in the audit report.

The information on this can be found in the section "General terms of the engagement" (with reference to other attachments if necessary).

## 3.5 Dealing with Criteria Catalogue Updates

The BSI intends to update this criteria catalogue regularly in line with general technical developments and the ongoing development of the underlying standards.

In this context, Cloud Service Providers and auditors shall have sufficient time to make the necessary adjustments to the systems and processes and to the execution of the audit associated with the updating of this criteria catalogue.

The criteria in this criteria catalogue shall be applied for periods being assessed ending on or after February 15, 2021. Earlier application of these criteria is permitted.

In the course of a specified period, it may happen that the assessment of the effectiveness of the policies, procedures and measures applied by the Cloud Service Provider relates both to the status before and after the implementation of such adjustments. The system description should include the adjustments made (cf. Section 3.4.4.1). In the case of a direct engagement, the auditor must obtain and disclose this information.

If the specified period ends in a period which is up to three months before February 15, 2021, the Cloud Service Provider shall provide additional information in the system description regarding the necessary changes to its service-related internal control system which have not been completed. The details should include what measures are to be completed or effectively implemented. In the case of a direct engagement, the auditor shall obtain and disclose this information.

# 4 Information on the General Conditions of the Cloud Service

# 4 Information on the General Conditions of the Cloud Service

The information on the general conditions of the cloud service, serves to provide customers with additional information on the level of information security offered by the cloud service. The information enables cloud customers to assess the suitability of the cloud service for their individual use case. They are also intended to ensure a comparable reporting to make it easier for customers to compare several cloud providers or cloud services for which a C5 report has been issued.

Since in the case of a direct engagement, the audit is not based on a system description provided by the Cloud Service Provider, the auditor must document details of the general conditions in accordance with the information provided by the Cloud Service Provider.

## BC-01 Information on jurisdiction and locations

**Information on the General Conditions of the cloud service**

In the system description and the contractual agreements (e.g. service description), the Cloud Service Provider clearly provides comprehensible and transparent information on:

- Its jurisdiction; and
- System component locations, including its subcontractors, where the cloud customer's data is processed, stored and backed up.

The scope of information is based on the requirements of subject matter experts of the cloud customers who define information security requirements, implement them or check their effectiveness and assess the suitability of the cloud service from a legal and regulatory perspective (e.g. IT, compliance, internal audit).

**Supplementary Information – Notes on the General Conditions**

If the processing, backup and storage of customer data takes place in different locations, this is to be described comprehensibly and transparently in the system description.

## BC-02 Information on availability and incident handling during regular operation

**Information on the General Conditions of the cloud service**

In contractual agreements (e.g. service description), the Cloud Service Provider provides comprehensible, binding and transparent information on:

- Availability of the cloud service;
- Categorisation and Prioritisation of incidents;
- Response times for disruptions of regular operation according to the categorisation (time elapsed between the reporting and the resolution of the disruption by the Cloud Service Provider);
- Recovery time (time elapsed until the incident has been resolved); and
- Legal consequences of non-compliance.

The details are based on definitions that allow subject matter experts of the cloud customers to assess the cloud service against their business requirements.

The system description describes where this information can be found.

If information on availability and remediation of disruptions represent average values that are not binding in individual cases, this is highlighted separately.

#### Supplementary Information – Notes on the General Conditions

In addition to the reference in the system description where this information can be found, the information itself may also be an optional part of the report, e.g. in a section "Other information provided by the legal representatives of the Cloud Service Provider". The auditor does not provide an opinion on the information.

### BC-03 Information on recovery parameters in emergency operation

#### Information on the General Conditions of the cloud service

The Cloud Service Provider provides subject matter experts of the cloud customers with comprehensible and transparent information on the following recovery parameters of the cloud service, if required:

- Maximum tolerable downtime/Recovery Time Objective (RTO)
- Maximum allowable data loss/Recovery Point Objective (RPO)
- Recovery time to start emergency operation
- Recovery level (capacity related to regular operation)
- Restore time until normal operation

The information enables cloud customers to evaluate the cloud service as part of their own business impact analysis.

#### Supplementary Information – Notes on the General Conditions

In addition to the reference in the system description where this information can be found, the information itself may also be an optional part of the report, e.g. in a section "Other information provided by the legal representatives of the Cloud Service Provider". The auditor does not provide an opinion on the information.

### BC-04 Information on the availability of the data centre

#### Information on the General Conditions of the cloud service

The cloud provider provides subject matter experts of cloud customers with comprehensible and transparent information on the availability of the data centres used to provide the cloud service (including data centres operated by subcontractors), as needed. The information shows availability and downtime over one year according to industry standard classification schemes. The information enables cloud customers to assess the cloud service as part of their business impact analysis.

#### Supplementary Information – Notes on the General Conditions

The Uptime Institute's Tier classification system is a classification customary in the industry. It defines the following levels (Tiers) for availability and downtime in relation to one year:

- Tier I: 99.671 %; up to 28.8 hours cumulative downtime per year
- Tier II: 99.741 %; up to 22.7 hours cumulative downtime per year
- Tier III: 99.982 %; up to 1.6 hours cumulative downtime per year
- Tier IV: 99.995 %; up to 25 minutes cumulative downtime per year

If there are requirements towards high availability of a data centre, the BSI HV benchmark, which provides the following availability classes (AC), is suitable:

- AC 0: without availability requirements (~ 95 %); up to 438 hours cumulative downtime per year
- AC 1: normal availability (99 %); up to 88 hours cumulative downtime per year
- AC 2: high availability (99.9 %); up to 9 hours cumulative downtime per year
- AC 3: very high availability (99.99 %); up to 53 minutes cumulative downtime per year
- AC 4: highest availability (99.999 %); up to 6 minutes cumulative downtime per year
- AC 5: Disaster-tolerant

This information may be an optional part of the report, e.g. in a section “Other information provided by the legal representatives of the cloud provider”. The practitioner themselves do not provide an opinion on the information.

## BC-05 Information on how investigation enquiries from government authorities are handled

### Information on the General Conditions of the cloud service

In the system description, the Cloud Service Provider provides comprehensible and transparent information on how investigation enquiries by government agencies for access to or disclosure of cloud customer data are handled. The information includes the following aspects:

- Procedures to verify the legal basis of such enquiries;
- Procedures for informing and involving the affected cloud customers upon receipt of such enquiries;
- the ability of the affected cloud customers to object; and
- whether the Cloud Service Provider has the ability to decrypt encrypted data of the cloud customers in case of such requests and how this ability for access or disclosure is used.

The scope of the information corresponds to the needs of the subject matter experts of the cloud customers who define specifications on information security, implement these or validate their implementation and assess the suitability of the cloud service from a legal and regulatory point of view (e.g. IT, compliance, internal audit).

### Supplementary Information – Notes on the General Conditions

The legal foundation on which these governmental services are based (e.g. law enforcement agencies, intelligence services) vary from region to region. In particular, the applicable jurisdiction at the locations where data of cloud customers is processed, stored, backed up and stored must be considered.

In Germany, such powers are governed by the laws of the German Federal Criminal Police Office (or the laws of the respective state offices), various procedural codes for courts and the laws for intelligence services (BNDG, BVerfSchG, respective laws on the constitutional protection offices of the federal states, MADG) and the G10 Act.

In other countries, other laws are relevant, and the cloud customer may only occasionally be aware of them from the media, e.g. the CLOUD Act (“Clarifying Lawful Overseas Use of Data Act”) from the United States of America or the Cyber Security Law of the People’s Republic of China. In conjunction with the other information on the cloud service, the cloud customer should be able to use this information to carry out a risk assessment assessing if and how these are relevant.

## BC-06 Information on certifications or attestations

### Information on the General Conditions of the cloud service

In the system description, the Cloud Service Provider provides comprehensible and transparent information on existing and valid certifications or attestations by independent third parties relating to the following aspects of the cloud service:

- compliance of the management systems for information security, business continuity and quality with applicable international standards;
- compliance with the European General Data Protection Regulation (GDPR);
- the suitability and effectiveness of the internal control system in relation to the applicable criteria; and
- certifications or attestations according to industry-specific requirements of cloud customers.

To the extent applicable for the certification or attestation, the following information are provided:

- date of issuance;
- issuing organisation; and
- date or period of validity or coverage.

The scope of the information corresponds to the needs of the subject matter experts of the cloud customers who define specifications on information security, implement these or validate their implementation and assess the suitability of the cloud service from a legal and regulatory point of view (e.g. IT, compliance, internal audit).

### Supplementary Information – Notes on the General Conditions

Transparency can be additionally increased by disclosing SLAs based on ISO/IEC 19086 or comparable standards.

Fulfilment of the General Condition does not require the Cloud Service Provider to hold a certification or attestation for all listed aspects.

# 5 Basic Criteria, Additional Criteria and Supplementary Information

# 5 Basic Criteria, Additional Criteria and Supplementary Information

## 5.1 Organisation of Information Security (OIS)

**Objective:** Plan, implement, maintain and continuously improve the information security framework within the organisation.

### OIS-01 Information Security Management System (ISMS)

#### Basic Criterion

The Cloud Service Provider operates an information security management system (ISMS) in accordance with ISO/IEC 27001. The scope of the ISMS covers the Cloud Service Provider's organisational units, locations and procedures for providing the cloud service.

The measures for setting up, implementing, maintaining and continuously improving the ISMS are documented. The documentation includes:

- Scope of the ISMS (Section 4.3 of ISO/IEC 27001);
- Declaration of applicability (Section 6.1.3), and
- Results of the last management review (Section 9.3).

#### Additional Criterion

The Information Security Management System (ISMS) has a valid certification according to ISO/IEC 27001 or ISO 27001 based on IT-Grundschutz.

#### Supplementary Information

*About the Criterion*

The basic criterion can also be fulfilled without valid certification of the ISMS according to ISO/IEC 27001 or ISO 27001 based on IT-Grundschutz, if the submitted documentation meets the requirements of ISO/IEC 27001.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: partially

A continuous audit of the ISO 27001 certificate is partially feasible because the existence of a certificate can be continuously verified through the creation date of the certificate and passing an authenticity check. However, the certificate is usually issued for three years and there will be no dynamic changes as a rule.

### OIS-02 Information Security Policy

#### Basic Criterion

The top management of the Cloud Service Provider has adopted an information security policy and communicated it to internal and external employees as well as cloud customers.

The policy describes:

- the importance of information security, based on the requirements of cloud customers in relation to information security;

- the security objectives and the desired security level, based on the business goals and tasks of the Cloud Service Provider;

- the most important aspects of the security strategy to achieve the security objectives set; and

- the organisational structure for information security in the ISMS application area.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

The top management is a natural person or group of persons who make the final decision for the institution and is responsible for that decision.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: partially

A policy can change ad-hoc. However, the continuous audit of policies is only partially feasible as the only attributes that can be tested are the last change date and the status of review or approval, as far as this information is stored in a system. The content of a policy can hardly be tested automatically.

## OIS-03 Interfaces and Dependencies

### Basic Criterion

Interfaces and dependencies between cloud service delivery activities performed by the Cloud Service Provider and activities performed by third parties are documented and communicated. This includes dealing with the following events:

- Vulnerabilities;

- Security incidents; and

- Malfunctions.

The type and scope of the documentation is geared towards the information requirements of the subject matter experts of the affected organisations in order to carry out the activities appropriately (e.g. definition of roles and responsibilities in guidelines, description of cooperation obligations in service descriptions and contracts).

The communication of changes to the interfaces and dependencies takes place in a timely manner so that the affected organisations and third parties can react appropriately with organisational and technical measures before the changes take effect.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

The Cloud Service Provider can define and document the interfaces and dependencies described in the basic criterion in guidelines and instructions. For example, cloud customers' obligations to cooperate should be described in service descriptions and contracts.

Third parties in the sense of this basic criterion are, e.g. cloud customers and sub-service providers.

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls, that the guidelines and requirements for compliance with the contractual agreements with the Cloud Service Provider (i.e., responsibilities, cooperation obligations and interfaces for reporting security incidents) are adequately defined, documented and set up.

*Notes on Continuous Auditing*

Feasibility: no

An automated continuous audit for critical dependencies and interfaces is currently only possible at a high cost to the Cloud Service Provider.

## OIS-04 Segregation of Duties

### Basic Criterion

Conflicting tasks and responsibilities are separated based on an OIS-06 risk assessment to reduce the risk of unauthorised or unintended changes or misuse of cloud customer data processed, stored or transmitted in the cloud service.

The risk assessment covers the following areas, insofar as these are applicable to the provision of the Cloud Service and are in the area of responsibility of the Cloud Service Provider:

- Administration of rights profiles, approval and assignment of access and access authorisations (cf. IDM-01);
- Development, testing and release of changes (cf. DEV-01); and
- Operation of the system components.

If separation cannot be established for organisational or technical reasons, measures are in place to monitor the activities in order to detect unauthorised or unintended changes as well as misuse and to take appropriate actions.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

Identified events that may constitute unauthorised or unintentional changes to or misuse of cloud customer data may, for example, be treated as a security incident, cf. SIM-01.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

A continuous audit is possible, especially in the case of changes to role profiles and responsibilities. This would require an initial check of the defined roles and responsibilities by the Cloud Service Provider. The roles that are added or changed on a monthly basis could then be automated and continuously checked.

## OIS-05 Contact with Relevant Government Agencies and Interest Groups

### Basic Criterion

The Cloud Service Provider leverages relevant authorities and interest groups in order to stay informed about current threats and vulnerabilities. The information flows into the procedures for handling risks (cf. OIS-06) and vulnerabilities (cf. OPS-19).

### Additional Criterion

If the cloud service is used by public sector organisations in Germany, the Cloud Service Provider leverages contacts with the National IT Situation Centre and the CERT Association of the BSI.

### Supplementary Information

*About the Criterion*

Relevant contacts are for example:

- Federal Office for Information Security (BSI);
- OWASP Foundation; and
- CERT networks DFN-CERT, TF-CSIRT etc.

Public sector organisations in Germany are e.g. authorities and ministries.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

A continuous audit of the Cloud Service Provider's contacts with relevant authorities and stakeholders can be achieved by continuously storing relevant information on a monthly basis, such as a list of contacted entities and evidence of receipt of a response. A continuous flow of information demonstrates a constant connection to relevant authorities and interest groups. Furthermore, the distribution of the information and, if necessary, the documentation of the handling of identified risks and vulnerabilities could be continuously audited for the coverage of this criterion.

## OIS-06 Risk Management Policy

### Basic Criterion

Policies and instructions for risk management procedures are documented, communicated and provided in accordance with SP-01 for the following aspects:

- Identification of risks associated with the loss of confidentiality, integrity, availability and authenticity of information within the scope of the ISMS and assigning risk owners;
- Analysis of the probability and impact of occurrence and determination of the level of risk;
- Evaluation of the risk analysis based on defined criteria for risk acceptance and prioritisation of handling;
- Handling of risks through measures, including approval of authorisation and acceptance of residual risks by risk owners; and
- Documentation of the activities implemented to enable consistent, valid and comparable results.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

The risk level can be determined by qualitative, semi-quantitative and quantitative methods (cf. ISO 31010) based on the likelihood and impacts.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: partially

A policy can change ad-hoc. However, the continuous audit of policies is only partially feasible as the only attributes that can be tested are the last change date and the status of review or approval, as far as this information is stored in a system. The content of a policy can hardly be tested automatically.

### OIS-07 Application of the Risk Management Policy

#### Basic Criterion

The Cloud Service Provider executes the process for handling risks as needed or at least once a year. The following aspects are taken into account when identifying risks, insofar as they are applicable to the cloud service provided and are within the area of responsibility of the Cloud Service Provider:

- Processing, storage or transmission of data of cloud customers with different protection needs;
- Occurrence of vulnerabilities and malfunctions in technical protective measures for separating shared resources;
- Attacks via access points, including interfaces accessible from public networks;
- Conflicting tasks and areas of responsibility that cannot be separated for organisational or technical reasons; and
- Dependencies on subservice organisations.

The analysis, evaluation and treatment of risks, including the approval of actions and acceptance of residual risks, is reviewed for adequacy at least annually by the risk owners.

#### Additional Criterion

–

#### Supplementary Information

*About the Criterion*

This criterion applies only to risks that reside within the area of responsibility of the cloud service provider. Risks that arise for the cloud customer when using the cloud service are not covered by this criterion. When outsourcing activities for the provision of cloud services to subservice organisations, the responsibility for these risks remains with the Cloud Service Provider. Requirements for measures to manage these risks can be found in the criteria area “Control and Monitoring of Service Providers and Suppliers (SSO)”.

Shared resources are e.g. networks, RAM or storage.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: partially

The procedure for handling risks must be tested at least once a year and is therefore part of the standard audit cycle. However, the continuous audit of handling risk is only partially feasible as the only attributes that can be tested are the last review date and the status of review or approval, as far as this information is stored in a system. The content of the risks can hardly be tested automatically.

## 5.2 Security Policies and Instructions (SP)

**Objective:** Provide policies and instructions regarding security requirements and to support business requirements.

### SP-01 Documentation, communication and provision of policies and instructions

#### Basic Criterion

Policies and instructions (incl. concepts and guidelines) are derived from the information security policy and are documented according to a uniform structure. They are communicated and made available to all internal and external employees of the Cloud Service Provider in an appropriate manner.

The policies and instructions are version controlled and approved by the top management of the Cloud Service Provider or an authorised body.

The policies and instructions describe at least the following aspects:

- Objectives;
- Scope;
- Roles and responsibilities, including staff qualification requirements and the establishment of substitution rules;
- Roles and dependencies on other organisations (especially cloud customers and subservice organisations);
- Steps for the execution of the security strategy; and
- Applicable legal and regulatory requirements.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

The appropriateness of the demand-oriented communication and provision must be assessed against the size and complexity of the Cloud Service Provider's organisation and the type of cloud service offered. Possible criteria are:

- Integration of guidelines and instructions in the onboarding of new employees
- Training and information campaigns when adopting new or revising existing policies and instructions
- Form of provision

Policies and instructions are required for the following basic criteria in which the content is specified in more detail:

- Risk management policy (OIS-06)
- Acceptable use and handling of assets policy (AM-02)
- Security requirements for premises and buildings (PS-01)
- Physical site access control (PS-04)
- Concept for protection against malware (OPS-04)
- Concept for data protection and recovery (OPS-06)
- Concept for logging and monitoring (OPS-10)
- Concept for meta data handling (OPS-11)
- Concept for handling of vulnerabilities, malfunctions and errors (OPS-18)
- Policy for system and data access authorisations (IDM-01)
- Policy for the use of encryption procedures and key management (CRY-01)
- Policies for data transmission (COS-08)
- Policies for the development/procurement of information systems (DEV-01)
- Policies for changes to information systems (DEV-03)
- Policies and instructions for controlling and monitoring third parties (SSO-01)
- Policy for security incident management (SIM-01)
- Business impact analysis policies and procedures (BCM-02)

- Policy for planning and conducting audits (COM-02)

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: partially

Regarding the uniformity and content of the policies and instructions, there is a need for manual testing, so continuous testing cannot be fully achieved.

The communication/provision of policies and instructions can be queried via various registers. Registries for all approved policies and instructions can serve as a basis for reviewing the policies/rejections provided in the usual channels and may be combined with a conditional access check. These requirements must first be met by the Cloud Service Provider.

Versioning after approval by authorised personnel can be automatically audited and is therefore suitable for continuous audit.

## SP-02 Review and Approval of Policies and Instructions

### Basic Criterion

Information security policies and instructions are reviewed at least annually for adequacy by the Cloud Service Provider’s subject matter experts.

The review shall consider at least the following aspects:

- Organisational and technical changes in the procedures for providing the cloud service; and
- Legal and regulatory changes in the Cloud Service Provider’s environment.

Revised policies and instructions are approved before they become effective.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

–

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: partially

A continuous, automated audit of the content changes to policies and instructions is only partially practicable at the current state-of-the-art.

A continuous audit of the reviewers’ authorisation and expertise does not appear to be effective either, as this cannot be linked to specified parameters of an automated evaluation. A continuous examination of this criterion could therefore only consist of returning the date of the last examination.

## SP-03 Exceptions from Existing Policies and Instructions

### Basic Criterion

Exceptions to the policies and instructions for information security as well as respective controls go through the OIS-06 risk management process, including approval of these exceptions and acceptance of the associated risks by the risk owners. The approvals of exceptions are documented, limited in time and are reviewed for appropriateness at least annually by the risk owners.

#### Additional Criterion

–

#### Supplementary Information

*About the Criterion*

Exceptions in the sense of the basic criterion can have organisational or technical causes, such as

- An organisational unit should deviate from the intended processes and procedures in order to meet the requirements of a cloud customer; and
- A system component lacks technical properties to configure it according to the applicable requirements.

Cloud customers can use appropriate controls to ensure that they obtain information from the Cloud Service Provider about deviations from information security policies and instructions in order to assess and appropriately manage the associated risks to their own information security.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: partially

Exceptions to policies and instructions are to be reviewed annually. However, the continuous audit of these exceptions is only partially feasible as the only attributes that can be tested are the last change date and the status or review or approval, as far as this information is stored in a system. The content of an exception can hardly be tested automatically.

## 5.3 Personnel (HR)

**Objective:** Ensure that employees understand their responsibilities, are aware of their responsibilities with regard to information security, and that the organisation's assets are protected in the event of changes in responsibilities or termination.

### HR-01 Verification of qualification and trustworthiness

#### Basic Criterion

The competency and integrity of all internal and external employees of the Cloud Service Provider with access to cloud customer data or system components under the Cloud Service Provider's responsibility who are responsible to provide the cloud service in the production environment shall be verified prior to commencement of employment in accordance with local legislation and regulation by the Cloud Service Provider.

To the extent permitted by law, the review will cover the following areas:

- Verification of the person through identity card;
- Verification of the CV;
- Verification of academic titles and degrees;
- Request of a police clearance certificate for applicants;
- Certificate of good conduct or national equivalent; and
- Evaluation of the risk to be blackmailed.

#### Additional Criterion

–

### Supplementary Information

*About the Criterion*

External employees in the sense of the criteria are those who perform activities in accordance with the processes and procedures of the Cloud Service Provider. Employees of sub-service providers who perform activities according to the sub-service own processes and procedures are not covered by this criterion.

The verification of qualification and trustworthiness can be supported by a specialised service provider. Depending on national legislation, national equivalents of the German certificate of good conduct may also be permitted. The assessment of the extent to which a potential employee can be blackmailed can be carried out, for example, by checking his creditworthiness.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: partially

A continuous audit is only partially achievable due to the complications between local deviations in laws and regulations.

It would be conceivable to continuously query the process steps stored in the system for each new hire in relation to the specified areas based on a list of employees maintained in the HR system in which new hires are registered.

To do this, the Cloud Service Provider would have to go through and document these steps applying a system-based approach. The auditor could then use an agent or a connected monitoring system to detect any deviations from the standard process.

## HR-02 Employment terms and conditions

### Basic Criterion

The Cloud Service Provider's internal and external employees are required by the employment terms and conditions to comply with applicable policies and instructions relating to information security.

The information security policy, and the policies and instructions based on it, are to be acknowledged by the internal and external personnel in a documented form before access is granted to any cloud customer data or system components under the responsibility of the Cloud Service Provider used to provide the cloud service in the production environment.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

The Cloud Service Provider ensures that the policies and instructions reflect applicable legal and regulatory requirements in accordance with SP-01.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

Due to the obligation of employees to comply with certain requirements, a continuous audit is not practical as compliance with the requirements can be verified as part of a standard audit cycle

A continuous audit of the granting of access only after acknowledgement of the instructions is achievable as far as the Cloud Service Provider designs the approval system to document the appropriate data (e.g., date of acknowledgement, which data the employee had access to and when). A clear definition and differentiation of customer data as well as data in the productive environment is essential.

With the help of this data, the auditor can perform a comparison and detect deviations accordingly. The data could be monitored using an agent on a monitoring system.

## HR-03 Security training and awareness programme

### Basic Criterion

The Cloud Service Provider operates a target group-oriented security awareness and training program, which is completed by all internal and external employees of the Cloud Service Provider on a regular basis. The program is regularly updated based on changes to policies and instructions and the current threat situation and includes the following aspects:

- Handling system components used to provide the cloud service in the production environment in accordance with applicable policies and procedures;
- Handling cloud customer data in accordance with applicable policies and instructions and applicable legal and regulatory requirements;
- Information about the current threat situation; and
- Correct behaviour in the event of security incidents.

### Additional Criterion

The learning outcomes achieved through the awareness and training programme are measured and evaluated in a target group-oriented manner. The measurements cover quantitative and qualitative aspects. The results are used to improve the awareness and training programme.

### Supplementary Information

*About the Criterion*

–

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

The concept behind the security awareness and training program does not require continuous assessment and is sufficiently covered by the recurring audit.

However, the completion of the training can be traced via training portals. For a continuous audit that each employee has completed and, if necessary, repeated the relevant training courses for his role description, a clear system-based definition of the necessary training courses for each role description must be carried out at the Cloud Service Provider. The expected dates which the respective training course is to be completed must also be recorded. The documentation that the training has been completed by the employee and, if necessary, successfully completed with an examination, should take place in the same portal.

The auditor then has the option of examining the results of the training courses for employees of the Cloud Service Provider for deviations by automatically and continuously comparing the expected training dates with the actual date on which the employees completed the training.

## HR-04 Disciplinary measures

### Basic Criterion

In the event of violations of policies and instructions or applicable legal and regulatory requirements, actions are taken in accordance with a defined policy that includes the following aspects:

- Verifying whether a violation has occurred; and
- Consideration of the nature and severity of the violation and its impact.

The internal and external employees of the Cloud Service Provider are informed about possible disciplinary measures.

The use of disciplinary measures is appropriately documented.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

The Cloud Service Provider ensures that the policies and instructions reflect applicable legal and regulatory requirements in accordance with SP-01.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: no

Continuous audit not practical, as the associated processes and steps can be tested once within a recurring audit.

A system-based definition of the violations as well as the corresponding regulations does not appear practical, since in this context individual case decisions are often necessary which cannot be covered by predefined algorithms.

## HR-05 Responsibilities in the event of termination or change of employment

### Basic Criterion

Internal and external employees have been informed about which responsibilities, arising from employment terms and conditions relating to information security, will remain in place when their employment is terminated or changed and for how long.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

The Cloud Service Provider ensures that the policies and instructions reflect applicable legal and regulatory requirements in accordance with SP-01.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

As part of a comprehensive, system-based documentation of HR data, it is conceivable that the employee will receive confirmation that he or she has been informed about the required topics. This should be requested again at the end of the employment relationship.

If such documentation was available in standardised and digital form, the auditor would be able to check each termination for this confirmation and identify any deviations. This makes continuous verification possible.

### HR-06 Confidentiality agreements

#### Basic Criterion

The non-disclosure or confidentiality agreements to be agreed with internal employees, external service providers and suppliers of the Cloud Service Provider are based on the requirements identified by the Cloud Service Provider for the protection of confidential information and operational details.

The agreements are to be accepted by external service providers and suppliers when the contract is agreed. The agreements must be accepted by internal employees of the Cloud Service Provider before authorisation to access data of cloud customers is granted.

The requirements must be documented and reviewed at regular intervals (at least annually). If the review shows that the requirements need to be adapted, the non-disclosure or confidentiality agreements are updated.

The Cloud Service Provider must inform the internal employees, external service providers and suppliers and obtain confirmation of the updated confidentiality or non-disclosure agreement.

#### Additional Criterion

–

#### Supplementary Information

*About the Criterion*

In a confidentiality agreement it should be described:

- Which information must be kept confidential;
- The period for which this confidentiality agreement applies;
- What actions must be taken upon termination of this agreement, e.g. destruction or return of data medium;
- How the ownership of information is regulated;
- What rules apply to the use and disclosure of confidential information to other partners, if necessary; and
- The consequences of a breach of the agreement.

Confidentiality or non-disclosure agreements can be signed by means of an electronic signature, insofar as this is legally binding.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

The signing of confidentiality agreements with internal employees, external service providers and suppliers can be standardised and stored digitally.

An automated continuous evaluation can then be carried out to check whether all parties have signed such a confidentiality agreement and whether the agreement is up to date.

## 5.4 Asset Management (AM)

**Objective:** Identify the organisation’s own assets and ensure an appropriate level of protection throughout their lifecycle.

### AM-01 Asset Inventory

#### Basic Criterion

The Cloud Service Provider has established procedures for inventorying assets.

The inventory is performed automatically and/or by the people or teams responsible for the assets to ensure complete, accurate, valid and consistent inventory throughout the asset lifecycle.

Assets are recorded with the information needed to apply the Risk Management Procedure (cf. OIS-07), including the measures taken to manage these risks throughout the asset lifecycle. Changes to this information are logged.

### Additional Criterion

Logging and monitoring applications take into account the information collected on the assets in order to identify the impact on cloud services and functions in case of events that could lead to a breach of protection objectives, and to support information provided to affected cloud customers in accordance with contractual agreements.

### Supplementary Information

*About the Criterion*

Assets within the meaning of this criteria area are the objects required for the information security of the cloud service during the creation, processing, storage, transmission, deletion or destruction of information in the Cloud Service Provider's area of responsibility, e.g. firewalls, load balancers, web servers, application servers and database servers.

These objects consist of hardware and software objects:

Hardware objects are

- Physical and virtual infrastructure resources (e.g. servers, storage systems, network components); and
- As well as end devices if the Cloud Service Provider has determined in a risk assessment that these could endanger the information security of the cloud service in the event of loss or unauthorised access (e.g. mobile devices used as security tokens for authentication).

Software objects are e.g. hypervisors, containers, operating systems, databases, microservices and programming interfaces (APIs).

The lifecycle of an asset includes:

- Acquisition;
- Commissioning;
- Maintenance;
- Decommissioning; and
- Disposal.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

The Cloud Service Provider must ensure that assets are automatically captured (in a database). The automatic capture of physical assets must also be ensured. However, it would be conceivable to automatically capture these assets when logging on to a network for the first time. The creation of virtual assets can be directly linked to the entry into the database.

If all assets are recorded automatically, changes to the database can be documented (logs) and these logs can then be continuously evaluated. It is important to ensure that the information contained in the inventory and logs is complete.

If automated processes are available, the auditor can create an evaluation of the changes in the inventory based on the logs.

In order to check the completeness, the first step would be to query all current assets at the Cloud Service Provider. This asset list could then be compared with the entries in the asset management database.

## AM-02 Acceptable Use and Safe Handling of Assets Policy

### Basic Criterion

Policies and instructions for acceptable use and safe handling of assets are documented, communicated and provided in accordance with SP-01 and address the following aspects of the asset lifecycle as applicable to the asset:

- Approval procedures for acquisition, commissioning, maintenance, decommissioning, and disposal by authorised personnel or system components;
- Inventory;
- Classification and labelling based on the need for protection of the information and measures for the level of protection identified;
- Secure configuration of mechanisms for error handling, logging, encryption, authentication and authorisation;
- Requirements for versions of software and images as well as application of patches;
- Handling of software for which support and security patches are not available anymore;
- Restriction of software installations or use of services;
- Protection against malware;
- Remote deactivation, deletion or blocking;
- Physical delivery and transport;
- dealing with incidents and vulnerabilities; and
- Complete and irrevocable deletion of the data upon decommissioning.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

–

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: partially

A policy can change ad-hoc. However, the continuous audit of policies is only partially feasible as the only attributes that can be tested are the last change date and the status of review or approval, as far as this information is stored in a system. The content of a policy can hardly be tested automatically.

## AM-03 Commissioning of Hardware

### Basic Criterion

The Cloud Service Provider has an approval process for the use of hardware to be commissioned, which is used to provide the cloud service in the production environment, in which the risks arising from the commissioning are identified, analysed and mitigated. Approval is granted after verification of the secure configuration of the mechanisms for error handling, logging, encryption, authentication and authorisation according to the intended use and based on the applicable policies.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

The basic criterion applies only to physical hardware objects, such as servers, storage systems, and network components.

Virtual hardware and software objects are considered in the criteria areas (OPS) and (DEV).

The approval process typically considers both the basic approval to use the hardware and the final approval of the configured assets.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

The approval of the commissioning of hardware by authorised personnel or system components must be digitally documented to allow continuous testing. A ticketing system, for example, is suitable for this purpose.

Both the instance and the verification of the configuration must be stored in the respective ticket.

This makes it possible for the auditor to check the tickets in an automated procedure. This requires an automated comparison of the authorised instance against a database containing all potential approvers. In addition, the verification of the configuration in the ticket must be audited automatically.

The compliant use of the assets can then be ensured via an agent system which checks active assets. The status of this system can then be queried by the auditor for a continuous audit.

## AM-04 Decommissioning of Hardware

### Basic Criterion

The decommissioning of hardware used to operate system components supporting the cloud service production environment under the responsibility of the Cloud Service Provider requires approval based on the applicable policies.

The decommissioning includes the complete and permanent deletion of the data or proper destruction of the media.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

The deletion of data or physical destruction of data mediums can take place, for example, according to DIN 66399 or BSI IT-Grundschutz module CON.6.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

The approval of the decommissioning of hardware by authorised personnel or system components must be digitally documented to allow continuous testing. A ticketing system, for example, is suitable for this purpose.

Both the instance and the verification of the complete deletion of the data must be stored in the respective ticket.

This enables the auditor to check the tickets in an automated procedure. This requires an automated comparison of the authorised instance against a database containing all potential approvers. In addition, the deletion of the data documented in the ticket must be audited automatically.

The compliant use of the assets can be ensured via an agent system which checks active assets. The status of this system can then be queried by the auditor for a continuous audit.

## AM-05 Commitment to Permissible Use, Safe Handling and Return of Assets

### Basic Criterion

The Cloud Service Provider's internal and external employees are provably committed to the policies and instructions for acceptable use and safe handling of assets before they can be used if the Cloud Service Provider has determined in a risk assessment that loss or unauthorised access could compromise the information security of the Cloud Service.

Any assets handed over are provably returned upon termination of employment.

### Additional Criterion

Physical assets of internal and external employees are managed centrally.

Central management enables software, data, and policy distribution, as well as remote deactivation, deletion, or locking.

### Supplementary Information

*About the Criterion*

The basic criterion essentially concerns mobile devices (e.g. notebooks, tablets, smartphones, etc.), where confidential information is stored on them which can be used in the event of unauthorised access to obtain privileged access to the cloud service (e.g. if these are used as security tokens for authentication).

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

The obligation of the employees to follow the policies and instructions can be made in digital form. This can be used to create a monitoring system that documents the non-obligation to employee guidelines in the form of logs.

In this case, the auditor can check the exceptions in the form of logs and request evidence of what additional steps the Cloud Service Provider has taken in these cases to minimise the risk.

The compliant use of the assets can then be ensured via an agent system which checks active assets. The status of this system can then be queried by the auditor for a continuous audit.

## AM-06 Asset Classification and Labelling

### Basic Criterion

Assets are classified and, if possible, labelled. Classification and labelling of an asset reflect the protection needs of the information it processes, stores, or transmits.

The need for protection is determined by the individuals or groups responsible for the assets of the Cloud Service Provider according to a uniform schema. The schema provides levels of protection for the confidentiality, integrity, availability, and authenticity protection objectives.

### Additional Criterion

Logging and monitoring applications take the asset protection needs into account in order to inform the responsible stakeholder of events that could lead to a violation of the protection goals, so that the necessary measures are taken with an appropriate priority. Actions for events on assets with a higher level of protection take precedence over events on assets with a lower need for protection.

### Supplementary Information

*About the Criterion*

If the Cloud Service Provider does not make a differentiated classification of the assets, all assets are to be assigned to the highest defined protection requirement.

*Complementary Customer Criterion*

Cloud customers can use appropriate controls to ensure that the need for protection of the information that can be processed or stored with the cloud service is adequately determined.

Cloud customers can also use appropriate controls to ensure that the information processed or stored with the cloud service is protected against tampering, copying, modifying, redirecting or deleting in accordance with its protection needs.

*Notes on Continuous Auditing*

Feasibility: yes

The classification of the assets and the determination of the need for protection should take place during the initial acquisition of the assets. Thus, the classification should also be documented in an asset management tool. The determination of the protection requirement can also be carried out in a standardised form and stored digitally. If there are changes in the classification, these should also be recorded in logs.

The auditor can then automatically test whether all assets in the platform are classified and whether the classification was determined using a standardised format. For changes in the classification, it can be automatically reconstructed whether these were also carried out based on the uniform schema. For this purpose, the logs produced can be evaluated as part of a continuous audit.

## 5.5 Physical Security (PS)

**Objective:** Prevent unauthorised physical access and protect against theft, damage, loss and outage of operations.

### PS-01 Physical Security and Environmental Control Requirements

### Basic Criterion

Security requirements for premises and buildings related to the cloud service provided, are based on the security objectives of the information security policy, identified protection requirements for the cloud service and the assessment of risks to physical and environmental security. The security requirements are documented, communicated and provided in a policy or concept according to SP-01.

The security requirements for data centres are based on criteria which comply with established rules of technology. They are suitable for addressing the following risks in accordance with the applicable legal and contractual requirements:

- Faults in planning;
- Unauthorised access;
- Insufficient surveillance;
- Insufficient air-conditioning;
- Fire and smoke;
- Water;
- Power failure; and
- Air ventilation and filtration.

If the Cloud Service Provider uses premises or buildings operated by third parties to provide the Cloud Service, the document describes which security requirements the Cloud Service Provider places on these third parties.

The appropriate and effective verification of implementation is carried out in accordance with the criteria for controlling and monitoring subcontractors (cf. SSO-01, SSO-02).

### Additional Criterion

The security requirements include time constraints for self-sufficient operation in the event of exceptional events (e.g. prolonged power outage, heat waves, low water in cold river water supply) and maximum tolerable utility downtime.

The time limits for self-sufficient operation provide for at least 48 hours in the event of a failure of the external power supply.

For a self-sufficient operation during a heat period, the highest outside temperatures measured to date within a radius of at least 50 km around the locations of the premises and buildings have been determined with a safety margin of 3 K. The security requirements stipulate that the permissible operating and environmental parameters of the cooling supply must also be observed on at least five consecutive days with these outside temperatures including the safety margin (cf. PS-06 Protection against failure of the supply facilities).

If water is taken from a river for air conditioning, it is determined at which water levels and water temperatures the air conditioning can be maintained for how long.

The maximum tolerable downtimes of utility facilities are suitable for meeting the availability requirements contained in the service level agreement.

### Supplementary Information

*About the Criterion*

Premises and buildings related to the cloud service provided include data centres and server rooms housing system components used to process cloud customer data and the technical utilities required to operate these system components (e.g. power supply, refrigeration, fire-fighting, telecommunications, security, etc.). Backup or redundancy computer centres.

Premises and buildings operated by third parties are e.g. server housing, colocation, IaaS.

Premises and buildings in which no data from cloud customers is processed or stored (e.g. offices of the Cloud Service Provider, server rooms with system components for internal development and test systems) are not subject to this criteria area.

The recognised rules of technology are defined in relevant standards, e.g. EN 50600 (facilities and infrastructures of data centres).

Incorrect planning can endanger the operational safety and availability of the premises or buildings. This can result from an incorrect assessment of elementary hazards at the site (e.g. air traffic, earthquakes, floods, hazardous substances) as well as an incorrect conception of the bandwidth or energy supply.

Time specifications for self-sustaining operation as well as maximum tolerable downtimes of utility facilities are typically collected during the business impact analysis (cf. BCM-02, BCM-03).

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: partially

A policy can change ad-hoc. However, the continuous audit of policies is only partially feasible as the only attributes that can be tested are the last change date and the status of review or approval, as far as this information is stored in a system. The content of a policy can hardly be tested automatically.

## PS-02 Redundancy model

### Basic Criterion

The cloud service is provided from two locations that are redundant to each other. The locations meet the security requirements of the Cloud Service Provider (cf. PS-01 Security Concept) and are located in an adequate distance to each other to achieve operational redundancy. Operational redundancy is designed in a way that ensures that the availability requirements specified in the service level agreement are met. The functionality of the redundancy is checked at least annually by suitable tests and exercises (cf. BCM-04 – Verification, updating and testing of business continuity).

### Additional Criterion

The cloud service is provided from more than two locations that provide each other with redundancy. The locations are sufficiently far apart to achieve georedundancy. If two locations fail at the same time, at least one third location is still available to prevent a total service failure. The georedundancy is designed in a way that ensures that the availability requirements specified in the service level agreement are met. The functionality of the redundancy is checked at least annually by suitable tests and exercises (cf. BCM-04 – Verification, updating and testing of business continuity).

### Supplementary Information

*About the Criterion*

Operational redundancy of the sites to each other in the sense of the basic requirement is given, if based on the assessment of elementary risks at the site corresponding distances of the premises and buildings to these risks are maintained. Very extensive events which, due to their extent, could affect several sites of the same redundancy group simultaneously or in a timely manner (e.g. floods, earthquakes) are not considered.

A georedundancy of the sites to each other in the sense of the optional, more far-reaching requirement is given if a very extensive event at a site under no circumstances affects several sites of the same redundancy group simultaneously or promptly. The BSI publication “Kriterien für die Standortwahl höchstverfügbarer und georedundanter Rechenzentren” provides assistance in this regard.

There are cloud providers who no longer address the issue of reliability of the cloud service on a physical level through redundancy from two independent locations, but through resilience. The cloud service is provided simultaneously from more than two locations. The underlying distributed data centre architecture ensures that the failure of a location or components of a location does not violate the defined availability criteria of the cloud service. Such an architecture can represent an alternative fulfilment (cf. Chapter 3.4.7) of the criterion. The tests and exercises on functionality required in the criterion also apply analogously to resilient architectures.

*Complementary Customer Criterion*

By means of suitable controls, cloud customers ensure that the existing redundancy model of the cloud provider and the evidence for the verification of the model comply with their own requirements for the availability and reliability of the cloud service.

*Notes on Continuous Auditing*

Feasibility: partially

**An annual audit of the effectiveness of the redundancy is only partially suitable for a continuous audit. A continuous audit could return the date of the last transaction to bring about redundancy.** In addition, it would be possible to document every transaction that contributes to redundancy by means of logs and to evaluate these logs automatically and continuously. In addition, the status of the redundancy could be continuously queried.

## PS-03 Perimeter Protection

### Basic Criterion

The structural shell of premises and buildings related to the cloud service provided are physically solid and protected by adequate security measures that meet the security requirements of the Cloud Service Provider (cf. PS-01 Security Concept).

The security measures are designed to detect and prevent unauthorised access so that the information security of the cloud service is not compromised.

The outer doors, windows and other construction elements exhibit an appropriate security level and withstand a burglary attempt for at least 10 minutes.

The surrounding wall constructions as well as the locking mechanisms meet the associated requirements.

### Additional Criterion

The security measures installed at the site include permanently present security personnel (at least 2 individuals), video surveillance and anti-burglary systems.

### Supplementary Information

*About the Criterion*

Security measures for detecting unauthorised access can be security personnel, video surveillance or burglar alarm systems.

The resistance class RC4 according to DIN EN 1627 stipulates that doors, windows and other components must withstand a break-in attempt for at least 10 minutes. The US standard SD-STD-01.01 Rev.G. is an international equivalent to this standard.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: partially

A continuous inspection of the structural shell of buildings is only partially feasible. Only the protection against unauthorised access can provide evaluable data in the form of access logs that are stored.

## PS-04 Physical site access control

### Basic Criterion

At access points to premises and buildings related to the cloud service provided, physical access controls are set up in accordance with the Cloud Service Provider’s security requirements (cf. PS-01 Security Concept) to prevent unauthorised access.

Access controls are supported by an access control system.

The requirements for the access control system are documented, communicated and provided in a policy or concept in accordance with SP-01 and include the following aspects:

- Specified procedure for the granting and revoking of access authorisations (cf. IDM-02) based on the principle of least authorisation (“least-privilege-principle”) and as necessary for the performance of tasks (“need-to-know-principle”);
- Automatic revocation of access authorisations if they have not been used for a period of 2 month;
- Automatic withdrawal of access authorisations if they have not been used for a period of 6 months;

- Two-factor authentication for access to areas hosting system components that process cloud customer information;

- Visitors and external personnel are tracked individually by the access control during their work in the premises and buildings, identified as such (e.g. by visible wearing of a visitor pass) and supervised during their stay; and

- Existence and nature of access logging that enables the Cloud Service Provider, in the sense of an effectiveness audit, to check whether only defined personnel have entered the premises and buildings related to the cloud service provided.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

–

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

Access control via an access card system can be documented by the Cloud Service Provider in the form of logs. These logs can be evaluated automatically. In addition, unauthorised access can also be traced through these logs. This can also be evaluated automatically.

Therefore, a continuous audit is possible.

Insofar as the withdrawal of access authorisations is standardised and documented in the same way, an automated evaluation is also possible here and thus a continuous audit can be carried out.

## PS-05 Protection from fire and smoke

### Basic Criterion

Premises and buildings related to the cloud service provided are protected from fire and smoke by structural, technical and organisational measures that meet the security requirements of the Cloud Service Provider (cf. PS-01 Security Concept) and include the following aspects:

a) Structural Measures:

Establishment of fire sections with a fire resistance duration of at least 90 minutes for all structural parts.

b) Technical Measures:

- Early fire detection with automatic voltage release. The monitored areas are sufficiently fragmented to ensure that the prevention of the spread of incipient fires is proportionate to the maintenance of the availability of the cloud service provided;

- Extinguishing system or oxygen reduction; and

- Fire alarm system with reporting to the local fire department.

c) Organisational Measures

- Regular fire protection inspections to check compliance with fire protection requirements; and

- Regular fire protection exercises.

### Additional Criterion

The environmental parameters are monitored. When the permitted control range is exceeded, alarm messages are generated and forwarded to the Cloud Service Provider’s subject matter experts.

### Supplementary Information

*About the Criterion*

The monitoring of the environmental parameters is addressed in PS-01. When exceeding the allowed control range, alarm messages are generated and forwarded to the responsible Cloud Service Provider.

Structural parts are walls, ceilings, floors, doors, ventilation flaps, etc.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

Continuous testing is possible insofar as the built-in technology for testing the protective measures produces evaluable data and these are stored in a standardised form. This would allow the security measures to be continuously evaluated by the auditor.

If this technology is not fully available and an inspection of the data centre is necessary, the possibility of continuous auditing is achievable only to a limited extent.

## PS-06 Protection against interruptions caused by power failures and other such risks

### Basic Criterion

Measures to prevent the failure of the technical supply facilities required for the operation of system components with which information from cloud customers is processed, are documented and set up in accordance with the security requirements of the Cloud Service Provider (cf. PS-01 Security Concept) with respect to the following aspects:

a) Operational redundancy (N+1) in power and cooling supply

b) Use of appropriately sized uninterruptible power supplies (UPS) and emergency power systems (NEA), designed to ensure that all data remains undamaged in the event of a power failure. The functionality of UPS and NEA is checked at least annually by suitable tests and exercises (cf. BCM-04 – Verification, updating and testing of business continuity).

c) Maintenance (servicing, inspection, repair) of the utilities in accordance with the manufacturer's recommendations.

d) Protection of power supply and telecommunications lines against interruption, interference, damage and eavesdropping. The protection is checked regularly, but at least every two years, as well as in case of suspected manipulation by qualified personnel regarding the following aspects:

- Traces of violent attempts to open closed distributors;
- Up-to-datedness of the documentation in the distribution list;
- Conformity of the actual wiring and patching with the documentation;
- The short-circuits and earthing of unneeded cables are intact; and
- Impermissible installations and modifications.

### Additional Criterion

Uninterruptible Power Supplies (UPS) and Emergency Power Supplies (NPS) are designed to meet the availability requirements defined in the Service Level Agreement.

The cooling supply is designed in such a way that the permissible operating and environmental parameters are also ensured on at least five consecutive days with the highest outside temperatures measured to date within a radius of at least 50 km around the locations of the premises and buildings, with a safety margin of 3 K (in relation to the outside temperature). The Cloud Service Provider has previously determined the highest outdoor temperatures measured to date (cf. PS-01 Security Concept).

The connection to the telecommunications network is designed with sufficient redundancy so that the failure of a telecommunications network does not impair the security or performance of the Cloud Service Provider.

### Supplementary Information

*About the Criterion*

Measures to prevent the failure of the technical supply facilities are e.g. power supply, cooling, fire-fighting technology, telecommunications, security technology, etc.

Cloud Service Providers can ensure that all data remains undamaged in the event of a power failure by shutting down servers following a defined procedure.

Power supply and telecommunications lines can be protected against interruption, interference, damage and eavesdropping by e.g. underground supply via different supply routes.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: partially

The physical security of premises, as well as failure precautions of the technical supply facilities should be ensured on site by an inspection of the data centre. Therefore, a continuous examination is achievable only to a limited extent. If the built-in technology for failure prevention produces evaluable log data, this requirement can partly be audited continuously. However, this does not replace an inspection.

Otherwise, a continuous inspection can be carried out at least partially by indicating the last inspection date.

## PS-07 Surveillance of operational and environmental parameters

### Basic Criterion

The operating parameters of the technical utilities (cf. PS-06) and the environmental parameters of the premises and buildings related to the cloud service provided are monitored and controlled in accordance with the security requirements of the Cloud Service Provider (cf. PS-01 Security Concept). When the permitted control range is exceeded, the responsible departments of the Cloud-Provider are automatically informed in order to promptly initiate the necessary measures for return to the control range.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

Operating parameters and environmental parameters of the premises and buildings are, e.g. air temperature and humidity, leakage.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

The monitoring and control of the operating parameters of the technical supply facilities is carried out automatically and documented in a standardised manner, for example in logs.

These logs are then automated by the inspector and can be continuously evaluated.

## 5.6 Operations (OPS)

**Objective:** Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.

### ■ OPS-01 Capacity Management – Planning

#### Basic Criterion

The planning of capacities and resources (personnel and IT resources) follows an established procedure in order to avoid possible capacity bottlenecks. The procedures include forecasting future capacity requirements in order to identify usage trends and manage system overload.

Cloud Service Providers take appropriate measures to ensure that they continue to meet the requirements agreed with cloud customers for the provision of the cloud service in the event of capacity bottlenecks or outages regarding personnel and IT resources, in particular those relating to the dedicated use of system components, in accordance with the respective agreements.

#### Additional Criterion

The forecasts are considered in accordance with the service level agreement for planning and preparing the provisioning.

#### Supplementary Information

*About the Criterion*

For economic reasons, Cloud Service Providers typically strive for a high utilisation of IT resources (CPU, RAM, storage space, network). In multi-tenant environments, existing resources must still be shared between cloud users (clients) in such a way that service level agreements are adhered to. In this respect, proper planning and monitoring of IT resources is critical to the availability and competitiveness of the cloud service. If the procedures are not documented or are subject to a higher degree of confidentiality as a trade secret of the Cloud Service Provider, the Cloud Service Provider must be able to explain the procedures at least orally within the scope of this audit.

Cloud customers must use appropriate controls to ensure that the capacity and resource requirements to be covered by the Cloud Service Provider are planned and reflected in the SLA with the Cloud Service Provider. The requirements can also be reviewed regularly through appropriate controls and the SLA can be adjusted accordingly.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: no

An audit of the planning of capacities and resources requires an assessment of the plausibility or meaningfulness of the content. At present, this can hardly be audited automatically and continuously.

### ■ OPS-02 Capacity Management – Monitoring

#### Basic Criterion

Technical and organisational safeguards for the monitoring and provisioning and de-provisioning of cloud services are defined. Thus, the Cloud Service Provider ensures that resources are provided and/or services are rendered according to the contractual agreements and that compliance with the service level agreements is ensured.

#### Additional Criterion

To monitor capacity and availability, the relevant information is available to the cloud customer in a self-service portal.

### Supplementary Information

*About the Criterion*

Technical and organisational measures typically include:

- Use of monitoring tools with alarm function when defined threshold values are exceeded;
- Process for correlating events and interface to incident management;
- Continuous monitoring of the systems by qualified personnel; and
- Redundancies in the IT systems.

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls, that the contractual agreements made with the Cloud Service Provider for the provision of resources or services can be monitored. In case of deviations, appropriate controls ensure that the Cloud Service Provider is informed so that the Cloud Service Provider can take appropriate action.

*Notes on Continuous Auditing*

Feasibility: yes

The part of resource monitoring can be continuously audited by checking capacity forecasts and monitoring the resource management tool. Furthermore, the logs of provisioning and de-provisioning and their impact on resource management can be continuously audited by the changes in resource management.

## OPS-03 Capacity Management – Controlling of Resources

### Basic Criterion

Depending on the capabilities of the respective service model, the cloud customer can control and monitor the allocation of the system resources assigned to the customer for administration/use in order to avoid overcrowding of resources and to achieve sufficient performance.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

Resources according to the possibilities of the service model are for example

- Computing capacity;
- Storage capacity;
- Configuration of network properties;
- Application Programming Interfaces (APIs); and
- Databases.

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls, that they manage and monitor the system resources in their area of responsibility.

*Notes on Continuous Auditing*

Feasibility: partially

The existence of tools for controlling resources by the cloud customers themselves is, in itself, a continuous process, which can be continuously checked provided that the Cloud Service Provider can prove the functionality of these tools by means of logs. However, continuously checking this only generates a limited value. The functionality of the tools provided can be continuously audited, if they are documented and can be evaluated by the Cloud Service Provider.

## OPS-04 Protection Against Malware – Concept

### Basic Criterion

Policies and instructions with specifications for protection against malware are documented, communicated, and provided in accordance with SP-01 with respect to the following aspects:

- Use of system-specific protection mechanisms;
- Operating protection programs on system components under the responsibility of the Cloud Service Provider that are used to provide the cloud service in the production environment; and
- Operation of protection programs for employees' terminal equipment.

### Additional Criterion

The Cloud Service Provider creates regular reports on the checks performed, which are reviewed and analysed by authorised bodies or committees. Policies and instructions describe the technical measures taken to securely configure and monitor the management console (both the customer's self-service and the service provider's cloud administration) to protect it from malware. Updates are applied at the highest frequency that the vendor(s) contractually offer(s).

### Supplementary Information

*About the Criterion*

Protection programs for employee devices can be, for example, server-based protection programs that scan files in attachments on the server or filter network traffic.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: partially

A policy can change ad-hoc. However, the continuous audit of policies is only partially feasible as the only attributes that can be tested are the last change date and the status of review or approval, as far as this information is stored in a system. The content of a policy can hardly be tested automatically.

## OPS-05 Protection Against Malware – Implementation

### Basic Criterion

System components under the Cloud Service Provider's responsibility that are used to deploy the cloud service in the production environment are configured with malware protection according to the policies and instructions. If protection programs are set up with signature and behaviour-based malware detection and removal, these protection programs are updated at least daily.

### Additional Criterion

The configuration of the protection mechanisms is monitored automatically. Deviations from the specifications are automatically reported to the subject matter experts so that the deviations are immediately assessed and the necessary measures taken.

### Supplementary Information

*About the Criterion*

Protection against malicious programs can be implemented by operating system-specific protection mechanisms or explicit protection programs (e.g. for signature- and behaviour-based detection and removal of malicious programs).

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls, that the layers of the cloud service which they are responsible for, have security products in place to detect and remove malware.

*Notes on Continuous Auditing*

Feasibility: yes

The first step should be to check whether all systems are covered. This should be monitored by continuously checking a tool including the additions and deletions of entries.

In the second step, the log files for the updates of the individual servers and the regular scans should be audited continuously. Identified malware or irregularities should be marked and tracked as part of the continuous scan.

## OPS-06 Data Backup and Recovery – Concept

### Basic Criterion

Policies and instructions for data backup and recovery are documented, communicated and provided in accordance with SP-01 regarding the following aspects.

- The extent and frequency of data backups and the duration of data retention are consistent with the contractual agreements with the cloud customers and the Cloud Service Provider's operational continuity requirements for Recovery Time Objective (RTO) and Recovery Point Objective (RPO);
- Data is backed up in encrypted, state-of-the-art form;
- Access to the backed-up data and the execution of restores is performed only by authorised persons; and
- Tests of recovery procedures (cf. OPS-08).

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

The data backup concept specifies which type of data backup is to be carried out (e.g. type, manner, duration) and specifies which data must also be backed up in special cases (e.g. pure use of compute nodes without data storage). When backing up data, a distinction must be made between backups and snapshots of virtual machines. Snapshots do not replace backups, but can be part of the backup strategy to achieve Recovery Point Objectives (RPO) if they are additionally stored outside the original data location. The business requirements of the Cloud Service Provider for the scope, frequency and duration of the data backup result from the business impact analysis (cf. BCM-03) for development and operational processes of the cloud service. If different data backup and recovery procedures exist for data under the responsibility of the cloud customer and the Cloud Service Provider, both variants must be included in a test according to this criteria catalogue. For procedures to secure the data of the Cloud Service Provider, only the adequacy and implementation of the controls must be proven, but not their effectiveness. For procedures to secure the data of cloud customers, proof of effectiveness must also be provided.

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls, that the contractual agreements made with the Cloud Service Provider regarding the scope, frequency and duration of data retention meet business requirements. The business requirements are assessed as part of the Business Impact Analysis (cf. BCM-02).

*Notes on Continuous Auditing*

Feasibility: partially

A policy can change ad-hoc. However, the continuous audit of policies is only partially feasible as the only attributes that can be tested are the last change date and the status of review or approval, as far as this information is stored in a system. The content of a policy can hardly be tested automatically.

## OPS-07 Data Backup and Recovery – Monitoring

### Basic Criterion

The execution of data backups is monitored by technical and organisational measures. Malfunctions are investigated by qualified staff and rectified promptly to ensure compliance with contractual obligations to cloud customers or the Cloud Service Provider's business requirements regarding the scope and frequency of data backup and the duration of storage.

### Additional Criterion

The relevant logs or summarised results are available to the cloud customer in a self-service portal for monitoring the data backup.

### Supplementary Information

*About the Criterion*

If the data backup is not part of the contract concluded between the Cloud Service Provider and the cloud customer, this criterion is not applicable. The Cloud Service Provider must present this situation transparently in the system description.

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls, that the backup of data within their area of responsibility is monitored by technical and organisational measures.

*Notes on Continuous Auditing*

Feasibility: yes

The execution of different data backups can be performed by continuously auditing the log files and the associated results of the data backup. Any errors in the data backup would be continuously detected and could be explained by appropriate measures and documentation in the audit.

## OPS-08 Data Backup and Recovery – Regular Testing

### Basic Criterion

Restore procedures are tested regularly, at least annually. The tests allow an assessment to be made as to whether the contractual agreements as well as the specifications for the maximum tolerable downtime (Recovery Time Objective, RTO) and the maximum permissible data loss (Recovery Point Objective, RPO) are adhered to (cf. BCM-02).

Deviations from the specifications are reported to the responsible personnel or system components so that these can promptly assess the deviations and initiate the necessary actions.

### Additional Criterion

At the customer's request, the Cloud Service Provider inform the cloud customer of the results of the recovery tests. Recovery tests are embedded in the Cloud Service Provider's emergency management.

### Supplementary Information

*About the Criterion*

If the data backup is not part of the contract concluded between the Cloud Service Provider and the cloud customer, this criterion is not applicable. The Cloud Service Provider must present this situation transparently in the system description.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: partially

If the tests on the restoration procedures are performed at regular intervals, the time of execution and results can be audited automatically. However, the effort of a continuous audit of this criterion is high and the added value limited if the tests are carried out in an annual cycle

## OPS-09 Data Backup and Recovery – Storage

### Basic Criterion

The Cloud Service Provider transfers data to be backed up to a remote location or transports these on backup media to a remote location. If the data backup is transmitted to the remote location via a network, the data backup or the transmission of the data takes place in an encrypted form that corresponds to the state-of-the-art. The distance to the main site is chosen after sufficient consideration of the factors recovery times and impact of disasters on both sites. The physical and environmental security measures at the remote site are at the same level as at the main site.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

If the data backup is not part of the contract concluded between the Cloud Service Provider and the cloud customer, this criterion is not applicable. The Cloud Service Provider must present this situation transparently in the system description.

A remote location can be e.g. another data centre of the Cloud Service Provider.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

If the data is transported physically, a continuous audit of this criterion means that the successful storage has been confirmed. In the case of electronic transmission, the log files of the transmission can be continuously evaluated, and the result of this audit can be transmitted.

## OPS-10 Logging and Monitoring – Concept

### Basic Criterion

The Cloud Service Provider has established policies and instructions that govern the logging and monitoring of events on system components within its area of responsibility. These policies and instructions are documented, communicated and provided according to SP-01 with respect to the following aspects:

- Definition of events that could lead to a violation of the protection goals;
- Specifications for activating, stopping and pausing the various logs;
- Information regarding the purpose and retention period of the logs;
- Define roles and responsibilities for setting up and monitoring logging;
- Time synchronisation of system components; and
- Compliance with legal and regulatory frameworks.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

Legal and regulatory frameworks can define e.g. legal requirements for retention and deletion of data.

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls, that appropriate logging and monitoring of events that may affect the security and availability of the cloud service (e.g. administrator activities, system failures, authentication checks, data deletions, etc.) takes place for those layers of the cloud service under their responsibility.

*Notes on Continuous Auditing*

Feasibility: partially

A policy can change ad-hoc. However, the continuous audit of policies is only partially feasible as the only attributes that can be tested are the last change date and the status of review or approval, as far as this information is stored in a system. The content of a policy can hardly be tested automatically.

## OPS-11 Logging and Monitoring – Metadata Management Concept

### Basic Criterion

Policies and instructions for the secure handling of metadata (usage data) are documented, communicated and provided according to SP-01 with regard to the following aspects:

- Metadata is collected and used solely for billing, incident management and security incident management purposes;
- Exclusively anonymous metadata to deploy and enhance the cloud service so that no conclusions can be drawn about the cloud customer or user;
- No commercial use;
- Storage for a fixed period reasonably related to the purposes of the collection;
- Immediate deletion if the purposes of the collection are fulfilled and further storage is no longer necessary; and
- Provision to cloud customers according to contractual agreements.

### Additional Criterion

Personal data is automatically removed from the log data before the Cloud Service Provider processes it as far as technically possible. The removal is done in a way that allows the Cloud Service Provider to continue to use the log data for the purpose for which it was collected.

### Supplementary Information

*About the Criterion*

Metadata is all data that is generated by the Cloud Service Provider through the use of its service by the cloud customer and is not content-related data. This includes login/logout times, IP addresses, customer’s GPS location, which resources (network, storage, computer) were used, which data was accessed when, with whom data was shared, with whom it was communicated, etc. This data is partly used for billing purposes and for (security) incident management. However, it can also be used to analyse customer behaviour (depending on the cloud service) and to make the decision making and work processes visible to the Cloud Service Provider. The criteria aim to provide a transparent and clear definition of the collection and use of metadata. In addition, metadata refers to data that is generated when the Cloud Service Provider accesses customer data (e.g. for indexing).

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: partially

A policy can change ad-hoc. However, the continuous audit of policies is only partially feasible as the only attributes that can be tested are the last change date and the status of review or approval, as far as this information is stored in a system. The content of a policy can hardly be tested automatically.

## OPS-12 Logging and Monitoring – Access, Storage and Deletion

### Basic Criterion

The requirements for the logging and monitoring of events and for the secure handling of metadata are implemented by technically supported procedures with regard to the following restrictions:

- Access only for authorised users and systems;
- Retention for the specified period; and
- Deletion when further retention is no longer necessary for the purpose of collection.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

–

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: no

A continuous check is only of limited use here, since the primary purpose of checking the handling of metadata is to check the guidelines and the associated configurations of the tools for securing, processing and deleting metadata. In addition, the contractual basis for the use of metadata may also need to be considered.

A continuous audit could include the configuration for deleting or anonymising the metadata and automatically recording whether the configuration still exists and is implemented correctly. In this case, there would be a partial possibility for continuous auditing.

## OPS-13 Logging and Monitoring – Identification of Events

### Basic Criterion

The logging data is automatically monitored for events that may violate the protection goals in accordance with the logging and monitoring requirements. This also includes the detection of relationships between events (event correlation).

Identified events are automatically reported to the appropriate departments for prompt evaluation and action.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

–

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

The Cloud Service Provider can automatically test the list of assets critical for monitoring and record this test in logs.

The auditor can audit the log files for irregularities automatically and continuously.

## OPS-14 Logging and Monitoring – Storage of the Logging Data

### Basic Criterion

The Cloud Service Provider retains the generated log data and keeps these in an appropriate, unchangeable and aggregated form, regardless of the source of such data, so that a central, authorised evaluation of the data is possible. Log data is deleted if it is no longer required for the purpose for which they were collected.

Between logging servers and the assets to be logged, authentication takes place to protect the integrity and authenticity of the information transmitted and stored. The transfer takes place using state-of-the-art encryption or a dedicated administration network (out-of-band management).

### Additional Criterion

The Cloud Service Provider provides a customer-specific logging (in terms of scope and duration of retention period) upon request of the Cloud Customer. Depending on the protection requirements of the Cloud Service Provider and the technical feasibility, a logical or physical separation of log and customer data is carried out.

### Supplementary Information

*About the Criterion*

–

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

The storage of logging data at a central location can be documented by logs when the data is saved. The deletion of this data can also be automated and documented by logs.

The auditor can then perform an automated and continuous evaluation of these logs.

## OPS-15 Logging and Monitoring – Accountability

### Basic Criterion

The log data generated allows an unambiguous identification of user accesses at tenant level to support (forensic) analysis in the event of a security incident.

Interfaces are available to conduct forensic analyses and perform backups of infrastructure components and their network communication.

### Additional Criterion

On request of the cloud customer, the Cloud Service Provider provides the logs relating to the cloud customer in an appropriate form and in a timely manner so that the cloud customer can investigate any incidents relating to them.

### Supplementary Information

*About the Criterion*

Infrastructure components in the sense of this criterion are e.g. fabric controllers, network components and virtualisation servers.

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls, that unique user IDs are assigned which allow a corresponding analysis in the event of a security incident.

*Notes on Continuous Auditing*

Feasibility: no

For the generated logging data to allow unambiguous identification of user accesses at the tenant level, the creation of this data must be configured accordingly. This configuration does not have to be audited continuously, but only if it is changed.

The interfaces can also be audited initially and then tested again if changes are made.

## OPS-16 Logging and Monitoring – Configuration

### Basic Criterion

Access to system components for logging and monitoring in the Cloud Service Provider's area of responsibility is restricted to authorised users. Changes to the configuration are made in accordance with the applicable policies (cf. DEV-03).

### Additional Criterion

Access to system components for logging and monitoring in the Cloud Service Provider's area of responsibility requires two-factor authentication.

### Supplementary Information

*About the Criterion*

–

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

The continuous audit of this access restriction can be tested by log files of all changes to access rights for the system components for logging and monitoring. Changes can be automatically and continuously audited according to the person's sense and need for access.

## OPS-17 Logging and Monitoring – Availability of the Monitoring Software

### Basic Criterion

The Cloud Service Provider monitors the system components for logging and monitoring in its area of responsibility. Failures are automatically and promptly reported to the Cloud Service Provider's responsible departments so that these can assess the failures and take required action.

### Additional Criterion

The system components for logging and monitoring are designed in such a way that the overall functionality is not restricted if individual components fail.

### Supplementary Information

*About the Criterion*

–

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

Automatically communicated failures can be tracked in logs.

A continuous and automated audit of these failures can be carried out by evaluating these logs.

## OPS-18 Managing Vulnerabilities, Malfunctions and Errors – Concept

### Basic Criterion

Guidelines and instructions with technical and organisational measures are documented, communicated and provided in accordance with SP-01 to ensure the timely identification and addressing of vulnerabilities in the system components used to provide the cloud service. These guidelines and instructions contain specifications regarding the following aspects:

- Regular identification of vulnerabilities;
- Assessment of the severity of identified vulnerabilities;
- Prioritisation and implementation of actions to promptly remediate or mitigate identified vulnerabilities based on severity and according to defined timelines; and
- Handling of system components for which no measures are initiated for the timely remediation or mitigation of vulnerabilities.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

Identified vulnerabilities can be classified according to established metrics such as CVSS or OWASP. The decision not to remediate or mitigate identified vulnerabilities must be made by the Cloud Service Provider based on a risk assessment. If necessary, risk-compensating measures must be taken.

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls, that they check system components in their area of responsibility for vulnerabilities on a regular basis and mitigate these with appropriate measures.

*Notes on Continuous Auditing*

Feasibility: no

A policy can change ad-hoc. However, the continuous audit of policies is only partially feasible as the only attributes that can be tested are the last change date and the status of review or approval, as far as this information is stored in a system. The content of a policy can hardly be tested automatically.

## OPS-19 Managing Vulnerabilities, Malfunctions and Errors – Penetration Tests

### Basic Criterion

The Cloud Service Provider has penetration tests carried out by qualified internal personnel or external service providers at least once a year. The penetration tests are carried out according to a documented test methodology and include the system components relevant to the provision of the cloud service in the area of responsibility of the Cloud Service Provider, which have been identified as such in a risk analysis.

The Cloud Service Provider assess the severity of the findings made in penetration tests according to defined criteria.

For findings with medium or high criticality regarding the confidentiality, integrity or availability of the cloud service, actions must be taken within defined time windows for prompt remediation or mitigation.

#### Additional Criterion

The tests are carried out every six months. They must always be performed by independent external auditors. Internal personnel for penetration tests may support the external service providers.

#### Supplementary Information

*About the Criterion*

Vulnerabilities should be classified according to damage potential and a period of time should be specified for the required response. The following classification according to the BSI publication "Ein Praxis-Leitfaden für IS-Penetrationstests" can serve as an orientation:

- High: Immediate reaction;
- Medium: Short-term response;
- Low: Medium-term response; and
- Information: Long-term response.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: partially

Since penetration tests are carried out annually, a continuous audit is not practical, since the effort required to automate the execution of the test is probably greater than the benefit.

### OPS-20 Managing Vulnerabilities, Malfunctions and Errors – Measurements, Analyses and Assessments of Procedures

#### Basic Criterion

The Cloud Service Provider regularly measures, analyses and assesses the procedures with which vulnerabilities and incidents are handled to verify their continued suitability, appropriateness and effectiveness.

Results are evaluated at least quarterly by accountable departments at the Cloud Service Provider to initiate continuous improvement actions and to verify their effectiveness.

#### Additional Criterion

–

#### Supplementary Information

*About the Criterion*

Common Vulnerabilities and Exposures (CVE) or similar methods are a suitable way of documenting vulnerabilities and incidents.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

The measurements, analyses and evaluations are based on data that could be continuously queried in order to verify the plausibility of the results derived from them.

The initiation and review of measures for continuous improvement require a manual audit.

### OPS-21 Involvement of Cloud Customers in the Event of Incidents

#### Basic Criterion

The Cloud Service Provider periodically informs the cloud customer on the status of incidents affecting the cloud customer, or, where appropriate and necessary, involve the customer in the resolution, in a manner consistent with the contractual agreements.

As soon as an incident has been resolved from the Cloud Service Provider's perspective, the cloud customer is informed according to the contractual agreements, about the actions taken.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

–

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls that they receive notifications from the Cloud Service Provider regarding incidents that affect them, and that these notifications are forwarded in a timely manner to the department responsible for processing them so that appropriate action can be taken.

*Notes on Continuous Auditing*

Feasibility: yes

A continuous audit is possible if customers are informed about incidents via a standardised communication channel and this is documented (e-mails, logs).

The auditor can then evaluate the compiled documentation automatically and continuously.

However, it seems more effective to combine the evaluation of the communication of incidents to cloud customers with the evaluation of the elimination of the incidents. As soon as the incidents have been resolved automatically in the best case, an automatic message is generated and sent to the cloud customer. This message is to be documented.

This makes it possible for the auditor to evaluate whether the cloud customer has been properly informed on a regular basis about all incidents affecting them, but not beyond.

## OPS-22 Testing and Documentation of known Vulnerabilities

### Basic Criterion

System components in the area of responsibility of the Cloud Service Provider for the provision of the cloud service are automatically checked for known vulnerabilities at least once a month in accordance with the policies for handling vulnerabilities (cf. OPS-18), the severity is assessed in accordance with defined criteria and measures for timely remediation or mitigation are initiated within defined time windows.

### Additional Criterion

Available security patches are applied depending on the severity of the vulnerabilities, as determined based on the latest version of the Common Vulnerability Scoring System (CVSS):

- Critical (CVSS = 9.0 – 10.0), 3 hours;
- High (CVSS = 7.0 – 8.9), 3 days;
- Average (CVSS = 4.0 – 6.9), 1 month; and
- Low (CVSS = 0.1 – 3.9), 3 months.

### Supplementary Information

*About the Criterion*

In contrast to penetration tests (cf. OPS-20), which are carried out manually and according to an individual scheme, the check for open vulnerabilities is performed automatically, using so-called vulnerability scanners.

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls, that system components under their responsibility are regularly checked for vulnerabilities and to mitigate these by appropriate measures.

*Notes on Continuous Auditing*

Feasibility: yes

The periodic check for vulnerabilities and the corresponding results as well as the analysis and remediation of identified vulnerabilities are documented by the Cloud Service Provider.

An automated and continuous audit of this procedure can be implemented by the auditor by automatically evaluating the documented results.

## OPS-23 Managing Vulnerabilities, Malfunctions and Errors – System Hardening

### Basic Criterion

System components in the production environment used to provide the cloud service under the Cloud Service Provider's responsibility are hardened according to generally accepted industry standards. The hardening requirements for each system component are documented.

If non-modifiable ("immutable") images are used, compliance with the hardening specifications as defined in the hardening requirements is checked upon creation of the images. Configuration and log files regarding the continuous availability of the images are retained.

### Additional Criterion

System components in the Cloud Service Provider's area of responsibility are automatically monitored for compliance with hardening specifications. Deviations from the specifications are automatically reported to the appropriate departments of the Cloud Service Provider for immediate assessment and action.

### Supplementary Information

*About the Criterion*

System components in the sense of the basic criterion are the objects required for the information security of the cloud service during the creation, processing, storage, transmission, deletion or destruction of information in the Cloud Service Provider's area of responsibility, e.g. firewalls, load balancers, web servers, application servers and database servers. These system components in turn consist of hardware and software objects. This criterion is limited to software objects such as hypervisors, operating systems, databases, programming interfaces (APIs), images (e.g. for virtual machines and containers) and applications for logging and monitoring security events.

The configuration and log files for non-modifiable mages include e.g.:

- Configuration of the images used with regards to implemented hardening specifications including version history; and
- Logs for file integrity monitoring of images in productive use.

Generally accepted industry standards are, for example, the Security Configuration Benchmark of the "Centre for Internet Security" (CIS) or the corresponding modules in the BSI IT-Grundschutz-Kompendium.

Compliance with hardening specifications can be monitored with e.g. file integrity monitoring.

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls that layers of the cloud service which are under their responsibility are hardened according to generally established and accepted industry standards. The hardening specifications applied are derived from a risk assessment of the planned usage of the cloud service.

*Notes on Continuous Auditing*

Feasibility: yes

The verification of compliance with the specifications for the hardening of system components can be automatically tested and subsequently documented (logs).

The auditor can evaluate these logs automatically and continuously and thus carry out a continuous audit.

### OPS-24 Separation of Datasets in the Cloud Infrastructure

#### Basic Criterion

Cloud customer data stored and processed on shared virtual and physical resources is securely and strictly separated according to a documented approach based on OIS-07 risk analysis to ensure the confidentiality and integrity of this data.

#### Additional Criterion

Resources in the storage network are segmented by secure zoning (LUN binding and LUN masking).

#### Supplementary Information

*About the Criterion*

Shared resources include memory, cores and storage networks. Technical segregation (separation) of the stored and processed data of cloud customers into shared resources can be achieved through firewalls, access lists, tagging, VLANs, virtualisation and measures in the storage network (e.g. LUN binding and LUN masking). Where the adequacy and effectiveness of segregation cannot be assessed with reasonable assurance (e.g. due to complex implementation), evidence may also be provided through expert third party review results (e.g. penetration tests to validate the concept). The segregation of transmitted data is subject to control COS-06.

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls that the functions provided by the cloud service for segregating shared virtual and physical resources are used in such way that risks related to segregation are adequately addressed according to the data's protection requirements.

*Notes on Continuous Auditing*

Feasibility: partially

The segregation according to a documented concept is implemented by means of a configuration which does not change with high frequency. A continuous audit of this configuration could check whether the configuration and thus the segregation of the data is implemented correctly. However, the effort for a continuous audit would be high and the benefit limited due to the low change rate of the configuration. Thus, a continuous audit would only be of limited use here. If compliance with the measures taken is monitored, this criterion can be audited automatically.

It would also be conceivable to continuously audit the actual data segregation. For this purpose, the Cloud Service Provider would have to set up appropriate agents to monitor the data flow between the customer instances (or its absence) on a permanent and documented basis (logs).

## 5.7 Identity and Access Management (IDM)

**Objective:** Secure the authorisation and authentication of users of the Cloud Service Provider (typically privileged users) to prevent unauthorised access.

### IDM-01 Policy for user accounts and access rights

#### Basic Criterion

A role and rights concept based on the business and security requirements of the Cloud Service

Provider as well as a policy for managing user accounts and access rights for internal and external employees of the Cloud Service Provider and system components that have a role in automated authorisation processes of the Cloud Service Provider are documented, communicated and made available according to SP-01:

- Assignment of unique usernames;
- Granting and modifying user accounts and access rights based on the "least-privilege-principle" and the "need-to-know" principle;
- Segregation of duties between operational and monitoring functions ("Segregation of Duties");
- Segregation of duties between managing, approving and assigning user accounts and access rights;
- Approval by authorised individual(s) or system(s) for granting or modifying user accounts and access rights before data of the cloud customer or system components used to provision the cloud service can be accessed;
- Regular review of assigned user accounts and access rights;
- Blocking and removing access accounts in the event of inactivity;
- Time-based or event-driven removal or adjustment of access rights in the event of changes to job responsibility;
- Two-factor or multi-factor authentication for users with privileged access; and
- Requirements for the approval and documentation of the management of user accounts and access rights.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

System components in the sense of the basic criterion cf. definition in OPS-23. Automated authorisation processes in the sense of this basic criterion concern procedures for automated software provisioning (continuous delivery) as well as for automated provisioning and deprovisioning of user accounts and access rights based on approved requests.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: partially

A policy can change ad-hoc. However, the continuous audit of policies is only partially feasible as the only attributes that can be tested are the last change date and the status of review or approval, as far as this information is stored in a system. The content of a policy can hardly be tested automatically.

The aspects mentioned in the policy can be converted into individual criteria and embedded in a continuous audit. Individual aspects of the policy which can be examined on an ongoing basis:

- Unique user name;
- Segregation of duties;
- Rights profile management (approvals);
- Authorised bodies or individuals;
- Regular review;
- Deactivation due to inactivity; and
- Multi-factor authentication.

Approval and documentation Individual aspects of the policy which cannot be continuously examined in a practicable manner:

- Implementation of least-privilege/need-to-know principles; and
- Withdrawal or adjustment of access rights as the task area changes.

## IDM-02 Granting and change of user accounts and access rights

### Basic Criterion

Specified procedures for granting and modifying user accounts and access rights for internal and external employees of the Cloud Service Provider as well as for system components involved in automated authorisation processes of the Cloud Service Provider ensure compliance with the role and rights concept as well as the policy for managing user accounts and access rights.

### Additional Criterion

The Cloud Service Provider offers cloud customers a self-service with which they can independently assign and change user accounts and access rights.

### Supplementary Information

*About the Criterion*

–

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: no

A continuous audit of procedures is strongly dependent on the underlying systematics and automation of the Cloud Service Provider's procedures. This may vary in individual cases, but in general a continuous audit does not appear to be effective.

## IDM-03 Locking and withdrawal of user accounts in the event of inactivity or multiple failed logins

### Basic Criterion

User accounts of internal and external employees of the Cloud Service Provider as well as for system components involved in automated authorisation processes of the Cloud Service Provider are automatically locked if they have not been used for a period of two months. Approval from authorised personnel or system components are required to unlock these accounts.

Locked user accounts are automatically revoked after six months. After revocation, the procedure for granting user accounts and access rights (cf. IDM-02) must be repeated.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

Locking can result from a longer absence of the employee, for example, due to illness, parental leave, or sabbatical.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

Automated processes can easily be included in the continuous audit. Appropriate evaluation and reporting mechanisms must be used by the Cloud Service Provider. The auditor must use data analyses to detect deviations.

## IDM-04 Withdraw or adjust access rights as the task area changes

### Basic Criterion

Access rights are promptly revoked if the job responsibilities of the Cloud Service Provider's internal or external staff or the tasks of system components involved in the Cloud Service Provider's automated authorisation processes change. Privileged access rights are adjusted or revoked within 48 hours after the change taking effect. All other access rights are adjusted or revoked within 14 days. After revocation, the procedure for granting user accounts and access rights (cf. IDM-02) must be repeated.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

Changes in the task area of internal and external employees can be triggered by changes in the employment relationship (e.g. termination, transfer) or in contracts and agreements. For privileged access rights the definition in IDM-06 applies.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

It is necessary to record the changes to the task area in terms of content together with the date of entry into force in order to compare these with the adjustments made to the access rights. A continuous audit seems possible but requires a great deal of effort to implement.

## IDM-05 Regular review of access rights

### Basic Criterion

Access rights of internal and external employees of the Cloud Service Provider as well as of system components that play a role in automated authorisation processes of the Cloud Service Provider are reviewed at least once a year to ensure that they still correspond to the actual area of use. The review is carried out by authorised persons from the Cloud Service Provider's organisational units, who can assess the appropriateness of the assigned access rights based on their knowledge of the task areas of the employees or system components. Identified deviations will be dealt with promptly, but no later than 7 days after their detection, by appropriate modification or withdrawal of the access rights.

### Additional Criterion

Privileged access rights are reviewed at least every six months.

### Supplementary Information

*About the Criterion*

–

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

The review audit cannot be recorded automatically. A registration of documents used for documentary purposes could take place (e.g. confirmation that the assignment of the access rights has been reviewed). A continuous audit could indicate when this review was last carried out. The Cloud Service Provider must automate the review process (in particular the confirmation that the review has been performed) so that the auditor can audit the steps to be performed in case deviations are detected.

## IDM-06 Privileged access rights

### Basic Criterion

Privileged access rights for internal and external employees as well as technical users of the Cloud Service Provider are assigned and changed in accordance to the policy for managing user accounts and access rights (cf. IDM-01) or a separate specific policy.

Privileged access rights are personalised, limited in time according to a risk assessment and assigned as necessary for the execution of tasks ("need-to-know principle"). Technical users are assigned to internal or external employees of the Cloud Service Provider.

Activities of users with privileged access rights are logged in order to detect any misuse of privileged access in suspicious cases. The logged information is automatically monitored for defined events that may indicate misuse. When such an event is identified, the responsible personnel are automatically informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken in accordance with HR-04.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

Privileged access rights in the sense of the Basic Criterion are those that enable employees of the Cloud Service Provider to perform any of the following activities:

- Read or write access to the cloud customers' data processed, stored or transmitted in the cloud service, unless such data is encrypted or the encryption can be deactivated for access by the Cloud Service Provider; and

- Changes to the operational and/or security configuration of the system components in the production environment, in particular the starting, stopping, deleting or deactivating of system components, if this can affect the confidentiality, integrity or availability of the data of the cloud customers (also indirectly, e.g. by deactivating the logging and monitoring of security-relevant events).

Misused privileged access rights can be treated e.g. as a security incident, cf. SIM-01.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: partially

The assignment of audit authorisations must be audited manually. This includes the classification as privileged, personalisation, and evaluation of the need-to-know principle. The time limit could be read, but the implementation effort would be very high. A continuous audit does not appear to be sensible here. Only the system status could be audited continuously. The automatic triggering of a notification in suspicious cases could be compared with documented measures to handle these cases. However, this entire process must be digitised for this purpose, and the effort involved currently appears to be very high. However, a continuous audit could show the time of the last manual audit.

## IDM-07 Access to cloud customer data

### Basic Criterion

The cloud customer is informed by the Cloud Service Provider whenever internal or external employees of the Cloud Service Provider read or write to the cloud customer’s data processed, stored or transmitted in the cloud service or have accessed it without the prior consent of the cloud customer. The Information is provided whenever data of the cloud customer is/was not encrypted, the encryption is/was disabled for access or the contractual agreements do not explicitly exclude such information. The information contains the cause, time, duration, type and scope of the access. The information is sufficiently detailed to enable subject matter experts of the cloud customer to assess the risks of the access. The information is provided in accordance with the contractual agreements, or within 72 hours after the access.

### Additional Criterion

Access to the data processed, stored or transmitted in the cloud service by internal or external employees of the Cloud Service Provider requires the prior consent of an authorised department of the cloud customer, provided that the cloud customer’s data is not encrypted, encryption is disabled for access, or contractual agreements do not explicitly exclude such consent. For the consent, the cloud customer’s department is provided with meaningful information about the cause, time, duration, type and scope of the access supporting assessing the risks associated with the access.

### Supplementary Information

*About the Criterion*

Subject matter experts in the sense of this basic criterion is personnel from e.g. IT, Compliance or Internal Audit.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

A continuous audit of the notifications carried out only appears practical if the accesses mentioned are also logged and classified automatically. The content of the notifications can only be audited if the content is specified by the Cloud Service Provider according to a specific scheme. Then, a comparison and plausibility check can take place. A continuous audit would test all notifications after they have been received and thus check whether the process has been executed correctly in all cases.

## IDM-08 Confidentiality of authentication information

### Basic Criterion

The allocation of authentication information to access system components used to provide the cloud service to internal and external users of the cloud provider and system components that are involved in automated authorisation processes of the cloud provider is done in an orderly manner that ensures the confidentiality of the information. If passwords are used as authentication information, their confidentiality is ensured by the following procedures, as far as technically possible:

- Users can initially create the password themselves or must change an initial password when logging on to the system component for the first time. An initial password loses its validity after a maximum of 14 days.
- When creating passwords, compliance with the password specifications (cf. IDM-09) is enforced as far as technically possible.
- The user is informed about changing or resetting the password.
- The server-side storage takes place using cryptographically strong hash functions.

Deviations are evaluated by means of a risk analysis and mitigating measures derived from this are implemented.

### Additional Criterion

The users sign a declaration in which they assure that they treat personal (or shared) authentication information confidentially and keep it exclusively for themselves (within the members of the group).

### Supplementary Information

*About the Criterion*

Argon2i, for example, is suitable for using a password hash function.

Insofar as this is legally binding, declarations can be signed using an electronic signature.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

If the implementation is enforced by appropriate system configuration (automated control), the status or the last change of the configuration can be checked regularly.

## IDM-09 Authentication mechanisms

### Basic Criterion

System components in the Cloud Service Provider's area of responsibility that are used to provide the cloud service, authenticate users of the Cloud Service Provider's internal and external employees as well as system components that are involved in the Cloud Service Provider's automated authorisation processes. Access to the production environment requires two-factor or multi-factor authentication. Within the production environment, user authentication takes place through passwords, digitally signed certificates or procedures that achieve at least an equivalent level of security. If digitally signed certificates are used, administration is carried out in accordance with the Guideline for Key Management (cf. CRY-01). The password requirements are derived from a risk assessment and documented, communicated and provided in a password policy according to SP-01. Compliance with the requirements is enforced by the configuration of the system components, as far as technically possible.

### Additional Criterion

Access to the non-production environment requires two-factor or multi-factor authentication. Within the non-production environment, users are authenticated using passwords, digitally signed certificates, or procedures that provide at least an equivalent level of security.

### Supplementary Information

*About the Criterion*

–

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

If the implementation is enforced by appropriate system configuration (automated control), the status of the configuration or its last change can be checked regularly.

## 5.8 Cryptography and Key Management (CRY)

**Objective:** Ensure appropriate and effective use of cryptography to protect the confidentiality, authenticity or integrity of information.

### CRY-01 Policy for the use of encryption procedures and key management

#### Basic Criterion

Policies and instructions with technical and organisational safeguards for encryption procedures and key management are documented, communicated and provided according to SP-01, in which the following aspects are described:

- Usage of strong encryption procedures and secure network protocols that correspond to the state-of-the-art;
- Risk-based provisions for the use of encryption which are aligned with the information classification schemes (cf. AM-06) and consider the communication channel, type, strength and quality of the encryption;
- Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys; and
- Consideration of relevant legal and regulatory obligations and requirements.

#### Additional Criterion

–

#### Supplementary Information

*About the Criterion*

The state-of-the-art of strong encryption procedures and secure network protocols is specified in the following BSI Technical Guidelines valid at the given time:

- BSI TR-02102-1 Cryptographic Mechanisms: Recommendations and Key Lengths;
- BSI TR-02102-2 Cryptographic Mechanisms: Use of Transport Layer Security (TLS);
- BSI TR-02102-3 Cryptographic Mechanisms: Use of Internet Protocol Security (IPSec) and Internet Key Exchange (IKEv2); and
- BSI TR-02102-4 Cryptographic Mechanisms: Use of Secure Shell (SSH).

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: partially

A policy can change ad-hoc. However, the continuous audit of policies is only partially feasible as the only attributes that can be tested are the last change date and the status of review or approval, as far as this information is stored in a system. The content of a policy can hardly be tested automatically.

### CRY-02 Encryption of data for transmission (transport encryption)

#### Basic Criterion

The Cloud Service Provider has established procedures and technical measures for strong encryption and authentication for the transmission of data of cloud customers over public networks.

#### Additional Criterion

The Cloud Service Provider has established procedures and technical measures for strong encryption and authentication for the transmission of all data.

### Supplementary Information

*About the Criterion*

When transmitting data with normal protection requirements within the Cloud Service Provider's infrastructure, encryption is not mandatory provided that the data is not transmitted via public networks. In this case, the non-public environment of the Cloud Service Provider can generally be deemed trusted. The protocols TLS 1.2 and TLS 1.3 are currently regarded as strong, state-of-the-art transport encryptions, in each case in combination with Perfect Forward Secrecy. The specific configuration should comply with the recommendations of the (current) version of the BSI Technical Guideline TR-02102-2 "Cryptographic Procedures: Recommendations and key lengths. Part 2 – Use of Transport Layer Security (TLS)". Generally, the use of wildcard certificates is not considered a secure procedure.

The basic criterion for the transmission cloud customers' data, relates to e.g. the sending of electronic messages via public networks.

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls for those parts of the cloud service under their responsibility, that their data is transmitted over encrypted connections in accordance with the respective protection requirements.

*Notes on Continuous Auditing*

Feasibility: partially

The procedures and technical measures for encrypting data during transmission are configured centrally. This configuration rarely changes. Therefore, a continuous audit would not be sensible, as only changes to this configuration would have to be checked. However, the system status can be audited continuously. This also applies to the additional criterion.

## CRY-03 Encryption of sensitive data for storage

### Basic Criterion

The Cloud Service Provider has established procedures and technical safeguards to encrypt cloud customers' data during storage. The private keys used for encryption are known only to the cloud customer in accordance with applicable legal and regulatory obligations and requirements. Exceptions follow a specified procedure. The procedures for the use of private keys, including any exceptions, must be contractually agreed with the cloud customer.

### Additional Criterion

The private keys used for encryption are known to the customer exclusively and without exception in accordance with applicable legal and regulatory obligations and requirements.

### Supplementary Information

*About the Criterion*

An exception to the requirement that keys are known only to the cloud customers may be the use of a master key by the Cloud Service Provider. If the Cloud Service Provider established a procedure to use a master key, the Cloud Service Provider must perform sample-based checks regarding the suitability and effectiveness of the procedure, on a regular basis. This criterion does not apply to data that cannot be encrypted for the provision of the cloud service for functional reasons.

*Complementary Customer Criterion*

Through suitable controls, cloud customers ensure for parts of the cloud service under their responsibility (e. g. virtual machines within an IaaS solution), that their data is encrypted during storage in accordance with the respective protection requirements.

*Notes on Continuous Auditing*

Feasibility: partially

The encryption of data of cloud customers is configured centrally; therefore, it is only suitable for continuous auditing to a limited extent. Exceptions to the encryption of data according to a specified procedure and the coordination of this with cloud customers should be documented and approved. This, too, is only suitable to a limited extent for continuous auditing, as these exceptions are decided on a case-by-case basis and do not occur at a high enough frequency. In a continuous audit, the system status can be queried to determine whether the encryption is active and whether the approved exceptions are being adhered to.

## CRY-04 Secure key management

### Basic Criterion

Procedures and technical safeguards for secure key management in the area of responsibility of the Cloud Service Provider include at least the following aspects:

- Generation of keys for different cryptographic systems and applications;
- Issuing and obtaining public-key certificates;
- Provisioning and activation of the keys;
- Secure storage of keys (separation of key management system from application and middleware level) including description of how authorised users get access;
- Changing or updating cryptographic keys including policies defining under which conditions and in which manner the changes and/or updates are to be realised;
- Handling of compromised keys;
- Withdrawal and deletion of keys; and
- If pre-shared keys are used, the specific provisions relating to the safe use of this procedure are specified separately.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

Keys should be withdrawn or deleted e.g. in the event of compromise or employee changes. The Cloud Service Provider protects the keys which are created and inserted into the cloud service by the cloud customers according to the same criteria as the keys created by the Cloud Service Provider.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: partially

For procedures and technical measures for key management to take into account the required aspects, these aspects must be implemented in the corresponding configuration. These configurations are rarely changed and only these changes would have to be audited continuously. However, the system status could be reviewed and, in the event of irregularities, indicated and documented.

## 5.9 Communication Security (COS)

**Objective:** Ensure the protection of information in networks and the corresponding information processing systems

### COS-01 Technical safeguards

#### Basic Criterion

Based on the results of a risk analysis carried out according to OIS-06, the Cloud Service Provider has implemented technical safeguards which are suitable to promptly detect and respond to network-based attacks on the basis of irregular incoming or outgoing traffic patterns and/or Distributed Denial of Service (DDoS) attacks. Data from corresponding technical protection measures implemented is fed into a comprehensive SIEM (Security Information and Event Management) system, so that (counter) measures regarding correlating events can be initiated. The safeguards are documented, communicated and provided in accordance with SP-01.

#### Additional Criterion

Technical measures ensure that no unknown (physical or virtual) devices join the Cloud Service Provider's (physical or virtual) network (e.g. MACSec according to IEEE 802.1X:2010).

#### Supplementary Information

*About the Criterion*

Network-based attacks can be conducted e.g. with MAC spoofing and ARP poisoning attacks. Technical measures to prevent unknown physical or virtual devices from joining a physical or virtual network can be based on e.g. MACSec according to IEEE 802.1X:2010.

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls for parts of the cloud service under their responsibility (e.g. virtual machines within an IaaS solution), that they detect and respond to network-based attacks based on anomalous inbound and outbound traffic patterns (e.g. MAC spoofing and ARP poisoning attacks) and/or Distributed Denial of Service (DDoS), in a timely manner.

*Notes on Continuous Auditing*

Feasibility: yes

The technical protective measures are suitable for continuous auditing, but are rarely changed. However, the data fed into the overall SIEM system and the detection of correlating events are suitable for continuous auditing. This data can be evaluated automatically and continuously, as can the monitoring of correlating events.

### COS-02 Security requirements for connections in the Cloud Service Provider's network

#### Basic Criterion

Specific security requirements are designed, published and provided for establishing connections within the Cloud Service Provider's network. The security requirements define for the Cloud Service Provider's area of responsibility:

- in which cases the security zones are to be separated and in which cases cloud customers are to be logically or physically segregated;
- which communication relationships and which network and application protocols are permitted in each case;
- how the data traffic for administration and monitoring is segregated from each on network level;
- which internal, cross-location communication is permitted; and
- which cross-network communication is allowed.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

Cross-location communication can be realised for e.g. individual regions or data centres via e.g. WAN, LAN, VPN, RAS.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: no

The required security requirements are centrally documented and rarely changed. Continuous auditing is not practical.

## COS-03 Monitoring of connections in the Cloud Service Provider's network

### Basic Criterion

A distinction is made between trusted and untrusted networks. Based on a risk assessment, these are separated into different security zones for internal and external network areas (and DMZ, if applicable). Physical and virtualised network environments are designed and configured to restrict and monitor the established connection to trusted or untrusted networks according to the defined security requirements.

The entirety of the conception and configuration undertaken to monitor the connections mentioned is assessed in a risk-oriented manner, at least annually, with regard to the resulting security requirements.

Identified vulnerabilities and deviations are subject to risk assessment in accordance with the risk management procedure (cf. OIS-06) and follow-up measures are defined and tracked (cf. OPS-18).

At specified intervals, the business justification for using all services, protocols, and ports is reviewed. The review also includes the justifications for compensatory measures for the use of protocols that are considered insecure.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

The review of the security requirements depends on the measures implemented to design the networks. For example, monitoring and reviewing firewall rules or log files for abnormalities, as well as visual inspections of physical network components for changes.

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls that the virtual networks within the cloud service for which they are responsible are designed, configured and documented in accordance with their network security requirements (e.g. logical segmentation of the cloud customer's organisational units).

*Notes on Continuous Auditing*

Feasibility: yes

If the business justification and the regular review of the monitoring concept are documented in a standardised way, these processes can be evaluated automatically. Thus, a continuous audit can be conducted. The separation of the networks is suitable for continuous auditing as well, since the status of the separation can be continuously audited here.

## COS-04 Cross-network access

### Basic Criterion

Each network perimeter is controlled by security gateways. The system access authorisation for cross-network access is based on a security assessment based on the requirements of the cloud customers.

### Additional Criterion

Each network perimeter is controlled by redundant and highly-available security gateways.

### Supplementary Information

*About the Criterion*

Cross-network access is access from one network to another network via a defined network perimeter.

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls that access is controlled according to their protection needs by security gateways on the perimeters of the virtual networks within the cloud service for which they are responsible.

*Notes on Continuous Auditing*

Feasibility: yes

If the control of the network perimeters is documented (e.g. by logs), these logs can be evaluated automatically. This offers the possibility of a continuous audit for this part of the criterion. If the security evaluation for access authorisations is carried out in a standardised form at the Cloud Service Provider, this can also be evaluated automatically. In this case, a continuous audit for the second part of the criterion would also be possible.

## COS-05 Networks for administration

### Basic Criterion

There are separate networks for the administrative management of the infrastructure and for the operation of management consoles. These networks are logically or physically separated from the cloud customer's network and protected from unauthorised access by multi-factor authentication (cf. IDM-09). Networks used by the Cloud Service Provider to migrate or create virtual machines are also physically or logically separated from other networks.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

–

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: no

A continuous audit is not practical since infrastructure components and the logical and physical separation of the networks are implemented initially and a continuous audit of these components may require a system status, but it is difficult to test all aspects continuously.

## COS-06 Segregation of data traffic in jointly used network environments

### Basic Criterion

Data traffic of cloud customers in jointly used network environments is segregated on network level according to a documented concept to ensure the confidentiality and integrity of the data transmitted.

### Additional Criterion

In the case of IaaS/PaaS, the secure segregation is ensured by physically separated networks or by means of strongly encrypted VLANs. For the definition of strong encryption, the BSI Technical Guideline TR-02102 must be considered.

### Supplementary Information

*About the Criterion*

If the suitability and effectiveness of the logical segmentation cannot be assessed with sufficient certainty (e.g. due to a complex implementation), evidence can also be provided based on audit results of expert third parties (e.g. security audits to validate the concept). The segregation of stored and processed data is subject of the criterion OPS-24.

After successful authentication via an insecure communication channel (HTTP), a secure communication channel (HTTPS) is to be used.

With IaaS/PaaS, secure segregation is ensured by physically separated networks or strong encryption of the networks. For the definition of strong encryption, the BSI Technical Guideline TR-02102 must be considered (cf. CRY-01).

If the Cloud Service Provider does not use shared network environments for cloud customers and instead uses a physical segregation, the basic criterion is not applicable.

*Complementary Customer Criterion*

Through suitable controls, cloud customers ensure for parts of the cloud service under their responsibility that virtual networks are designed, configured and documented in accordance with their network security requirements (e.g. logical segmentation of organizational units).

*Notes on Continuous Auditing*

Feasibility: no

The logical segregation of cloud customer network traffic at the network level is centrally configured and rarely changed. Thus, a continuous audit is not beneficial, since no highly frequented automated query can be performed to support the continuous audit.

## COS-07 Documentation of the network topology

### Basic Criterion

The documentation of the logical structure of the network used to provision or operate the Cloud Service, is traceable and up-to-date, in order to avoid administrative errors during live operation and to ensure timely recovery in the event of malfunctions in accordance with contractual obligations. The documentation shows how the subnets are allocated and how the network is zoned and segmented. In addition, the geographical locations in which the cloud customers' data is stored are indicated.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

Zoning is a segmentation of the subnets with a firewall implemented at the network perimeters.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: no

The documentation of the logical structure of the network is rarely changed and is stored centrally. Therefore, a continuous audit is not effective. However, a continuous audit could return the date of the last change to the documentation.

### COS-08 Policies for data transmission

#### Basic Criterion

Policies and instructions with technical and organisational safeguards in order to protect the transmission of data against unauthorised interception, manipulation, copying, modification, redirection or destruction are documented, communicated and provided according to SP-01. The policies and instructions establish a reference to the classification of information (cf. AM-06).

#### Additional Criterion

–

#### Supplementary Information

*About the Criterion*

A safeguard against unauthorised interception, manipulation, copying, modification, redirection or destruction of data during transmission is e.g. the use of transport encryption according to CRY-02.

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls that the transmitted data transmitted to the cloud service is protected against tampering, copying, modifying, redirecting or deleting in accordance with their protection needs.

*Notes on Continuous Auditing*

Feasibility: no

A policy can change ad-hoc. However, the continuous audit of policies is only partially feasible as the only attributes that can be tested are the last change date and the status of review or approval, as far as this information is stored in a system. The content of a policy can hardly be tested automatically.

## 5.10 Portability and Interoperability (PI)

**Objective:** Enable the ability to access the cloud service via other cloud services or IT systems of the cloud customers, to obtain the stored data at the end of the contractual relationship and to securely delete it from the Cloud Service Provider.

### PI-01 Documentation and safety of input and output interfaces

#### Basic Criterion

The cloud service can be accessed by other cloud services or IT systems of cloud customers through documented inbound and outbound interfaces. Further, the interfaces are clearly documented for subject matter experts on how they can be used to retrieve the data.

Communication takes place through standardised communication protocols that ensure the confidentiality and integrity of the transmitted information according to its protection requirements. Communication over untrusted networks is encrypted according to CRY-02.

The type and scope of the documentation on the interfaces is geared to the needs of the cloud customers' subject matter experts in order to enable the use of these interfaces. The information is maintained in such a way that it is applicable for the cloud service's version which is intended for productive use.

#### Additional Criterion

–

#### Supplementary Information

*About the Criterion*

–

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls that the interfaces provided (and their security) are adequate for its protection requirements by means of appropriate checks before the start of use of the cloud service and each time the interfaces are changed.

*Notes on Continuous Auditing*

Feasibility: partially

The defined input and output interfaces of cloud services are rarely changed. Therefore, it is sufficient for the auditor to test these interfaces, the communication of potential changes, and the associated documentation as part of the recurring audit.

In a continuous audit, however, the system status of the interfaces could be queried and evaluated, continuously.

### PI-02 Contractual agreements for the provision of data

#### Basic Criterion

In contractual agreements, the following aspects are defined with regard to the termination of the contractual relationship, insofar as these are applicable to the cloud service:

- Type, scope and format of the data the Cloud Service Provider provides to the cloud customer;
- Definition of the timeframe, within which the Cloud Service Provider makes the data available to the cloud customer;
- Definition of the point in time as of which the Cloud Service Provider makes the data inaccessible to the cloud customer and deletes these; and
- The cloud customers' responsibilities and obligations to cooperate for the provision of the data.

The definitions are based on the needs of subject matter experts of potential customers who assess the suitability of the cloud service with regard to a dependency on the Cloud Service Provider as well as legal and regulatory requirements.

#### Additional Criterion

The design of the aspects is based on legal and regulatory requirements in the environment of the Cloud Service Provider. The Cloud Service Provider identifies the requirements regularly, at least once a year, and checks these for actuality and adjusts the contractual agreements accordingly.

#### Supplementary Information

*About the Criterion*

The type and scope of the data and the responsibilities for its provision depend on the service model of the cloud service or the services and functions provided:

In the case of IaaS and PaaS, the cloud customer is generally responsible for extracting and backing up the data which is stored in the cloud service before termination of the contractual relationship (cf. complementary requirement).

The Cloud Service Provider's responsibility is typically limited to the provision of data for the configuration of the infrastructure or platform that the cloud customer has set up within its environment (e.g. configuration of networks, images of virtual machines and containers).

With SaaS, the cloud customer typically relies on export functions provided by the Cloud Service

Provider. Data created by the cloud customer should be available in the same format as stored in the cloud service. Other data, including relevant log files and metadata, should be available in an applicable standard format, such as CSV, JSON or XML.

In Germany, legal requirements for retention can be found, for example, in the German Tax Code (§ 147 AO) and the German Commercial Code (§ 257 HGB). These provide for a retention obligation of six or ten years.

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls that the data to which they are contractually entitled is requested from the Cloud Service Provider at the end of the contract or accessed via defined interfaces (the type and scope of the data correspond to the contractual agreements that were concluded prior to the use of the cloud service) and that it is stored in accordance with the legal requirements applicable to this data.

*Notes on Continuous Auditing*

Feasibility: no

The Cloud Service Provider should have a standardised template for its contracts. Hence, all contracts are structured according to the same pattern.

This template is rarely changed. Therefore, a continuous audit is not practical. Therefore, it is sufficient to test the contracts and the associated template as part of the recurring audit.

## PI-03 Secure deletion of data

### Basic Criterion

The Cloud Service Provider's procedures for deleting the cloud customers' data upon termination of the contractual relationship ensure compliance with the contractual agreements (cf. PI-02).

The deletion includes data in the cloud customer's environment, metadata and data stored in the data backups.

The deletion procedures prevent recovery by forensic means.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

Suitable methods for data deletion are e.g. multiple overwriting or deletion of the encryption key.

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls that the legal and regulatory framework (e.g. legal requirements for storage and deletion) is identified and that the deletion of their data is initiated accordingly.

*Notes on Continuous Auditing*

Feasibility: yes

The complete deletion of the data is documented by the Cloud Service Provider using logs. The logs should include which data has been deleted so that it can be tracked whether data has been deleted in the cloud customer's environment, metadata and data in the backup.

The auditor can then perform an automated evaluation of these logs. The auditor can also check the system status of the procedure for deleting the data.

The fact that the deletion procedures prevent recovery by forensic means does not have to be audited continuously. The deletion procedures used can be tested as part of the recurring audit.

## 5.11 Procurement, Development and Modification of Information Systems (DEV)

**Objective:** Ensure information security in the development cycle of information systems.

### DEV-01 Policies for the development/ procurement of information systems

#### Basic Criterion

Policies and instructions with technical and organisational measures for the secure development of the cloud service are documented, communicated and provided in accordance with SP-01.

The policies and instructions contain guidelines for the entire life cycle of the cloud service and are based on recognised standards and methods with regard to the following aspects:

- Security in Software Development (Requirements, Design, Implementation, Testing and Verification);
- Security in software deployment (including continuous delivery); and
- Security in operation (reaction to identified faults and vulnerabilities).

#### Additional Criterion

In procurement, products are preferred which have been certified according to the “Common Criteria for Information Technology Security Evaluation” (short: Common Criteria – CC) according Evaluation Assurance Level EAL 4. If non-certified products are to be procured for available certified products, a risk assessment is carried out in accordance with OIS-07.

#### Supplementary Information

*About the Criterion*

The software provision can be carried out e.g. with Continuous Delivery methods.

Accepted standards and methods are, for example:

- ISO/IEC 27034; and
- OWASP Secure Software Development Lifecycle (S-SDLC).

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: no

The contents of the policies and instructions for the proper development or procurement of information systems do not change at a high frequency. A continuous audit of this documentation is not practical. Therefore, the integration of these tests into the recurring audit is sufficient.

### DEV-02 Outsourcing of the development

#### Basic Criterion

In the case of outsourced development of the cloud service (or individual system components), specifications regarding the following aspects are contractually agreed between the Cloud Service Provider and the outsourced development contractor:

- Security in software development (requirements, design, implementation, tests and verifications) in accordance with recognised standards and methods;
- Acceptance testing of the quality of the services provided in accordance with the agreed functional and non-functional requirements; and

- Providing evidence that sufficient verifications have been carried out to rule out the existence of known vulnerabilities.

#### Additional Criterion

–

#### Supplementary Information

*About the Criterion*

Outsourced development in the sense of the basic criterion refers to the development of system components used specifically for the cloud service by a contractor of the Cloud Service Provider. The development takes place according to the processes of the contractor.

The purchase of software available on the market as well as the integration of external employees into the processes of the Cloud Service Provider do not constitute outsourcing in the sense of this basic criterion.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: no

An outsourced development of a Cloud Service Provider's cloud services and the associated contract creation and signing will not be performed with high frequency. Changes in contract structures are also rare. Therefore, a continuous audit in these cases is not effective.

### DEV-03 Policies for changes to information systems

#### Basic Criterion

Policies and instructions with technical and organisational safeguards for change management of system components of the cloud service within the scope of software deployment are documented, communicated and provided according to SP-01 with regard to the following aspects:

- Criteria for risk assessment, categorisation and prioritisation of changes and related requirements for the type and scope of testing to be performed, and necessary approvals for the development/implementation of the change and releases for deployment in the production environment by authorised personnel or system components;
- Requirements for the performance and documentation of tests;
- Requirements for segregation of duties during development, testing and release of changes;
- Requirements for the proper information of cloud customers about the type and scope of the change as well as the resulting obligations to cooperate in accordance with the contractual agreements;
- Requirements for the documentation of changes in system, operational and user documentation; and
- Requirements for the implementation and documentation of emergency changes that must comply with the same level of security as normal changes.

#### Additional Criterion

–

#### Supplementary Information

*About the Criterion*

Changes in the sense of the basic criterion are those that can lead to changes in the configuration, functionality or security of system components of the cloud service in the production environment. This includes changes to the infrastructure as well as to the source code.

If individual changes are combined in a new release, update, patch or comparable software object for the purpose of software provisioning, this software object is deemed to be a change within the meaning of the basic criterion, but not the individual changes contained therein.

Changes to the existing network configuration must also undergo a specified procedure, as they are necessary for effective segregation of cloud customers.

Personnel and system components receive authorisation to approve changes in accordance with the requirements for access and access authorisations (cf. IDM-01) via a specified procedure (cf. IDM-02). Relevant information includes descriptions of e.g. new functions.

The cloud customer's obligations to cooperate can define that, e.g. the cloud customer must carry out certain tests.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: no

The contents of the policies and instructions for managing and modifying system components are not changed at a high frequency. A continuous audit of this documentation is therefore not effective. It is sufficient to integrate these tests into the recurring audit.

## DEV-04 Safety training and awareness programme regarding continuous software delivery and associated systems, components or tools.

### Basic Criterion

The Cloud Service Provider provides a training program for regular, target group-oriented security training and awareness for internal and external employees on standards and methods of secure software development and provision as well as on how to use the tools used for this purpose. The program is regularly reviewed and updated with regard to the applicable policies and instructions, the assigned roles and responsibilities and the tools used.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

–

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

The Cloud Service Provider can automatically check the valid policies and instructions, the assigned roles and responsibilities and the tools used and document the results in logs.

These logs can be automatically evaluated by the auditor and thus a continuous audit can be carried out.

## DEV-05 Risk assessment, categorisation and prioritisation of changes

### Basic Criterion

In accordance with the applicable policies (cf. DEV-03), changes are subjected to a risk assessment with regard to potential effects on the system components concerned and are categorised and prioritised accordingly.

### Additional Criterion

In accordance with the contractual agreements, meaningful information about the occasion, time, duration, type and scope of the change is submitted to authorised bodies of the cloud customer so that they can carry out their own risk assessment before the change is made available in the production environment. Regardless of the contractual agreements, this is done for changes that have the highest risk category based on their risk assessment.

### Supplementary Information

*About the Criterion*

–

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

The evaluation of changes in releases can be standardised and automated by the Cloud Service Provider. If this evaluation is carried out in standardised and digital form (tickets/logs), an automated evaluation can be carried out by the auditor.

## DEV-06 Testing changes

### Basic Criterion

Changes to the cloud service are subject to appropriate testing during software development and deployment.

The type and scope of the tests correspond to the risk assessment. The tests are carried out by appropriately qualified personnel of the Cloud Service Provider or by automated test procedures that comply with the state-of-the-art. Cloud customers are involved into the tests in accordance with the contractual requirements.

The severity of the errors and vulnerabilities identified in the tests, which are relevant for the deployment decision, is determined according to defined criteria and actions for timely remediation or mitigation are initiated.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

The errors and vulnerabilities identified in tests can be assessed, for example, according to the Common Vulnerability Scoring System (CVSS).

*Complementary Customer Criterion*

Where changes are to be tested by the cloud customers in accordance with the contractual agreements prior to deployment in the production environment, the cloud customers ensure through suitable controls that the tests are performed appropriately to identify errors. In particular, this includes timely execution of the tests by qualified personnel in accordance with the conditions specified by the Cloud Service Provider.

*Notes on Continuous Auditing*

Feasibility: yes

If the tests are carried out automatically, the execution and associated results can be documented in logs. These logs can then be read continuously by the auditor.

Measures for the elimination of identified vulnerabilities can also be documented and carried out in a standardised manner, so that continuous auditing is possible.

## DEV-07 Logging of changes

### Basic Criterion

System components and tools for source code management and software deployment that are used to make changes to system components of the cloud service in the production environment are subject to a role and rights concept according to IDM-01 and authorisation mechanisms. They must be configured in such a way that all changes are logged and can therefore be traced back to the individuals or system components executing them.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

–

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

The changes to the role and rights concept according to IDM-01 are documented in logs by the Cloud Service Provider. Thus, an automatic and continuous evaluation of these logs can be carried out. Irregularities are detected and logged.

The auditor can perform a continuous audit by automatically evaluating the logs and logged irregularities.

## DEV-08 Version Control

### Basic Criterion

Version control procedures are set up to track dependencies of individual changes and to restore affected system components back to their previous state as a result of errors or identified vulnerabilities.

### Additional Criterion

Version control procedures provide appropriate safeguards to ensure that the integrity and availability of cloud customer data is not compromised when system components are restored back to their previous state.

### Supplementary Information

*About the Criterion*

–

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

The procedures for version control of the Cloud Service Provider and, if necessary, resetting to previous states can be automated. This must be documented in logs. An automatic evaluation of these logs makes continuous auditing possible.

## DEV-09 Approvals for provision in the production environment

### Basic Criterion

Authorised personnel or system components of the Cloud Service Provider approve changes to the cloud service based on defined criteria (e.g. test results and required approvals) before these are made available to the cloud customers in the production environment.

Cloud customers are involved in the release according to contractual requirements.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

The definitions for criterion DEV-03 apply.

*Complementary Customer Criterion*

Where changes are to be approved by the cloud customers in accordance with the contractual agreements before they are made available in the production environment, the cloud customers ensure through suitable controls that authorised and qualified personnel receives the information made available, assesses the impact on the ISMS framework and decides on the approval in accordance with the conditions specified by the Cloud Service Provider.

*Notes on Continuous Auditing*

Feasibility: yes

Verification that all tests have been completed, successful and approved by an authorised body can be automated by the Cloud Service Provider and documented in logs.

These logs can then be evaluated automatically and continuously by the auditor.

## DEV-10 Separation of environments

### Basic Criterion

Production environments are physically or logically separated from test or development environments to prevent unauthorised access to cloud customer data, the spread of malware, or changes to system components. Data contained in the production environments is not used in test or development environments in order not to compromise their confidentiality.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

–

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

Since fundamental changes in test and development environments, which would affect the physical or logical separation, are rarely made, a continuous audit is not practical. The respective environments must be tested initially and then audited again if changes are made.

## 5.12 Control and Monitoring of Service Providers and Suppliers (SSO)

**Objective:** Ensure the protection of information that service providers or suppliers of the Cloud Service Provider (subcontractors) can access and monitor the agreed services and security requirements.

### SSO-01 Policies and instructions for controlling and monitoring third parties

#### Basic Criterion

Policies and instructions for controlling and monitoring third parties (e.g. service providers or suppliers) whose services contribute to the provision of the cloud service are documented, communicated and provided in accordance with SP-01 with respect to the following aspects:

- Requirements for the assessment of risks resulting from the procurement of third-party services;
- Requirements for the classification of third parties based on the risk assessment by the Cloud Service Provider and the determination of whether the third party is a subcontractor (cf. Supplementary Information);
- Information security requirements for the processing, storage or transmission of information by third parties based on recognised industry standards;
- Information security awareness and training requirements for staff;
- applicable legal and regulatory requirements;
- Requirements for dealing with vulnerabilities, security incidents and malfunctions;
- Specifications for the contractual agreement of these requirements;
- Specifications for the monitoring of these requirements; and
- Specifications for applying these requirements also to service providers used by the third parties, insofar as the services provided by these service providers also contribute to the provision of the cloud service.

#### Additional Criterion

Subservice organisations of the Cloud Service Provider are contractually obliged to provide regular reports by independent auditors on the suitability of the design and operating effectiveness of their service-related internal control system.

The reports include the complementary subservice organisations that are required, together with the controls of the Cloud Service Provider, to meet the applicable basic criteria of BSI C5 with reasonable assurance.

In case no reports can be provided, the Cloud Service Provider agrees appropriate information and audit rights to assess the suitability and effectiveness of the service-related internal control system, including the complementary controls, by qualified personnel.

#### Supplementary Information

*About the Criterion*

Reports by independent auditors on the suitability of the design and operating effectiveness of their service-related internal control system are, for example, attestation reports in accordance with ISAE 3402, IDW PS 951, SOC 2 or BSI C5.

Qualified personnel works, for example, in the Cloud Service Provider's internal audit department or is commissioned by the Cloud Service Provider in form of expert third parties, such as audit firms, and may hold relevant certifications such as "Certified Internal Auditor (CIA)".

The complementary controls at the sub-service provider are necessary in order to, together with the controls of the Cloud Service Provider, fulfil the applicable C5 criteria with reasonable assurance.

Applicable legal and regulatory requirements may exist, for example, in the areas of data protection, intellectual property rights or copyright.

If legal or regulatory requirements provide for a regulation deviating from these criteria for the control of subcontractors, these regulations remain unaffected by the C5 criteria.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: partially

Regarding the availability of the documentation, a continuous audit is not practical, since the associated processes and steps can be tested in a recurring audit.

A continuous audit of whether changes have been made to the policies is possible, provided that these changes are documented by the Cloud Service Provider and can be evaluated. However, an automated audit of the meaningfulness of the changes is difficult to implement.

Regarding the proof that a communication/provision has taken place, a continuous audit is considered possible.

For this, the Cloud Service Provider would have to realise the notification based on a system (e.g. based on tickets or notes in the respective service provider contract).

## SSO-02 Risk assessment of service providers and suppliers

### Basic Criterion

Service providers and suppliers of the Cloud Service Provider undergo a risk assessment in accordance with the policies and instructions for the control and monitoring of third parties prior to contributing to the delivery of the cloud service. The adequacy of the risk assessment is reviewed regularly, at least annually, by qualified personnel of the Cloud Service Provider during service usage.

The risk assessment includes the identification, analysis, evaluation, handling and documentation of risks with regard to the following aspects:

- Protection needs regarding the confidentiality, integrity, availability and authenticity of information processed, stored or transmitted by the third party;

- Impact of a protection breach on the provision of the cloud service;

- The Cloud Service Provider’s dependence on the service provider or supplier for the scope, complexity and uniqueness of the service purchased, including the consideration of possible alternatives.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

–

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: no

Continuous auditing of the risk assessment is not effective, as only its regular execution could be audited automatically, but not the content.

In addition, the specified frequency of at least one year is covered by the recurring audit. Risk assessments are rarely carried out dynamically and therefore do not often change during the year.

## SSO-03 Directory of service providers and suppliers

### Basic Criterion

The Cloud Service Provider maintains a directory for controlling and monitoring the service providers and suppliers who contribute services to the delivery of the cloud service. The following information is maintained in the directory:

- Company name;
- Address;
- Locations of data processing and storage;
- Responsible contact person at the service provider/supplier;
- Responsible contact person at the cloud service provider;
- Description of the service;
- Classification based on the risk assessment;
- Beginning of service usage; and
- Proof of compliance with contractually agreed requirements.

The information in the list is checked at least annually for completeness, accuracy and validity.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

It is not necessary to maintain a single central register in order to fulfil the basic criterion.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: no

An ad-hoc completeness checks on the specified criteria can safely take place automatically, as can a comparison of changed data with relevant company databases. This can be set up by the Cloud Service Provider.

The auditor can then examine deviations as part of the recurring audit.

However, due to the frequency and the completeness analysis, a continuous audit is not efficient due to the large effort required.

## SSO-04 Monitoring of compliance with requirements

### Basic Criterion

The Cloud Service Provider monitors compliance with information security requirements and applicable legal and regulatory requirements in accordance with policies and instructions concerning controlling and monitoring of third-parties.

Monitoring includes a regular review of the following evidence to the extent that such evidence is to be provided by third parties in accordance with the contractual agreements:

- reports on the quality of the service provided;
- certificates of the management systems' compliance with international standards;
- independent third-party reports on the suitability and operating effectiveness of their service-related internal control systems; and
- Records of the third parties on the handling of vulnerabilities, security incidents and malfunctions.

The frequency of the monitoring corresponds to the classification of the third party based on the risk assessment conducted by the Cloud Service Provider (cf. SSO-02). The results of the monitoring are included in the review of the third party's risk assessment.

Identified violations and deviations are subjected to analysis, evaluation and treatment in accordance with the risk management procedure (cf. OIS-07).

### Additional Criterion

The procedures for monitoring compliance with the requirements are supplemented by automatic procedures relating to the following aspects:

- Configuration of system components;
- Performance and availability of system components;
- Response time to malfunctions and security incidents; and
- Recovery time (time until completion of error handling).

Identified violations and discrepancies are automatically reported to the responsible personnel or system components of the Cloud Service Provider for prompt assessment and action.

### Supplementary Information

*About the Criterion*

Evidence for the review of the suitability and operating effectiveness of the service-related internal control system include reports in accordance with ISAE 3402, IDW PS 951, SOC 2 or BSI C5.

In the evidence provided by the third parties, the Cloud Service Provider reviews, for example, the following aspects and, if necessary, incorporates the findings into the risk assessment in order to derive and initiate mitigating actions:

- The scope and the validity respectively the period covered by the evidence;
- For attestation reports: Qualifications of the opinion, included deviations/other observations including management's response and corresponding controls to be implemented and executed by the Cloud Service Provider;
- Disclosed subcontractors incl. any changes among those (e.g. additional subcontractor); and
- Stated security incidents.

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls that they stay informed about subservice organisations of their Cloud Service Provider (e.g. on the basis of the information in the C5 attestation report) and decide on the basis of their need for protection of their data processed and stored in the cloud service whether further action should be taken to monitor and check these subservice organisations.

*Notes on Continuous Auditing*

Feasibility: partially

A continuous audit of some of the required evidence, such as the reviews conducted and their results, can be performed once the Cloud Service Provider documents the associated steps using a tool.

However, a review on content-level, such as reviewing the response to risk assessments and violations of service provider requirements, is difficult as it requires a semantic understanding. As a result, at least parts of the criterion are suitable for continuous audit.

## SSO-05 Exit strategy for the receipt of benefits

### Basic Criterion

The Cloud Service Provider has defined and documented exit strategies for the purchase of services where the risk assessment of the service providers and suppliers regarding the scope, complexity and uniqueness of the purchased service resulted in a very high dependency (cf. Supplementary Information).

Exit strategies are aligned with operational continuity plans and include the following aspects:

- Analysis of the potential costs, impacts, resources and timing of the transition of a purchased service to an alternative service provider or supplier;
- Definition and allocation of roles, responsibilities and sufficient resources to perform the activities for a transition;
- Definition of success criteria for the transition; and
- Definition of indicators for monitoring the performance of services, which should initiate the withdrawal from the service if the results are unacceptable.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

A very high dependency can be assumed in the following situations in particular:

- The purchased service is absolutely required for the provision of the cloud service – this situation is given when the Cloud Service Provider:
  - provides the cloud service from data centres operated by third parties; and
  - provides a SaaS service and uses the IaaS or PaaS of another Cloud Service Provider.
- The service cannot be obtained within one month from an alternative service provider or supplier, as:
  - It is unique on the market and no other supplier can deliver it;
  - It is strongly individualised by the service provider or supplier and/or the Cloud Service Provider;
  - It cannot be supplied by any other provider in the required quality of service; and
  - It requires specific knowledge that is only/mainly available to the current service provider or supplier and not to the Cloud Service Provider.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: no

The existence of individual exit strategies is not a practical test item for continuous audit.

## 5.13 Security Incident Management (SIM)

**Objective:** Ensure a consistent and comprehensive approach to the capture, assessment, communication and escalation of security incidents.

### SIM-01 Policy for security incident management

#### Basic Criterion

Policies and instructions with technical and organisational safeguards are documented, communicated and provided in accordance with SP-01 to ensure a fast, effective and proper response to all known security incidents.

The Cloud Service Provider defines guidelines for the classification, prioritisation and escalation of security incidents and creates interfaces to the incident management and business continuity management.

In addition, the Cloud Service Provider has set up a “Computer Emergency Response Team” (CERT), which contributes to the coordinated resolution of occurring security incidents.

Customers affected by security incidents are informed in a timely and appropriate manner.

#### Additional Criterion

There are instructions as to how the data of a suspicious system can be collected in a conclusive manner in the event of a security incident. In addition, there are analysis plans for typical security incidents and an evaluation methodology so that the collected information does not lose its evidential value in any subsequent legal assessment.

#### Supplementary Information

*About the Criterion*

–

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls that they receive notifications from the Cloud Service Provider about security incidents that affect them and that these notifications are forwarded in a timely manner to the responsible departments for handling so that an appropriate response can be triggered.

*Notes on Continuous Auditing*

Feasibility: partially

A continuous audit of the documented policies and instructions is not effective because they are not subject to high frequency changes. Thus, the audit of the policies and instructions can be performed in the recurring audit.

Similarly, setting up a CERT is not suitable for continuous auditing as it is an organisational body and does not require continuous monitoring.

The timely communication of security incidents to affected customers can be covered by a continuous audit approach. In addition, the Cloud Service Provider can document not only the security incidents by means of logs, but also that they have been communicated to the customer via e-mail, for example. The fact that there was communication to affected customers for every security incident can thus be evaluated automatically and continuously by the auditor.

However, this procedure can be combined with the audit approach of further requirements of Security Incident Management.

## SIM-02 Processing of security incidents

### Basic Criterion

Subject matter experts of the Cloud Service Provider, together with external security providers where appropriate, classify, prioritise and perform root-cause analyses for events that could constitute a security incident.

### Additional Criterion

The Cloud Service Provider simulates the identification, analysis and defence of security incidents and attacks at least once a year through appropriate tests and exercises (e.g. Red Team training).

### Supplementary Information

*About the Criterion*

–

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

The Cloud Service Provider documents all security incidents in digital form, which contains information about the classification, prioritisation and root cause analysis of the incidents. The root cause analysis should be standardised to facilitate continuous auditing.

An automatic and continuous evaluation of these security incidents can then be carried out by the auditor by excluding the logs or tickets produced and testing whether the security incident has been classified and prioritised and whether these steps have been carried out based on a standardised root cause analysis. The continuous audit thus provides a constant statement as to whether security incidents have been correctly recorded, classified and subjected to a root cause analysis.

## SIM-03 Documentation and reporting of security incidents

### Basic Criterion

After a security incident has been processed, the solution is documented in accordance with the contractual agreements and the report is sent to the affected customers for final acknowledgement or, if applicable, as confirmation.

### Additional Criterion

The customer can either actively approve solutions or the solution is automatically approved after a certain period.

Information on security incidents or confirmed security breaches is made available to all affected customers.

The contract between the Cloud Service Provider and the cloud customer regulates which data is made available to the cloud customer for his own analysis in the event of security incidents.

### Supplementary Information

*About the Criterion*

–

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls that they receive notifications from the Cloud Service Provider about security incident that affect them and their resolution and that these notifications are forwarded promptly to the entity responsible for handling them so that an appropriate response can be made.

*Notes on Continuous Auditing*

Feasibility: yes

In the logs or tickets that document the security incidents (cf. SIM-03), the Cloud Service Provider also describes the solution pursued to eliminate the incident. In addition, the Cloud Service Provider also documents the confirmation to the customer.

The auditor can then automatically and continuously read out whether the documented security incidents have been resolved and whether a solution has been documented. The same applies to the communication of the resolution of the incidents to affected customers. If this is not the case, the unresolved security incident can be documented as the output value of the continuous audit.

## SIM-04 Duty of the users to report security incidents to a central body

### Basic Criterion

The Cloud Service Provider informs employees and external business partners of their obligations. If necessary, they agree to or are contractually obliged to report all security events that become known to them and are directly related to the cloud service provided by the Cloud Service Provider to a previously designated central office of the Cloud Service Provider promptly.

In addition, the Cloud Service Provider communicates that "false reports" of events that do not subsequently turn out to be incidents do not have any negative consequences.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

–

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls that identified security events, which the Cloud Service Provider is required to process, are communicated promptly to previously designated, responsible personnel.

The identification of such security events is supported by suitable controls (cf. complementary criterion for OPS-10).

*Notes on Continuous Auditing*

Feasibility: partially

The Cloud Service Provider should inform its employees and external business partners about their obligations in a standardised and digital format. This obligation usually occurs when the employee joins the company or the business relationship.

This enables the auditor to automatically and continuously audit whether all employees and external business partners are notified of their obligations by automatically testing whether the clause, if any, is included in the contract when the contract is signed.

## SIM-05 Evaluation and learning process

### Basic Criterion

Mechanisms are in place to measure and monitor the type and scope of security incidents and to report them to support agencies. The information obtained from the evaluation is used to identify recurrent or significant incidents and to identify the need for further protection.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

Supporting bodies may be external service providers or government agencies such as the BSI.

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls that they include into their ISMS the findings and measures related to previous security incidents reported by the Cloud Service Provider. The cloud customers evaluate whether and which supporting measures they might take on their side.

*Notes on Continuous Auditing*

Feasibility: no

The existing mechanisms for measuring the type and scope of security incidents are rarely changed. As a result, continuous auditing is not effective. In addition, in some cases it can be a manual task carried out by employees to identify recurring incidents or incidents with significant consequences and to develop associated protective measures.

## 5.14 Business Continuity Management (BCM)

**Objective:** Plan, implement, maintain and test procedures and measures for business continuity and emergency management.

### BCM-01 Top management responsibility

**Basic Criterion**

The top management (or a member of the top management) of the Cloud Service Provider is named as the process owner of business continuity and emergency management and is responsible for establishing the process within the company as well as ensuring compliance with the guidelines. They must ensure that sufficient resources are made available for an effective process.

People in management and other relevant leadership positions demonstrate leadership and commitment to this issue by encouraging employees to actively contribute to the effectiveness of continuity and emergency management.

**Additional Criterion**

–

**Supplementary Information**

*About the Criterion*

–

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: no

The responsibilities for continuity and emergency management processes are initially named and rarely changed afterwards. Therefore, a continuous audit is not effective.

A continuous audit can, however, return the date of the last revision of the guidelines for continuity and emergency management.

### BCM-02 Business impact analysis policies and instructions

**Basic Criterion**

Policies and instructions to determine the impact of any malfunction to the cloud service or enterprise are documented, communicated and made available in accordance with SP-01. The following aspects are considered as minimum:

- Possible scenarios based on a risk analysis;
- Identification of critical products and services;
- Identify dependencies, including processes (including resources required), applications, business partners and third parties;
- Capture threats to critical products and services;

- Identification of effects resulting from planned and unplanned malfunctions and changes over time;
- Determination of the maximum acceptable duration of malfunctions;
- Identification of restoration priorities;
- Determination of time targets for the resumption of critical products and services within the maximum acceptable time period (RTO);
- Determination of time targets for the maximum reasonable period during which data can be lost and not recovered (RPO); and
- Estimation of the resources needed for resumption.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

Scenarios to be considered according to the basic criterion are, for example, the loss of personnel, buildings, infrastructure and service providers.

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls that the scenarios for a failure of the cloud service or the Cloud Service Provider are sufficiently considered in the context of their business impact analysis.

*Notes on Continuous Auditing*

Feasibility: partially

A policy can change ad-hoc. However, the continuous audit of policies is only partially feasible as the only attributes that can be tested are the last change date and the status of review or approval, as far as this information is stored in a system. The content of a policy can hardly be tested automatically.

## BCM-03 Planning business continuity

### Basic Criterion

Based on the business impact analysis, a single framework for operational continuity and business plan planning will be implemented, documented and enforced to ensure that all plans are consistent. Planning is based on established standards, which are documented in a “Statement of Applicability”.

Business continuity plans and contingency plans take the following aspects into account:

- Defined purpose and scope with consideration of the relevant dependencies;
- Accessibility and comprehensibility of the plans for persons who are to act accordingly;
- Ownership by at least one designated person responsible for review, updating and approval;
- Defined communication channels, roles and responsibilities including notification of the customer;
- Recovery procedures, manual interim solutions and reference information (taking into account prioritisation in the recovery of cloud infrastructure components and services and alignment with customers);
- Methods for putting the plans into effect;
- Continuous process improvement; and
- Interfaces to Security Incident Management.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

The consistency of plans according to the basic criterion must also be maintained when different locations are used.

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls that the results of the Business Impact Analysis are sufficiently considered when planning the operational continuity and the business plan in order to provide for the effects of a failure of the cloud service or Cloud Service Provider.

Cloud customers ensure through suitable controls that the availability of the cloud service, its recovery time according to the BCM plan and the data loss of the cloud service are consistent with their own availability requirements and tolerable data loss.

*Notes on Continuous Auditing*

Feasibility: no

The introduction of the framework and the business plan based on a business impact analysis is a manual process of the Cloud Service Provider.

A continuous audit is not practical. The plans can be tested as part of the recurring audit.

## BCM-04 Verification, updating and testing of the business continuity

### Basic Criterion

The business impact analysis, business continuity plans and contingency plans are reviewed, updated and tested on a regular basis (at least annually) or after significant organisational or environmental changes. Tests involve affected customers (tenants) and relevant third parties. The tests are documented and results are taken into account for future operational continuity measures.

### Additional Criterion

In addition to the tests, exercises are also carried out which, among other things, have resulted in scenarios from security incidents that have already occurred in the past.

### Supplementary Information

*About the Criterion*

Tests are primarily conducted at the operational level and are aimed at operational target groups. Tests include e.g.:

- Test of technical precautionary measures;
- Functional tests; and
- Plan review.

Exercises also take place on a tactical and strategic level. These include e.g.:

- Plan meeting;
- Staff exercise;
- Command post exercise;
- Communication and alerting exercise;
- Simulation of scenarios; and
- Emergency or full exercise.

After a completed exercise:

- Review and possible adaptation of the existing alarm plan.

Relevant third parties are in particular service providers and suppliers of the Cloud Service Provider who contribute to the provision of the cloud service (cf. basic criteria SSO-02 and SSO-05).

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls that measures to prevent the impact of a cloud service or Cloud Service Provider outage are regularly reviewed, updated, tested and exercised. The Cloud Service Provider is involved in the tests and exercises in accordance with the contractual agreements.

Cloud customers ensure through suitable controls that the results of the Cloud Service Provider's BCM tests and exercises are incorporated into their own BCM and that they are fully appreciated with regard to ensuring the customer's operational continuity.

In tests and exercises that involve the customer and therefore require own measures on the customer side, cloud customers ensure that the appropriate measures for coping with the scenario are practiced and tested by means of suitable BCM controls.

*Notes on Continuous Auditing*

Feasibility: partially

Implementing the tests of the operational continuity plans in an annual cycle does not make a continuous audit of the entire criterion effective. The effort for both Cloud Service Providers and auditors to automate and continuously test this process would be higher than the results.

However, it is possible to continuously audit whether a test was carried out within the required time span. To do this, the Cloud Service Provider must document in a standardised manner that and when a test was carried out.

## 5.15 Compliance (COM)

**Objective:** Avoid non-compliance with legal, regulatory, self-imposed or contractual information security and compliance requirements.

### COM-01 Identification of applicable legal, regulatory, self-imposed or contractual requirements

#### Basic Criterion

The legal, regulatory, self-imposed and contractual requirements relevant to the information security of the cloud service as well as the Cloud Service Provider's procedures for complying with these requirements are explicitly defined and documented.

#### Additional Criterion

–

#### Supplementary Information

*About the Criterion*

The Cloud Service Provider's documentation may refer to the following requirements, among others:

- Requirements for the protection of personal data (e.g. EU General Data Protection Regulation);
- Compliance requirements based on contractual obligations with cloud customers (e.g. ISO/IEC 27001, SOC 2, PCI-DSS);
- generally accepted accounting principles (e.g. in accordance with HGB or IFRS);

- Requirements regarding access to data and auditability of digital documents (e.g. according to GDPdU); and
- Other laws (e.g. according to BSIG or AktG).

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: no

A continuous audit of contract specifications, regulations and their documentation does not seem to be effective. In this case, the test within the recurring audit is sufficient.

A continuous audit could assist in giving the date of the last audit of the criteria.

### COM-02 Policy for planning and conducting audits

#### Basic Criterion

Policies and instructions for planning and conducting audits are documented, communicated and made available in accordance with SP-01 and address the following aspects:

- Restriction to read-only access to system components in accordance with the agreed audit plan and as necessary to perform the activities;
- Activities that may result in malfunctions to the cloud service or breaches of contractual requirements are performed during scheduled maintenance windows or outside peak periods; and
- Logging and monitoring of activities.

#### Additional Criterion

The Cloud Service Provider grants its cloud customers contractually guaranteed information and audit rights.

#### Supplementary Information

*About the Criterion*

–

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls that appropriate responses are made to malfunctions to the cloud service through such audits.

To the extent that contractually guaranteed information and audit rights exist, the cloud customers ensure through suitable controls that these rights are designed and executed in accordance with their own requirements.

*Notes on Continuous Auditing*

Feasibility: partially

A policy can change ad-hoc. However, the continuous audit of policies is only partially feasible as the only attributes that can be tested are the last change date and the status of review or approval, as far as this information is stored in a system. The content of a policy can hardly be tested automatically.

### COM-03 Internal audits of the information security management system

#### Basic Criterion

Subject matter experts check the compliance of the information security management system at regular intervals, at least annually, with the relevant and applicable legal, regulatory, self-imposed or contractual requirements (cf. COM-01) as well as compliance with the policies and instructions (cf. SP-01) within their scope of responsibility (cf. OIS-01) through internal audits.

Identified vulnerabilities and deviations are subject to risk assessment in accordance with the risk management procedure (cf. OIS-06) and follow-up measures are defined and tracked (cf. OPS-18).

### Additional Criterion

Internal audits are supplemented by procedures to automatically monitor applicable requirements of policies and instructions with regard to the following aspects:

- Configuration of system components to provide the cloud service within the Cloud Service Provider's area of responsibility;
- Performance and availability of these system components;
- Response time to malfunctions and security incidents;
- Recovery time (time to completion of error handling);

Identified vulnerabilities and deviations are automatically reported to the appropriate Cloud Service Provider's subject matter experts for immediate assessment and action.

Cloud customers can view compliance with selected contractual requirements in real time.

### Supplementary Information

*About the Criterion*

Subject matter experts operate, e.g., in the Cloud Service Provider's internal revision department or expert third parties commissioned by the Cloud Service Provider, such as auditing companies, and may hold relevant certifications such as "Certified Internal Auditor (CIA)".

With regard to ISMS compliance, see Section 9.2 of ISO/IEC 27001.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

The regular performance of an internal audit of the ISMS can be set up as part of compliance monitoring. For this purpose, the results of the internal audit must be digitally documented, as well as the individual audit steps.

A continuous audit of this internal audit is not effective but can only be considered after compliance monitoring has been set up.

The continuous audit can then supply the date of the last audit as the output value.

## COM-04 Information on information security performance and management assessment of the ISMS

### Basic Criterion

The top management of the Cloud Service Provider is regularly informed about the information security performance within the scope of the ISMS in order to ensure its continued suitability, adequacy and effectiveness. The information is included in the management review of the ISMS at is performed at least once a year.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

The top management is a natural person or group of people who make final decisions for the institution and are responsible for these.

The aspects to be dealt with in the management review of the ISMS are listed in Section 9.3 of ISO/ IEC 27001.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: partially

The actual transmission of information to the Cloud Service Provider's management can be logged and automated. However, the testing of the contents of the communication and the that these have also been included in the management assessment must still be carried out within the regular audit.

## 5.16 Dealing with investigation requests from government agencies (INQ)

**Objective:** Ensure appropriate handling of government investigation requests for legal review, information to cloud customers, and limitation of access to or disclosure of data.

### INQ-01 Legal Assessment of Investigative Inquiries

Basic Criterion

Investigation requests from government agencies are subjected to a legal assessment by subject matter experts of the Cloud Service Provider. The assessment determines whether the government agency has an applicable and legally valid legal basis and what further steps need to be taken.

Additional Criterion

–

Supplementary Information

*About the Criterion*

–

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls that the type and scope of government investigation requests and the associated disclosure of their own data has been dealt with in their own risk management and that the use of the cloud service only takes place when this risk has been deemed acceptable.

*Notes on Continuous Auditing*

Feasibility: no

Although a continuous audit of the performance of the assessment and its documentation is conceivable, a continuous audit is not practical. Rather the criterion aims at the qualification of the auditing personnel as well as the process behind it, which is both subject to manual audit.

### INQ-02 Informing Cloud Customers about Investigation Requests

Basic Criterion

The Cloud Service Provider informs the affected Cloud Customer(s) without undue delay, unless the applicable legal basis on which the government agency is based prohibits this or there are clear indications of illegal actions in connection with the use of the Cloud Service.

Additional Criterion

–

### Supplementary Information

*About the Criterion*

This does not affect other legal or regulatory requirements that requires earlier information for cloud customers.

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls that such notifications are received and legally checked according to their own specifications and possibilities.

*Notes on Continuous Auditing*

Feasibility: partially

For internal process monitoring at the Cloud Service Provider and facilitation of the audit, a continuous audit of the period between receipt of the request and information of the customers is conceivable.

However, as this depends on local legal basis, the effort to establish this in the respective regions will be quite high.

If a transaction processing system is implemented at the Cloud Service Provider, at least the process in this system can be continuously audited.

## ■ INQ-03 Conditions for Access to or Disclosure of Data in Investigation Requests

### Basic Criterion

Access to or disclosure of cloud customer data in connection with government investigation requests is subject to the proviso that the Cloud Service Provider's legal assessment has shown that an applicable and valid legal basis exists and that the investigation request must be granted on that basis.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

–

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

To the extent that a separate role is assigned to the investigator in order to gain access to the data, the prerequisites specified in the request can be entered and checked by the system and linked to the assignment of the investigator role.

A continuous query can then be made to ensure that the role was only granted if the prerequisites defined by the system were fulfilled. Deviations can be audited manually.

## ■ INQ-04 Limiting Access to or Disclosure of Data in Investigation Requests

### Basic Criterion

The Cloud Service Provider's procedures establishing access to or disclosing data of cloud customers in the context of investigation requests from governmental agencies ensure that the agencies only gain access to or insight into the data that is the subject of the investigation request.

If no clear limitation of the data is possible, the Cloud Service Provider anonymises or pseudonymises the data so that government agencies can only assign it to those cloud customers who are subject of the investigation request.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

–

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: partially

A separate role for the investigator is to be provided (cf. also INQ-03). It is conceivable that certain data types for this role may not be visible, pseudonymised or anonymised, or that data of customers that are not part of the investigation may be excluded.

However, this requires a manual effort in the configuration and assignment of the investigator role.

Under these conditions, however, a continuous audit of whether and to what extent the investigator had access to data is conceivable.

## 5.17 Product Safety and Security (PSS)

**Objective:** Provides up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers, appropriate mechanisms for troubleshooting and logging, as well as authentication and authorisation of users of cloud customers.

### PSS-01 Guidelines and Recommendations for Cloud Customers

### Basic Criterion

The Cloud Service Provider provides cloud customers with guidelines and recommendations for the secure use of the cloud service provided. The information contained therein is intended to assist the cloud customer in the secure configuration, installation and use of the cloud service, to the extent applicable to the cloud service and the responsibility of the cloud user.

The type and scope of the information provided will be based on the needs of subject matter experts of the cloud customers who set information security requirements, implement them or verify the implementation (e.g. IT, Compliance, Internal Audit). The information in the guidelines and recommendations for the secure use of the cloud service address the following aspects, where applicable to the cloud service:

- Instructions for secure configuration;
- Information sources on known vulnerabilities and update mechanisms;
- Error handling and logging mechanisms;
- Authentication mechanisms;
- Roles and rights concept including combinations that result in an elevated risk; and
- Services and functions for administration of the cloud service by privileged users.

The information is maintained so that it is applicable to the cloud service provided in the version intended for productive use.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

–

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls that the Cloud Service Provider's information is used to derive policies, concepts and measures for the secure configuration and use (according to their own risk assessment) of the cloud service. Compliance with these policies, concepts and measures is checked. Changes to the information are promptly assessed for their impact on these documents and any necessary changes are implemented.

*Notes on Continuous Auditing*

Feasibility: partially

The provision of information from the Cloud Service Provider to cloud customers can only be audited continuously to a limited extent. For example, the Cloud Service Provider can make the guidelines and recommendations available via its internal customer portal, which makes a continuous audit only partially effective.

Here, only an audit for completeness and the last modification date is conceivable, although a discussion of the content of the changes is not effective. For this, a semantic evaluation would be necessary.

## PSS-02 Identification of Vulnerabilities of the Cloud Service

### Basic Criterion

The Cloud Service Provider applies appropriate measures to check the cloud service for vulnerabilities which might have been integrated into the cloud service during the software development process.

The procedures for identifying such vulnerabilities are part of the software development process and, depending on a risk assessment, include the following activities:

- Static Application Security Testing;
- Dynamic Application Security Testing;
- Code reviews by the Cloud Service Provider's subject matter experts; and
- Obtaining information about confirmed vulnerabilities in software libraries provided by third parties and used in their own cloud service.

The severity of identified vulnerabilities is assessed according to defined criteria and measures are taken to immediately eliminate or mitigate them.

### Additional Criterion

The procedures for identifying such vulnerabilities also include annual code reviews or security penetration tests by qualified external third parties.

### Supplementary Information

*About the Criterion*

Known vulnerabilities in externally related system components (e.g. operating systems) used for the development and provision of the cloud service but not going through the Cloud Service Provider's software development process are the subject of criteria OPS-23 (Management of vulnerabilities, malfunctions and errors – open vulnerability assessment).

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

The Cloud Service Provider automatically checks its cloud services for vulnerabilities. This check is documented in a standardised digital form.

By auditing this documentation, the auditor verifies, whether the Cloud Service Provider has performed a vulnerability scan. In addition, the severity of the identified vulnerabilities can be integrated into this continuous audit if the defined criteria and their application are standardised and machine-readable.

The information on identified and/or repaired vulnerabilities can also be transferred directly to the affected customer and thus increased transparency can be achieved.

## PSS-03 Online Register of Known Vulnerabilities

### Basic Criterion

The Cloud Service Provider operates or refers to a daily updated online register of known vulnerabilities that affect the Cloud Service Provider and assets provided by the Cloud Service Provider that the cloud customers have to install, provide or operate themselves under the customers responsibility.

The presentation of the vulnerabilities follows the Common Vulnerability Scoring System (CVSS).

The online register is easily accessible to any cloud customer. The information contained therein forms a suitable basis for risk assessment and possible follow-up measures on the part of cloud users.

For each vulnerability, it is indicated whether software updates (e.g. patch, update) are available, when they will be rolled out and whether they will be deployed by the Cloud Service Provider, the cloud customer or both of them together.

### Additional Criterion

Assets provided by the Cloud Service Provider, which must be installed, provided or operated by cloud users within their area of responsibility, are equipped with automatic update mechanisms. After approval by the respective cloud user, software updates can be rolled out in such a way that they can be distributed to all affected users without human interaction.

### Supplementary Information

*About the Criterion*

Assets provided by the Cloud Service Provider that cloud customers have to install, deploy or operate themselves in their area of responsibility are for example local software clients and apps as well as tools for integrating the cloud service.

If the cloud service relies on other cloud services, this registry has to incorporate or refer to the vulnerabilities of those other cloud services in order for this criterion to be met.

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls that the information in this register is incorporated sufficiently quickly into their own risk management, evaluated and, if necessary, taken into account in their own area of responsibility.

*Notes on Continuous Auditing*

Feasibility: yes

A continuous audit includes, above all, whether the information is updated daily. The distribution of software updates must be documented by the Cloud Service Provider (logs). This documentation can then be automatically and continuously evaluated by the auditor to ensure that the software used on assets in the cloud users' area of responsibility is up-to-date.

## PSS-04 Error handling and Logging Mechanisms

### Basic Criterion

The cloud service provided is equipped with error handling and logging mechanisms. These enable cloud users to obtain security-related information about the security status of the cloud service as well as the data, services or functions it provides.

The information is detailed enough to allow cloud users to check the following aspects, insofar as they are applicable to the cloud service:

- Which data, services or functions available to the cloud user within the cloud service, have been accessed by whom and when (Audit Logs);
- Malfunctions during processing of automatic or manual actions; and
- Changes to security-relevant configuration parameters, error handling and logging mechanisms, user authentication, action authorisation, cryptography, and communication security.

The logged information is protected from unauthorised access and modification and can be deleted by the Cloud Customer.

If the cloud customer is responsible for the activation or type and scope of logging, the Cloud Service Provider must provide appropriate logging capabilities.

### Additional Criterion

Cloud users can retrieve security-related information via documented interfaces which are suitable for further processing this information as part of their Security Information and Event Management (SIEM).

### Supplementary Information

*About the Criterion*

In the case of a SaaS service for secure data exchange, the terms data, services or functions would mean, for example, the logging of all read or write accesses to the stored files and their metadata.

*Complementary Customer Criterion*

If the cloud service is equipped with error handling and logging mechanisms, cloud customers must activate these and configure them according to defined requirements. The cloud customer must incorporate his own information security management for this purpose.

*Notes on Continuous Auditing*

Feasibility: yes

The information about the security status of cloud services and further data provided can be read automatically and continuously, as these must be made available to cloud users in digital form.

This enables continuous auditing.

## PSS-05 Authentication Mechanisms

### Basic Criterion

The Cloud Service Provider provides authentication mechanisms that can force strong authentication (e.g. two or more factors) for users, IT components or applications within the cloud users' area of responsibility.

These authentication mechanisms are set up at all access points that allow users, IT components or applications to interact with the cloud service.

For privileged users, IT components or applications, these authentication mechanisms are enforced.

### Additional Criterion

The cloud service offers out-of-band authentication (OOB), in which the factors are transmitted via different channels (e.g. Internet and mobile network).

### Supplementary Information

*About the Criterion*

IT components in the sense of this criterion are independently usable objects with external interfaces that can be connected with other IT components.

Access points in the sense of this criterion are those that can be accessed by users, IT components or applications via networks (for users, for example, the login screen on the publicly accessible website of the Cloud Service Provider).

Multi-factor authentication can be performed with cryptographic certificates, smart cards or tokens, for example.

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls that the authentication mechanisms offered by the cloud service are used in accordance with the customer's identity and authorisation management requirements.

*Notes on Continuous Auditing*

Feasibility: partially

The implementation of authentication mechanisms for users takes place via configurations that are only adapted at a low frequency. Thus, continuous auditing is only partially effective here.

Nevertheless, it is conceivable to monitor the status of the underlying authentication system, but only deviations from target configurations can be checked. Whether these deviations are desired or not must still be recorded in a manual audit.

## PSS-06 Session Management

### Basic Criterion

To protect confidentiality, availability, integrity and authenticity during interactions with the cloud service, a suitable session management system is used that at least corresponds to the state-of-the-art and is protected against known attacks. Mechanisms are implemented that invalidate a session after it has been detected as inactive. The inactivity can be detected by time measurement. In this case, the time interval can be configured by the Cloud Service Provider or – if technically possible – by the cloud customer.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

Known attacks include manipulation, forgery, session takeover, Denial of Service attacks, enveloping, replay and null cipher attacks.

*Complementary Customer Criterion*

Cloud customers can use appropriate controls to ensure that they are using the session management protection features of the cloud service in accordance with their own ISMS. They also set the time period after which a session becomes invalid according to their own ISMS specifications.

*Notes on Continuous Auditing*

Feasibility: partially

The use of Session Management is controlled by configurations. These configurations are changed or adapted at a low frequency, so continuous auditing is only partially effective.

Nevertheless, monitoring the status of the underlying authentication system is conceivable, but only deviations from target configurations can be checked. Whether these deviations are normal must still be tested in a manual audit.

## PSS-07 Confidentiality of Authentication Information

### Basic Criterion

If passwords are used as authentication information for the cloud service, their confidentiality is ensured by the following procedures:

- Users can initially create the password themselves or must change an initial password when logging in to the cloud service for the first time. An initial password loses its validity after a maximum of 14 days.
- When creating passwords, compliance with the length and complexity requirements of the Cloud Service Provider (cf. IDM-09) or the cloud customer is technically enforced.
- The user is informed about changing or resetting the password.
- The server-side storage takes place using state-of-the-art cryptographically strong hash functions in combination with at least 32-bit long salt values.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

The state-of-the-art regarding cryptographically strong hash functions is described in the current version of the BSI Technical Guideline TR-02102-1 “Cryptographic mechanisms: Recommendations and key lengths”. In version 2019-01 of this guideline these were:

- SHA-256, SHA-512/256, SHA-384, SHA-512; and
- SHA3-256, SHA3-384, SHA3-512.

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls that they use sufficiently secure passwords (cf. IDM-09) according to their own assessment and that the risks of unauthorised access associated with their own choice are borne.

*Notes on Continuous Auditing*

Feasibility: no

Compliance with security policies for password assignment is configured centrally and adjusted at a low frequency. A continuous audit is therefore only of limited use.

## PSS-08 Roles and Rights Concept

### Basic Criterion

The Cloud Service Provider provides cloud users with a roles and rights concept for managing access rights. It describes rights profiles for the functions provided by the cloud service.

The rights profiles are suitable for enabling cloud users to manage access authorisations and permissions in accordance with the principle of least-privilege and how it is necessary for the performance of tasks (“need-to-know principle”) and to implement the principle of functional separation between operational and controlling functions (“separation of duties”).

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

In IaaS, a role and rights concept would describe, among other things, the rights profiles for the following functions of the cloud service:

- Administration of the states of virtual machines (start, pause, stop) as well as for their migration or monitoring;
- Management of available images that can be used to create virtual machines; and
- Management of virtual networks (e.g. configuration of virtual routers and switches).

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls that:

- the granting of permissions to users in their area of responsibility is subject to authorisation; and
- the appropriateness of the assigned authorisations is regularly reviewed and authorisations are adjusted or withdrawn in a timely manner in the event of necessary changes (e.g. employee resignation).

*Notes on Continuous Auditing*

Feasibility: partially

The existence of a roles and rights concept in the form of a configuration in the system can be monitored. However, it should be noted that, regarding the content of this concept, only deviations from target configurations can be checked. Whether these deviations are desired or not must still be recorded in a manual audit.

## PSS-09 Authorisation Mechanisms

### Basic Criterion

Access to the functions provided by the cloud service is restricted by access controls (authorisation mechanisms) that verify whether users, IT components, or applications are authorised to perform certain actions.

The Cloud Service Provider validates the functionality of the authorisation mechanisms before new functions are made available to cloud users and in the event of changes to the authorisation mechanisms of existing functions (cf. DEV-06). The severity of identified vulnerabilities is assessed according to defined criteria based on industry standard metrics (e.g. Common Vulnerability Scoring System) and measures for timely resolution or mitigation are initiated. Vulnerabilities that have not been fixed are listed in the online register of known vulnerabilities (cf. PSS-02).

### Additional Criterion

Access controls are attribute-based to enable granular and contextual checks against multiple attributes of a user, IT component, or application (e.g., role, location, authentication method).

### Supplementary Information

*About the Criterion*

–

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

The changes to authorisation mechanisms and the identification of vulnerabilities are documented in a standardised manner by the Cloud Service Provider. This documentation can be automated and continuously audited. If the elimination of the vulnerabilities and their prioritisation also takes place in a standardised form (according to standardised criteria), these points can be integrated into the continuous audit.

## PSS-10 Software Defined Networking

### Basic Criterion

If the Cloud Service offers functions for software-defined networking (SDN), the confidentiality of the data of the cloud user is ensured by suitable SDN procedures.

The Cloud Service Provider validates the functionality of the SDN functions before providing new SDN features to cloud users or modifying existing SDN features. Identified defects are assessed and corrected in a risk-oriented manner.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

This criterion is typically not applicable to the SaaS service model.

Suitable SDN methods for increasing confidentiality are, for example, L2 overlay networking (tagging) or tunnelling/encapsulation.

*Complementary Customer Criterion*

–

*Notes on Continuous Auditing*

Feasibility: yes

Validation during provision and modification of SDN functions and identification of defects can be documented in a standardised manner by the Cloud Service Provider.

This documentation can be audited continuously and automatically by the auditor.

The “marking” of the data is carried out by a configuration that has to be tested centrally. A continuous audit of all transmitted data packets would not be effective here.

The status of the configuration can be continuously audited against a target value, a content evaluation must be carried out manually.

## PSS-11 Images for Virtual Machines and Containers

### Basic Criterion

If cloud customers operate virtual machines or containers with the cloud service, the Cloud Service Provider must ensure the following aspects:

- The cloud customer can restrict the selection of images of virtual machines or containers according to his specifications, so that users of this cloud customer can only launch the images or containers released according to these restrictions.
- If the Cloud Service Provider provides images of virtual machines or containers to the Cloud Customer, the Cloud Service Provider appropriately inform the Cloud Customer of the changes made to the previous version.
- In addition, these images provided by the Cloud Service Provider are hardened according to generally accepted industry standards.

### Additional Criterion

At startup and runtime of virtual machine or container images, an integrity check is performed that detects image manipulations and reports them to the cloud customer.

### Supplementary Information

*About the Criterion*

This criterion is typically not applicable to the SaaS service model.

Generally accepted industry standards are, for example, the Security Configuration Benchmark of the Centre for Internet Security (CIS) or the corresponding modules in the BSI IT-Grundschutz-Kompendium.

*Complementary Customer Criterion*

Cloud customers use appropriate controls to ensure that the images of virtual machines or containers they operate with the cloud service comply with their information security management requirements and that the results of the integrity checks at startup and at runtime are processed according to these requirements.

*Notes on Continuous Auditing*

Feasibility: partially

These functions must be centrally audited at regular intervals, but not continuously. Therefore, it is sufficient to integrate this into the recurring audit.

With an agent system, it would be possible to continuously query the configurations of the individual virtual machines and thus compare them with the target image. This could also be set up on demand and thus become part of the control that takes over the integrity check.

## PSS-12 Locations of Data Processing and Storage

### Basic Criterion

The cloud customer is able to specify the locations (location/country) of the data processing and storage including data backups according to the contractually available options.

This must be ensured by the cloud architecture.

### Additional Criterion

–

### Supplementary Information

*About the Criterion*

This criterion supplements the General Condition BC-01.

The cloud architecture must exist in such a way that it enables the technical design of the IT infrastructure to provide the cloud service in accordance with the data location specifications agreed with the customer.

*Complementary Customer Criterion*

Cloud customers ensure through suitable controls that, when selecting service providers and configuring the cloud service, they are informed about the available data processing and storage locations and, if there is a choice between different locations, that they select those that meet their own requirements.

Depending on the use case and especially when using services of a Cloud Service Provider which is based in another country, cloud customers take the laws applicable to them into account when making their selection (e.g. when processing personal data; compliance with legal retention obligations for business documents, etc.).

*Notes on Continuous Auditing*

Feasibility: yes

A continuous survey of the location of the data and the country from which the service is provided can be carried out automatically by the Cloud Service Provider. This information can then be made available to the customer, for example on his dashboard or on request.

# Errata

The following corrections have been applied to the C5:2020 after its first publication on January 21th, 2020:

- Adjustments to the chapter numbers: The Preface of the President is now unnumbered, all other chapter numbers have been decremented by one.
- Errata: This chapter has been added.
- 3.4.4.1 Description, First enumeration, last element:
  "... as well as the resulting dependency of the Cloud Service Provider, and the availability of audit reports according to the criteria in this criteria catalogue" changed to
  "... as well as the resulting dependency of the Cloud Service Provider, (if carve-out method is applied) complementary controls assumed in the design of the Cloud Service Provider's controls, and the availability of audit reports according to the criteria in this criteria catalogue"
- HR-05, Basic Criterion:
  "which responsibilities, arising from the guidelines and instructions relating to information security, ..." changed to
  "which responsibilities, arising from employment terms and conditions relating to information security, ..."
- HR-06, Additional Criterion: Removed, since already covered in Basic Criterion
- PS-03, Basic Criterion:
  "The security measures are designed to detect and prevent unauthorised access in a timely manner so that it does not compromise the information security of the cloud service. The outer doors, windows and other construction elements reach a level appropriate to the security requirements and withstand ..." changed to
  "The security measures are designed to detect and prevent unauthorised access so that the information security of the cloud service is not compromised. The outer doors, windows and other construction elements exhibit an appropriate security level and withstand ..."
- OPS-04, Basic Criterion:
  "Policies and instructions that provide protection ..." changed to
  "Policies and instructions with specifications for protection ..."
- OPS-06, Title: "Data Protection" changed to "Data Backup"
- IDM-08, Basic Criterion: Change reference from IDM-12 to IDM-09
- CRY-01, Basic Criterion: Add reference to AM-06
- COS-06, Supplementary Information: Removed information about session IDs, since these are addressed in PSS-06.
- SSO-05, Basic Criterion: Supplementary Information: Correct indentation levels of bullet points
- COM-03, Basis Criterion: Remove reference to ISO/IEC 27001 as it is present in Supplementary Information
- COM-03, Supplementary Information:
  ”see Section 9.3 of ISO/IEC 27001” changed to
  "see Section 9.2 of ISO/IEC 27001."
- INQ-04, Basis Criterion:
  "... procedures for setting up access to or disclosure of cloud customer data as part of an investigation requests, ensure that government agencies only have access to the data they need to investigate." changed to
  "... procedures establishing access to or disclosing data of cloud customers in the context of investigation requests from governmental agencies ensure that the agencies only gain access to or insight into the data that is the subject of the investigation request."

# Legal notice

**Published by:**
Bundesamt für Sicherheit in der Informationstechnik (BSI)
53175 Bonn

**Source:**
Federal Office for Information Security (BSI)
Godesberger Allee 185–189
53175 Bonn
Phone: +49 (0) 228 999582-0
Fax: +49 (0) 228 999582-5400
Email: cloudsecurity@bsi.bund.de
Internet: https://www.bsi.bund.de/EN/C5/

**Last updated:**
October 2020

**Printed by:**
Appel & Klinger Druck und Medien GmbH
Bahnhofstraße 3 a
96277 Schneckenlohe
Internet: www.ak-druck-medien.de

**Content and editing:**
Federal Office for Information Security (BSI)

**Image credits:**
Fotolia © sdecore

**Item number:**
BSI-Cloud 20/202

This brochure is part of the Federal Office for Information Security’s public relations work.
It is provided free of charge and is not intended for sale.

www.bsi.bund.de