Community Draft of the Cloud Computing Compliance Criteria Catalogue (C5:2025)

Federal Office for Information Security (BSI)

Preface by the President

[t.b.d]

Contents

1 Introduction

1.1 Preliminary remarks

[t.b.d]

1.2 Definitions

1.2.1 Terms related to Cloud Security

For the purposes of this criteria catalogue, the following definitions apply. They are derived from the BSI's IT-Grundschutz-Compendium and the international standard ISO/IEC 22123:2023 (Information Technology - Cloud Computing - Part 1: Vocabulary) and enriched by our own work:

Account data

Class of data specific to each cloud service customer that is required to administer the cloud service. Account data (e.g. billing data, contact information, etc.) is typically generated when a cloud service is purchased and is under the control of the cloud service provider.

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

Paradigm for enabling network access to a scalable and elastic pool of shared physical or virtual resources with self-service provisioning and administration on-demand. Examples of resources include servers, operating systems, networks, software, applications, and storage equipment. Self-service provisioning refers to the provisioning of resources provided to cloud services performed by cloud service customers through automated means.

Cloud service

Information technology service offered via 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 service customer

Natural or legal person who has a business relationship with the cloud service provider for the purpose of using the cloud service.

Cloud service customer data

Class of data objects under the control, by legal or other reasons, of the cloud service customer that were input to the cloud service (including credentials to control access to information or other resources), or resulted from using the functionalities of the cloud ser-

vice by or on behalf of the cloud service customer via the published interface of the cloud service.

Cloud service derived data

Class of data objects under cloud service provider control that are derived as a result of interaction with the cloud service by the cloud service customer. Cloud service derived data includes the portion of log data containing records of who used the service, at what times, which functions, types of data involved and so on. It can also include information about the numbers of authorised users and their identities. It can also include any configuration or customisation data, where the cloud service has such configuration and customisation functionalities.

Cloud service provider data

Class of data objects, specific to the operation of the cloud service, under the control of the cloud service provider. Cloud service provider data includes but is not limited to configuration and utilisation information of system components, storage and network resource allocations, physical and virtual resource failure rates, operational costs and so on.

Cybersecurity risk

Cybersecurity risks are effects of uncertainty associated with information and technology. Cybersecurity risks relate to the loss of confidentiality, integrity, or availability of information, data, or information systems. They reflect potential adverse impacts to organisational operations (i.e., mission, functions, image, or reputation) and assets, in particular with regards to the security of network and information systems.

Functional component

Functional building block needed to engage in an activity, backed by an implementation.

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).

Incident

Event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, system components of the cloud service. An incident is a materialized cybersecurity risk.

Information Security

Information security refers to the practices and principles designed to protect information from unauthorized access, use, disclosure, disruption, modification or destruction. In the context of this catalogue, it ensures confidentiality, integrity, authenticity and availability of cloud service customer data, cloud service provider data, cloud service derived data and account data.

Integrity

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

Location

A location is a single premises containing one or more data halls, each with separate power supply, network connectivity, and fire protection. Each location is physically separated from all other locations and is exclusive to a single zone.

Partition

A partition is an overarching grouping of regions (see definition below) that share a unified identity and access management (IAM) system for both cloud provider staff and customers. Each region is exclusively part of one partition, and there is strict separation without shared infrastructure between partitions.

Penetration test

Authorised, simulated real-world attack of system components for identifying ways to exploit vulnerabilities to circumvent or defeat the security features of the cloud service.

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. The protection need of system components and data is inherited from the protection need of the cloud service. The cloud service customer has to decide themselves whether or not the level of information security for the cloud service customer data, cloud service derived data and account data suffices according to their own protection need.

Region

A region comprises one or more zones, all situated within a single metropolitan area (metropole). Cloud service providers may use any name for a region, such as "EU-south-west," but the region's infrastructure must be confined to one metropolitan area and never dispersed as broadly as an entire country or continent. Note: In cases where a region consists of only one zone (common with smaller providers), the practical difference between region and zone may be minimal; however, the conceptual distinction remains: a region covers the metropolitan management scope, and a zone constitutes an availability grouping within that scope.

System components

Elements of information and communication technology systems 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, which may be classified into the following five categories: infrastructure, software, people, procedures, and data.

Vulnerability scan

Use of a variety of automated tools combined with manual verification of identified issues to identify, assess, and report vulnerabilities that, if exploited, may result in intentional or unintentional compromise of the cloud service and its data.

1.2.2 Terms related to Audits

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" issued by the International Federation of Accountants (IFAC), ISO/IEC 17029:2019 "Conformity assessment — General principles and requirements for validation and verification bodies" issued by the International Organization for Standardization (ISO) and the publication "Internal Control - Integrated Framework" issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

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.

Carve-out method

Method of addressing the services provided by a subservice organisation in which the components of the subservice organisation's system of internal control used to provide the services to the cloud service provider are excluded from the description of the cloud service provider's system of internal control relevant to the development and operation of the cloud service, and from the scope of the audit. However, the description identifies (a) the nature of the services performed by the subservice organisation; (b) the types of controls expected to be performed at the subservice organisation that are necessary, in combination with controls at the cloud service provider, to provide reasonable assurance that the applicable C5 criteria were achieved; and (c) the controls at the cloud service provider used to monitor the effectiveness of the subservice organisation's controls.

Claim

Information declared by the cloud service provider.

Complementary user entity controls (CUEC)

Controls that a cloud service provider assumed, in

the design of its system of internal control relevant to the development and operation of the cloud service, would be implemented by cloud service customers (user entities). The implemented complementary user entity controls together with the cloud service provider internal controls are necessary to ensure with reasonable assurance that the applicable C5 criteria are met.

Complementary subservice organisation controls (CSOC)

Controls that cloud service provider assumed, in the design of its system of internal control relevant to the development and operation of the cloud service, would be implemented by the subservice organisation. The complementary subservice organisation controls together with the cloud service provider internal controls are necessary to provide reasonable assurance that the applicable C5 criteria are be met.

Control

Policy or procedure 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. Controls exist within each of the five components of the cloud service provider's system of internal control (control environment, risk assessment, control activities, information and communication and monitoring activities). A control is either preventive (designed to avoid an unintended event or result at the time of initial occurrence) or detective (designed to discover an unintended event or result after the initial processing has occurred, but before the ultimate objective has concluded, and with action taken to correct or avoid an unintended event our result).

Control activities

Actions established by policies and procedures to help ensure that management directives to mitigate risks to the achievement of objectives are carried out.

Control environment

Set of standards, processes and structures that provide the basis for carrying out internal control across the organisation.

Deficiency

Term used to identify misstatements resulting from controls that were not suitably designed or did not operate effectively.

Deviation

Term used to identify misstatements resulting from the failure of a control to operate in a specific instance. A deviation may, individually or in combination with other deviations, result in a deficiency.

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.

Inclusive method

Method of addressing the services provided by a subservice organisation in which the description of the cloud service provider's system of internal control relevant to the development and operation of the cloud service includes a description of (a) the nature of the services provided by the subservice organisation; (b) the components of the subservice organisation's system of internal control used to provide services to the cloud service provider, including the subservice organisation's controls that are necessary, in combination with controls at the cloud service provider, to provide reasonable assurance that the applicable C5 criteria were met; and (c) the controls at the cloud service provider used to monitor the effectiveness of the subservice organisation's controls. (When using the inclusive method, controls at the subservice organisation are subject to the auditor's test procedures. Because the subservice organisation's system components are included in the description, those components are included in the scope of the audit.)

Information and communication

Information is necessary for the entity to carry out internal control responsibilities in support achievement of its objectives. Communication occurs both internally and externally and provides the organisation with the information needed to carry out day-to-day controls

Material misstatement

Deficiencies in the statement, e.g.:

- Information does 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.

Monitoring activities

Ongoing evaluations, separate evaluations, or some combination thereof to ascertain whether each of the five components of internal controls is present and functioning.

Risk assessment

Process for identifying and analysing risks to achieving the entity's objectives.

Service Organisation

Partners, vendors, or other third parties that provide services to the cloud service provider associated with the development or operation of the cloud service.

Subservice organisation

Service organisations for which the following characteristics apply in combination:

- The services provided by the service organisation are likely to be relevant to the cloud service customers' understanding of the applicable C5 criteria. A service is likely relevant, if the service organisation has access to system components of the cloud service and may access confidential information or transmit information between themselves and the cloud service.
- Complementary subservice organisation controls (CSOC) 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.

System of internal control

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. This catalogue outlines criteria for the cloud service provider's control environment, risk assessment, control activities, information and communication and monitoring activities that are relevant to the development and operation of the cloud service.

Validation

The confirmation of a claim by the cloud service provider itself, through the provision of objective evidence, that the requirements for a specific intended future use or application have been fulfilled.

Verification

The confirmation of a claim by the cloud service provider itself, through the provision of objective evidence, that specified requirements have been fulfilled.

Written statement

Assertions on the description of the cloud service provider's system of internal control 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 (management) of the cloud service provider.

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.

The criteria are divided into basic criteria and additional criteria (C5 criteria). If the criteria address several aspects for archieving the objective, they are broken down into subcriteria. This is done to ease the mapping of controls of 1. the cloud service provider internal control system controls, 2. customer controls to cloud service provider controls and 3. to ease the documentation of testing procedures for auditors. In addition, the additional criteria are divided into criteria that sharpen or complement the basic (sub)criteria. According to the BSI, the basic criteria reflect the minimum level of information security that a cloud service must offer when cloud service 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 service customers to assess for their individual use case to what extent the basic criteria adequately reflect the protection needs of their information. For cloud service 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.

In addition to the basic criteria, additional criteria and supplementary information, the Criteria Catalogue also contains 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 service customer's side which must be set up together with the controls of the cloud service provider in order to meet the C5 criteria;
- 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 service 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 2.3). 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 2.1).

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.

Table 2.1: Areas of the criteria catalogue with assigned objectives

No.	Area (Identifier)	Objective
1	Organisation of Information Security (OIS)	Plan, implement, maintain and continuously improve the information security framework within the organisation.
2	Security Policies and Instructions (SP)	Provide policies and instructions regarding security requirements and to support business requirements.
3	Personnel (HR)	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)	Identify the organisation's own assets and ensure an appropriate level of protection throughout their lifecycle.
5	Physical Security (PS)	Prevent unauthorised physical access and protect against theft, damage, loss and outage of operations.
6	Operations (OPS)	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 (IAM)	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)	Ensure appropriate and effective use of cryptography to protect the confidentiality, authenticity or integrity of information.
9	Communication Security (COS)	Ensure the protection of information in networks and the corresponding information processing systems.
10	Portability and Interoperability (PI)	Enable the ability to access the cloud service via other cloud services or IT systems of the cloud service customers, to obtain the stored data at the end of the contractual relationship and to securely delete it from the cloud service provider.
11	Procurement, Development and Modification of Information Systems (DEV)	Ensure information security in the development cycle of cloud service system components.

No.	Area (Identifier)	Objective
12	Control and Monitoring of Service Providers and Suppliers (SSO)	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)	Ensure a consistent and comprehensive approach to the capturing, evaluation, communication and handling of security incidents.
14	Business Continuity Management (BCM)	Plan, implement, maintain and test procedures and measures for business continuity and emergency management.
15	Compliance (COM)	Avoid non-compliance with legal, regulatory, self-imposed or contractual information security and compliance requirements.
16	Dealing with Investigation Requests from Government Agencies (INQ)	Ensure appropriate handling of government investigation requests for legal review, information to cloud service customers, and limitation of access to or disclosure of data.
17	Product Safety and Security (PSS)	Provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud service customers, appropriate mechanisms for troubleshooting and logging, as well as authentication and authorisation of users of cloud service customers.

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

- ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection - Information security management systems - Requirements
- ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection - Information security controls
- ISO/IEC 27017:2015 - Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- BSI - IT-Grundschutz-Compendium, 2023
- CSA (Cloud Security Alliance, a non-profit organisation for the dissemination of security standards in cloud computing) - Cloud Controls Matrix 4.0.12 (CSA CCM)
- AICPA (American Institute of Certified Public Accountants) - TSP Section 100 - 2027 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (March 2020 updates)
- ANSSI (Agence nationale de la sécurité des systèmes d'information, National Cybersecurity Agency of France) - Providers of cloud computing services v. 3.2 (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 of November 4, 2015
- ANNEX 'Technical and methodological requirements', C(2024)7151, Implementing Regulation to the NIS2-Directive (2022/2555)
- CEN/CTS 18026:2024, 'Three-level approach for a set of cybersecurity requirements for cloud services', 2024
- AC/322-D(2021)0032-REV1, 'Technical and Implementation Directive for the Protection of NATO Information within Public Cloud-Based Communication and Information Systems', 2024

Cloud service providers who already align 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/C5). Cloud service providers should consider the tables as aids when assessing compliance. Notwithstanding the information contained in the reference tables, cloud service providers shall determine to what extent existing policies, procedures and measures meet the C5 criteria on a case-by-case basis (cf. Section 3.4.8).

3 Providing Conformity through Independent Audits

3.1 Introduction

Cloud service providers and cloud service 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 service 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. 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 below sets out its view of the requirements for such audits.

The cloud service 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 service 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 service 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 service 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 equivalents 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. The scope of audits in accordance with these standards comprises the policies and procedures designed and implemented by the service organisation (here: the cloud service provider) to provide user entities (here: the cloud service customers) with their services. They require the service organisation to define control ob-

jectives and controls to achieve these objectives. In the context of C5, controls include aspects of the cloud service provider's control environment, risk assessment, control activities, information and communication and monitoring activities that are relevant to the development and operation of the cloud service in accordance with the criteria in this catalogue. The combination of the aforementioned aspects is also known as 'system of internal control' as described by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in its publication 'Internal Control - Integrated Framework'.

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, for which the cloud service provider may have already engaged independent auditors. In this context, especially audits according to ISAE 3402/SOC 1 or SOC 2 should be mentioned. In these instances, it is more efficient to align these audits with one that follows this criteria catalog, both in terms of organisation and timing. This enables auditors and cloud service providers to use records in parallel for reporting to different standards. 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 audit methodology and compared with the 'reasonable assurance' required for an attestation engagement or a direct engagement (cf. Section 3.4.4). 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 shall 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 auditor's responsibility.

3.4 Supplementary Requirements of the BSI

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

3.4.1 Assurance Engagement

Conformity assessments are always to be provided in accordance with ISAE 3000 (Revised) or other national equivalents to ISAE 3000 (Revised), e.g. the German Audit Standard (PS) 860. ISAE 3000 (Revised) distinguishes between assurance engagements with 'reason-

able assurance and assurance engagements with 'limited assurance'. Auditors (also referred to as 'practitioner') shall perform reasonable assurance engagements to evaluate the conformity with this criteria catalogue.

A distinction is also made between 'attestation engagements' and 'direct engagements'. Both variants are suitable for evaluating the conformity with this criteria catalogue. In addition, audits may be carried out regarding the suitability of the design or the operating effectiveness of controls. The operating effectiveness has to be evaluated in order to issue an opinion on the cloud service provider's controls to meet the C5 criteria throughout a specified period. Assurance engagements on the suitability of the design of controls are limited to the design as of a specified date only. Such engagements shall only be carried out in case of an initial engagement for a (set of) services, when there is not yet sufficient evidence to issue an opinion about the operating effectiveness throughout a specified period (e.g. when a new cloud service is supposed to be launched on the market). As such, assurance engagements only on the suitability of the design are not to be performed on a recurring basis.

3.4.2 Qualification of the Auditor

According to ISAE 3000 (Revised), the auditor shall 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.

Audits based on this criteria catalogue place special requirements on the qualification of the auditor and the members of the audit team. 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 Management' of the audit report.

3.4.3 Criteria to be Applied

3.4.3.1 Criteria for Information Security of the Cloud Service

The basic criteria reflect the minimum level of information security that a cloud service shall offer when cloud service customers use it to process information that has a normal protection need. The basic criteria define the minimum scope of an audit according to this criteria catalogue. Nevertheless, it is up to

the cloud service customers to assess for their individual use case to what extent the basic criteria adequately reflect the protection needs of their information. For cloud service customers whose information has a higher need for protection, the additional criteria can provide a starting point to address this need together with a solid architecture of their cloud workload. Cloud service providers may include the additional criteria in an audit in addition to the basic criteria. The cloud service provider is free in selecting which of the additional criteria to include in the scope of an audit. However, the selection should be based on the contractual requirements with the cloud service customers. If conformity with certain contractual requirements could be demonstrated by including additional criteria to the scope, these criteria should be included. If the cloud service provider includes only certain of the additional criteria, the rationale for the selection shall be stated in the description.

The cloud service provider shall present the applicable C5 criteria in the description of its system of internal control for the cloud service. If individual criteria are not applicable, the presentation shall include justifications for exclusion. Justifications for exclusions shall be limited to the nature and design of the cloud service or the principles, procedures and measures of the cloud service provider (e.g. C5 criteria that are applicable to IaaS only, when the cloud service is SaaS). Based on the information provided by the cloud service provider, the auditor shall assess the fair presentation of the justifications. Criteria shall not be excluded from the scope because the cloud service provider's controls were not suitably designed or operating effectively to meet these criteria, or the provider is not willing or able to demonstrate conformity.

If a criterion demands for a risk-based approach and the cloud service provider's risk assessment concluded that there are no risks to mitigate, the cloud service provider shall present this justification as well.

3.4.3.2 Further Criteria for Transparency and Reporting

The so-called 'Boundary Conditions' define a special set of criteria that are intended to provide more transparency on the general conditions of the cloud service as well as the requirements concerning the system description and written statement (cf. Section 3.5.1; 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.

3.4.4 Subject Matter and Objective of the Audit

3.4.4.1 Attestation Engagement

The subject matter of an attestation engagement is the description of the cloud service provider's system of internal control relevant to the development and operation of the cloud service in accordance with the criteria in this catalogue (hereafter the 'Description'). The audit is based on a written statement by the cloud service provider's management (management statement) about the suitability of the design of controls to meet the applicable C5 criteria as of a specified date (type 1 report), or about the suitability of the design and operating effectiveness of the controls throughout a specified period (type 2 report). The objective of the audit is to enable the auditor to issue an opinion with reasonable assurance as to whether:

- the Description fairly presents the cloud service provider's system of internal control relevant to the development and operation of the cloud service that was designed and implemented as of the specified date (type 1 report) or throughout the specified period (type 2 report) in accordance with the description criteria as set forth in section 3.4.6.1 of this catalogue;
- the controls stated in the Description were suitably designed to provide reasonable assurance that the applicable criteria would be met as of the specified date (type 1 report) or (if mandated) throughout the specified period (type 2 report), if these controls operated effectively as of that date (type 1 report) or throughout that period (type 2 report); and
- if mandated (type 2 report), the controls stated in the Description operated effectively to provide reasonable assurance that the applicable criteria were met throughout the specified period.

Type 1 reports should be mandated for initial engagements only. Subsequent engagements should mandate a type 2 report. If a type 2 report is mandated, the minimum period should cover at least 3 months. For shorter periods the auditor will not be able to obtain sufficient evidence regarding the operating effectiveness of controls. The maximum period should not cover more than 12 months.

The auditor's opinion on the design and operation of the cloud service provider's controls may refer to complementary controls at subservice organisations and/or user entities (cloud service customers) that the cloud service provider assumes in the design of its own controls to meet the criteria. Because of shared responsibilities between the cloud service provider, subservice organisations (e.g. data centre operators; SaaS service operated on an IaaS platform) and customers (e.g. identity and access management for employees that belong to the customer organisation) that are inherent to cloud computing, it is likely that complementary controls are required along the cloud service provider's controls to meet certain of the criteria. However, the auditor's procedures will not extent to actual controls at subservice organisations and/or user entities to address such complementary controls, but will be limited to the fair presentation of the cloud service provider's assumptions about these controls in the Description.

Cloud service providers who already prepared a description of their system of internal control may reuse it in audits according to this criteria catalogue. However, an existing description that was prepared to meet the requirements of another standard shall be adapted to the description criteria of this catalogue, as necessary.

3.4.4.2 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 aspects of the system of internal control for the development and operation of the cloud service 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 suitably designed to provide reasonable assurance that the applicable criteria would be met as of the specified date (type 1 report) or (if mandated) throughout the specified period (type 2 report), if these principles, procedures and measures operated effectively as of that date (type 1 report) or throughout that period (type 2 report); and
- if mandated (type 2 report), the principles, procedures and measures stated in the Description operated effectively to provide reasonable assurance that the applicable criteria were met throughout the specified period.

Type 1 reports should be mandated for initial engagements only. Subsequent engagements should mandate a type 2 report. If a type 2 report is mandated, the minimum period should cover at least 3 months. For shorter periods the auditor will not be able to obtain sufficient evidence regarding the operating effectiveness of controls. The maximum period should not cover more than 12 months.

The direct engagement is particularly suitable for cloud service providers who have not yet sufficiently documented their system of internal control for the development and operation of the cloud service in a description.

3.4.5 Requirements for the Description and the Management Statement

3.4.5.1 Description Criteria

For an attestation engagement, the description of the cloud service provider's system of internal control relevant to the development and operation of the cloud service (the 'System') shall be prepared in accordance with the following description criteria.

1.) Fair presentation of the System that was designed and implemented as of the specified date (type 1 re-

port) or throughout the specified period (type 2 report) with the following minimum content, in order to provide customers with sufficient transparency about the information security of the cloud services in scope:

- 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 4 of this criteria catalogue, which enable potential customers to assess its suitability for their use case;
- Applicability of the C5 criteria, including justifications if individual criteria are not applicable in accordance with the requirements outlined in section 'Criteria to be Applied';
- Control environment, risk assessment, control activities, information and communication and monitoring activities that are relevant to the development and operation of the cloud service in accordance with the applicable 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 (also called complementary user entity controls (CUEC)) 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

    1. nature of the services performed by the subservice organisation, including (1) the name of the company with which a contractual relationship exists for the services performed, (2) location of processing and storage of data, (3) assessment of the complexity and uniqueness of the services performed as well as the resulting dependency of the cloud service provider from the subservice organisation and (4) the availability of audit reports according to the criteria of this catalogue;
    2. the types of controls expected to be performed at the subservice organisation that are necessary, in combination with controls at the cloud service provider, to provide reasonable assurance that the applicable C5 criteria were achieved; and
    3. the controls at the cloud service provider used to monitor the effectiveness of the subservice organisation's controls

In case of type 2 report, the following contents shall be included as well:

- Details on significant changes to the cloud service provider's system of internal control applicable to the C5 Criteria, that have been implemented during the specified period;

- 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 cloud service customer data, or
    – the integrity of the cloud service customer data 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 service 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 vulnerabilities or potential points of attack. Furthermore, the details presented in the description of the System shall not jeopardise the information security of individual cloud service customers and should therefore not contain a detailed description of individual incidents.

2.) The description of the System shall not omit or distort any information relevant to meet the applicable C5 criteria, while acknowledging that the description is prepared to meet the common needs of a broad

range of specified parties (intended users of the report) and may not, therefore, include every aspect of the System that each individual within the specified parties may consider important to his or her own particular needs.

In the case of a direct engagement, the auditor shall present the cloud service provider's System in all material aspects as part of the audit report so that the specified parties can obtain an appropriate understanding of the information security of the cloud service.

3.4.5.2 Management Statement

Management of the cloud service provider shall provide a written statement to confirm to the best of their knowledge and belief that:

- The description fairly presents the cloud service provider's System that was designed and implemented as of the specified date (type 1 report) or throughout the specified period (type 2 report) in accordance with the Description Criteria as set forth in section 'Description Criteria' of this catalogue;
- The controls stated in the description were suitably designed to provide reasonable assurance that the applicable criteria would be met as of the specified date (type 1 report) or (if mandated) throughout the specified period (type 2 report), if these controls operated effectively as of that date (type 1 report) or throughout that period (type 2 report). The criteria to be used in making that statement shall be that

1. The risks that threaten the applicable criteria from being met have been identified;
2. The controls identified in the Description would, if operating effectively, provide reasonable assurance that those risks would not prevent the applicable criteria from being met.

- If mandated (type 2 report), the controls stated in the description operated effectively to provide reasonable assurance that the applicable criteria were met throughout the specified period. The criterion to be used in making that statement shall be that the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

If the management statement covers a period of more than 12 months, the management statement shall state the reason for this.

Management of the cloud service provider shall have a reasonable basis for its written statement. In the case of a type 2 report, this statement may be based on the cloud service provider's monitoring activities regarding the effectiveness of controls over time. It involves identifying and reporting deficiencies to appropriate individuals within the cloud service provider's organisation, and taking necessary corrective actions. The cloud service provider may accomplish monitoring of controls through ongoing activities, separate evaluations, or a combination of both. Internal auditors or personnel performing similar functions may contribute to such activities. It may also include using information communicated by external parties, such as customer complaints and regulator comments, which may indicate problems or highlight areas in need of improvement. The fact that the auditor will report on the operating effectiveness of controls is not a substitute for the cloud service provider's own processes to provide a reasonable basis for its statement.

3.4.6 Consideration of Subservice Organisations

If necessary, the cloud service provider will outsource parts of its business processes for the development or operation of the cloud service to other business partners, vendors, or other third parties (service organisations). The cloud service provider shall select the method to be used at its own discretion and state it accordingly in its description of its System by applying either the 'inclusive method' or the 'carve-out method' (see section 'Definition'), and the auditor shall take this into consideration accordingly.

For the purposes of this criteria catalogue, a service organisation of the cloud service provider shall be considered as a subservice organisation if the following characteristics apply in combination:

- The services provided by the service organisation are likely to be relevant to the cloud service customers' understanding of the applicable C5 criteria. A service is likely relevant, if the service organisation has access to system components of the cloud service and may access confidential information or transmit information between themselves and the cloud service.
- Complementary subservice organisation controls (CSOC) 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 criteria in 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 CSOC, typically does not apply, for example, to business relationships of the cloud service provider with cleaning companies or advertising agencies.

The cloud service provider shall perform monitoring activities for subservice organisations in accordance with the criteria specified in the area 'Control and Monitoring of Service Organisations' set forth in section 5.12 of this catalogue, especially criterion SSO-05. This is intended to prevent the cloud service provider from using the carve-out method as a method of not paying appropriate and due attention to conformity with certain criteria in this catalogue. The cloud service provider remains ultimately responsible for ensuring that the development and operation of the cloud service meets the applicable C5 criteria.

The cloud service provider shall disclose the following information in the description of the System, as specified in the section 'Description Criteria' of this catalogue:

1. the nature of the services performed by the subservice organisation, including

   - Name of the company with which a contractual relationship exists for the services performed;
   - Location of processing and storage of data (Country-level information is sufficient);
   - Assessment of the complexity and uniqueness of the services performed as well as the resulting dependency of the cloud service provider from the subservice organisation (e.g. presented as 'Low', 'Medium', 'High', 'Very high' including a justification for the assessment);

2. the types of controls expected to be performed at the subservice organisation that are necessary, in combination with controls at the cloud service provider, to provide reasonable assurance that the applicable C5 criteria were achieved; and
3. the controls at the cloud service provider used to monitor the effectiveness of the subservice organisation's controls In the case of a direct engagement, where there is no description prepared by the cloud service provider, the above auditor shall be present the aforementioned information accordingly.

3.4.7 Obtaining Evidence Regarding the Description

The auditor shall adhere to the requirements of ISAE 3402.21-22, which requires the auditor to obtain and read the cloud service provider's description of its System, and to evaluate whether those aspects of the description included in the scope of the engagement are fairly presented. Special considerations shall be given to the minimum content of the description as outlined in the section Description Criteria.
It also requires the auditor determine, through other procedures in combination with inquiries, whether the cloud service providers' System has been implemented. Those other procedures shall include observation, and inspection of records and other documentation, of the manner in which the cloud service provider's system operates and controls are applied.

A presentation shall be considered to be fairly presented only if it was prepared in accordance with the requirements in the section 'Description Criteria' of this catalogue. This requires, amongst other things, that it includes information on the general conditions of the cloud service in accordance with the criteria in section 4 as well as specific information on subservice organisations.

3.4.8 Assessing the Fulfilment of the C5 Criteria

The auditor shall assess the fulfilment of each criterion by considering the combination of controls assigned to it. The descriptions of the controls presented in the cloud service provider's description of its System may not address all elements of the C5 criteria to which they are assigned. This may especially be the case, if the cloud service provider already performs audits in accordance with other standards and publications and did not properly adopt its controls to the criteria of this catalogue.

The auditor shall report to the cloud service provider any identified gaps related to elements of the C5 criteria not being fully met by controls. If the cloud service provider can remediate these gaps by providing evidence for additional controls not previously stated in the description, the cloud service provider shall include these controls in the description of its System. 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 fully met by the control description were addressed. Such test procedures shall be presented in the report in an appropriate form (e.g. 'Assessing the Fulfilment of the C5 Criteria').

If the cloud service provider cannot remediate the gap, the auditor shall modify its conclusion in the audit report with respect to the C5 criteria not being fully met by controls. In such events the auditor shall conclude that the related controls are not suitably designed.

3.4.9 Obtaining Evidence Regarding Design of Controls

The auditor shall determine whether the cloud service provider's controls to meet the applicable C5 criteria were suitably designed. A control is suitably designed if, individually or in combination with other controls, it would, when complied with satisfactorily, provide reasonable assurance that the C5 criteria to which it relates are met. When evaluating whether controls are suitably designed, the service auditor should generally consider the following:

- Whether the control (and if applicable, considered with other controls) addresses the elements of the C5 criteria to which it relates (the control is commensurate with the measures specified in the criteria).
- If a criterion demands for a risk-based approach, whether the cloud service provider's risk assessment was suitably performed, considering the completeness and accuracy of threats and vulnerabilities identified by management compared to the auditor's own risk assessment.
- The frequency or timing of the occurrence or performance of the control.
- The authority and competence of the individual responsible for performing the control (for example, the hierarchical level of the individual performing the control, the individual's role in the organisation, and conflicting duties).
- The tasks within the control being performed and the precision and sensitivity of those tasks (for example, the results of reviews and related follow-up activities)
- Whether the information used in the operation of the controls is reliable.
- Whether the control is adequately changing, adapting, and evolving, when new threats and vulnerabilities are identified.
- Whether the control is implemented as presented in the cloud service provider's description of the System as of the specified date (type 1 report) or throughout the specified period (type 2 report).

3.4.10 Obtaining Evidence Regarding Operating Effectiveness of Controls

The auditor shall adhere to the requirements of ISAE 3402.24-29.

3.4.11 Considerations for Initial Engagements

If the cloud service was not yet subject to an assurance engagement in accordance with this catalogue (e.g. newly developed cloud service), controls may not be implemented as of the specified date (type 1 report) or throughout the specified period (type 2 report). The cloud service provider may provide evidence for such controls as follows:

- If controls are not yet fully executed (e.g. completion of Business Impact Analysis within all organisational units, disaster recovery tests), the cloud service provider may provide evidence for the implementation of such controls by providing e.g. records about the planning of such activities or templates for their documentation.
- If control are not yet implemented in a production environment, the cloud service provider may provide evidence for such controls in a non-production environment that is configured as it was a production environment.

It is not required to mandate a type 1 report, before mandating a type 2 report. Type 1 reports should be limited to the initial engagement only and should not be mandated for consecutive engagements. If a type 2 report is mandated, the minimum period should cover at least 3 months. For shorter periods the auditor will not be able to obtain sufficient evidence regarding the operating effectiveness of controls. The maximum period should not cover more than 12 months.

3.4.12 Deviation Handling

In adoption of the requirements of ISAE 3402.55, if the auditor concludes that

- The cloud service provider's description does not fairly present, in all material respects, the System as designed and implemented;
- The controls related to the applicable C5 criteria were not suitably designed, in all material respects;
- In the case of a type 2 report, the controls tested did not operate effectively, in all material respects; or
- The auditor is unable to obtain sufficient appropriate evidence, the auditor's opinion shall be modified, and the audit report shall include a section with a clear description of all the reasons for the modification.

For each deviation noted regarding the description, the design of controls or their operation, the auditor shall consider the following procedures to determine whether the opinion needs to be modified:

- Inquiry of management of the cloud service provider regarding the root cause analysis of the identified deviation;
- Assessment of the cloud service provider's handling of the identified deviation;
- Assessment whether such deviations have been identified by the cloud service provider's monitoring activities and what corrective actions have been taken as a result thereof; and,
- Assessment whether compensating controls are suitably designed and, if mandated (type 2 report) operating effectively to address the risks arising from the deviation in such a way that the C5 criterion is still met with reasonable assurance. This concerns, for example, the assessment of alternative organisational and technical measures 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.

The procedures performed and the results thereof should be presented in the audit report, irrespective of the assessment as to whether the opinion needs to be modified. The information is intended to enable the specified parties to determine the effects of the deviation on their risk assessments.

The following additional information from the cloud service provider shall be added to 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 previous audit report, a reference to this report and an explanation as to why the deviation was not yet subject to effective corrective and preventive actions.

- Corrective and preventive action planned or taken to eliminate the causes of the deviation and to prevent the occurrence of such deviations in the future, including when these actions 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. The information shall be provided in a separately marked section of the audit report, e.g. 'Other Information Provided by the Cloud Service Provider' (cf. the following section 'Reporting').

3.4.13 Reporting

The reporting on an attestation engagement is based on the requirements of ISAE 3402.53. 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 shall include the following elements:

1. Independent Practitioner's Reasonable Assurance Report
    1. Scope

       In this section the auditor (practitioner) shall refer to the description and the management statement prepared by the cloud service provider.

       If the description refers to the need for complementary user entity controls, a statement that the auditor has not evaluated the suitability of design or operating effectiveness of complementary user entity controls, and that the applicable C5 criteria stated in the cloud service provider's description of its system can be met only if complementary user entity controls are suitably designed or operating effectively, along with the controls at the cloud service provider

       If services are performed by subservice organisation, the nature of activities performed by the subservice organisations as described in the cloud service provider's description of its System and whether the carve-out method or the inclusive method has been used in relation to them. Where the carve-out method has been used, a statement that the auditor's procedures did not extend to controls at the subservice organisation and, if presented in the description, that applicable C5 criteria stated in the cloud service provider's description of its system can be met only if complementary subservice organisation controls are suitably designed or operating effectively, along with the controls at the cloud service provider. Where the inclusive method has been used, a statement that the cloud service provider's description of its System includes the controls at the subservice organisations, and that the auditor's procedures extended to controls at the subservice organisations.
2. Cloud Service Provider's Responsibilities

   A statement that the cloud service provider is responsible for
    - preparing the description of its System and the management statement, including the completeness, accuracy, and method of presentation of the description and the statement;
    - providing the cloud services covered by the description;
    - selecting the applicable C5 criteria stated in the description;
    - identifying the risks that threaten the applicable C5 criteria from being met; and
    - designing, implementing, maintaining, monitoring and documenting the controls that are suitably designed, and, in case of type 2 report, operating effectively to meet the applicable C5 criteria stated in the description.
3. Independence and Quality Management

   A statement that the audit firm
    - complies with the independence and other ethical requirements of the International Code of Ethics for Professional Accountants (including Inter-

national Independence Standards) issued by the International Ethics Standards Board for Accountants (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour;
- applies the International Standard on Quality Management (ISQM) 1, or other professional requirements, or requirements in law or regulation, that are at least as demanding as ISQM 1; and
- adhered to the supplementary requirements on the qualifications of the engagement team as set forth in section 'Qualification of the Auditor' of this catalogue.

If the practitioner is not a public auditor or a public audit firm, the statement shall identify the professional requirements, or requirements in law or regulation, applied that are at least as demanding as the IESBA Code and ISQM 1.

4. Practitioner's Responsibility

   A statement that the practitioner's responsibility is to express an opinion on the cloud service provider's description, on the design of controls to meet the applicable C5 criteria and, in the case of a type 2 report, on the operating effectiveness of those controls, based on the practitioner's procedures.

5. Inherent limitations

   A statement of the limitations of controls and, in the case of a type 2 report, of the risk of projecting to future periods any evaluation of the operating effectiveness of controls.

6. Conclusion

   Practitioner's opinion in accordance with the objectives set forth in section 'Subject Matter and Objectives of the Audit' of this catalogue.

7. Restricted Use

   A statement on the specified parties considered as the intended users of the report. Specified parties in the context of this catalogue are user entities (customers and prospective customers), their independent auditors and practitioners providing services to such user entities and regulators, who have sufficient knowledge and understanding of the following:

   - Name, type and scope of cloud services provided;
   - The nature of the cloud services provided;
   - How the cloud service provider's System interacts with user entities, subservice organisations, and other parties;
   - Internal control and its limitations;
   - Complementary controls of user entities and how they interact with related controls at the cloud service provider to meet the applicable C5 criteria;
   - User entity responsibilities and how they may affect the user entity's ability to effectively use cloud services;
   - The criteria set out in this catalogue; and
   - The risks that may threaten the applicable C5 criteria from being met and how controls address those risks.

8. General Terms of Engagement

   Reference to the engagement terms, for professional accountants in Germany typically on the basis of the General Engagement Terms for German Public Auditors and Public Audit Firms. The section shall also disclose information on applicable liability regulations, which is considered to be an important information for the intended users of the report. 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 preformulated contractual conditions. In this context, a reference to a liability agreement shall be made in the report.

2. Management Statement

   Written statement by the cloud service provider's management in accordance with the requirements set forth in section 'Management Statement' of this catalogue.

3. Cloud Service Provider's Description of the System

   Presentation of the system of internal control relevant to the development and operation of the cloud in accordance with the requirements set forth in section 'Description Criteria' of this catalogue.

4. Cloud Service Provider's Controls, Practitioner's Test Procedures and Results

   Presentation of the cloud service provider's controls along the applicable C5 criteria, the practitioner's test procedures and the results thereof. The test procedures performed shall be described in both types of reports, not only in type 2 reports, but also type 1 reports. In its description of the test procedures the practitioner shall outline

   - The nature of the tests performed (e.g. inquiry, observation, inspection, or reperformance) in sufficient detail to enable the specified parties to determine the effect on their risk assessments. This shall include the title and role of cloud service provider personnel to whom inquiries were directed and abstract descriptions of the documents or electronic files to which the practitioner referred to obtain evidence.
   - The extent of testing, including whether the items tested represent all or a selection (sample) of the items in the population. While it is not required to list the number of items in the population and the sample sizes for each test procedure, the practitioner shall describe at least the general approach to determine the extent of testing, e.g. by disclosing the sample sizes for ranges of items in the population or the frequency of a control.

   The presentation of results may be limited to the statement 'No deviation noted'. If deviations have been identified, the auditor shall include the extent of testing performed that led to identification of the deviations (including the sample size where sampling has been used), and the number and nature of the deviations noted. The auditor shall report deviations even if, on the basis of tests performed, the auditor has concluded that the related c5 criteria were achieved.

5. Optional: Other information provided by the Cloud Service Provider

   The cloud service provider may use this section to present other information, e.g. management response to deviations noted (see section 'Deviation Handling') or mapping of controls to other standards. This information is not subject to the auditor's procedures, and, accordingly, the auditor does not issue an opinion on it.

In case of a direct engagement, the components 2 'Management statement' and 3 'Description of the cloud service provider's System' are omitted. Nevertheless, as stated in the section 'Description Criteria', the practitioner shall present the cloud service provider's System in all material aspects as part of the audit report so that the specified parties can obtain an appropriate understanding of the information security of the cloud service. Such information shall be provided in a separate section, e.g. 'Practitioner's Presentation of the Cloud Service Provider's System'.

3.5 Dealing with Revisions of this Criteria Catalogue

The BSI intends to revise and 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 their system of internal control and to the execution of the audit associated with revisions of this criteria catalogue.

The criteria in this criteria catalogue shall be applied for periods being assessed beginning on or after January 1st, 2027. Earlier adoption is permitted.

In the course of a specified period, it may happen that the evaluation of the suitability of the design or operating effectiveness of controls relates both to the status before and after the implementation of such adjustments. The cloud service provider's description of its system of internal control relevant to the development and operation of the cloud service shall include the adjustments made, as they are considered to be a significant change to the system of internal control (see section 'Description Criteria' of this catalogue). In the case of a direct engagement, the auditor shall obtain and disclose this information.

If the specified period ends in a period which is up to three months before January 1st, 2027, the cloud service provider shall provide additional information in the description of its system of internal control relevant to the development and operation of the cloud service which have not yet 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

The information on the general conditions of the cloud service - also called 'boundary conditions' or 'BC' for short - serves to provide customers with additional information on the level of information security offered by the cloud service. The information enables cloud service 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 applicable law, jurisdiction, partitions, regions, zones and locations

Information on the General Conditions of the Cloud service

In the description of the cloud service provider's system of internal control relevant to the development and operation of the cloud service and the contractual agreements (e.g. service level agreements), the cloud service provider clearly provides comprehensible and transparent information on:

- Its applicable law;
- Its jurisdiction;
- Its partitions, regions, zones and locations and
- System component locations, including its subcontractors, where the following data is processed, stored and backed up:
- cloud service customer data; and
- cloud service derived data;
- cloud service customer account data.

The scope of information is based on the requirements of subject matter experts of the cloud service 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

Definitions of ISO/IEC 22123-1:2023 apply for the listed types of data. If the processing, backup and storage of customer data takes place in different locations, zones or regions, this has 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 level agreements), 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 service customers to assess the cloud service against their business requirements.

The description of the cloud service provider's system of internal control relevant to the development and operation of the cloud service 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 description of the cloud service provider, the information itself may also be an optional part of the report, e.g. in a section 'Other information provided by the cloud service provider'. Only in the latter case, this information is not subject to the auditor's procedures, and, accordingly, the auditor does not issue an opinion on it.

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 service customers with comprehensible and transparent information on the following recovery parameters of the cloud service, if required:

- Maximum tolerable period of downtime (MTPD) and Recovery Time Objective (RTO);
- Maximum allowable data loss / Recovery Point Objective (RPO);
- Recovery time to start emergency operation;
- Minimum business continuity objective (MBCO) (capacity related to regular operation); and
- Restore time until normal operation.

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

The description of the cloud service provider's system of internal control relevant to the development and operation of the cloud service describes where this information can be found.

Supplementary Information - Notes on the General Conditions

In addition to the reference in the description of the cloud service provider, the information itself may also be an optional part of the report, e.g. in a section 'Other information provided by the cloud service provider'. Only in the latter case, this information is not subject to the auditor's procedures, and, accordingly, the auditor does not issue an opinion on it.

BC-04 Information on the availability of the data centre

Information on the General Conditions of the Cloud service

The cloud service provider provides subject matter experts of cloud service customers with comprehensible and transparent information on the availability of the data centres used to provide the cloud service (including data centres operated by service organisations), as needed. The information shows availability and downtime over one year according to industry standard classification schemes. The information enables cloud service 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; and
- 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; and
- AC 5: Disaster-tolerant.

The description of the cloud service provider's system of internal control relevant to the development and operation of the cloud service describes where this information can be found. In addition to the reference in the description of the cloud service provider, the information itself may also be an optional part of the report, e.g. in a section 'Other information provided by the cloud service provider'. Only in the latter case, this information is not subject to the auditor's procedures, and, accordingly, the auditor does not issue an opinion on it.

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

Information on the General Conditions of the Cloud service

In the description of the cloud service provider's system of internal control relevant to the development and operation of the cloud service, the cloud service provider provides comprehensible and transparent information on how investigation requests by government agencies for access to or disclosure of cloud service customer data are handled. The information includes the following aspects:

- Procedures to verify the legal basis of such requests;
- Procedures for informing and involving the affected cloud service customers upon receipt of such requests;
- The ability of the affected cloud service customers to object;
- Whether the cloud service provider stores cloud service customer data or cloud service derived data in unencrypted form;
- Whether the cloud service provider has the ability to decrypt cloud service customer data or cloud service derived data in case of such requests and how this ability for access or disclosure is used;
- The number of investigation requests for cloud service customer data or cloud service derived data and the countries from which these requests originate; and
- How often those requests resulted in the cloud service provider sharing cloud service customer data or cloud service derived data with the government agency.

The scope of the information corresponds to the needs of the subject matter experts of the cloud service 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).

Additional information on the technical procedures for data disclosure is to be communicated with cloud service customers according to INQ-05.

Supplementary Information - Notes on the General Conditions

The legal foundation on which these governmental services are based (e.g. law enforcement agencies, intelligence services) may vary from country to country. In

particular, the applicable jurisdiction at the locations where cloud service customer data and cloud service derived data is processed, stored and backed up 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 service 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 service 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 description of the cloud service provider's system of internal control relevant to the development and operation of the cloud service, 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;
- Certifications or reporting according to industry-specific requirements of cloud service customers; and
- Certifications or reporting related to environmental, social and governance standards (ESG).

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 service 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.

Examples for ESG reporting include reporting according to the EU Corporate Sustainability Reporting Directive (CSRD) and certifications such as ISO 50001, ISO 14001 and the German ecolabel Blue Angel.

Fulfilment of the Boundary Condition does not require the cloud service provider to hold a certification or attestation for all listed aspects.

BC-07 Use of AI in internal control system

Information on the General Conditions of the Cloud service

In the description of the cloud service provider's system of internal control relevant to the development and operation of the cloud service, the cloud service provider discloses which internal control activities significantly depend on the use of AI models. The information provided should include whether the AI model is trained internally or provided by a third party as well as how it is ensured that the model is secure, robust and effective.

Supplementary Information - Notes on the General Conditions

Reliance on AI is considered significant if the control cannot function as designed without it.

The cloud service provider may refer to AI standards, reports and certificates such as AIC4 from BSI or AICM from Cloud Security Alliance to communicate how it is ensured that the AI model is secure, robust and effective.

5 Basic Criteria, Additional Criteria, 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 Criteria

OIS-01.01B

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, zones, regions and procedures relevant to the development and operation of the cloud service.

OIS-01.02B

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

- Context of the cloud service provider;
- Scope of the ISMS (Section 4.3 of ISO/IEC 27001);
- Declaration of applicability (Section 6.1.3);
- Description of how the cloud service is covered by activities in the ISMS;
- Description of how the security of the cloud service is maintained and improved; and
- Results of the last management review (Section 9.3).

OIS-01.03B

Additionally, the cloud service provider documents the scope of the cloud service that is under the cloud service provider's control and the boundaries.

Additional (Sharpening)

–

Additional (Complementing)

OIS-01.01AC

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 Criteria

Applicable to: OIS-01.01B

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. The auditor has to evaluate whether the documentation meets the referenced requirements of the ISO standard. This does not require a full certification audit of the management system in accordance with ISO 17021, but a focused inspection of the related documentation.

Cross-sectional functions do not need to be integrated into a single ISMS. Instead, multiple ISMS can be es-

tablished to cover both service-related internal control systems and central functions effectively.

The scope of the ISMS may go beyond the scope of the cloud service provider's system of internal control for the cloud service in scope of an assurance engagement with this criteria catalogue. If the scope of the ISMS is broader than the scope of the assurance engagement, evidence to be obtained about the design and operation of the ISMS can be limited to records that are applicable to the cloud service in scope of the assurance engagement.

Supplementary Information - Complementary Customer Criteria

–

OIS-02 Information Security Policy

Basic Criteria

OIS-02.01B

Top management of the cloud service provider has adopted an information security policy.

OIS-02.02B

Top management of the cloud service provider has communicated the information security policy to internal and external employees as well as cloud service customers.

OIS-02.03B

The information security policy describes:

- The importance of information security, based on the requirements of cloud service customers in relation to information security;
- The security objectives and the desired security level, based on the business goals and activities as well as compliance obligations of the cloud service provider;
- The commitment of the cloud service provider to implement the security measures required to achieve the established security objectives;
- The most important aspects of the security strategy to achieve the security objectives set; and
- The organisational structure for information security in the scope of the ISMS.

OIS-02.04B

The cloud service provider reviews the information security policy in accordance with SP-02 on a regular basis and at least in the event of significant changes that are likely to affect the principles defined in the policy. The review process of the information security policy includes the approval and endorsement by top management.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: OIS-02.01B, OIS-02.02B

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.

Supplementary Information - Complementary Customer Criteria

–

OIS-03 Interfaces and Dependencies

Basic Criteria

OIS-03.01B

The cloud service provider establishes, documents, and communicates the Cloud Shared Security Responsibility Model (SSRM) to define and manage interfaces and dependencies between cloud service delivery activities performed by the cloud service provider and those performed by third parties.

OIS-03.02B

The SSRM documentation clearly defines the responsibilities between both parties for handling vulnerabil-

ities, 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).

OIS-03.03B

The cloud service provider regularly reviews and validates the SSRM documentation to ensure its accuracy and relevance for all cloud service offerings.

OIS-03.04B

The cloud service provider implements, operates, and assesses the SSRM components for which it is responsible, ensuring adherence to the defined security measures.

OIS-03.05B

The communication of changes to the SSRM, 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.

OIS-03.06B

By maintaining an up-to-date and clearly communicated SSRM, the cloud service provider ensures a comprehensive understanding of security responsibilities, fostering a secure and reliable cloud environment for all stakeholders.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: OIS-03.01B, OIS-03.05B

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

Applicable to: OIS-03.01B, OIS-03.02B, OIS-03.03B, OIS-03.04B, OIS-03.05B, OIS-03.06B

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

The cloud service provider can present the underlying Shared Responsibility Model of their cloud service in the guidelines and instructions to help cloud service customers understand their roles and responsibilities in terms of security and operational management.

Supplementary Information - Complementary Customer Criteria

Cloud service 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.

OIS-04 Segregation of Duties

Basic Criteria

OIS-04.01B

Conflicting tasks and responsibilities are segregated based on a risk assessment in accordance with OIS-07 to reduce the risk of unauthorised or unintended changes or misuse of cloud service customer data, cloud service derived data and cloud service provider data. 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. IAM-01);
- Development, testing and release of changes (cf. DEV-01); and
- Operation of the system components.

OIS-04.02B

The cloud service provider implements the mitigating measures defined in the risk treatment plan, prioritising segregation of duties.

OIS-04.03B

If segregation 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.

OIS-04.04B

The cloud service provider introduces and maintains an inventory of conflicting tasks and responsibilities, including resolving measures and enforces the segregation of duties during the assignment or modification of roles as part of the role management process.

Additional (Sharpening)

–

Additional (Complementing)

OIS-04.01AC

The cloud service provider monitors and enforces measures related to segregation of duties to resolve conflicting roles.

OIS-04.02AC

Any deviations identified during monitoring are addressed through timely and appropriate remediation measures.

Supplementary Information

About the Criteria

Applicable to: OIS-04.01B

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

Supplementary Information - Complementary Customer Criteria

–

OIS-05 Threat Intelligence

Basic Criteria

OIS-05.01B

The cloud service provider collects information from selected internal and external sources to gain a comprehensive view of the threat landscape that lead to cybersecurity risks.

OIS-05.02B

The collected information is correlated and analysed to identify its potential impact on the cloud service provider's organisation.

OIS-05.03B

The threat intelligence insights are included in the risk management process (cf. OIS-07 and OIS-08) to ensure that the current internal and external threats are reflected in risk handling measures.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

OIS-06 Contact with Relevant Government Agencies and Interest Groups

Basic Criteria

OIS-06.01B

If the cloud service is used by public sector organisations in Germany, the cloud service provider establishes and maintains contacts with the National IT Situation Centre and the CERT Association of the BSI.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: OIS-06.01B

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

Supplementary Information - Complementary Customer Criteria

–

OIS-07 Risk Management Policy

Basic Criteria

OIS-07.01B

Policies and instructions for risk management procedures are documented, communicated and provided in accordance with SP-01. Risk management procedures are based on a risk assessment methodology that enables reproducibility and comparability for the following aspects:

- Identification of cybersecurity risks and other 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 risk handling;
- Treatment of risks through measures, including approval of authorisation and acceptance of residual risks by risk owners;
- Documentation of the activities implemented to enable consistent, valid and comparable results; and
- Conducting a review of the risk assessment and status of risk treatment plans by the management responsible for the security of the cloud service.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: OIS-07.01B

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

Supplementary Information - Complementary Customer Criteria

–

OIS-08 Application of the Risk Management Policy

Basic Criteria

OIS-08.01B

The cloud service provider executes the process for handling risks as needed or at least once a year.

OIS-08.02B

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 cloud service customer data and cloud service derived data 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 and accidentally exposed interfaces;
- Conflicting tasks and areas of responsibility that cannot be separated for organisational or technical reasons;
- Dependencies on subservice organisations;
- An encryption and key management risk programme which addresses the risks of unauthorised disclosure, modification, destruction, or information loss of cryptographic keys; and
- Segregation of cloud users and their data within systems, networks and storage.

OIS-08.03B

The cloud service provider implements the policies and procedures covering risk assessments on the entire cloud service.

OIS-08.04B

The results of the risk assessments are made available to relevant internal parties.

OIS-08.05B

Information, specific for their purposes, is made available to relevant external parties.

OIS-08.06B

The analysis, evaluation and treatment of risks, including the approval of actions and acceptance of residual risks, is reviewed by the risk owners for adequacy at least annually, and after each significant change that may affect the security of the cloud service.

OIS-08.07B

The cloud service provider monitors the evolution of the risk and reviews the risk assessments accordingly.

OIS-08.08B

The cloud service provider prioritises the risk treatment according to the level of cyber risks related to the cloud service.

OIS-08.09B

The cloud service provider documents and implements a risk treatment plan based on the risk assessment (OIS-07).

OIS-08.10B

The risk treatment plan reduces the risk level to a residual risk acceptable to the risk owners.

OIS-08.11B

The risk treatment plan is made available to relevant internal parties, including appropriately summarised and abstracted versions.

OIS-08.12B

The cloud service provider determines if relevant external parties shall receive information, specific to their purposes, about the risk treatment plan and to what extent this should happen.

OIS-08.13B

The risk treatment plan is reviewed by the cloud service provider every time the risk assessment is modified and formally accepted by the risk owners.

OIS-08.14B

If the cloud service provider shares risks with the cloud service customers, the shared risks are associated with complementary customer controls and described in the user documentation.

Additional (Sharpening)

–

Additional (Complementing)

OIS-08.01AC

The cloud service provider integrates information security risks into a documented Enterprise Risk Management (ERM) programme which addresses the following aspects:

- Integration of information security risks at the enterprise level to promote information security risk-awareness across the entire organisation;
- Leadership awareness and support for identification, analysis and treatment of information security risks to foster continuous improvement;
- Consideration of the cloud service provider's strategic objectives when managing risks to align risk treatment with the organisation's goals; and
- Review of information security risks at least on an annual basis.

Supplementary Information

About the Criteria

Applicable to: OIS-08.01B, OIS-08.02B, OIS-08.03B, OIS-08.04B, OIS-08.05B, OIS-08.06B, OIS-08.07B, OIS-08.08B, OIS-08.09B, OIS-08.10B, OIS-08.11B, OIS-08.12B, OIS-08.13B, OIS-08.14B

This criterion applies only to risks that reside within the area of responsibility of the cloud service provider. Risks that arise for the cloud service 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)'.

Applicable to: OIS-08.02B

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

When determining protection needs of customer data, regulatory requirements applicable to customer data should be considered such as PCI-DSS, HIPAA, DORA (regulation on digital operational resilience for the financial sector and amending regulations), NIS 2 Directive and KRITIS.

Supplementary Information - Complementary Customer Criteria

–

OIS-09 Information Security in Project Management

Basic Criteria

OIS-09.01B

Information security is considered in project management. The cloud service provider performs a risk assessment according to OIS-07 and, if necessary, proceeds with risk treatment to assess and treat the risks on all projects that may affect the provision of the cloud service, regardless of the nature of the project.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

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 Criteria

SP-01.01B

Policies and instructions (incl. concepts and guidelines) are derived from the information security policy and are documented according to a uniform structure. 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 service customers and subservice organisations);
- Steps for the execution of the security strategy; and
- Applicable legal and regulatory requirements.

SP-01.02B

The policies and instructions are communicated and made available to all internal and external employees of the cloud service provider in an appropriate manner.

SP-01.03B

The policies and instructions are subject to version control.

SP-01.04B

The policies and instructions are approved by the top management of the cloud service provider or an authorised body.

SP-01.05B

The responsible business units of the cloud service provider shall report at least annually to the top management on the policies and instructions and their implementation. This reporting includes at least:

- Implemented changes to address cybersecurity risks for the topic addressed in the policy or instruction;
- Information security incidents for the topic addressed in the policy or instruction and the follow-up;
- Performance of the internal controls regarding information security for the topic addressed in the policy or instruction (cf. COM-04); and
- Planned changes for the topic addressed in the policy or instruction to address cybersecurity risks and information security and cybersecurity.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: SP-01.01B

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

- Risk Management Policy (OIS-07);
- Policy for Remote Working (HR-07);
- Asset Management Concept (AM-01);
- Acceptable Use and Safe Handling of Assets Policy (AM-05);
- Policy for Removable Media and Endpoint Devices (AM-12);
- Physical Security and Environmental Control Requirements (PS-01);
- Physical Site Access Control (PS-04);
- Workplace Security Requirements (PS-08);
- Protection Against Malware - Concept (OPS-04);
- Data Backup and Recovery - Concept (OPS-06);
- Logging and Monitoring - Concept (OPS-10);
- Logging and Monitoring - Metadata Management Concept (OPS-11);
- Managing Vulnerabilities - Concept (OPS-18);
- Managing Incidents and Crashes - Concept (OPS-19);
- Separation of Datasets - Guideline (OPS-28);
- Confidential Computing - Policies and Instructions (OPS-30);
- Guideline for Container Management (OPS-32);
- Managing Vulnerabilities - Patch Management (OPS-33);
- Policy for User Accounts and Access Rights (IAM-01);
- Authentication Mechanisms (authentication policy) (IAM-09);
- Policy for the Use of Cryptographic Mechanisms (CRY-01);
- Technical Safeguards (COS-01);
- Policies for Data Transmission (COS-08);

- Policies for Changes to System Components (DEV-03);
- Development Service Organisations Security (policies and instructions for the use of third party and open source software) (DEV-14);
- Policies and Instructions for Controlling and Monitoring Service Organisations (SSO-01);
- Controlling Exchanges with Suppliers of Functional Components (SSO-08);
- Policy for Security Incident Management (SIM-01);
- Business Continuity and Emergency Management System (BCM-01);
- Policy for Business Continuity Management (BCM-05);
- Policy for Planning and Conducting Audits (COM-02); and
- Communication of Technical Procedures for Data Disclosure in Investigation Requests (INQ-05).

Applicable to: SP-01.02B

The appropriateness of the demand-oriented communication and provision should 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; and
- Form of provision.

Supplementary Information - Complementary Customer Criteria

–

SP-02 Review and Approval of Policies and Instructions

Basic Criteria

SP-02.01B

Information security policies and instructions are reviewed for adequacy by the cloud service provider's subject matter experts at least annually, and when significant changes may affect the security of the cloud service. 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.

SP-02.02B

Revised policies and instructions are approved by the appropriate level of management before they become effective and are communicated and made available to internal and external employees.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

SP-03 Exceptions from Existing Policies and Instructions

Basic Criteria

SP-03.01B

The cloud service provider maintains a list of exceptions to the policies and instructions for information security, including associated controls.

SP-03.02B

Exceptions to the policies and instructions for information security as well as respective controls go through risk management procedures in accordance with OIS-07, including approval of these exceptions and acceptance of the associated risks by the risk owners.

SP-03.03B

The approvals of exceptions are documented.

SP-03.04B

The approvals of exceptions are limited in time.

SP-03.05B

The approvals of exceptions are reviewed for appropriateness at least annually by the risk owners.

SP-03.06B

Exceptions leading to a nonconformity to any of the certification requirements of a certified cloud service are not allowed.

Additional (Sharpening)

–

Additional (Complementing)

SP-03.01AC

The exceptions to policies or instructions are approved by the appropriate level of management who approved the policies or instructions.

SP-03.02AC

The list of exceptions is monitored to ensure that the approved exceptions have not expired and that all reviews and approvals are up-to-date.

SP-03.03AC

Any exceptions for which deviations were identified during monitoring are addressed through timely and appropriate remediation measures.

Supplementary Information

About the Criteria

Applicable to: SP-03.01B, SP-03.02B, SP-03.03B, SP-03.04B, SP-03.05B, SP-03.06B, SP-03.01AC, SP-03.02AC, SP-03.03AC

Exceptions in the sense of the 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 service customer; and
- A system component lacks technical properties to configure it according to the applicable requirements.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure through suitable controls 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.

5.3 Personnel (HR)

Objective: 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.

HR-01 Verification of Qualification and Trustworthiness

Basic Criteria

HR-01.01B

The cloud service provider identifies which roles within the organisation can access cloud service customer data, cloud service derived data, cloud service provider data, account data or system components under the cloud service provider's responsibility that provide the cloud service in the production environment.

HR-01.02B

The competency and integrity of all internal and external employees to which these roles are assigned is verified prior to employment. The verification considers the following measures, to the extent permitted by local legislation and regulation and as considered appropriate by the cloud service provider to mitigate risks related to inappropriate access to the respective data type:

- Verification of the person's identity via identity card or passport;
- Verification of professional experience through the CV;
- Verification of academic titles and degrees;
- Request for a certificate of good conduct, police clearance or other national equivalents; and
- Evaluation of susceptibility to blackmail.

HR-01.03B

The cloud service provider follows-up changes in work-related personal situations and identifies and mitigates related risks.

HR-01.04B

The cloud service provider assesses the competence and integrity of its personnel before commencement of employment in a position with a higher risk classification than their current position within the company.

HR-01.05B

The extent of the assessment defined in this requirement is proportional to the business context, the sensitivity of the information that will be accessed by the personnel, and the associated risks.

Additional (Sharpening)

–

Additional (Complementing)

HR-01.01AC

The cloud service provider reviews annually their assessment of the competence and integrity of its personnel for the individuals in positions with the highest levels of risk classification, starting at a level to be defined in the human resource policy.

Supplementary Information

About the Criteria

Applicable to: HR-01.02B

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 service organisations who perform activities according to the service organisation's own processes and procedures are not covered by this criterion.

Permissible verifications of competency and integrity may vary based on local law as well as the role of the employee. Depending on these factors and the nature of the checks conducted, explicit consent by the employee may be necessary.

The verification of qualification and trustworthiness can be supported by specialised service providers or be based on voluntary self-disclosure of the employee. Depending on national legislation, national equivalents of the German certificate of good conduct ('Führungszeugnis') may also be permitted. Assessing the vulnerability of a potential employee to blackmail can involve evaluating their creditworthiness. However, this assessment may only be legally permissible for positions with significant financial responsibility, depending on local regulations.

Risks related to inappropriate access to cloud service customer data may be mitigated by the use of encryption or monitoring system access for suspicious events. Although such measures are not supposed to completely substitute the above-mentioned verification measures, the extent of such measures may be reduced.

Supplementary Information - Complementary Customer Criteria

–

HR-02 Employment Terms and Conditions

Basic Criteria

HR-02.01B

The cloud service provider's internal and external employees are required by employment terms and conditions to comply with the information security policy, the policies, procedures and instructions based on it, and the code of ethics.

HR-02.02B

The cloud service provider ensures that the terms for all internal and external employees include a non-disclosure provision. The non-disclosure provision covers any information that has been obtained or generated as part of the cloud service, even if anonymised and decontextualised.

HR-02.03B

The cloud service provider gives a presentation of the information security policy, the policies, procedures and instructions based on it and the code of ethics.

HR-02.04B

The cloud service provider requires the information security policy, the policies, procedures and instructions based on it and the code of ethics to be acknowledged by the internal and external personnel in a documented form before access is granted to any cloud service customer data, cloud service derived data, cloud service provider data and account data or system components under the responsibility of the cloud service provider used to provide the cloud service in the production environment.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

HR-03 Security Training and Awareness Programme

Basic Criteria

HR-03.01B

The cloud service provider operates a target group-oriented security awareness and training programme.

HR-03.02B

All internal and external employees of the cloud service provider undergo a role-based programme at least annually, and when changing target group, taking into consideration at least their position's risk classification and technical duties.

HR-03.03B

The programme is regularly updated based on changes to policies and instructions and the current threat situation and includes the following aspects insofar as they are applicable to each employee's role:

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

Additional (Sharpening)

–

Additional (Complementing)

HR-03.01AC

The cloud service provider monitors the completion of the security awareness and training programme.

HR-03.02AC

Any deviations identified during monitoring are addressed through timely and appropriate remediation measures.

HR-03.03AC

The learning outcomes achieved through the awareness and training programme are measured and evaluated in a target group-oriented manner.

HR-03.04AC

The measurements cover quantitative and qualitative aspects.

HR-03.05AC

The results are used to improve the awareness and training programme.

Supplementary Information

About the Criteria

Applicable to: HR-03.03AC

The measurement and evaluation of learning outcomes in a target group-oriented manner, as specified by the additional criterion, do not require assessing each employee individually. Instead, evaluations can be performed at an aggregated level, focusing on the overall effectiveness of the training program for specific target groups. This approach allows for the identification of trends and areas for improvement within the program while respecting employees' privacy requirements.

Supplementary Information - Complementary Customer Criteria

–

HR-04 Disciplinary Measures

Basic Criteria

HR-04.01B

The cloud service provider classifies information of security-sensitive positions according to their level of risk, including positions related to IT administration and all positions with access to cloud service customer data or system components for the provisioning of the cloud service in the production environment.

HR-04.02B

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.

HR-04.03B

The internal and external employees of the cloud service provider are informed about possible disciplinary measures.

HR-04.04B

The use of disciplinary measures is appropriately documented.

Additional (Sharpening)

–

Additional (Complementing)

HR-04.01AC

In case of a security breach, the cloud service provider is prepared to inform affected cloud service customers about the disciplinary actions taken against involved personnel, if requested by the customers.

Supplementary Information

About the Criteria

Applicable to: HR-04.02B

The cloud service provider ensures that the policies and instructions reflect applicable legal and regulatory requirements in accordance with SP-01.

Applicable to: HR-04.04B

With regards to the use of disciplinary measures, the submission of anonymised evidence is acceptable and does not imply that the basic criterion is not fully fulfilled.

Supplementary Information - Complementary Customer Criteria

–

HR-05 Responsibilities in the Event of Termination or Change of Employment

Basic Criteria

HR-05.01B

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.

HR-05.02B

The cloud service provider applies a specific procedure to revoke the access rights and to process the identities and assets of internal and external employees appropriately when their engagement is terminated or changed. This procedure includes defining specific roles and responsibilities as well as a documented checklist of all required steps.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: HR-05.01B

The cloud service provider ensures that the employment terms and conditions reflect applicable legal and regulatory requirements in accordance with SP-01.

Supplementary Information - Complementary Customer Criteria

–

HR-06 Non-disclosure Agreements

Basic Criteria

HR-06.01B

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.

HR-06.02B

The agreements are to be accepted by external service providers and suppliers when the contract is agreed.

HR-06.03B

The agreements are to be accepted by internal employees of the cloud service provider before authorisation to access cloud service customer data, cloud service derived data, cloud service provider data and account data is granted.

HR-06.04B

The requirements are 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.

HR-06.05B

The cloud service provider informs the internal employees, external service providers and suppliers and obtains confirmation of the updated confidentiality or non-disclosure agreement.

HR-06.06B

In instances where agreement on the updates cannot be reached, the cloud service provider shall assess the resulting risks to information security according to OIS-07.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: HR-06.01B

A non-disclosure agreement should cover:

- Which information or data types 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.

Applicable to: HR-06.02B, HR-06.03B, HR-06.05B

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

Supplementary Information - Complementary Customer Criteria

–

HR-07 Policy for Remote Working

Basic Criteria

HR-07.01B

Policies and instructions for the protection of information when employees work remotely are documented, communicated and provided in accordance with SP-01 and address the following aspects:

- Assessment of the security of remote working locations;
- Establishing guidelines for the safe handling and storage of sensitive information and data types;
- Definition of remote access security requirements;
- Utilisation of secure communication methods and enforcement of secure network use; and
- Provision of organisation-approved equipment and prohibition of unregulated personal devices.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

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 Management Concept

Basic Criteria

AM-01.01B

An asset management concept is documented, communicated and provided according to SP-01, in which the following aspects are described:

- Identification of assets which are used to provide the cloud service in the production environment;
- Definition of a scheme for identifying protection requirements based on information processed on the asset;

- Definition of asset types, considering at a minimum the differentiation of hardware and software objects;
- Definition of asset lifecycles based on the asset type; and
- Definition of procedures for inventory of hardware and software assets.

Additional (Sharpening)

–

Additional (Complementing)

AM-01.01AC

The information collected about assets is considered in logging and monitoring applications 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 service customers in accordance with contractual agreements.

AM-01.02AC

The cloud service provider monitors the process that is maintaining the inventory of assets to assure this inventory is up-to-date.

Supplementary Information

About the Criteria

Applicable to: AM-01.01B, AM-01.01AC, AM-01.02AC

Assets within the meaning of this domain 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
- End user 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, depending on the asset type:

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

Supplementary Information - Complementary Customer Criteria

–

AM-02 Asset Inventory

Basic Criteria

AM-02.01B

The cloud service provider maintains an asset inventory of hardware and software assets in accordance with the asset management concept.

AM-02.02B

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.

AM-02.03B

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.

AM-02.04B

Changes to the recorded information are logged.

AM-02.05B

The inventory system maintained by the cloud service provider can provide a detailed list of all users who have access to a specific resource, along with their respective access rights.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: AM-02.01B, AM-02.02B, AM-02.03B, AM-02.04B, AM-02.05B

Cloud service providers who procure their cloud infrastructure as virtual infrastructure from subservice providers (e.g. virtual machines or containers) may use tools provided by the subservice provider to inventory those assets, insofar as the cloud service provider deems these suitable based on their asset management concept.

Supplementary Information - Complementary Customer Criteria

–

AM-03 Hardware Asset Inventory

Basic Criteria

AM-03.01B

The hardware asset inventory maintained by the cloud service provider includes the following details for each entry:

- Identification details (such as name, IP address, MAC address, etc.);
- The function of the asset;
- The model of the asset;
- The location of the asset;
- The owner of the asset; and
- Information security requirements for the asset.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: AM-03.01B

An 'Asset Owner' is an individual or role assigned with the responsibility and accountability for managing and protecting an organisation's asset and does not imply legal ownership of the assets.

If cloud service customers operate virtual machines or containers with the cloud service, the cloud service provider should inventory the containers and document their life cycle (cf. OPS-32)

Supplementary Information - Complementary Customer Criteria

–

AM-04 Software Asset Inventory

Basic Criteria

AM-04.01B

The cloud service provider maintains a comprehensive inventory of all software assets, including used software. This inventory includes the following details for each software asset:

- Identification details (such as name, IP address, MAC address, etc.);
- The version of the software; and
- The devices on which the software is installed.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

AM-05 Policy for the proper and secure use of assets

Basic Criteria

AM-05.01B

Policies and instructions for the proper and secure use 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 cloud service customer data, cloud service derived data, cloud service provider data and account data as well as 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;
- Complete and irrevocable deletion of the data upon decommissioning; and
- Secure handling and usage of removable media, e.g. by specifying which devices are permitted to interact with removable media and what data can be stored on them or by banning the reuse of removable media.

AM-05.02B

The applicability of these aspects is defined based on the cloud service provider's asset management concept (cf. AM-01).

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

AM-06 Commissioning of Hardware

Basic Criteria

AM-06.01B

The cloud service provider has implemented an approval process for commissioning hardware used to provide the cloud service in the production environment. This process involves identifying, analysing, and mitigating any risks (cf. OIS-07) associated with the commissioning.

AM-06.02B

Approval is granted after verification of the secure configuration of the mechanisms for error handling, log-

ging, encryption, authentication and authorisation according to the intended use and based on the applicable policies.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: AM-06.01B, AM-06.02B

The 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.

Supplementary Information - Complementary Customer Criteria

–

AM-07 Decommissioning of Hardware

Basic Criteria

AM-07.01B

The cloud service provider defines, documents and implements a procedure for the decommissioning of hardware used to operate system components supporting the cloud service production environment under the responsibility of the cloud service provider. As part of this procedure, approval by authorised personnel of the cloud service provider based on the applicable policies is required.

AM-07.02B

The decommissioning includes the complete and permanent deletion of all cloud service customer data, cloud service derived data, cloud service provider data and account data or proper destruction of the media. However, account data is only to be deleted if the data is located in the production environment for the operation of system components.

Additional (Sharpening)

–

Additional (Complementing)

AM-07.01AC

The cloud service provider requires approval for the disposal of any hardware used outside the organisation's premises.

AM-07.02AC

Additionally, the destruction of data on such hardware is carried out in a manner that ensures that data recovery is impossible.

Supplementary Information

About the Criteria

Applicable to: AM-07.02B, AM-07.02AC

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.

Supplementary Information - Complementary Customer Criteria

–

AM-08 Commitment to Proper Use, Safe and Secure Handling and Return of Assets

Basic Criteria

AM-08.01B

The cloud service provider determines in a risk assessment (cf. OIS-07) if loss of or unauthorised access to assets could compromise the information security of the cloud service. If so, the cloud service provider's internal and external employees are provably committed to the policies and instructions for proper use and

safe and secure handling of assets before they can be used.

AM-08.02B

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

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: AM-08.01B, AM-08.02B

The criterion essentially concerns mobile devices (e.g. notebooks, tablets, smartphones, etc.), especially if confidential information is stored on them that 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).

Supplementary Information - Complementary Customer Criteria

–

AM-09 Asset Classification and Labelling

Basic Criteria

AM-09.01B

Assets are classified and, if possible, labelled. Classification and labelling of an asset reflect the protection needs of the category of cloud service customer data, cloud service derived data, cloud service provider data and account data it processes, stores, or transmits.

AM-09.02B

Classification levels are reviewed at least annually and updated, where appropriate.

AM-09.03B

The need for protection is determined by the individuals or groups responsible for the assets of the cloud service provider according to a uniform and documented classification schema.

AM-09.04B

The classification schema provides levels of protection for the confidentiality, integrity, availability, and authenticity protection objectives. These protection objectives are aligned with delivery and recovery objectives set out in business and disaster recovery plans.

Additional (Sharpening)

–

Additional (Complementing)

AM-09.01AC

All physical assets are uniquely identified. This unique identification of devices serves as an additional method for connection authentication.

AM-09.02AC

Device identification is integrated into the asset classification and labeling processes.

AM-09.03AC

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.

AM-09.04AC

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 Criteria

Applicable to: AM-09.01B, AM-09.02B, AM-09.03B, AM-09.04B

If the cloud service provider does not categorize the assets specifically, then all assets may be treated as requiring the highest level of protection needs.

Applicable to: AM-09.01AC

To ensure that all physical assets are uniquely identified, the cloud service provider may implement practices such as:

- Use of a centralised device management platform to monitor and control all devices;
- Assigning unique identifiers (e.g. MAC addresses, serial numbers) to all devices; and
- Use of automated mechanisms to register connecting devices.

Supplementary Information - Complementary Customer Criteria

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

Cloud service customers ensure through suitable controls 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.

AM-10 Protection of Hardware on Hold

Basic Criteria

AM-10.01B

The cloud service provider has documented and implemented a procedure for protecting hardware that is temporarily not in use. The procedure ensures that inactive hardware is stored securely and protected against unauthorised access or damage until it is needed again.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

AM-11 Transfer of Hardware

Basic Criteria

AM-11.01B

The cloud service provider ensures the secure and controlled transfer of hardware used in the cloud service production environment to an offsite or alternate location.

AM-11.02B

The transfer of hardware is authorised by designated personnel.

AM-11.03B

The transfer of hardware is conducted using secure methods to prevent unauthorised access, tampering, or loss during transit.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

AM-12 Policy for Removable Media and Endpoint Devices

Basic Criteria

AM-12.01B

Policies and instructions for endpoint devices and removable storage media are documented, communicated and provided in accordance with SP-01 regarding the following aspects:

- The use of removable media is forbidden except for unavoidable essential system administration actions, and then only in the event that no other mechanism is possible;
- Use of removable media is dedicated to a single specific purpose;
- The decision to use removable media is documented;
- Storage encryption is enabled on managed endpoints and removable storage media to protect information from unauthorised disclosure;
- Managed endpoints are configured with anti-malware detection and prevention technology and services;
- Self-execution from removable storage is disabled and storage media is scanned before use on the cloud service provider's systems;
- Measures are to be taken by users to protect mobile endpoints and removable storage in transit and in storage;
- Protection during the transfer of any equipment containing cloud service customer data off-site for disposal to guarantee that the level of protection in terms of confidentiality and integrity of the assets during their transport is equivalent to that on the site;
- Sharing equipment containing media with data (including cloud service customer data and cloud service derived data) with a third party only if the data (including cloud service customer data and cloud service derived data) stored on it is encrypted in accordance with CRY-05 or has been destroyed beforehand using a secure deletion mechanism;
- Users are to use mobile endpoints and removable storage in a secure manner, this includes for example not leaving media openly accessable in public spaces, using screen locks and screen privacy films; and
- Measures for maintaining proper security of third party endpoints with access to organisational assets are to be defined.

Additional (Sharpening)

–

Additional (Complementing)

AM-12.01AC

Policies and instructions for endpoint devices and removable storage media shall furthermore contain the following aspects:

- Managed endpoints are configured with appropriate software firewalls;
- Managed endpoints are configured with Data Loss Prevention (DLP) technologies and rules in accordance with a risk assessment (cf. OIS-07);
- Remote geo-location capabilities are enabled for all managed mobile endpoints; and
- Define, implement and evaluate processes, procedures and technical measures to enable the deletion of company data remotely on managed endpoint devices.

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

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 Criteria

PS-01.01B

The cloud service provider defines and documents at least two security areas, with at least one sensitive area covering sensitive activities such as the buildings and premises hosting the information system for the provision of the cloud service, and at least one public area covering all remaining buildings and premises, not covered by other security areas.

PS-01.02B

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.

PS-01.03B

Security requirements for data centres are based on criteria in accordance with established rules of technology and the criteria PS-02 to PS-07. They are suitable for addressing the following risks in accordance with the applicable legal and contractual requirements:

- Faults in planning;
- Unauthorised access;
- Insufficient surveillance;
- Lightning and overvoltage (aligned with the internationally harmonised standards of IEC 62305);
- Fire and smoke;
- Unwanted water;
- Failures and/or unavailable telecommunications;
- Power failure; and
- Heating, ventilation, airconditioning (HVAC) and filtration.

PS-01.04B

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

PS-01.05B

If the cloud service provider operates the cloud service in data centres operated by service organisations, the document describes the complementary subservice organisation controls (CSOC) expected at the service organisations and the measures for monitoring the design and operation of controls at the service organisations with respect to these CSOC (cf. SSO-05).

PS-01.06B

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 (Sharpening)

–

Additional (Complementing)

PS-01.01AC

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.

PS-01.02AC

The time limits for self-sufficient operation provide for at least 72 hours in the event of a failure of the external power supply.

PS-01.03AC

For a self-sufficient operation during a heat period, the highest outside temperatures measured to date at the three nearest official measurement stations around the locations of the premises and buildings have been determined with a safety margin of 3 K.

PS-01.04AC

The security requirements stipulate that the permissible operating and environmental parameters of the cooling supply shall also be maintained on at least five consecutive days with these outside temperatures including the safety margin (cf. PS-06).

PS-01.05AC

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.

Supplementary Information

About the Criteria

Applicable to: PS-01.01B, PS-01.02B, PS-01.03B, PS-01.04B, PS-01.05B, PS-01.06B, PS-01.01AC, PS-01.02AC, PS-01.03AC, PS-01.04AC, PS-01.05AC

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.

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

Premises and buildings in which no data from cloud service customers is processed or stored (e.g. offices of the cloud service provider, server rooms with system components for internal development and test systems) adhere to requirements specifically covered under PS-08.

Applicable to: PS-01.05B, PS-01.05B

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

Applicable to: PS-01.03B

The recognised established rules of technology are defined in relevant standards, e.g. EN 50600 (facilities and infrastructures of data centres). Note for German readers: The German version of C5 uses the term *Stand der Technik* for established rules of technology although the German reader might expect the term *state of the art*. Without discussing the semantic, please note that *state of the art* defines a higher level than *Stand der Technik* and therefore *established rules of technology* is used here.

Applicable to: PS-01.01AC

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).

Applicable to: PS-01.02AC

The 72-hour timeframe for self-sufficient operation aligns with guidelines for government agencies, businesses and critical infrastructure operators (KRITIS) as per the Federal Office for Civil Protection and Disaster Assistance (BBK).

Supplementary Information - Complementary Customer Criteria

–

PS-02 Redundancy Model

Basic Criteria

PS-02.01B

The cloud service is provided from at least two locations that provide each other with operational redundancy and resilience. The locations meet the security requirements of the cloud service provider (cf. PS-01) and are located in an adequate distance to each other to achieve operational redundancy.

PS-02.02B

Operational redundancy is designed in a way that ensures that the availability requirements specified in the service level agreement are met.

PS-02.03B

The functionality of the redundancy is checked at least annually by suitable tests and exercises (cf. BCM-04).

Additional (Sharpening)

PS-02.01AS, sharpening PS-02.01B

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.

PS-02.02AS, sharpening PS-02.02B

The georedundancy is designed in a way that ensures that the availability requirements specified in the service level agreement are met.

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: PS-02.01B, PS-02.02B

Operational redundancy of the sites to each other in the sense of this criterion 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.

There are cloud service 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 3.4.8) of the criterion. The tests and exercises on functionality required in the criterion also apply analogously to resilient architectures.

Applicable to: PS-02.01AS, PS-02.02AS

A georedundancy of the sites to each other in the sense of this criterion 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 von Rechenzentren' provides assistance in this regard.

Supplementary Information - Complementary Customer Criteria

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

PS-03 Perimeter Protection

Basic Criteria

PS-03.01B

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).

PS-03.02B

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

PS-03.03B

The outer doors, windows and other construction elements exhibit an appropriate security level and withstand a break-in attempt for at least ten minutes.

PS-03.04B

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

PS-03.05B

If any construction element on its own does not fully meet the associated requirements, additional security measures are implemented to restore the appropriate security level.

PS-03.06B

Data centre personnel are trained on how to respond effectively to attempts of unauthorised ingress or egress attempts.

Additional (Sharpening)

–

Additional (Complementing)

PS-03.01AC

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

Supplementary Information

About the Criteria

Applicable to: PS-03.02B

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

Applicable to: PS-03.03B, PS-03.04B

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

Applicable to: PS-03.05B

Compensating measures can include additional security layers (e.g. security areas) on the premise, an increased presence of security personnel, video surveillance and anti-burglary systems.

Supplementary Information - Complementary Customer Criteria

–

PS-04 Physical Site Access Control

Basic Criteria

PS-04.01B

Preventive and detective physical access controls in premises and buildings related to the cloud service provided are implemented. They are in accordance with the cloud service provider's security requirements (cf. PS-01) and based on the principles defined in IAM-01 to prevent unauthorised access. They are documented and communicated 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. IAM-02) based on the principle of least authorisation ('least-privilege-principle') and as necessary for the performance of tasks ('need-to-know-principle');
- Revocation of access authorisations if they have not been used for a period of 2 months. Exceptions are only made for well-founded individual cases and follow a defined exception process according to SP-03;
- Authentication with at least one factor for access to any non-public area;
- Two-factor authentication for access to areas hosting system components that process cloud service customer data;
- 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 by employees who authorise or deny their actions, and question them if needed about their actions;
- 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;
- Physical access control derogations in case of emergency, including an analysis procedure after every use of these derogations; and
- Measures to identify individuals who are not part of the personnel, incorporating them into the access policy system and defining the conditions, if any, under which they may be granted access to the premises.

PS-04.02B

At the entrance of applicable non-public perimeters, the cloud service provider displays a warning concerning the limits and access conditions to the corresponding areas.

PS-04.03B

Physical access controls are supported by an access control system.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: PS-04.01B

For implementing access control based on the need-to-know-principle, a zoning concept can be deployed with each on-premises area having separate access permissions. If a zoning concept is implemented, each on-premises area should be physically separated with its own access control system. Examples for zoning on-premises can be:

- Green zone: Public area, contains no resources that are relevant to the provisioning of the cloud service;
- Yellow zone: Private area, contains means for supporting the cloud service such as development, administration and supervision; and
- Red zone: Sensitive area for production systems such as the server rooms.

Exceptions to the revocation of access authorisations after two months of inactivity are limited to cases where employees with specific roles, such as management positions or supervisors, require only occasional but crucial entry. For all other employees, the revocation of access rights takes place after two months as described in the criterion.

Supplementary Information - Complementary Customer Criteria

–

PS-05 Protection against Threats from Outside and from the Environment

Basic Criteria

PS-05.01B

Premises and buildings related to the cloud service provided are protected from fire, smoke, lightning and unwanted water by structural, technical and organisational measures that meet the security requirements of the cloud service provider (cf. PS-01).

PS-05.02B

Structural Measures include the following aspects:

- Establishment of fire sections with a fire resistance duration of at least 90 minutes for all structural parts, or alternatively, equivalent organisational and technical measures that ensure the same level of protection standard as 90-minutes fire-resistant structural parts or establishment of compensating measures for containing fires and maintaining operational capability;
- Effective implementation of measures to protect against lightning and overvoltage damage; and
- Effective implementation of measures to protect against flooding and heavy rain, unless critical facilities are located significantly above the highest flood level or the backwater level at the location of the cloud data centre.

PS-05.03B

Technical Measures include the following aspects:

- 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.

PS-05.04B

Organisational Measures include the following aspects:

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

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: PS-05.02B

Structural parts are walls, ceilings, floors, doors, windows and other breakthroughs like ventilation flaps, etc.

Compensating measures can take into account aspects such as:

- Partitioning and layout of fire sections;
- Extinguishing systems within the fire sections;
- Early and very early fire detection mechanisms;
- Arrival time of the fire brigade after the fire alarm was triggered; and
- Redundancy of systems and supply facilities within the premise.

The location of all critical facilities in relation to the highest historically recorded flood level at the cloud data centre site or the site's backwater level acts as the starting point for considering flood and heavy rain protection measures.

Applicable to: PS-05.03B

The monitoring of the environmental parameters is addressed in PS-07. When exceeding the allowed control range, alarm messages are generated and forwarded to the responsible cloud service provider.

Supplementary Information - Complementary Customer Criteria

–

PS-06 Protection against Interruptions caused by Power Failures and similar Risks to Supply Facilities

Basic Criteria

PS-06.01B

Measures to prevent the failure of the technical supply facilities required for the operation of system components with which cloud service customer data is processed and to protect equipment holding cloud service customer data, are documented and set up in accordance with the security requirements of the cloud service provider (cf. PS-01) with respect to the following aspects:

- Operational redundancy (N+1) in power and cooling supply;
- Use of appropriately sized uninterruptible power supplies (UPS) and emergency power supplies (EPS), 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);
- Maintenance (servicing, inspection, repair) of the utilities in accordance with the manufacturer's recommendations; and
- Protection of power supply and telecommunications lines against interruption, interference, damage and eavesdropping.

PS-06.02B

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

PS-06.03B

The cloud service provider ensures that equipment containing media with data (including cloud service customer data and cloud service derived data) is shared with a third party only if the data (including cloud service customer data and cloud service derived data) stored on it is encrypted in accordance with CRY-05 or

has been destroyed beforehand using a secure deletion mechanism.

PS-06.04B

The protection of power supply and telecommunications lines 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-dateness of the documentation within the distributor;
- 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 (Sharpening)

–

Additional (Complementing)

PS-06.01AC

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 at the three nearest official measurement stations 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).

PS-06.02AC

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.

PS-06.03AC

Measures are implemented to ensure that the conditions for installation, maintenance and servicing of the related technical equipment (e.g., electrical power, air conditioning, fire protection) are compatible with the cloud service's availability and security requirements.

PS-06.04AC

The cloud service provider ensures that the maintenance agreements for equipment used to host the cloud service enables to have security updates installed in timely fashion on this equipment.

Supplementary Information

About the Criteria

Applicable to: PS-06.01B

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.

Supplementary Information - Complementary Customer Criteria

–

PS-07 Surveillance of Operational and Environmental Parameters

Basic Criteria

PS-07.01B

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).

PS-07.02B

When the permitted control range is exceeded, the responsible departments at the cloud service provider are automatically informed in order to promptly initiate the necessary measures for return to the control range.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: PS-07.01B

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

Supplementary Information - Complementary Customer Criteria

–

PS-08 Workplace Security Requirements

Basic Criteria

PS-08.01B

Based on risk assessment according to OIS-07, security requirements for office environments, including home offices, are documented, communicated and provided in accordance with SP-01. These security requirements encompass various aspects to ensure a safe and secure working environment, including:

- Physical access controls, such as key cards and biometric scanners, for office buildings;
- Use of screen locks and privacy screens for workstations;
- No openly visible confidential data at temporarily unattended workstations;
- Disposal of all company documents that are no longer required within the company premise;
- Prohibition of the use of third party equipment;
- Secure office networks with firewalls and secure WIFI configurations as well as VPN for remote access; and
- Secure office premises with alarm systems and surveillance cameras.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

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 Criteria

OPS-01.01B

The planning of capacities and resources (personnel and IT resources) follows an established procedure in order to avoid possible capacity bottlenecks.

OPS-01.02B

The procedures include forecasting future capacity requirements in order to identify usage trends and manage system overload.

OPS-01.03B

Cloud service providers take appropriate measures to ensure that they continue to meet the requirements

agreed with cloud service customers for the provision of the cloud service in the event of capacity bottlenecks or outages regarding personnel and IT resources. This applies in particular to those relating to the dedicated use of system components, in accordance with the respective agreements.

Additional (Sharpening)

–

Additional (Complementing)

OPS-01.01AC

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

Supplementary Information

About the Criteria

Applicable to: OPS-01.01B, OPS-01.02B, OPS-01.03B, OPS-01.01AC

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 should 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 should be able to explain the procedures at least orally within the scope of this audit.

Applicable to: OPS-01.01B

Capacity bottlenecks are limitations in the cloud service provider's resources, resulting in disruptions of the cloud service or impacting compliance with contractual agreements and service levels.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure through suitable controls 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 are reviewed regularly and the adjustment of SLA demanded accordingly.

OPS-02 Capacity Management - Monitoring

Basic Criteria

OPS-02.01B

Technical and organisational safeguards for the monitoring and provisioning and de-provisioning of cloud services are defined. The cloud service provider ensures that resources are delivered as contractually agreed with the customers. The cloud service provider ensures compliance with the service level agreements.

OPS-02.02B

Capacity bottlenecks are to be reported to cloud service customers analogous to OPS-24.

Additional (Sharpening)

–

Additional (Complementing)

OPS-02.01AC

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

Supplementary Information

About the Criteria

Applicable to: OPS-02.01B

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.

Supplementary Information - Complementary Customer Criteria

Cloud service 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.

OPS-03 Capacity Management - Controlling of Resources

Basic Criteria

OPS-03.01B

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

OPS-03.02B

The cloud service provider informs the cloud service customer about significant security changes in the allocated IT resources and the planned significant security changes.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: OPS-03.01B

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.

System resource allocation may need to take into account any container-based infrastructure used in the service models.

Supplementary Information - Complementary Customer Criteria

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

OPS-04 Protection Against Malware - Concept

Basic Criteria

OPS-04.01B

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 programmes on system components under the responsibility of the cloud service provider that are used to provide the cloud service in the production environment;
- Operation of protection programmes for employees' terminal equipment; and
- Operation of protection programmes on all the incoming flows, including those over cloud service provider end-devices.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: OPS-04.01B

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

Supplementary Information - Complementary Customer Criteria

–

OPS-05 Protection Against Malware - Implementation

Basic Criteria

OPS-05.01B

System components under the cloud service provider's responsibility that are used to operate the cloud service in the production environment are configured with malware protection according to the policies and instructions.

OPS-05.02B

If protection programmes are set up with signature or behaviour-based malware detection and removal, these protection programmes are regularly updated with the latest malware definitions when such updates are available, at least on a daily basis.

Additional (Sharpening)

OPS-05.01AS, sharpening OPS-05.02B

If protection programmes are set up with signature and behaviour-based malware detection and removal, these protection programmes are regularly updated with the latest malware definitions when such updates are available, at the highest frequency that the vendor(s) contractually offer(s).

Additional (Complementing)

OPS-05.01AC

The cloud service provider creates regular reports on the checks performed by the operated protection programs, which are reviewed and analysed by authorised bodies or committees.

OPS-05.02AC

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.

OPS-05.03AC

The configuration of the protection mechanisms is monitored automatically.

OPS-05.04AC

Deviations from the specifications are automatically reported to the cloud service provider's subject matter experts so that they can be immediately assessed and the necessary measures taken.

Supplementary Information

About the Criteria

Applicable to: OPS-05.01B, OPS-05.02B, OPS-05.01AS

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

If the cloud provider operates malware protected containers or virtual machines to provide the cloud service, the malware protection should include container-specific measures. This can include, for example, monitoring the container images and the container runtime, and due to the frequent start and stop of the containers, real-time scans and -monitoring processes.

Supplementary Information - Complementary Customer Criteria

Cloud service 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.

OPS-06 Data Backup and Recovery - Concept

Basic Criteria

OPS-06.01B

Policies and instructions for at least daily backup and restore of cloud service customer data, cloud service derived data and cloud service provider data according to the sensitivity of the data 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 service 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;
- Secure storage, transfer, management and disposal of backup data;
- Access to the backed-up data and the execution of restores is performed only by authorised persons;
- Tests of data restore procedures by the cloud service provider (cf. OPS-08); and
- If part of the contractual agreement: Execution of actual data restore requests or restore tests initiated by the cloud service customer.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: OPS-06.01B

If the data backup of cloud service customer data is not part of the contract concluded between the cloud service provider and the cloud service customer, this criterion is not applicable for cloud service customer data, but it is still applicable for cloud service derived data and cloud service provider data. The extent to which the criterion is applicable to the cloud service is presented in the system description. The data backup concept specifies which type of data backup is to be carried out (e.g. scope, frequency and duration) and specifies which data shall also be backed up in special cases (e.g. pure use of compute nodes without data storage). When backing up data, one has to distinct 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-02) for development and operational processes of the cloud service. If different data backup and recovery procedures exist for cloud service customer data and cloud service provider data, both variants should be in scope for tests of controls according to this criteria catalogue.

Existing contractual agreements prior to a C5 attestation do not need to be updated to incorporate the requirements specified in this criterion. Instead, new contractual agreements should be designed to ensure that specified requirements are clearly defined and agreed upon with cloud service customers.

Supplementary Information - Complementary Customer Criteria

Cloud service 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).

OPS-07 Data Backup and Recovery - Monitoring

Basic Criteria

OPS-07.01B

The execution of backups of cloud service customer data, cloud service derived data and cloud service provider data is monitored by technical and organisational measures documented and implemented in accordance with the policies and instructions defined in OPS-06.

OPS-07.02B

Malfunctions are investigated by qualified staff and rectified promptly to ensure compliance with contractual obligations to cloud service customers or the cloud service provider's business requirements regarding the scope and frequency of data backup and the duration of storage.

Additional (Sharpening)

–

Additional (Complementing)

OPS-07.01AC

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

Supplementary Information

About the Criteria

Applicable to: OPS-07.01B, OPS-07.02B, OPS-07.01AC

If the data backup of cloud service customer data is not part of the contract concluded between the cloud service provider and the cloud service customer, this criterion is not applicable for cloud service customer data, but it is still applicable for cloud service derived data and cloud service provider data. The extent to which the criterion is applicable to the cloud service is presented in the system description.

Supplementary Information - Complementary Customer Criteria

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

OPS-08 Data Backup and Recovery - Regular Testing

Basic Criteria

OPS-08.01B

Restore procedures are tested regularly, at least annually. The tests include cloud service customer data, cloud service derived data and cloud service provider data in accordance with the contractual agreements.

OPS-08.02B

The tests allow an assessment 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).

OPS-08.03B

Cloud service customer data is only restored in environments that are subject to the same access restrictions as the production environment.

OPS-08.04B

The cloud service provider thoroughly documents restore tests, including the safe disposal of restored data.

OPS-08.05B

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.

OPS-08.06B

If the data backup is not part of the contract concluded between the cloud service provider and the cloud service customer, this criterion is not applicable. The cloud service provider shall present this situation transparently in the system description.

Additional (Sharpening)

–

Additional (Complementing)

OPS-08.01AC

At the customer's request, the cloud service provider informs the cloud service customer of the results of the recovery tests.

OPS-08.02AC

Recovery tests are included in the cloud service provider's business continuity management.

Supplementary Information

About the Criteria

Applicable to: OPS-08.01B

The use of cloud service customer data in backup and restore procedures as described in the basic criterion is a carefully considered exception. This exception does not extend to general software development or other testing environments and the use of cloud service customer data for testing is restricted specifically to backup and restore procedures.

Applicable to: OPS-08.03B

If cloud service customer data is restored in an environment with differing access restrictions, the confidentiality of the data may be affected.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure through suitable controls that they actively request information on the results of recovery tests from the cloud service provider. Customers assess the effectiveness of applied data recovery strategies and integrate insights into their own emergency plans in alignment with their business needs and security standards.

OPS-09 Data Backup and Recovery - Storage

Basic Criteria

OPS-09.01B

The cloud service provider transfers cloud service provider data and, if contractually agreed upon, cloud service customer data and cloud service derived data to be backed up to a remote location or transports these on backup media to a remote location.

OPS-09.02B

The data classification of the original data is applied to backups.

OPS-09.03B

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.

OPS-09.04B

The distance to the main site is chosen after sufficient consideration of the factors recovery times and impact of disasters on both sites.

OPS-09.05B

The physical and environmental security measures at the remote site are at the same level as at the main site.

OPS-09.06B

If the data backup is not part of the contract concluded between the cloud service provider and the cloud service customer, this criterion is not applicable. The cloud service provider shall present this situation transparently in the system description.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: OPS-09.01B, OPS-09.03B, OPS-09.04B, OPS-09.05B

A remote location can be e.g. another data centre of the cloud service provider.

Supplementary Information - Complementary Customer Criteria

–

OPS-10 Logging and Monitoring - Concept

Basic Criteria

OPS-10.01B

The cloud service provider has established policies and instructions that govern the logging and monitoring of events on system components within its area of re-

sponsibility. 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, responsibilities and authorities for setting up and monitoring logging;
- Definition of log data that may be transferred to cloud service customers and technical requirements of such log forwarding;
- Information about timestamps in event creation;
- Time synchronisation of system components with one or more approved time sources that are consistent with each other and that the cloud service provider considers to be reliable based on defined criteria. These sources can themselves be synchronised to several external reliable sources, except for isolated networks; and
- Compliance with legal and regulatory frameworks.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: OPS-10.01B

Logs as referred to in the basic criterion include cloud service derived data and cloud service provider data. Legal and regulatory frameworks can define e.g. legal requirements for retention and deletion of data.

Supplementary Information - Complementary Customer Criteria

Cloud service 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.

OPS-11 Logging and Monitoring Management Concept for Cloud Service Derived Data and Account Data

Basic Criteria

OPS-11.01B

Policies and instructions for the secure handling of cloud service derived data and account data are documented, communicated and provided according to SP-01 with regard to the following aspects:

- Cloud service derived data and account data is collected and used solely to administer and operate the cloud service, including purposes related to the implementation of security controls;
- Protection in confidentiality and integrity of the logs;
- As far as technically possible, anonymised cloud service derived data is used only in a way so that no conclusions can be drawn about the usage behaviour of individual users of the cloud service customer;
- No commercial use beyond the aforementioned purpose to administer and operate the cloud service;
- Storage for a fixed period reasonably related to the purposes of the collection;
- Cloud service derived data that has been fully anonymised and cannot be traced back to individual cloud service customers may be further processed and retained, provided no contractual or legal restrictions exist, otherwise immediate deletion if the purposes of the collection are fulfilled and further storage is no longer necessary; and
- Provision to cloud service customers according to contractual agreements.

OPS-11.02B

The cloud service provider lists in the contractual agreements with the cloud service customers all purposes for the collection and use of cloud service derived data that are not related to the universal requirements that apply inherently to all cloud services.

Additional (Sharpening)

–

Additional (Complementing)

OPS-11.01AC

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.

OPS-11.02AC

Cloud service derived data, including log data, is taken into consideration in regulatory compliance assessments.

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure through suitable controls that their contracts with the cloud service provider clearly outline the permissible uses of cloud service derived data. Cloud service customers verify that such data processing complies with contractual or legal restrictions and understand that the provider is obligated to delete data when it is no longer necessary for its initial purposes, unless agreed otherwise.

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

Basic Criteria

OPS-12.01B

The requirements for the logging and monitoring of events and for the secure handling of cloud service derived data and cloud service provider data 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 (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

OPS-13 Security Information and Event Management

Basic Criteria

OPS-13.01B

The cloud service provider integrates relevant log data (cloud service derived data and cloud service provider data) into a Security Information and Event Management (SIEM) system to establish a seamless connection between logging, monitoring, and security incident management.

OPS-13.02B

The SIEM system can be deployed within the cloud environment or externally and shall include the following capabilities:

- Standardisation of log data;

- Automated analysis to identify and correlate potential security incidents;
- Capabilities to detect unusual behaviour and potential threats;
- Real-time alerting to inform the incident response team of critical events;
- Reporting to the incident response team in case new information relevant to an event becomes available; and
- Automated response mechanisms for addressing security incidents.

OPS-13.03B

The cloud service provider protects all SIEM logs to avoid tampering and deletion.

Additional (Sharpening)

–

Additional (Complementing)

OPS-13.01AC

The cloud service provider validates that event detection processes operate as intended on appropriate assets as identified in the asset classification schema (cf. AM-09).

OPS-13.02AC

Any deviations identified during validation are addressed through timely and appropriate remediation measures.

OPS-13.03AC

Issued events which can lead to security incidents trigger incident handling activities by the cloud service provider without undue delay.

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

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

Basic Criteria

OPS-14.01B

The cloud service provider retains the generated log data and keeps it 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.

OPS-14.02B

Log data is deleted if it is no longer required for the purpose for which it was collected.

OPS-14.03B

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

Additional (Sharpening)

–

Additional (Complementing)

OPS-14.01AC

Depending on the protection requirements of the cloud service provider and the technical feasibility, log data and cloud service customer data is logically or physically separated.

Supplementary Information

About the Criteria

Applicable to: OPS-14.01B, OPS-14.02B, OPS-14.03B, OPS-14.01AC

'Log' refers to a document used to record and describe or denote selected items identified during execution of a process or activity. Log data includes both cloud service derived data and cloud service provider data.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure through suitable controls that they actively request the customer-specific portion of the cloud service derived data that consists of log data, if required.

OPS-15 Logging and Monitoring - Accountability

Basic Criteria

OPS-15.01B

The log data generated (cloud service derived data and cloud service provider data) allows an unambiguous identification of user accesses at tenant level to support (forensic) analysis in the event of an incident.

OPS-15.02B

Each logged event shall include a time/date stamp to ensure accurate and traceable records.

OPS-15.03B

The cloud service provider is able to support forensic analysis of incidents and to retain a chain of evidence. This implies that the cloud service provider capture the state of infrastructure components and network communication during security events.

Additional (Sharpening)

–

Additional (Complementing)

OPS-15.01AC

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

OPS-15.02AC

Such logs are collected in a way that allows their use as credible evidence. This includes:

- Records are complete and have not been tampered with in any way;
- Logging systems are clock synchronised, logs include accurate timestamps;
- Copies of electronic evidence are provably identical to the originals; and
- Any information system from which evidence has been gathered was operating correctly at the time the evidence was recorded.

Supplementary Information

About the Criteria

Applicable to: OPS-15.03B

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

Applicable to: OPS-15.01AC

The additional criterion also refers to logs of system components under responsibility of the cloud service provider, to which the cloud service customer generally has no access, insofar as these logs are relevant for the analysis of security incidents and for identifying access to cloud service customer service data (cf. IAM-07 and INQ-04). For logging of system components under responsibility of the cloud service provider cf. PSS-04.

Supplementary Information - Complementary Customer Criteria

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

OPS-16 Logging and Monitoring - Configuration

Basic Criteria

OPS-16.01B

Access to system components for logging and monitoring in the cloud service provider's area of responsibility is restricted to authorised users and requires authentication with two or more factors.

OPS-16.02B

Changes to the configuration are made in accordance with the applicable policies (cf. DEV-03).

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

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

Basic Criteria

OPS-17.01B

The cloud service provider monitors the availability of the system components for logging and monitoring in its area of responsibility.

OPS-17.02B

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 (Sharpening)

–

Additional (Complementing)

OPS-17.01AC

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

OPS-17.02AC

The cloud service provider defines, documents and implements measures to protect the integrity, availability and confidentiality of the logs and the associated infrastructure.

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

OPS-18 Managing Vulnerabilities - Concept

Basic Criteria

OPS-18.01B

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 (proactive) identification of vulnerabilities through suitable measures, including vulnerability scans and penetration tests, considering typical vulnerability classes and Common Weaknesses (CWEs);
- Assessing the severity of identified vulnerabilities using the Common Vulnerability Scoring System (CVSS);
- Prioritising and implementing measures considering existing standards for timely remediation and/or mitigation of identified vulnerabilities based on severity according to defined timeframes and with reference to commonly used scoring systems like the Exploit Prediction Scoring System (EPSS) and the Stakeholder-Specific Vulnerability Categorisation (SSVC);
- Deployment of Security Patches;
- Handling system components for which no measures for timely remediation or mitigation of vul-

nerabilities are initiated based on a risk assessment;
- Interfaces to incident management in case vulnerabilites become incidents;
- If AI-based tools are used for performing vulnerability scans or penetration tests, requirements for the comprehensible (traceable, transparent) documentation on the use of such tools and that these tools shall be used to support the cloud service provider's subject matter experts, not to replace them; and
- Providing information on the configuration of system components and cloud services, the existing vulnerabilities, and the available patches and/or mitigation measures, using widely adopted, preferably automated, formats.

OPS-18.02B

The cloud service provider mandates in its policies and procedures that 'critical' vulnerabilities are to be timely engaged with after identification of the critical vulnerability, even outside the working day.

OPS-18.03B

The cloud service provider also mandates in its policies and procedures that for 'high' vulnerabilities, engagement is to begin within one working day after identification, with regular follow-up of the vulnerability until it has been remediated.

OPS-18.04B

Based on a risk-assessment (cf. OIS-07), the cloud service provider can decide not to remediate or mitigate identified vulnerabilities. Such a risk-assessment and the compensating or mitigating measures are regularily reviewed.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: OPS-18.01B

Suitable measures for the identification of vulnerabilities include implementing RFC 9116 in conjunction with a Coordinated Vulnerability Disclosure (CVD) Policy according to established guidelines like ISO/IEC TR 5895:2022 and ISO/IEC 29147:2018 and community standards like Google's Project Zero Vulnerability Disclosure Policy.

The Common Vulnerability Scoring System (CVSS) is a technical standard that can be used for assessing the severity of identified vulnerabilities. Scores are calculated based on a formula with several metrics that approximate ease and impact of an exploit. In CVSS version 4.0 the scores can be mapped to qualitative ratings as follows:

- Low: 0.1 - 3.9;
- Medium: 4.0 - 6.9;
- High: 7.0 - 8.9; and
- Critical: 9.0 - 10.0.

Widely adopted formats on the configuration of system components and cloud services, the existing vulnerabilities, and the available patches and/or mitigation measures include:

- Software Bill of Materials (SBOM),
- Common Vulnerabilities and Exposures (CVE) or European Vulnerability Database (EUVD),
- Vulnerability, Exploitability eXchange (VEX), and
- Common Security Advisory Frameworks (CSAF).

Applicable to: OPS-18.01B, OPS-18.02B, OPS-18.03B

ISO/IEC 30111:2019 provides requirements and recommendations for prioritising and implementing measures to ensure the timely remediation or mitigation of identified vulnerabilities.

Supplementary Information - Complementary Customer Criteria

Cloud service 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.

OPS-19 Managing Incidents and Crashes - Concept

Basic Criteria

OPS-19.01B

Guidelines and instructions with technical and organisational measures are documented, communicated, and provided in accordance with SP-01 to ensure the timely identification and management of incidents and crashes in the system components used to provide the cloud service or of parts or the whole cloud service. These guidelines and instructions include specifications regarding the following aspects:

- Classification and prioritisation of incidents and crashes;
- Incident models for addressing known issues;
- Escalation rules and procedures, including criteria for triggering Security Incident Management (SIM) processes in accordance with SIM-02 or internal incident management procedures;
- Knowledge sources for incidents and crashes;
- Criteria for determining when crashes are classified as incidents and when they trigger incident management processes;
- Mechanisms ensuring that access to crash files is restricted to authorised personnel only;
- Safeguards to prevent exposure of sensitive, personal, or confidential data within crash files;
- Encryption of crash files for storage and during transmission;
- Access management, logging, and review processes for access logs of crash files; and
- Retention periods and secure deletion processes for crash files once no longer needed.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: OPS-19.01B

A crash is a sudden and complete failure of a system or system component.

A crash file is the dump of a system's execution state, usually including contents of its storage or registers at the time of the crash (e.g. memory dump).

Supplementary Information - Complementary Customer Criteria

–

OPS-20 Managing Incidents - Implementation

Basic Criteria

OPS-20.01B

The cloud service provider identifies, records, classifies, and prioritises incidents according to the policies and instructions.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

OPS-21 Managing Crashes - Implementation

Basic Criteria

OPS-21.01B

Crashes of system components, parts of or the whole cloud service under the responsibility of the cloud service provider are identified, recorded, and addressed according to the policies and instructions.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

OPS-22 Managing Vulnerabilities, Malfunctions and Errors - Penetration Tests

Basic Criteria

OPS-22.01B

The cloud service provider performs penetration tests by qualified internal personnel or external penetration testers at least once a year and in case of significant changes to the cloud service.

OPS-22.02B

Penetration tests are carried out in accordance with a documented concept for penetration tests that outlines the types of penetration tests to be performed and the requirements for the qualification and competence of the personnel to perform such tests.

OPS-22.03B

Penetration tests target the system components relevant to the provision of the cloud service in the area of responsibility of the cloud service provider. System components to be targeted are identified in a risk assessment.

OPS-22.04B

Penetration tests are carried out in accordance with test plans that cover all relevant system components and specify which system components are to be tested.

OPS-22.05B

If penetration tests follow multi-annual test plans, all relevant system components are subjected to at least one penetration test within a maximum period of three years.

OPS-22.06B

The cloud service provider assesses the severity of identified vulnerabilities in accordance with the Common Vulnerability Scoring System (CVSS), in the latest version valid at the time of the execution of the control.

OPS-22.07B

The cloud service provider discloses identified vulnerabilities in the online register for known vulnerabilities in accordance with criterion PSS-03.

OPS-22.08B

Actions for remediation or mitigation are taken in accordance with the time frames as defined in the concept for managing vulnerabilities (cf. OPS-18).

OPS-22.09B

The cloud service provider performs a root cause analysis on the vulnerabilities discovered through penetration testing in order to assess to which extent similar vulnerabilities may be present in the cloud service. The cloud service provider correlates the possible exploits of discovered vulnerabilities with previous information security incidents to identify if the vulnerability may have been exploited before its discovery.

Additional (Sharpening)

OPS-22.01AS, sharpening OPS-22.01B

The cloud service provider performs penetration tests at least every six months and in case of significant changes to the cloud service by independent external penetration testers. The external penetration testers are engaged only if the personnel supposed to perform the test verifiably meets the cloud service provider's qualification and competence requirements. Internal personnel for penetration tests may support the external personnel.

OPS-22.02AS, sharpening OPS-22.02B

Pre-launch and post-launch penetration tests are performed in accordance with a documented concept for penetration tests that outlines the types of penetration tests to be performed and the requirements for the qualification and competence of the personnel to perform such tests.

Additional (Complementing)

OPS-22.01AC

Penetration tests are performed based on reviews of the architecture and configuration of the system components, and of the cloud service provider's source code.

OPS-22.02AC

The cloud service provider plans penetration testing in a multi-annual work programme.

OPS-22.03AC

The cloud service provider reviews the performance of penetration tests on system components at least annually, and in case of significant changes to the cloud service.

Supplementary Information

About the Criteria

Applicable to: OPS-22.01B, OPS-22.02B, OPS-22.03B, OPS-22.04B, OPS-22.05B, OPS-22.06B, OPS-22.07B, OPS-22.08B, OPS-22.09B, OPS-22.01AS, OPS-22.02AS, OPS-22.01AC, OPS-22.02AC, OPS-22.03AC

See section '1.2 Definitions' for the term penetration test. There are three types of penetration tests:

- Black-box testing: Testing performed without prior knowledge of the internal structure/design/implementation of the object being tested;
- Grey-box testing: Testing performed with partial knowledge of the internal structure/design/implementation of the object being tested; and
- White-box testing: Testing performed with knowledge of the internal structure/design/implementation of the object being tested.

It can further be distinguished between

- Pre-launch penetration testing: Testing already performed as part of the software development process during the test phase of the cloud service (cf. DEV-07); and
- Post-launch penetration testing: Testing carried out during the regular operations of the cloud service.

Applicable to: OPS-22.01B, OPS-22.01AS

The qualification and competence of personnel for penetration tests can be verified based on professional certifications, e.g. as BSI-certified IS penetration tester or CREST-certified Cyber Security Professional.

Applicable to: OPS-22.03B, OPS-22.05B

System components relevant to the provision of the cloud service in the area of responsibility of the cloud service provider can comprise such system components that are exposed at the external perimeter of the network or components accessible only from inside the network.

Supplementary Information - Complementary Customer Criteria

–

OPS-23 Managing Vulnerabilities, Malfunctions and Errors - Measurements, Analyses and Assessments of Procedures

Basic Criteria

OPS-23.01B

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.

OPS-23.02B

Results are evaluated at least quarterly in a documented form by responsible individuals or groups of the cloud service provider to initiate continuous improvement actions and to verify their effectiveness.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: OPS-23.01B

The assessment of the suitability, appropriateness and effectiveness of procedures for managing vulnerabilities and incidents may be based on the following information:

1. Regular reporting of KPIs that are volume, time-based or resolution/quality-based, e.g.

a. for vulnerabilities:

- Mean Time to Detect (MTTD, average time it takes to discover a vulnerability from its disclosure or creation);
- Mean Time to Remediate (MTTR, average time it takes to fix or patch a vulnerability after it has been detected);
- Number of open vulnerabilities at each severity level; and
- Percentage of vulnerabilities that have been patched within a set period.

b. for incidents:

- Number of incidents reported over a set period and how this evolved over the time;
- Average response and resolution time;
- Percentage of incidents resolved within the agreed-upon service level agreement; and
- Percentage of incidents resolved during the first attempt for resolution.

2. Customer complaints or the results of customer surveys about their satisfaction with the procedures; and
3. Results of internal or external audits.

Supplementary Information - Complementary Customer Criteria

–

OPS-24 Involvement of Cloud Service Customers in the Event of Incidents

Basic Criteria

OPS-24.01B

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

OPS-24.02B

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

OPS-24.03B

Capacity bottlenecks are to be communicated to cloud service customers in a similar manner.

Additional (Sharpening)

–

Additional (Complementing)

OPS-24.01AC

The cloud service provider defines and documents procedures in contractual agreements with cloud service customers that specify the involvement of the customer in confirming, within a specified time period,

that a resolution has effectively addressed the root cause of an incident.

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

Cloud service 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.

OPS-25 Managing Vulnerabilities, Malfunctions and Errors - Vulnerability Scans

Basic Criteria

OPS-25.01B

System components in the area of responsibility of the cloud service provider for the provision of the cloud service are subject to vulnerability scans at least once a month in accordance with the policies for handling vulnerabilities (cf. OPS-18). These vulnerability scans include a comparison of the Software Bill of Materials (SBOM) data against up-to-date vulnerability databases (e.g., CVE, EUVD, etc.) to identify known vulnerabilities.

OPS-25.02B

The cloud service provider assesses the severity of vulnerabilities in accordance with defined criteria.

OPS-25.03B

Measures for timely remediation or mitigation are initiated within defined time windows.

Additional (Sharpening)

OPS-25.01AS, sharpening OPS-25.02B

The cloud service provider assesses the severity of vulnerabilities using the latest version of the Common Vulnerability Scoring System (CVSS) valid at the time of the execution of the control.

Additional (Complementing)

OPS-25.01AC

Time frames for the initiation of remediation or mitigation efforts after a vulnerability is identified are defined and monitored according to a risk-based classification framework. This framework incorporates, but is not limited to, the CVSS severity level of vulnerabilities.

Supplementary Information

About the Criteria

Applicable to: OPS-25.01B

In contrast to penetration tests (cf. OPS-22), which are carried out manually and according to an individual scheme, the check for open vulnerabilities is performed automatically, using so-called vulnerability scanners.

Applicable to: OPS-25.01AC

An example of a framework for risk-based classification and definition of timeframes can be:

- Critical (CVSS = 9.0 - 10.0): 3 hour
- High (CVSS = 7.0 - 8.9): 8 hours
- Medium (CVSS = 4.0 - 6.9): 5 days
- Low (CVSS = 0.1 - 3.9): 1 month

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure through suitable controls that system components under their responsibility are regularly checked for vulnerabilities and to mitigate these by appropriate measures. If cloud service customers operate virtual machines or containers with the cloud service, this also includes performing vulnerability scans to ensure that secure images (so-called golden images) are used.

OPS-26 Managing Vulnerabilities, Malfunctions and Errors - System Hardening

Basic Criteria

OPS-26.01B

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.

OPS-26.02B

The hardening requirements for each system component are documented.

OPS-26.03B

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.

OPS-26.04B

Configurations and log files (cloud service provider data) regarding the continuous availability of the images are retained.

OPS-26.05B

The cloud service provider implements monitoring measures to ensure system components comply with hardening specifications.

OPS-26.06B

Any deviations from these specifications are promptly reported to the appropriate departments for immediate assessment and action.

Additional (Sharpening)

OPS-26.01AS, sharpening OPS-26.05B

System components in the cloud service provider's area of responsibility are automatically monitored for compliance with hardening specifications.

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: OPS-26.01B, OPS-26.05B, OPS-26.01AS

System components in the sense of the 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.

Applicable to: OPS-26.04B

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

- Configuration of the images used with regards to implemented hardening; and 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-Compendium.

Applicable to: OPS-26.05B, OPS-26.01AS

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

Supplementary Information - Complementary Customer Criteria

Cloud service 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.

OPS-27 Managing Vulnerabilities, Malfunctions and Errors - Externally Sourced Components

Basic Criteria

OPS-27.01B

The cloud service provider documents, communicates, and maintains processes and procedures to manage updates to system components used to provide the cloud service that incorporate third party or open-source libraries. This includes:

- Regularly identifying available updates and known vulnerabilities in third party or open-source libraries used within applications;
- Evaluating the potential impact of identified updates and vulnerabilities on the applications and the overall security posture;
- Implementing necessary updates and patches in a timely manner to address identified vulnerabilities; and
- Continuously monitoring applications to ensure updates are effectively applied and no new vulnerabilities are introduced.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

OPS-28 Separation of Datasets - Guideline

Basic Criteria

OPS-28.01B

Based on a risk-assessment (cf. OIS-07), the cloud service provider established guidelines and instructions with technical and organisational measures to ensure separation of cloud service customer data between different customers and between customers and the cloud service provider. These guidelines and instructions are documented, communicated and provided in accordance with SP-01 and contain specifications regarding the client separation based on a documented cloud layer model (cf. OPS-29) and include the following:

- Illustration of which cloud layers are used for the particular cloud service. The used cloud layers should be appropriate to enable client separation;
- Measures used to separate cloud service customer data along the used cloud layers. Those measures are categorised according to the protection goals of confidentiality, integrity and availability and if they are preventive, detective or reactive measures;
- Monitoring and compliance with these measures; and
- Initiation of suitable measures in the event of deviations.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: OPS-28.01B

The guidelines and instructions of this criteria are meant to serve as an umbrella guideline for all cyber security measures against all threats that stem from sharing physical or virtual ressources and that lead to a loss of separation of data sets. Ideally, the cloud service

provider has already ensured the separation of data sets between different customers and between customers and cloud service provider via all other guidelines, instructions and the corresponding measures. The systematic approach of the guidelines and instructions addressed by this criterion ensures that no aspect of this separation is overlooked. It also provides a good basis to explain the cyber security of the cloud service to the customer in an appealing manner (cf. PSS-01).

Cloud layers in the sense of this criterion can be found in the *CISA Cloud Security Technical Reverence Architecture*. The cloud service provider may use its own categorisation of cloud layers.

There are nine combinations for confidentiality, integrity and availability with prevention, detection and reaction. Applying this to every cloud layer may lead to a large number of combinations. However, depending on the cloud service, it can be acceptable that it may not be possible to provide meaningful information in the guideline for every possible combination of prevention, detection and reaction as well as confidentiality, integrity and availability. Those cases should be comprehensibly documented in the guidelines and instructions.

Supplementary Information - Complementary Customer Criteria

–

OPS-29 Separation of Datasets - Implementation

Basic Criteria

OPS-29.01B

Based on a risk-assessment (cf. OIS-07), the requirements for separating cloud service customer data between different customers and between customers and cloud service provider on shared virtual or shared ressources along the cloud layers, the cloud service provider implements measures and procedures against threats to the separation of data sets according to the guidelines and instructions of OPS-28. The measures address prevention against, detection of and reaction to any incidents infringing the separation.

OPS-29.02B

Cloud service 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 and following policies on cryptography (cf. CRY-01) to ensure the confidentiality and integrity of this data.

OPS-29.03B

The measures are regularily reviewed and improved accordingly.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: OPS-29.01B

The guidelines and instructions of this criteria are meant to serve as an umbrella guideline for all cyber security measures against all threats that stem from sharing physical or virtual ressources and that lead to a loss of separation of data sets. Ideally, the cloud service provider has already ensured the separation of data sets between different customers and between customers and cloud service provider via all other guidelines, instructions and the corresponding measures. The systematic approach of the guidelines and instructions addressed by this criterion ensures that no aspect of this separation is overlooked. It also provides a good basis to explain the cyber security of the cloud service to the customer in an appealing manner (cf. PSS-01).

Applicable to: OPS-29.02B

Shared resources include memory, cores and storage networks. The separation of cloud service customer data on shared resources can take place, for example, in accordance with cloud layers described in the CISA Cloud Security TRA. 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 separation of transmitted data is subject to criterion COS-06.

Supplementary Information - Complementary Customer Criteria

Cloud service 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.

OPS-30 Confidential Computing - Policies and Instructions

Basic Criteria

OPS-30.01B

If the cloud service comprises capabilities for confidential computing, policies and instructions with technical and organisational safeguards are documented, communicated and provided according to SP-01, in which the following aspects are described:

- Purpose and scope, including which information security risks are to be mitigated through the use of confidential computing (cf. OIS-07);
- Available confidential computing technologies;
- Determination of which parts of the cloud stack are protected with each technology and where third party access is possible;
- Listing of involved suppliers/service organisations; and
- Utilisation of Trusted Execution Environments (TEEs) or secure enclaves.

OPS-30.02B

The cloud service provider provides its customers with information on the above listed aspects according to PSS-01.

OPS-30.03B

Additional aspects addressed by the policies and instructions for confidential computing, not necessarily included in the information provided to the cloud service customers, include:

- Responsibilities for the implementation and monitoring of Confidential Computing measures;
- Security requirements to ensure the confidentiality, integrity, and authenticity of the data during processing, including that (a) neither the cloud service provider nor any other unauthorised entity shall be able to access the cloud service customer data or the keys used for protecting that data, and (b) use of cryptographic algorithms that comply with the cloud service provider's policy for the use of cryptographic mechanisms (cf. CRY-01); and
- Relevant legal and regulatory requirements applicable to confidential computing.

Additional (Sharpening)

–

Additional (Complementing)

OPS-30.01AC

The cloud service provider documents and implements a technical concept for confidential computing, demonstrating how certain information security risks are mitigated (cf. OIS-07). The concept includes at least the following technical measures and procedures:

- Usage of Trusted Execution Environments (TEEs) or secure enclaves to process sensitive data (data in use) in a protected environment;
- Documentation of all associated interfaces;
- Consideration of available hardware attestations;
- Utilisation of encryption techniques to secure data during processing, including secure key management;
- Measures to ensure the integrity and authenticity of the data and the executing code within the TEE (remote attestation);
- Implementation of monitoring and logging mechanisms to detect and respond to security incidents; and

- Conducting regular security reviews and penetration tests (cf. OPS-22) on an event-driven basis, but at least annually, to verify the effectiveness of confidential computing measures.

Supplementary Information

About the Criteria

Applicable to: OPS-30.01B, OPS-30.02B, OPS-30.03B, OPS-30.01AC

Confidential Computing within the meaning of this criterion uses hardware-based, attested TEEs to protect the confidentiality and integrity of data during processing ('in use'). A TEE represents an isolated part within a system that provides a specially protected runtime environment. The TEE can be part of the main processor (CPU) or part of the system-on-chip (SoC). Only authorised entities are allowed to introduce or modify applications or code within the TEE. The attestation of the TEE and the application running within the TEE serves to validate the trustworthiness of the processing.

Supplementary Information - Complementary Customer Criteria

–

OPS-31 Confidential Computing - Remote Attestation

Basic Criteria

OPS-31.01B

If the cloud service comprises capabilities for Confidential Computing, the cloud service provider offers remote attestation functionalities for data in-use protection.

OPS-31.02B

Remote attestation functionalities are based on cryptographic means rooted in trusted hard- and software.

OPS-31.03B

Remote attestation functionalities comprise an interface that allows the customer to verify the integrity of the remote attestation.

Additional (Sharpening)

–

Additional (Complementing)

OPS-31.01AC

The cloud service provider clearly defines, documents and communicates the available attestation levels.

OPS-31.02AC

The information is part of the guidelines and recommendations for the secure use of the cloud service provided (cf. PSS-01).

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

OPS-32 Guideline for Container Management

Basic Criteria

OPS-32.01B

Guidelines and instructions with technical and organisational measures for the planning and management of containers are documented, communicated and provided in accordance with SP-01. These guidelines and instructions contain specifications for the entire container life cycle regarding the following aspects:

- Image creation, testing, and accreditation;
- Image storage and retrieval;
- Container deployment and management;
- Container operations; and
- Decommissioning of images and container.

OPS-32.02B

The guidelines and instructions should describe measures along the life cycle of containers and address at least the following aspects:

- Containers are inventoried according to a documented process (cf. AM-02, AM-03, AM-09);
- The need for malware protection is assessed and, if necessary, ensured (cf. OPS-05);
- Logging and monitoring of events takes place along the container lifecycle and is executed according to a defined logging concept (cf. OPS-10, OPS-12);
- Cloud service customer data is separated based on a risk analysis (cf. OPS-29);
- Access to the container host should take place in accordance with a roles and rights concept and a policy for managing access and access authorisations (cf. IAM-01, IAM-06);
- Data stored on containers and data in transit should be encrypted as far as possible by the provider in accordance with the encryption policy (cf. CRY-01);
- Measures to ensure network security are established. This includes, for example, measures to detect network anomalies (cf. COS-01 and COS-03) such as unexpected data flows within the network or unwanted access attempts;
- Changes to containers and images follow a regulated process (cf. DEV-03); and
- Hardening processes are carried out according to general industry standards to ensure that no unnecessary system services are executed (cf. PSS-11).

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

OPS-33 Managing Vulnerabilities - Patch Management

Basic Criteria

OPS-33.01B

Guidelines and instructions with technical and organisational measures are documented, communicated and provided in accordance with SP-01 to ensure systems and applications in the responsibility of the cloud service provider are patched within a suitable time frame depending on contractual agreements and identified vulnerabilities or exploits. These guidelines and instructions contain specifications regarding the following aspects:

- Software is kept up-to-date with the latest security patches;
- Patches are scheduled within maintenance windows, where applicable, to minimise service disruption; and
- Patches are tested in non-production environments before they are rolled out into the production environment, provided testing was successful. Mechanisms are in place to revert to previous software versions in case of unexpected issues.

OPS-33.02B

Patch management procedures are harmonised with the cloud service provider's overall software change management process.

OPS-33.03B

Patches provided by third parties are identified, tested and deployed.

OPS-33.04B

Systems are scanned after application of patches to ensure vulnerabilities and exploits are remediated and no new vulnerabilities or exploits were deployed.

Additional (Sharpening)

OPS-33.01AS, sharpening OPS-33.03B

Patches provided by third parties are identified, tested and deployed in an automated manner. In case of patches where manual intervention is required, an exception handling process for manual patching is defined.

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: OPS-33.01B, OPS-33.02B, OPS-33.03B, OPS-33.04B, OPS-33.01AS

Patches are defined as software updates to systems, applications or network components with the goal of increasing security by addressing issues, vulnerabilities or exploits.

Supplementary Information - Complementary Customer Criteria

–

5.7 Identity and Access Management (IAM)

Objective: Secure the authorisation and authentication of users of the cloud service provider (typically privileged users) to prevent unauthorised access.

IAM-01 Policy for User Accounts and Access Rights

Basic Criteria

IAM-01.01B

The cloud service provider documents, communicates and makes available according to SP-01:

- A role, rights and authorities concept based on role-based access control and the business and security requirements of the cloud service provider; and
- 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.

IAM-01.02B

These documents address at least the following aspects:

- Aspects to be considered for making access control decisions;
- Assignment of unique usernames;
- Granting and modifying user accounts and access rights based on the 'least-privilege-principle' and the 'need-to-know' principle;
- Use of a role-based mechanism for the assignment of access rights;
- Definition of the different types of identities and role-based access supported, and assignment of access control parameters and roles to be considered for each type;
- Separation of duties between operational and monitoring functions ('Separation of Duties');
- Assigning and monitoring privileged access rights;
- Separation 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 cloud service customer data, cloud service derived data and cloud service provider data can be accessed;
- Regular review of assigned user accounts and access rights;
- Blocking and removing access accounts in the event of inactivity;
- Specific measures for the management of identities used infrequently for emergency recovery and similar scenarios;
- 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;
- Remote access and access across geographic boundaries;

- Requirements for the approval and documentation of the management of user accounts and access rights;
- Requirement to review access logs at least every month; and
- Measures to be taken in the event of potential identity compromise, such as disabling and removing identities.

IAM-01.03B

The cloud service provider links the policy for user accounts and access rights with the physical access control policy defined in PS-04, to ensure that access to premises and buildings related to the cloud service provided is also controlled.

IAM-01.04B

For the given identity under the responsibility of the cloud service provider, the cloud service provider is able to provide the list of the access rights currently granted to that identity.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: IAM-01.01B

External employees include freelancers, temporary workers, suppliers and service providers with access to system components.

Applicable to: IAM-01.02B

System components in the sense of the criterion are defined in OPS-26. 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.

For containers, user accounts and access rights should be managed according to a regulated process, especially for automated authorisation processes in container environments.

Supplementary Information - Complementary Customer Criteria

–

IAM-02 Granting and Change of User Accounts and Access Rights

Basic Criteria

IAM-02.01B

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.

IAM-02.02B

If the cloud service provider defines break glass accounts to be used when the main procedure for authentication is not available, the cloud service provider defines and enforces specific requirements and procedures for secure usage of those accounts.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: IAM-02.01B

This criterion applies to identities that refer to single, multiple or non-human entities.

Supplementary Information - Complementary Customer Criteria

–

IAM-03 Risk-Based Procedure for Locking and Withdrawal of User Accounts

Basic Criteria

IAM-03.01B

The cloud service provider has a risk-based procedure for managing user accounts in place (cf. IAM-01), taking into account the types of data accessible via the user accounts of internal and external employees.

IAM-03.02B

As part of this procedure, specific parameters for automatically locking and withdrawing access due to inactivity or multiple failed login attempts are defined, with exceptions for identities to be used in emergency recovery and similar scenarios.

IAM-03.03B

The cloud service provider documents and implements a process to monitor stolen and compromised credentials and to disable any identity for which an issue is identified, pending a review by an authorised person. This process is implemented on all identities under the cloud service provider's responsibility to which privileged access rights are assigned.

IAM-03.04B

Such processes include an exception mechanism for cases where all identities needed to manage the situation are potentially compromised.

Additional (Sharpening)

IAM-03.01AS, sharpening IAM-03.03B

The cloud service provider documents and implements a process to monitor stolen and compromised credentials and to disable any identity for which an issue is identified, pending a review by an authorised person. This process is implemented on all identities under the cloud service provider's responsibility.

Additional (Complementing)

IAM-03.01AC

The cloud service provider monitors the context of authentication attempts, e.g. IP addresses, the date and time or the device used, and flags suspicious events to authorised persons, as relevant.

IAM-03.02AC

The cloud service provider validates the effectiveness of its procedures for locking and withdrawal of user accounts.

IAM-03.03AC

Any deviations identified during validation are addressed through timely and appropriate remediation measures.

Supplementary Information

About the Criteria

Applicable to: IAM-03.01B, IAM-03.02B, IAM-03.03B, IAM-03.04B, IAM-03.01AS, IAM-03.01AC, IAM-03.02AC, IAM-03.03AC

This criterion applies to identities that refer to single, multiple or non-human entities.

Applicable to: IAM-03.02B

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

Supplementary Information - Complementary Customer Criteria

–

IAM-04 Withdrawal or Adjustment of Access Rights as the Task Area Changes

Basic Criteria

IAM-04.01B

Access rights are promptly adjusted or 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.

IAM-04.02B

Privileged access rights are adjusted or revoked within 48 hours after the change taking effect.

IAM-04.03B

All other access rights are adjusted or revoked within 14 days.

IAM-04.04B

After revocation, the procedure for granting user accounts and access rights (cf. IAM-02) shall be repeated.

IAM-04.05B

In cases of role changes where temporary access may need to be granted, these access rights are provided in accordance with the procedures for granting access rights outlined in IAM-02.

IAM-04.06B

If the cloud service provider defines break glass accounts to be used when the main procedure for authentication is not available, then the cloud service provider defines and enforces specific requirements and procedures for secure usage of those accounts.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: IAM-04.01B, IAM-04.02B, IAM-04.03B, IAM-04.04B, IAM-04.05B, IAM-04.06B

This criterion applies to identities that refer to single, multiple or non-human entities.

Applicable to: IAM-04.01B

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.'

Applicable to: IAM-04.02B

For privileged access rights the definition in IAM-06 applies.

Supplementary Information - Complementary Customer Criteria

–

IAM-05 Regular Review of Access Rights

Basic Criteria

IAM-05.01B

Identities and the associated 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.

IAM-05.02B

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.

IAM-05.03B

Identified deviations are dealt with promptly, but no later than seven days after their detection, by appropriate modification or withdrawal of the access rights.

IAM-05.04B

When revoking identities, the system ensures that all associated IT resources (e.g., virtual machines, storage, access rights) are identified, reassigned, or deleted to prevent the creation of orphaned resources. Clear processes and technical controls are established to identify and handle any orphaned resources that occur despite preventive measures, ensuring their timely reassignment or secure deletion.

Additional (Sharpening)

–

Additional (Complementing)

IAM-05.01AC

Privileged access rights are reviewed at least every six months.

Supplementary Information

About the Criteria

Applicable to: IAM-05.01B, IAM-05.02B, IAM-05.03B, IAM-05.04B

This criterion applies to identities that refer to single, multiple or non-human entities. As an alternative to the regular reviews of access rights, time-bound access rights that automatically expire may also be issued.

Supplementary Information - Complementary Customer Criteria

–

IAM-06 Privileged Access Rights

Basic Criteria

IAM-06.01B

Privileged access rights for internal and external employees as well as technical users of the cloud service provider are assigned and changed in accordance with the policy for managing user accounts and access rights (cf. IAM-01) or a separate specific policy.

IAM-06.02B

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').

IAM-06.03B

Non-nominative technical users shall only be accessed through authentication with a personalised user account.

IAM-06.04B

Activities of users with privileged access rights are logged in order to detect any misuse of privileged access in suspicious cases.

IAM-06.05B

The logged information is automatically monitored for defined events that may indicate misuse.

IAM-06.06B

When such an event is identified, the responsible personnel is automatically informed so that they can promptly assess whether misuse has occurred and take corresponding action.

IAM-06.07B

In the event of proven misuse of privileged access rights, disciplinary measures are taken in accordance with HR-04.

IAM-06.08B

For Docker containers and images, activities of users with privileged access shall be logged according to OPS-10.

IAM-06.09B

The cloud service provider requires two- or more factor authentication for accessing the administration interfaces used by the cloud service provider.

Additional (Sharpening)

–

Additional (Complementing)

IAM-06.01AC

The cloud service provider maintains an up-to-date inventory of the identities under its responsibility that have privileged access rights.

IAM-06.02AC

The cloud service provider reviews every six months the list of internal and external employees who are responsible for an identity assigned to a non-human entity within its scope of responsibility.

Supplementary Information

About the Criteria

Applicable to: IAM-06.01B, IAM-06.02B, IAM-06.03B, IAM-06.04B, IAM-06.05B, IAM-06.06B, IAM-06.07B, IAM-06.08B, IAM-06.09B, IAM-06.01AC, IAM-06.02AC

Privileged access rights in the sense of the 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 service 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 service customers (also indirectly, e.g. by deactivating the logging and monitoring of security-relevant events).

Applicable to: IAM-06.06B

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

Supplementary Information - Complementary Customer Criteria

–

IAM-07 Access to Cloud Service Customer Data

Basic Criteria

IAM-07.01B

The cloud service provider implements sufficient partitioning measures between the system components for providing the cloud service and system components of its other information systems, and suitable measures for partitioning between the cloud service customers (cf. OPS-28 and OPS-29).

IAM-07.02B

The cloud service provider designs the system so that the technical infrastructure is clearly separated from the management tools and the cloud service customer data it hosts.

IAM-07.03B

Unless legally forbidden, the cloud service customer is informed by the cloud service provider whenever internal or external employees of the cloud service provider read or write to the cloud service customer data processed, stored or transmitted in the cloud service or have accessed it without the prior consent of the cloud service customer. The information is provided whenever cloud service customer data is/was accessed in unencrypted form or the contractual agreements with customers do not explicitly exclude informing the customer of such access.

IAM-07.04B

Unless contractually agreed otherwise, the information contains the cause, time, duration, geographic location, type and scope of the access, as well as the retention time of other data generated during access, such as logs or copies containing cloud service customer data. The information is sufficiently detailed to enable subject matter experts of the cloud service customer to assess the risks of the access.

IAM-07.05B

The information is provided in accordance with the contractual agreements, but no later than 72 hours from the initiation of the access.

IAM-07.06B

The cloud service provider makes available to the cloud service customer, through contractual agreements, prior to offering its services, all instances where cloud service provider access in a non-encrypted form to the cloud service customer data processed, stored or transmitted in the cloud service may occur.

IAM-07.07B

If the cloud service provider offers to its cloud service customers interfaces for administrators and for end users, these interfaces are to be separated from one another, ensuring that access paths for customer administrators differ from those for end users.

Additional (Sharpening)

IAM-07.01AS, sharpening IAM-07.03B

Access to cloud service customer data and cloud service derived data by internal or external employees of the cloud service provider requires the prior consent of an authorised department of the cloud service customer, provided that the cloud service customer's data is accessible in unencrypted form or contractual agreements do not explicitly exclude such consent. Additionally, if encrypted data and its decryption key are stored separately within the same cloud environment, prior consent is required not only for accessing the decryption key but also for accessing the encrypted data itself (potentially together with the key).

IAM-07.02AS, sharpening IAM-07.04B

For the consent, the cloud service customer's department is provided with meaningful information about the cause, time, duration, geographic location, type and scope of the access, as well as the retention time of other data generated during access, such as logs or copies containing cloud service customer data. The information is sufficiently detailed to enable subject matter experts of the cloud service customer to assess the risks of the access. In addition to the provided information, the cloud service provider specifies a timeframe within which the cloud service customer shall respond to the access request.

IAM-07.03AS, sharpening IAM-07.06B

The cloud service provider makes available to the cloud service customer, through contractual agreements, prior to offering its services, all instances where cloud service provider access in a non-encrypted form to the cloud service customer data and cloud service derived data processed, stored or transmitted in the cloud service may occur.

Additional (Complementing)

IAM-07.01AC

The cloud service provider includes provisions through contractual agreements for cases where the cloud service provider has access in non-encrypted form to the cloud service customer data processed, stored or transmitted in the cloud service, where it is not feasible to seek prior consent. For example, where troubleshooting the service is necessary to ensure that the cloud service customer data remains confidential, available and its integrity preserved.

IAM-07.02AC

Before granting internal or external employees direct or indirect access to cloud service customer data, including in support operations, the cloud service provider verifies that the internal or external employees performing the action have passed an appropriate assessment or are supervised by employees who have passed an appropriate assessment (cf. HR-01).

IAM-07.03AC

In the case of supervised access, the cloud service provider ensures that:

- The access is performed using mechanisms that allow the supervising employees to authorise or deny individual actions and ask for explanations in real time;
- The access rights are revoked at the end of the operation;
- The operations performed are logged as administration actions;
- The supervision solution includes the authentication of the supervised employee and the device from which the supervised access is performed;
- The supervision solution logs the operations proposed by the supervised employee and the actions of the supervisor, including the operations denied by the supervisor; and
- The supervision solution prevents information flows toward the supervised employee's device.

Supplementary Information

About the Criteria

Applicable to: IAM-07.04B, IAM-07.02AS

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

Applicable to: IAM-07.03B, IAM-07.04B, IAM-07.05B, IAM-07.06B, IAM-07.01AS, IAM-07.02AS, IAM-07.01AC, IAM-07.02AC, IAM-07.03AC

Access to cloud service customer data also entails disclosure of data as part of investigation requests according to INQ-04. These are to be communicated to cloud service customers as far as it is legally not forbidden. The criteron aims at minimizing the cloud service provider capability to access cloud service customer data. Minimisation of the cloud service providers possibility to access cloud service customer data is often a question of the radius of the collusion circle. I.e. if four-eyes principle for access is applied with the access being logged, then three people build the collusion circle. In order to build trust into such access statements, the cloud service provider should describe in the system description the taken measures to enlarge the collusion circle.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure through suitable controls that their contracts with the cloud service provider include a comprehensive list of all instances where the provider might access customer data in an unencrypted form. Cloud service customers verify that these conditions are thoroughly documented before engaging the services, allowing them to make informed decisions about data security and compliance.

Cloud service customers ensure through suitable controls that they provide a response to data access requests by the cloud service provider within a specified timeframe as agreed upon in the contractual agreements.

IAM-08 Confidentiality of Authentication Information

Basic Criteria

IAM-08.01B

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.

IAM-08.02B

Authentication credentials are managed with a security level that matches or exceeds the classification of the system component they protect.

IAM-08.03B

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 shall 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. IAM-09) is enforced as far as technically possible;
- The user is informed about changing or resetting the password; and
- The server-side storage takes place using state-of-the-art cryptographic hash functions, except when passwords are stored for subsequent re-use in the plain text form, for example in a password manager. In this case, stored passwords are protected, using a state-of-the-art cryptographic mechanism.

IAM-08.04B

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

IAM-08.05B

The cloud service provider documents, communicates and makes available to all users under its responsibility rules and recommendations for the management of credentials, including at least:

- Non-reuse of credentials;
- Trade-offs between entropy and ability to memorise;
- Recommendations for renewal of passwords;
- Rules on storage of passwords;
- Confidentially of personal (or shared) authentication and non-sharing of credentials;

- Recommendations on password managers; and
- Recommendation to specifically address classical attacks, including phishing, social attacks, and whaling.

IAM-08.06B

If cryptographic mechanisms are used, they follow the policies and procedures from CRY-01.

IAM-08.07B

Any password reset procedure is not valid for more than 48 hours and the password is to be changed by the user after the use of the reset procedure.

Additional (Sharpening)

–

Additional (Complementing)

IAM-08.01AC

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 Criteria

Applicable to: IAM-08.01B, IAM-08.02B, IAM-08.03B, IAM-08.01AC

Authentication information as referred to in the basic criterion is cloud service provider data.

Applicable to: IAM-08.01AC

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

Supplementary Information - Complementary Customer Criteria

If cloud service customers operate virtual machines or containers with the cloud service, they ensure through suitable controls that the confidentiality of the information is also ensured for the allocation of authentication information of the virtual machines or containers.

IAM-09 Authentication Mechanisms

Basic Criteria

IAM-09.01B

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.

IAM-09.02B

Access to the production environment requires two-factor or multi-factor authentication.

IAM-09.03B

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).

IAM-09.04B

The authentication requirements are derived from a risk assessment and documented, communicated and provided in an authentication policy according to SP-01. Compliance with the requirements is enforced by the configuration of the system components, as far as technically possible. The authentication policy describes at least the following aspects:

- The selection of mechanisms suitable for every type of identity and each level of risk;
- The protection of credentials used by the authentication mechanism;
- The generation and distribution of credentials for new identities;
- Rules for the renewal of credentials, including periodic renewals, renewals in case of loss or compromise; and
- Rules on the required strength of credentials, together with mechanisms to communicate and enforce the rules.

IAM-09.05B

It is ensured that all system components under the responsibility of the cloud service provider used to provide the cloud service are neither acquired nor employed with an unchangeable authentication method.

IAM-09.06B

All authentication mechanisms include a mechanism to disable an identity after a predefined number of unsuccessful attempts.

IAM-09.07B

For access to non-personal identities assigned to multiple persons, the cloud service provider implements measures that require the users to be authenticated with their identity assigned to a single person, before being able to access these identities assigned to multiple persons.

Additional (Sharpening)

–

Additional (Complementing)

IAM-09.01AC

Access to the non-production environment requires two-factor or multi-factor authentication.

IAM-09.02AC

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 Criteria

–

Supplementary Information - Complementary Customer Criteria

If cloud service customers operate virtual machines or containers with the cloud service, they ensure through suitable controls that the authentication mechanisms cover container-specific scenarios, such as multi-factor authentication for container hosts and registry access.

IAM-10 Internal Authorisation Mechanisms

Basic Criteria

IAM-10.01B

The cloud service provider ensures that access to its internal data and system functions is controlled and restricted to authorised personnel.

IAM-10.02B

The cloud service provider establishes processes and technical controls to manage and verify access permissions within its internal systems.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

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 Cryptographic Mechanisms

Basic Criteria

CRY-01.01B

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

- Usage of encryption procedures and secure network protocols that correspond to the state-of-the-art;
- Usage of hash functions and salt values, that both correspond to the state-of-the-art;
- Usage of signature schemes that correspond to the state-of-the-art;
- Risk-based provisions for the use of encryption and authentication which are aligned with the information classification schemes (cf. AM-09) and consider the communication channel, type, strength and quality of the encryption;
- Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal, backup, restoration and deletion of the keys;
- Requirements for the rotation of cryptographic keys that follow industry best practices and consider the potential risk of information exposure;
- Consideration of relevant legal and regulatory obligations and requirements;
- Documentation of a change management process for managing cryptographic, encryption, authentication and key management technology changes; and
- Consideration of crypto-agility to allow for efficient substitution of implemented cryptographic mechanisms during their intended lifetimes.

CRY-01.02B

Reviews of policies and instructions regarding cryptographic mechanisms include checks for compliance with the BSI technical guideline for cryptographic mechanisms valid at the given time (BSI TR-02102). Deviations are analysed and documented in a risk assessment. Remediation measures are to be taken based on risk.

Additional (Sharpening)

–

Additional (Complementing)

CRY-01.01AC

The cloud service provider has defined and documented a Post-Quantum-Cryptography (PQC) strategy according to SP-01 to address threats posed by adversaries in possession of a quantum computer.

CRY-01.02AC

The cloud provider's PQC strategy is aligned with cryptography policies and procedures and includes the following aspects:

- Maintenance of an inventory of cryptographic mechanisms in use, including priority levels to each inventory item based on the impact and probabilities of the risks posed by quantum computing attacks and the effort to remediate such risks;
- Staying informed about encryption measures that are deemed state-of-the-art and secure against adversaries who possess a quantum computer;
- Usage of hybrid cryptography models to ensure security for both quantum and non-quantum computing based attacks; and
- Definition of trigger events, required resources, transition plans and success criteria for implementation of post-quantum cryptographic mechanisms.

CRY-01.03AC

The PQC strategy, including the inventory and risk assessment, is reviewed at least annually or in case of significant changes impacting the PQC strategy.

Supplementary Information

About the Criteria

Applicable to: CRY-01.01B, CRY-01.02B, CRY-01.01AC, CRY-01.02AC

The following Technical Guidelines (valid at the given time) provide recommendations and key lengths for state-of-the-art cryptographic mechanisms:

- BSI TR-02102-1 Cryptographic Mechanisms: Recommendations and Key Lengths;

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

If cloud service customers operate virtual machines or containers with the cloud service, appropriate encryption should be provided for virtual machines and containers where possible.

A change management process in the sense of the basic criterion can either be covered by the standard change management process described in DEV-03 or can be implemented as a separate process.

The risk assessment as part of the Post-Quantum-Cryptography strategy should consider:

- The threat landscape posed by advancements in quantum computing;
- Advancements in cryptographic mechanisms that are deemed secure against attackers in possession of a quantum computer;
- Vulnerabilities inherent to the cryptographic mechanism; and
- Vulnerabilities resulting from how cryptographic mechanisms are deployed (e.g. keys which are in use for an extended period of time and the data protected by those keys could already be harvested today and decrypted at a later date).

Supplementary Information - Complementary Customer Criteria

–

CRY-02 Cryptographic Change Management

Basic Criteria

CRY-02.01B

When implementing changes to cryptographic systems, the cloud service provider performs an evaluation of their potential impact. This process includes an analysis of downstream effects, such as residual risk, costs, and benefits that could arise from the planned changes to prevent any unforeseen consequences on the organisation's cryptographic systems.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure through suitable controls that, if notified about any changes to cryptographic systems by the cloud service provider, they engage actively in a thorough evaluation of potential impacts on their usage of the cloud service.

CRY-03 Review of Cryptography Practices

Basic Criteria

CRY-03.01B

The cloud service provider ensures that encryption, authentication and key management practices are regularly audited in accordance with COM-02 to identify and address potential vulnerabilities. At a minimum, reviews are performed annually and immediately following security incidents involving cryptographic components.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: CRY-03.01B

Further criteria for key management are found in criteria CRY-06, CRY-07, CRY-09 - CRY-19

Supplementary Information - Complementary Customer Criteria

–

CRY-04 Protection of Data for Transmission (Transport Protection)

Basic Criteria

CRY-04.01B

The cloud service provider has established procedures and technical measures for state-of-the-art encryption and authentication for the transmission of cloud service customer data and cloud service derived data both to or by the cloud service provider over public networks.

The cloud service provider uses state-of-the-art cryptographic mechanisms to protect the communication during remote access to the production environment, including personnel authentication.

Additional (Sharpening)

CRY-04.01AS, sharpening CRY-04.01B

The cloud service provider has established procedures and technical measures for state-of-the-art encryption and authentication for the transmission of all data.

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: CRY-04.01B, CRY-04.01AS

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. Configuration of the TLS protocol 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)'. Cipher Suites should provide Perfect Forward Secrecy. Generally, the use of wildcard certificates is not considered a secure procedure.

Supplementary Information - Complementary Customer Criteria

Cloud service 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.

CRY-05 Encryption of Sensitive Data at Rest

Basic Criteria

CRY-05.01B

The cloud service provider has established procedures and technical safeguards to encrypt cloud service customer data during storage (i.e. at rest).

CRY-05.02B

The private keys used for encryption are known only to the cloud service customer in accordance with applicable legal and regulatory obligations and requirements. Exceptions follow a specified procedure.

CRY-05.03B

The procedures for the use of private keys, including any exceptions, are contractually agreed with the cloud service customer.

CRY-05.04B

The cloud service provider notifies cloud service customers of security relevant updates of these procedures and technical safeguards and of changes in the

storage of cloud service customer data that may affect the confidentiality of the data.

Additional (Sharpening)

–

Additional (Complementing)

CRY-05.01AC

The cloud service provider ensures that secure encryption mechanisms are in place to prevent the recovery of cloud service customer data when resources are reallocated or physical media are recovered.

Supplementary Information

About the Criteria

Applicable to: CRY-05.02B, CRY-05.03B, CRY-05.04B, CRY-05.01AC

An exception to the requirement that keys are known only to the cloud service customers may be the use of a master key by the cloud service provider. If the cloud service provider uses a master key, the cloud service provider regularly tests the suitability of the design and operating effectiveness of the respective controls.

The requirement of 'known to the customer exclusively' means that encryption keys remain solely within the knowledge and control of the owner. This can be addressed by implementing a secure key management system. If a key management system is used, the keys need to be protected from usage not explicitly authorised by the owner of the key and remain inaccessible in plaintext.

This criterion does not apply to data that cannot be encrypted for the provision of the cloud service for functional reasons.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure through suitable controls for those 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.

CRY-06 Secure Key Generation

Basic Criteria

CRY-06.01B

Procedures and technical safeguards for the secure generation of keys for different cryptographic systems and applications are documented and implemented. These safeguards should require the use of secure random bit generators or generation based on keys that were created in this fashion.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: CRY-06.01B

For the definition of secure random number generators, cloud service providers should refer to BSI TR-02102-1 (Chapter 8).

The cloud service provider protects the keys which are created and inserted into the cloud service by the cloud service customers according to the same criteria as the keys created by the cloud service provider.

Supplementary Information - Complementary Customer Criteria

–

CRY-07 Rotation of Cryptographic Keys

Basic Criteria

CRY-07.01B

The cloud service provider has established a schedule for rotating cryptographic keys that aligns with the requirements for cryptographic key rotation established in CRY-01. If, based on the results of a risk analysis, the cloud service provider does not perform key rota-

tion, this decision is transparently communicated to the customer.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

CRY-08 Public-Key Certificate Issuance

Basic Criteria

CRY-08.01B

The cloud service provider has documented and implemented procedures to securely issue and obtain public-key certificates, ensuring the integrity and authenticity of cryptographic keys. These procedures include:

- Verification of identity before issuing public-key certificates to ensure they are granted to legitimate entities;
- Secure methods for issuing certificates to prevent unauthorised access; and
- Procedures for obtaining public-key certificates from trusted Certificate Authorities to ensure the authenticity of the certificates used.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

CRY-09 Secure Key Provisioning

Basic Criteria

CRY-09.01B

The cloud service provider has documented and implemented procedures and technical measures to ensure that cryptographic keys are provisioned and activated securely within its area of responsibility. These procedures include the verification of identity and authorisation before provisioning and activating keys to ensure they are granted to legitimate entities.

CRY-09.02B

Provisioned keys include activation and deactivation dates to ensure that their use is time limited.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

CRY-10 Secure Storage of Keys

Basic Criteria

CRY-10.01B

The cloud service provider has documented and implemented technical measures for the secure storage of cryptographic keys. This includes ensuring separation of the key management system from the application and middleware layers, defining how authorised users gain access and addressing the geographic residency of keys to comply with legal, regulatory, and security requirements.

Additional (Sharpening)

–

Additional (Complementing)

CRY-10.01AC

For the secure storage of cryptographic keys, the cloud service provider uses a suitable software or hardware security module.

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

CRY-11 Cryptographic Key Archival

Basic Criteria

CRY-11.01B

The cloud service provider has documented and implemented procedures and technical measures for the secure archiving of cryptographic keys. These include:

- Storage of archived keys in a secure repository to prevent unauthorised access;
- Restriction of access to archived keys to authorised personnel based on the principle of least privilege;
- Support of later recovery of information through archived keys;
- Retention of archived keys only for as long as needed and secure destruction afterwards; and
- Logging of all activities related to the storage and recovery of archived keys.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

CRY-12 Cryptographic Key Transition Management

Basic Criteria

CRY-12.01B

The cloud service provider has documented and implemented procedures to oversee the transition of cryptographic keys, including their movement into and out of suspension. These procedures ensure that all key transitions are thoroughly monitored, reviewed, and approved to maintain security and compliance with applicable laws and regulations.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

CRY-13 Handling of Compromised Keys

Basic Criteria

CRY-13.01B

The cloud service provider manages the use of compromised cryptographic keys to ensure they are only used in controlled circumstances and solely for decryption or verification (in case of signature keys), while adhering to legal and regulatory requirements.

CRY-13.02B

The cloud service provider notifies affected customers without undue delay that their keys have been compromised and will no longer be used for encryption.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

CRY-14 Secure Deactivation of Cryptographic Keys

Basic Criteria

CRY-14.01B

The cloud service provider has documented and implemented procedures to deactivate cryptographic keys once they expire. These procedures ensure that:

- Expired keys are no longer used for encryption purposes, but may still be used for decryption if necessary;
- Expired keys are no longer used for signature creation, but may still be used for signature verification;
- Deactivated keys are eventually destroyed when they are no longer required, with relevant metadata retained for auditing; and
- All actions related to key deactivation and destruction are recorded in the key management system to maintain a detailed audit log.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

CRY-15 Requirements for Pre-Shared Keys

Basic Criteria

CRY-15.01B

If pre-shared keys or wildcard certificates are used, the cloud service provider has documented and implemented dedicated procedures and technical measures to ensure their secure use and provisioning.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

CRY-16 Operational Continuity for Key Management

Basic Criteria

CRY-16.01B

The cloud service provider has assessed the balance between conducting backups of key material stored in a Hardware Security Module (HSM) for key restoration and building redundancy or comparable measures for securing keys to ensure operational continuity. This assessment includes evaluating the risk of key exposure if control over the key material is lost. Decisions regarding whether to use the backups of keys or to establish redundancy are documented, and the chosen measures are reviewed for their effectiveness and compliance with legal and regulatory requirements.

CRY-16.02B

Procedures for the recovery of lost or corrupted keys are in place.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: CRY-16.01B, CRY-16.02B

The cloud service provider should consider the following options for safeguarding key material:

- Backup of keys: Encrypted backups of keys are stored securely outside the HSM. The backup process should ensure that the keys are encrypted during storage and transit to prevent unauthorised access. Regular testing of backup and recovery procedures should be carried out to verify the effectiveness and integrity of the backups. Backups outside a HSM should only be considered after dilligent risk analysis.
- Redundant HSMs: Implementing multiple HSMs in geographically dispersed locations to create redundancy to ensure that keys remain available and secure even if one HSM fails. The HSMs should be synchronised to ensure consistency of key material across all devices. Regular health checks and failover tests are necessary to ensure that redundancy mechanisms function correctly. The particular manner this redundancy is built may depend on the details of the contractual agreements between provider and customer. E.g. when the customer choose a particular location, zone or region, this choice also applies to the redundancy mentioned in this criterion.

Supplementary Information - Complementary Customer Criteria

–

CRY-17 Cryptographic Key Lifecycle Management

Basic Criteria

CRY-17.01B

The cloud service provider has documented and implemented procedures and technical measures to monitor and document the lifecycle of cryptographic keys and materials. These measures ensure detailed records of each key from creation to destruction, including any status changes.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

CRY-18 Usage of External Key Management Systems

Basic Criteria

CRY-18.01B

In the case that external key management systems (KMS) are integrated into the service, the cloud service provider ensures that the procedures and technical measures for the usage of external key management systems (KMS) are established. The following aspects are taken into account:

- The external KMS have recognised security certifications that reflect the state of the art to comply with legal, regulatory and contractual requirements;
- The integration of the external KMS into the cloud infrastructure is secure to ensure the confidentiality, integrity, and availability of the keys;
- Strict access control are implemented to ensure that only authorised users and systems can access the keys (cf. IAM-01);
- Procedures for the regular rotation and renewal of keys are defined and implemented to ensure the security of the keys (cf. CRY-07); and
- All accesses and operations on the external KMS are logged and monitored to detect and respond to suspicious activities. The cloud service provider ensures that the external KMS is regularly checked for vulnerabilities and updated to meet current threats and technological developments.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure that their own key management procedures are compatible with the requirements of the external KMS and that they implement appropriate controls to ensure the security of their keys.

CRY-19 Secure Handling of Customer Managed Keys

Basic Criteria

CRY-19.01B

The cloud service provider implements procedures and technical safeguards to ensure the secure handling of cryptographic keys managed by cloud service customers. In these procedures, the following aspects are considered:

- Secure integration of customer-managed keys into the cloud environment;
- Logging of all activities related to customer-managed keys; and
- Definition of access control mechanisms to enable that only authorised users can gain access to customer-managed keys.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure through suitable controls that their agreements with the cloud service provider include robust procedures and technical safeguards for the secure handling of customer-managed cryptographic keys. Cloud service customers ensure that these procedures address the secure integration of their keys into the cloud environment, comprehensive logging of all activities related to their keys, and clearly defined access control mechanisms to restrict access solely to authorised users.

CRY-20 Regular Updates of Cryptographic Mechanisms and Procedures

Basic Criteria

CRY-20.01B

The cloud service provider ensures that the procedures and technical measures for cryptography are regularly updated to align with the state of the art. The following aspects are taken into account:

- Ensure that all cryptographic guidelines are up to date;
- All changes and adjustments to key management procedures are documented and traceable;
- A regular review cycle is defined to ensure that the procedures and measures always align with the state of the art; and
- Employees responsible for key management are regularly trained and informed about respective changes.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: CRY-20.01B

The state-of-the-art of cryptographic mechanisms 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).

Supplementary Information - Complementary Customer Criteria

–

5.9 Communication Security (COS)

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

COS-01 Technical Safeguards

Basic Criteria

COS-01.01B

Based on the results of a risk analysis carried out according to OIS-07, the cloud service provider has implemented technical safeguards which are suitable to promptly detect and respond to attacks on the network of information systems used for provisioning of the cloud service.

COS-01.02B

For these technical safeguards, technologies are used that provide protection and prevention at multiple tiers (defence in depth) within the cloud service to mitigate the risk of a vulnerability or bypass technique being able to effectively breach the deployed defensive systems. This includes network-based cyber attacks such as:

- Attacks on the basis of irregular incoming or outgoing traffic patterns;
- Distributed Denial-of-Service (DDoS) attacks;
- Spoofing attacks;
- Code injection attacks;
- DNS tunneling; and
- IoT attacks targeting devices within a network.

COS-01.03B

Data from corresponding technical safeguards implemented (cloud service provider data) is fed into the organisation's SIEM system (cf. OPS-13), so that (counter-) measures regarding correlating events can be initiated. The safeguards are documented, communicated and provided in accordance with SP-01.

Additional (Sharpening)

–

Additional (Complementing)

COS-01.01AC

Technical measures ensure that no unknown (physical or virtual) devices join the cloud service provider's (physical or virtual) network.

Supplementary Information

About the Criteria

Applicable to: COS-01.02B, COS-01.01AC

Technical safeguards that provide protection and prevention at multiple tiers are e.g. a special separation in Identity and Access Management, separate logging for protective systems and Web Application Firewalls (WAFs) for accessing protective systems.

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.

Supplementary Information - Complementary Customer Criteria

Cloud service 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.

COS-02 Security Requirements for Connections in the Cloud Service Provider's Network

Basic Criteria

COS-02.01B

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 service customers are to be logically or physically separated;
- Which communication relationships and which network and application protocols are permitted in each case;
- How the data traffic for administration and monitoring is separated from each on network level;
- Which internal, cross-partition communication is permitted; and
- Which cross-network communication is allowed.

The cloud service provider establishes and maintains an accurate representation of the technical and logical structure of the cloud service provider's systems based on its network topology documentation (cf. COS-07) and asset inventory (cf. AM-02).

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: COS-02.01B

Cross-partition communication can be realised for e.g. individual regions or locations via e.g. WAN, LAN, VPN, RAS.

Supplementary Information - Complementary Customer Criteria

–

COS-03 Monitoring of Connections in the Cloud Service Provider's Network

Basic Criteria

COS-03.01B

The cloud service provider distincts between trusted and untrusted networks. Based on a risk assessment according to OIS-07, these are separated into different security zones for internal and external network areas (and DMZ, if applicable).

COS-03.02B

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.

COS-03.03B

The cloud service provider ensures that the configuration of networks matches the security requirements (cf. COS-02) regardless of the means used to create the configuration. The cloud service provider reviews at least annually the design and implementation of configuration of the connections with regard to the defined security requirements.

COS-03.04B

Identified vulnerabilities and deviations are subject to risk assessment in accordance with the risk management procedure (cf. OIS-07) and follow-up measures are defined and tracked (cf. OPS-18).

COS-03.05B

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 (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: COS-03.03B, COS-03.04B, COS-03.05B

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

Supplementary Information - Complementary Customer Criteria

Cloud service 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 service customer's organisational units).

COS-04 Cross-Network Access

Basic Criteria

COS-04.01B

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 service customers.

Additional (Sharpening)

COS-04.01AS, sharpening COS-04.01B

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

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: COS-04.01B, COS-04.01AS

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

Supplementary Information - Complementary Customer Criteria

Cloud service 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.

COS-05 Networks for Administration

Basic Criteria

COS-05.01B

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 service customer's network and protected from unauthorised access by multi-factor authentication (cf. IAM-09).

COS-05.02B

Networks used by the cloud service provider to migrate or create virtual machines are also physically or logically separated from other networks.

Additional (Sharpening)

–

Additional (Complementing)

COS-05.01AC

When the administration networks are not physically separated from other networks, the administration flows are protected using a state-of-the-art encrypted communication.

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

COS-06 Separation of Data Traffic in Jointly Used Network Environments

Basic Criteria

COS-06.01B

Cloud service customer data traffic in jointly used network environments is separated on network level according to a documented concept to ensure the confidentiality and integrity of the data transmitted.

Additional (Sharpening)

–

Additional (Complementing)

COS-06.01AC

In the case of IaaS/PaaS, the secure separation is ensured by physically separated networks or by means of state-of-the-art encrypted VLANs or other network encapsulating techniques.

Supplementary Information

About the Criteria

Applicable to: COS-06.01B, COS-06.01AC

If the cloud service provider does not use shared network environments for cloud service customers and instead uses a physical separation, the basic criterion is not applicable.

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 separation of stored and processed data is subject of the criterion OPS-24. After successful authentica-

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

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

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure through suitable controls for those 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 organisational units).

COS-07 Documentation of the Network Topology

Basic Criteria

COS-07.01B

The documentation of the logical structure of the network used to provide 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, how the network is zoned and segmented, how it connects with third party and public networks and how the data flows between different subnets and system components within the network.

COS-07.02B

The partions, regions, zones or location in which the cloud service customer data is stored are indicated.

COS-07.03B

In liaison with the inventory of assets (cf. AM-02), the documentation includes the equipment that provides security functions and the servers that host the data or provide sensitive functions.

COS-07.04B

The cloud service provider performs a full review of the network topology documentation at least once a year.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: COS-07.01B

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

Supplementary Information - Complementary Customer Criteria

–

COS-08 Policies for Data Transmission

Basic Criteria

COS-08.01B

Policies and instructions with technical and organisational safeguards in order to protect the transmission of cloud service customer data, cloud service derived data, cloud service provider data and account data against unauthorised interception, manipulation, copying, modification, redirection, destruction or malware intrusion are documented, communicated and provided according to SP-01. The policies and instructions establish a reference to the Asset Classification and Labelling (cf. AM-09) and cryptography (cf. CRY-01).

COS-08.02B

Technical measures outlined in the documented policies and instructions to protect the transmission of data are implemented. These measures are regularly verified to maintain their operating effectiveness.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: COS-08.01B, COS-08.02B

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-04.

Supplementary Information - Complementary Customer Criteria

Cloud service 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.

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 service 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 Criteria

PI-01.01B

The cloud service provider establishes and maintains policies and procedures to document how the cloud service can be accessed by other cloud services or IT systems of cloud service customers through documented inbound and outbound interfaces. These policies and procedures specifically address:

- The use of standardised communication protocols for interactions between different application interfaces to ensure the confidentiality and integrity of the transmitted information according to its protection requirements, and the adequate authentication of the user;
- The use of encryption according to CRY-02 in case of communication over untrusted networks;
- The use of standardised data formats and common data processing standards to facilitate information processing interoperability; and
- The implementation of mechanisms to validate data integrity and establish backup and recovery processes to ensure data security and reliability during exchange, usage and transfer.

PI-01.02B

The policies and procedures contain clear documentation on the interfaces to provide subject matter experts with detailed guidance to facilitate effective usage for their intended purpose. This documentation is tailored to meet the needs of cloud service customers' subject matter experts and is kept up to date to reflect the current version of the cloud service intended for productive use.

Additional (Sharpening)

–

Additional (Complementing)

PI-01.01AC

The cloud service provider sets up an application firewall to protect the administration interfaces for cloud service customers that are accessible over public networks.

PI-01.02AC

The cloud service provides cloud service customers with interfaces for custom identity providers to manage cloud user access information and authentication. These interfaces are accompanied by a standardised protocol to facilitate communication between the cloud service and the external identity provider.

PI-01.03AC

The interfaces are clearly documented to enable subject matter experts of the cloud user to integrate their identity provider with the cloud service.

Supplementary Information

About the Criteria

Applicable to: PI-01.01B, PI-01.02B, PI-01.01AC, PI-01.02AC, PI-01.03AC

In this context, an interface is a system access point or library function with a well-defined syntax. It comprises documented methods that allow cloud service customers to securely access and interact with the cloud service, enabling the exchange of data.

While these interfaces provide the means for communication with the cloud service, they do not imply that cloud service customers can directly connect their custom systems as if they are natively integrated. Instead, cloud service customers can configure their systems by using methods, such as API calls, and adhering to the specified protocols and data formats provided by the cloud service provider.

To ensure seamless and secure communication between interfaces, the cloud service provider uses industry-standard API protocols and implements state-of-the-art transport layer security. The cloud service provider supports cross-platform information processing by employing containerisation technologies and cloud-neutral development frameworks. Infrastructre as Code practices are adopted to standardise infrastructre provisioning. Common data usage policies are defined and enforced to ensure consistent and secure access, utilisation and sharing of data. Upon contract termination, the cloud service provider assists customers in exporting and transferring their data, e.g. by providing technical documentation and data export tools.

Supplementary Information - Complementary Customer Criteria

Cloud service 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.

PI-02 Contractual Agreements for the Provision of Data

Basic Criteria

PI-02.01B

In contractual agreements, the following aspects are defined for provisioning of data, insofar as these are applicable to the cloud service:

- Type, scope and format of the cloud service customer data the cloud service provider provides to the cloud service customer;
- Delivery methods of the data to the cloud service customer;
- Conditions and timeframes for cloud service customer data provisioning throughout the duration of the contractual relationship;
- Right of termination of the contract and definition of the timeframe, within which the cloud service provider makes the cloud service customer data available to the cloud service customer after termination of the contract;
- Definition of the point in time as of which the cloud service provider makes the cloud service customer data inaccessible to the cloud service customer and deletes these after termination of the contract;
- The cloud service customers' responsibilities and obligations to cooperate for the provision of the cloud service customer data; and
- Cloud service customer data remains the property of the cloud service customer throughout the entire contractual relationship. After its termination, the data is once again the sole property and possession of the cloud service customer.

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 (Sharpening)

–

Additional (Complementing)

PI-02.01AC

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.

PI-02.02AC

The cloud service provider also provides cloud service derived data to the cloud service customer upon termination of the contractual relationship. The provision of this data is also defined in the contractual agreements and includes the aspects specified in the basic criterion.

Supplementary Information

About the Criteria

Applicable to: PI-02.01B, PI-02.01AC, PI-02.02AC

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-like services, the cloud service 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 service customer has set up within its environment (e.g. configuration of networks, images of virtual machines and containers).

With SaaS, the cloud service customer typically relies on export functions provided by the cloud service provider. Data created by the cloud service 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.

If contractual agreements do not include the aspects listed in the basic criterion, although these aspects are applicable to the cloud service due to its service model, the criterion is not met and a deviation is to be noted by the auditor.

Supplementary Information - Complementary Customer Criteria

Cloud service 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.

PI-03 Secure Deletion of Data

Basic Criteria

PI-03.01B

The cloud service provider's procedures for deleting cloud service customer data, cloud service derived data and Account data upon termination of the contractual relationship ensure compliance with the contractual agreements (cf. PI-02), except as required by a valid court order or as needed to fulfil known future financial and legal obligations.

PI-03.02B

The deletion procedures prevent recovery by state-of-the-art forensic means.

PI-03.03B

The cloud service provider documents the deletion of the cloud service customer data, cloud service derived data and Account data in a manner that enables the cloud service customer to obtain proof of the deletion of its data.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: PI-03.01B, PI-03.02B

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

Supplementary Information - Complementary Customer Criteria

Cloud service 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.

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

Objective: Ensure information security in the development cycle of cloud service system components.

DEV-01 Policies for the Development/Procurement of System Components

Basic Criteria

DEV-01.01B

Policies and instructions with technical and organisational measures for the secure development of system components 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 and quality in software development (requirements, design, implementation, testing and verification) including the existence of a security by design principle, enforcing the consideration of information security requirements in the software development phase;
- Security and quality in software deployment (including continuous delivery);
- Security and quality in operation (reaction to identified faults and vulnerabilities); and
- Secure coding standards and practices (reducing the introduction of vulnerabilities in code).

DEV-01.02B

Guidelines for the secure development of the cloud service define principles to ensure the system architecture and software operated by the cloud service provider within the production environment are designed in such a way that access to cloud service customer data by the cloud service provider is minimised wherever possible.

DEV-01.03B

The policies and instructions for the secure development of system components of the cloud service include measures for the enforcement of specified standards and guidelines, including any applicable automated tools.

Additional (Sharpening)

–

Additional (Complementing)

DEV-01.01AC

In procurement, products are preferred which have been certified according to the 'Common Criteria for Information Technology Security Evaluation' (short: Common Criteria - CC) 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 Criteria

Applicable to: DEV-01.01B, DEV-01.01AC

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

Accepted standards and methods for secure development are, for example:

- ISO/IEC 27034; and
- OWASP Secure Software Development Lifecycle (S-SDLC). Minimisation of customer data access during operation can be supported by following robust security models, such as Zero Trust, during cloud architecture development. Furthermore, aspects such as limiting data interfaces, API calls and access as well as ensuring end-to-end-encryption from transit to storage are relevant considerations.

For quality assurance in software development, the following can be considered to be relevant processes:

- Planning and definition of quality objectives: Definition of quality requirements based on customer needs and objectives, taking into account the requirements of the cloud system to be developed.
- Design phase: Carrying out design reviews and inspections of the cloud service to ensure that the design meets the quality requirements.
- Development phase: Use of code reviews and pair programming to ensure code quality. Use of static analysis tools to check the code for potential errors and violations of coding standards.
- Testing phase: Execution (automated where possible) of various types of tests (e.g. unit tests, integration tests, system tests, acceptance tests) to ensure the functionality and quality of the software.
- Integration and continuous integration (CI): Integration of the various software components and continuous checking of the integrations through automated builds and tests. Use of CI/CD pipelines to ensure that the code is regularly integrated and tested.
- Release and deployment: Preparation and implementation of the software release in accordance with defined quality standards.
- Maintenance and continuous improvement: Monitoring the software in operation to ensure that it continues to meet the quality requirements. This includes post release activities such as bug fixing and performance optimisation processes. Additionally, post-mortem analyses should be performed to learn from incidents and optimise processes for future releases.

An accepted standard and a method for quality in development processes is, for example, Google Site Reliability Engineering (SRE).

The scope of the DEV criteria and the requirements within includes not only the development of software applications but also platforms, virtual infrastructure, and other system components.

Supplementary Information - Complementary Customer Criteria

–

DEV-02 Outsourcing of the Development

Basic Criteria

DEV-02.01B

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, ensuring a security level equivalent to that of the cloud service provider's internal development;
- 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.

Before subcontracting the development of the cloud service or components thereof, the cloud service

provider conducts a risk assessment according to SSO-02 that considers at least the following aspects:

- Management of source code by the subcontractor;
- Availability of source code to the cloud service provider and where applicable, to evaluators;
- Human resource procedures implemented by the subcontractor;
- Required access to the cloud service provider's development, test and preproduction environments; and
- Security procedures related to the management of the subcontractor's service organisations.

Additional (Sharpening)

–

Additional (Complementing)

DEV-02.01AC

The cloud service provider documents and implements a procedure that makes it possible to supervise and control the outsourced development activity, in order to ensure that the outsourced development activity is compliant with the secure development policy of the cloud service provider and makes it possible to achieve a level of security of the external development that matches that of internal development.

DEV-02.02AC

Personnel of the cloud service provider run the tests that are relevant for the deployment decision when a change includes the result of outsourced development.

Supplementary Information

About the Criteria

Applicable to: DEV-02.01B

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.

Supplementary Information - Complementary Customer Criteria

–

DEV-03 Policies for Changes to System Components

Basic Criteria

DEV-03.01B

Policies and instructions with technical and organisational safeguards for change management of system components of the cloud service 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 separation of duties during development, testing and release of changes;
- Requirements for the proper information of cloud service 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;
- Requirements for the implementation and documentation of emergency changes that shall, to the extent possible in the emergency, comply with the same level of security as normal changes;

- Requirements for the handling of a change's unexpected effects, including corrective actions; and
- Requirements for the development of security features that implement technical mechanisms and safeguards, with increased testing requirements.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: DEV-03.01B

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 also fall under this criterion and should also undergo a specified procedure, as they are necessary for effective separation of cloud service customers.

Changes to the container environments, including the management of container images and versions, should also go through a regulated process.

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

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

A centralised change management process is not mandatory. The cloud service provider has the flexibility to adopt change management practices that best fit its operational needs, including agile methods, as long as they adhere to the technical and organisational safeguards.

Supplementary Information - Complementary Customer Criteria

–

DEV-04 Safety Training and Awareness Programme Regarding Continuous Software Delivery and Associated Systems, Components or Tools

Basic Criteria

DEV-04.01B

The cloud service provider provides a training programme for regular, target group-oriented security training and awareness for internal and external employees on standards and methods for:

- Secure software development and provision as well as on how to use the tools used for this purpose; and
- Risks linked to malicious code and best practices to reduce the impact of an infection.

DEV-04.02B

The programme is regularly reviewed and updated with regard to the applicable policies and instructions, the assigned roles and responsibilities and the tools used.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

DEV-05 Design Documentation for Security Features

Basic Criteria

DEV-05.01B

Design documentation for security features shall be based on a security analysis of the adequacy and planned effectiveness of the features. This documentation shall include a specification of expected inputs, outputs and possible errors.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

DEV-06 Risk Assessment, Categorisation and Prioritisation of Changes

Basic Criteria

DEV-06.01B

In accordance with the applicable policies (cf. DEV-03), changes are subjected to a risk assessment regarding the likelihood of adversely effects on system components concerned and dependencies with other changes, and are categorised and prioritised accordingly.

DEV-06.02B

If the risk associated to a planned change is high, then appropriate mitigation measures are taken before deploying the change in the cloud service's production environment.

Additional (Sharpening)

–

Additional (Complementing)

DEV-06.01AC

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 service 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 Criteria

–

Supplementary Information - Complementary Customer Criteria

–

DEV-07 Testing Changes

Basic Criteria

DEV-07.01B

Changes to the cloud service are subject to appropriate testing according to documented test procedures during software development and deployment.

DEV-07.02B

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 service customers are involved into the tests in accordance with the contractual requirements.

DEV-07.03B

Before using cloud service customer data for tests, the cloud service provider first obtains approval from that cloud service customer and anonymises the cloud service customer data. The cloud service provider ensures the confidentiality of the data during the whole process.

DEV-07.04B

The tests of the security features provide full coverage of the specification, including all specified error conditions. The documentation of these tests includes at least a description of the test, the initial conditions, the expected outcome and instructions for running the test.

DEV-07.05B

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 (Sharpening)

–

Additional (Complementing)

DEV-07.01AC

Pre-launch penetration tests are carried out during the test phase of the cloud service in accordance with the penetration test concept (cf. OPS-22 additional criterion). The severity of identified vulnerabilities is assessed according to defined criteria and actions for timely remediation or mitigation are initiated.

Supplementary Information

About the Criteria

Applicable to: DEV-07.01B, DEV-07.01AC

Tests should be used that contribute to the quality assurance of the software development as well as to the security of the cloud service.

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

Supplementary Information - Complementary Customer Criteria

Where changes are to be tested by the cloud service customers in accordance with the contractual agreements prior to deployment in the production environment, the cloud service 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.

DEV-08 Logging of Changes

Basic Criteria

DEV-08.01B

System components for version control and software deployment that are used to manage changes to system components of the cloud service in the production environment are subject to a role and rights concept according to IAM-01 and authorisation mechanisms.

DEV-08.02B

The configuration of these system components ensures that all changes to system components in the production environment are recorded and can be traced back to the individuals or system components contributing to their development, deployment or implementation.

Additional (Sharpening)

–

Additional (Complementing)

DEV-08.01AC

The changes to system components of the cloud service in the production environment are monitored to enforce the role and rights concept. Any deviations identified during monitoring are addressed through timely and appropriate remediation measures.

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

DEV-09 Version Control

Basic Criteria

DEV-09.01B

The cloud service provider uses a version control system. The configuration of the system ensures that the confidentiality, integrity and authenticity of the source code is adequately protected at all stages of development.

DEV-09.02B

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

DEV-09.03B

Version control covers all internally and externally developed software, configurations and third party commercial products under the responsibility of the cloud service provider.

Additional (Sharpening)

–

Additional (Complementing)

DEV-09.01AC

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

DEV-09.02AC

The cloud service provider retains a history of the software versions and of the systems that are implemented in order to be able to reconstitute, where applicable in a test environment, a similar environment such as was implemented.

The retention time for this history is risk-based (cf. OIS-07) defined in the policy for version control and aligned to the support life cycle of the cloud service.

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

DEV-10 Approvals for Provision in the Production Environment

Basic Criteria

DEV-10.01B

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 service customers in the production environment.

DEV-10.02B

Cloud service customers are involved in the release according to contractual agreements.

Additional (Sharpening)

–

Additional (Complementing)

DEV-10.01AC

The approval processes is monitored. Any deviations identified during monitoring are addressed through timely and appropriate remediation measures.

Supplementary Information

About the Criteria

Applicable to: DEV-10.01B

The definitions for criterion DEV-03 apply.

Applicable to: DEV-10.02B

If the contractual agreements do not foresee customer involvement of the approval, this should be clearly stated in the contractual agreements in order to fulfill this criterion.

Supplementary Information - Complementary Customer Criteria

Where changes are to be approved by the cloud service customers in accordance with the contractual agreements before they are made available in the production environment, the cloud service 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.

DEV-11 Protection of Development and Test Environments

Basic Criteria

DEV-11.01B

Development and test environments under the responsibility of the cloud service provider undergo a risk assesssment and are protected with appropriate security measures. This includes identifying potential risks and implementing safeguards to ensure the security of these environments.

DEV-11.02B

The cloud service provider includes the development environment as part of the backup plan in accordance with the backup concept (cf. OPS-06).

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

DEV-12 Separation of Environments

Basic Criteria

DEV-12.01B

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

DEV-12.02B

Unless unavoidable, the cloud service provider does not reuse the cryptographic secret and private keys and other secrets used in production environments in other, non-production environments. Any unavoidable reuse of the cryptographic secret and private keys between production and non-production environments is documented and justified in accordance with the process for handling exceptions (cf. SP-03) and the risk management procedures (cf. OIS-07).

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

DEV-13 Transparency about Software Components

Basic Criteria

DEV-13.01B

The cloud service provider ensures that, as part of the software development process, a Software Bill of Materials (SBOM) is created, maintained, and kept up-to-date for every developed or integrated software component. The structure, content, and management of Software Bills of Materials (SBOMs) should align with state-of-the-art concepts.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: DEV-13.01B

The state-of-the-art regarding the creation, maintenance, and utilisation of SBOMs, including their components and formats, is described in the current version of the BSI Technical Guideline TR-03183-2.

Automated tools for generating, maintaining, and validating SBOMs are recommended to ensure accuracy and integration into security and vulnerability management processes.

Supplementary Information - Complementary Customer Criteria

–

DEV-14 Development Service Organisations Security

Basic Criteria

DEV-14.01B

The cloud service provider maintains a list of dependencies to hardware and software (cf. DEV-13) products used in the development of the cloud service.

DEV-14.02B

Policies and instructions for the use of third party and open source software are documented, communicated and provided in accordance with SP-01.

DEV-14.03B

Third party software is retrieved only from trusted sources and authenticity is verified whenever possible.

Additional (Sharpening)

–

Additional (Complementing)

DEV-14.02AC

In procurement for the development of the cloud service, the cloud service provider performs a risk assessment in accordance with OIS-07 for every hardware and software product.

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

DEV-15 Exceptions to the Change Management Process

Basic Criteria

DEV-15.01B

The cloud service provider implements a procedure for the management of exceptions, including emergencies, in the change management process. This procedure aligns with the requirements of SP-03, ensuring that all exceptions to the standard change management process go through the OIS-07 risk management process and are incorporated in the risk handling measures described in OIS-08.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

DEV-16 Risk Assessments During the Development/Procurement of System Components

Basic Criteria

DEV-16.01B

The cloud service provider conducts risk assessments within the procurement and development lifecycle of system components of the cloud service and implements processes to manage the identified risks. These processes include the following aspects:

- Definition of security requirements that apply to the system components;
- Implementation of security updates during the entire lifecycle of the system components and plans for their replacement after the end of the support period;
- Documentation of all system components;
- Description of the cybersecurity features and configurations for secure operations for all system components; and
- Validation of the adherence to applicable security requirements for all system components.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

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 (subservice provider) can access and monitor the agreed services and security requirements.

SSO-01 Policies and Instructions for Controlling and Monitoring Service Organisations

Basic Criteria

SSO-01.01B

Policies and instructions for controlling and monitoring service organisations (e.g. suppliers, vendors or other third parties) whose services contribute to the development or operation 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 service organisations based on the risk assessment by the cloud service provider and the determination of whether the service organisation is a subservice organisation;
- Information security requirements for the processing, storage or transmission of information by service organisations based on recognised industry standards, and under consideration of the criteria in this catalogue;
- 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 subservice organisations used by the service organisations, insofar as the services provided by these subservice organisations also contribute to the development or operation of the cloud service.

Additional (Sharpening)

–

Additional (Complementing)

SSO-01.01AC

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 system of internal control system that allow the cloud service provider to determine whether the subservice organisation designed and operated controls that are commensurate with the expected complementary subservice organisation controls (CSOC).

SSO-01.02AC

In case no such reports can be provided, the cloud service provider agrees appropriate information and audit rights to assess the design and operations of the service-related system of internal control regarding the expected CSOC.

Supplementary Information

About the Criteria

Applicable to: SSO-01.01B, SSO-01.01AC

The basic criterion applies to all service organisations of the cloud service provider, regardless of applying the 'inclusive' or 'carve-out method'. The additional criterion applies only to those of the service organisations that are considered to be subservice organisations. See section 'Consideration of Subservice Organisations'.

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

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 subservice organisations, these regulations remain unaffected by the C5 criteria.

Supplementary Information - Complementary Customer Criteria

–

SSO-02 Risk Assessment of Service Organisations

Basic Criteria

SSO-02.01B

Service organisations of the cloud service provider undergo a risk assessment in accordance with the policies and instructions for the control and monitoring of service organisations prior to contributing to the development or operation of the cloud service.

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

- Protection needs regarding the confidentiality, integrity, availability and authenticity of cloud service customer data, cloud service derived data, cloud service provider data and account data 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 organisation for the scope, complexity and uniqueness of the provided service, including the consideration of possible alternatives;
- Complementary subservice organisation controls (CSOCs) assumed in the design of cloud service provider's controls to meet the applicable C5 criteria;
- Deviations regarding the design and operation of CSOCs assumed at service organisations considered as subservice organisations and mitigating measures by the cloud service provider to address such deviations; and
- The ability of the cloud service provider to diversify sources of supply and limit vendor lock-in.

SSO-02.02B

The adequacy of the risk assessment is reviewed regularly, at least annually, by qualified personnel of the cloud service provider during service usage.

Additional (Sharpening)

–

Additional (Complementing)

SSO-02.01AC

If the cloud service provider relies on assets from a supplier or on services from subservice organisations to operate the cloud service, the cloud service provider does not allow those suppliers or service organisations to access any cloud service customer data, cloud service derived data or account data, unless it is ensured that all operations requiring access to those data types are performed or supervised by personnel who have been authorised (cf. HR-01).

Supplementary Information

About the Criteria

Applicable to: SSO-02.01B

For assessing risks with service organisations, the cloud service provider can perform coordinated security risk assessments of specific critical ICT services, ICT systems or ICT products provided by service organisations. Apart from the aspects listed in SSO-02 Basic Criterion such a risk assessment should take into account technical and, where relevant, non-technical risk factors.

Supplementary Information - Complementary Customer Criteria

–

SSO-03 Data Processing of Service Organisations

Basic Criteria

SSO-03.01B

If the cloud service provider relies on assets from a supplier or on services from subservice organisations to operate the cloud service, the cloud service provider does not allow those suppliers or service organisations to access any cloud service customer data, cloud service derived data or account data, unless they have performed a risk assessment according to OIS-07 on the possible exposure of cloud service customer data, cloud service derived data or account data.

SSO-03.02B

The cloud service provider obtains written authorisation of the customer prior to the processing of cloud service customer data, cloud service derived data or account data when engaging service organisations. This can be achieved by authorisation of the customer, per service organisation, or by way of a general preauthorisation between the cloud service provider and the customer.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

SSO-04 Directory of Service Organisations

Basic Criteria

SSO-04.01B

The cloud service provider maintains a directory for controlling and monitoring the service organisations who contribute services to the delivery of the cloud service. The following information is maintained in the directory:

- Company name;
- Address;
- Locations of the processing and storage of cloud service customer data, cloud service derived data, cloud service provider data and account data;
- Responsible contact group/person at the service organisation;
- Responsible contact group/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.

SSO-04.02B

The inventory is reviewed at least annually for completeness, accuracy and validity of the information.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: SSO-04.01B

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

Supplementary Information - Complementary Customer Criteria

–

SSO-05 Monitoring of Compliance with Requirements

Basic Criteria

SSO-05.01B

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 service organisation.

SSO-05.02B

Monitoring includes a regular review of the following information to the extent that such information is to be provided by service organisations 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 design and operation of their service-related system of internal control; and
- Records of the service organisations on the handling of vulnerabilities, security incidents and malfunctions.

SSO-05.03B

The frequency of the monitoring corresponds to the classification of the service organisation based on the risk assessment conducted by the cloud service provider (cf. SSO-02).

SSO-05.04B

If a service organisation is considered to be a subservice organisation, the following applies: - The cloud service provider assesses this relationship and carries out appropriate procedures; - These procedures provide reasonable assurance that the subservice organization has designed and operated relevant controls; - The subservice organizations controls correspond to the expected complementary subservice organization controls (CSOCs) assumed in the design of the cloud service providers controls; and - This ensures that the applicable C5 criteria are met.

SSO-05.05B

Identified deviations are subjected to analysis, evaluation and treatment in accordance with the risk assessment of service organisations (cf. SSO-02).

SSO-05.06B

When a change in a third party contributing to the provision of the cloud service significantly adversely affects its level of security, the cloud service provider informs all of its cloud service customers without undue delay.

SSO-05.07B

The cloud service provider establishes and documents a procedure to regularly review non-disclosure or confidentiality requirements for all suppliers involved in providing the cloud service. This procedure is implemented in practice, and the review is conducted at least once per year.

Additional (Sharpening)

–

Additional (Complementing)

SSO-05.01AC

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).

SSO-05.02AC

Identified violations and discrepancies are automatically reported to the responsible personnel or system components of the cloud service provider for prompt assessment and action.

SSO-05.03AC

The cloud service provider defines and implements a process for conducting periodic security assessments for all third parties. The nature and scope of these security assessments correspond to the risk associated with each third party. These risk-based security assessments ensure that third parties meet the required security standards and that any potential risks are identified and mitigated appropriately.

Supplementary Information

About the Criteria

Applicable to: SSO-05.01B, SSO-05.02B, SSO-05.03B, SSO-05.04B, SSO-05.05B, SSO-05.06B, SSO-05.07B, SSO-05.01AC, SSO-05.02AC, SSO-05.03AC

Information obtained for monitoring of the design and operations of the service-related system of internal control typically includes reports in accordance with ISAE 3402, IDW PS 951, SOC 2 or BSI C5.

If such reports are provided by the service organisations, 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 report;

- Modifications of the opinion, deviations/exceptions noted and management's response thereon;
- Complementary User Entity Controls (CUEC) to be designed and operated by the cloud service provider;
- Disclosed subservice organisations incl. any changes among those (e.g. additional subservice organisations); and
- Stated security incidents.

Information on CSOC has to be obtained for subservice organisations only. Not every service organisation is a subservice organisation, see section "Consideration of Subservice Organisations"). Appropriate procedures may comprise the review of independent third party reports, or audit procedures performed by the cloud service provider at the subservice organisation.

The automated monitoring procedures outlined in the additional criterion are only applicable to service organisations for which monitoring automation is feasible based on the nature of the services provided to the cloud service provider.

Supplementary Information - Complementary Customer Criteria

Cloud service 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.

SSO-06 Contract Termination Strategy for Service Organisations

Basic Criteria

SSO-06.01B

The cloud service provider has defined and documented contract termination or exit strategies for the purchase of services where the risk assessment of the service organisations regarding the scope, complexity and uniqueness of the service provided resulted in a very high dependency (cf. Supplementary Information).

SSO-06.02B

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 organisation;
- 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 (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: SSO-06.01B, SSO-06.02B

A very high dependency can be assumed in particular if the purchased service is indispensable for the provision of the cloud service. This situation is the case if the cloud service provider:

- Provides the cloud service from data centres operated by service organisations; or
- Provides a SaaS service and uses the IaaS or PaaS of another cloud service provider.

A very high dependency can also be assumed if the service cannot be obtained within one month from an alternative service organisation, as:

- It is unique on the market and no other service organisation can deliver it;
- It is strongly individualised by the service organisation and/or the cloud service provider;
- It cannot be supplied by any other service organisation in the required quality of service; or
- It requires specific knowledge that is only/mainly available to the current service organisation and not to the cloud service provider.

Supplementary Information - Complementary Customer Criteria

–

SSO-07 Ensuring Transparency within Service Organisations

Basic Criteria

SSO-07.01B

Policies and instructions are defined to ensure transparency within service organisations of the cloud service provider with respect to the following aspects:

- Data flow and interfaces between the cloud service provider and third parties are documented, including measures regarding the secure transmission and access control for data shared with third parties;
- It is identified whether third parties used by the cloud service provider itself rely on service providers that contribute to the provisioning of the cloud service;
- If third parties rely on service providers, the types of data processed by the service providers are identified and risks related to the subcontracting of services are assessed (cf. SSO-02).
- If third parties rely on service providers, require the third parties to monitor the compliance of their service providers with relevant contractual, legal and regulatory requirements (cf. SSO-05); and
- Cloud service customers are informed of third parties and their service providers in use for provisioning the cloud service (both types being considered as subservice organisations of the cloud service provider) and what type of data these subservice organisations are processing.

SSO-07.02B

The cloud service provider documents this information and reviews its completeness, accuracy and validity at least annually.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: SSO-07.01B

Monitoring of third parties can occur via audits, certifications and third party reports (cf. SSO-05) and may be performed by the subcontracting third party. The cloud service provider remains responsible for reviewing the results of compliance monitoring and assessing the risk.

Supplementary Information - Complementary Customer Criteria

–

SSO-08 Controlling Exchanges with Suppliers of Functional Components

Basic Criteria

SSO-08.01B

When a functional component is used to provide the cloud service, and may have access, directly or indirectly, to cloud service customer data, the cloud service provider defines and implements:

- A policy according to SP-01 that does not allow such a component to exchange directly with its supplier;

- Instructions according to SP-01 for the cloud service provider to authorise any content provided by the supplier for its functional components before transferring the content to the functional components (for each transfer);
- Instructions according to SP-01 for the cloud service provider to authorise any content to be sent from a functional component to its supplier before transferring the content to the supplier (for each transfer); and
- When a procedure to authorise content transfers is automated, then the Cloud Serivce Provider implements this procedure using a solution that keeps traces of the operations proposed by the supplier of the functional component, of the verification performed to authorise the content and of the incoming and outgoing transfers effectively performed.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: SSO-08.01B

A supplier of a functional component is typically a service organisation of the cloud service provider. The authorisation for the transfer may be automated. Content provided by the supplier refers to updates of the functional components.

Supplementary Information - Complementary Customer Criteria

–

5.13 Security Incident Management (SIM)

Objective: Ensure a consistent and comprehensive approach to the capturing, evaluation, communication and handling of security incidents.

SIM-01 Policy for Security Incident Management

Basic Criteria

SIM-01.01B

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, escalation and root cause analysis of security incidents and creates interfaces to the incident management and business continuity management.

SIM-01.02B

The cloud service provider has set up a 'Computer Emergency Response Team' (CERT), which contributes to the coordinated resolution of occurring security incidents.

SIM-01.03B

Communication channels with the cloud service customers are identified and defined and customers affected by security incidents are informed in a timely and appropriate manner.

Additional (Sharpening)

–

Additional (Complementing)

SIM-01.01AC

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.

SIM-01.02AC

In addition, there are analysis plans for typical security incidents and an evaluation methodology which ensures the collected information does not lose its evidential value in any subsequent legal assessment.

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

Cloud service 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.

SIM-02 Security Incident Response Plans

Basic Criteria

SIM-02.01B

The cloud service provider has documented, approved and communicated one or more security incident response plans. The plans address all stages of incident response, including identification, containment, eradication, recovery, and lessons learned. They are approved by subject matter experts of the cloud service provider and communicated to all relevant stakeholders.

SIM-02.02B

The plans are evaluated and updated at least annually or as necessary to reflect changes in the organisational structure or environment.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

SIM-03 Processing of Security Incidents

Basic Criteria

SIM-03.01B

Subject matter experts of the cloud service provider classify, prioritise and perform root-cause analyses for events that could constitute a security incident.

SIM-03.02B

If the cloud service provider determines the need for external assistance, it selects a competent and trustworthy incident response service provider or one that is recommended by a national cybersecurity authority.

SIM-03.03B

The cloud service provider maintains a catalogue that clearly identifies the information security incidents that affect cloud service customer data and uses that catalogue to classify information security incidents.

SIM-03.04B

The incident classification mechanism includes provisions to correlate information security events. In addition, these correlated information security events are themselves assessed and classified according to their criticality.

SIM-03.05B

The results of these root-cause analyses are documented, shared with relevant stakeholders, and used as part of evaluation and learning processes.

SIM-03.06B

All documents and evidence that provide details on security incidents related to the cloud service are archived in a way that could be used as evidence in court. Security mechanisms and processes for protecting all the information about security incidents related to the cloud service are implemented in accordance with criticality levels and legal requirements.

SIM-03.07B

The analysis process also ensures traceability of the entire kill chain of a security incident.

Additional (Sharpening)

–

Additional (Complementing)

SIM-03.01AC

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).

SIM-03.02AC

The cloud service provider establishes, or contracts for the services of, an integrated team of forensic/incident responder personnel specifically trained on evidence preservation and chain of custody management.

SIM-03.03AC

The cloud service provider monitors the handling of information security incidents to verify the application of incident management policies and procedures. Any deviations identified during monitoring are addressed through timely and appropriate remediation measures.

Supplementary Information

About the Criteria

Applicable to: SIM-03.07B

The term 'kill chain' refers to the stages an attacker goes through to carry out a cyberattack, leading to a security incident. Understanding and ensuring traceability of the entire kill chain helps the cloud service provider identify weaknesses in their security posture and enhance defenses.

Supplementary Information - Complementary Customer Criteria

–

SIM-04 Documentation and Reporting of Security Incidents

Basic Criteria

SIM-04.01B

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 (Sharpening)

–

Additional (Complementing)

SIM-04.01AC

The customer can either actively approve solutions or the solution is automatically approved after a certain period.

SIM-04.02AC

Information on security incidents or confirmed security breaches is made available to all affected customers.

SIM-04.03AC

The contract between the cloud service provider and the cloud service customer regulates which data is made available to the cloud service customer for his own analysis in the event of security incidents.

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure through suitable controls that they receive notifications from the cloud service provider about security incidents 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.

SIM-05 Duty of the Employees to Report Security Incidents to a Central Body

Basic Criteria

SIM-05.01B

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.

SIM-05.02B

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.

SIM-05.03B

The cloud service provider makes the information security incident reporting mechanisms known as part of its communication to employees, cloud service customers and external business partners.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

Cloud service 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).

SIM-06 Evaluation and Learning Process

Basic Criteria

SIM-06.01B

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.

SIM-06.02B

The evaluation and learning process includes the results of root-cause analyses conducted in accordance with SIM-02.

SIM-06.03B

The cloud service provider defines, implements and maintains a knowledge repository of security incidents and the measures taken to solve them, as well as information related to the assets that these security incidents affected and uses that information to enrich the classification catalogue of incidents (cf. SIM-03).

SIM-06.04B

The intelligence gained from the incident management and gathered in the knowledge repository is used to identify recurring security events or incidents, or potential significant security incidents, to determine the need for advanced safeguards, and implement them.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: SIM-06.01B

Supporting bodies may be external service providers or government agencies such as the BSI.

Supplementary Information - Complementary Customer Criteria

Cloud service 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 service customers evaluate whether and which supporting measures they might take on their side.

5.14 Business Continuity Management (BCM)

Objective: Plan, implement, maintain and test procedures and measures for business continuity and emergency management.

BCM-01 Business Continuity and Emergency Management System

Basic Criteria

BCM-01.01B

The cloud service provider operates a business continuity and emergency management system in accordance with ISO 22301 and/or BSI 200-4.

BCM-01.02B

Policies and instructions for establishing the strategy and guidelines to ensure business continuity management for the cloud service are documented, communicated and provided in accordance with SP-01.

BCM-01.03B

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.

BCM-01.04B

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.

BCM-01.05B

Policies and instructions related to business impact analyses and business continuity plans are documented, communicated and made available in accordance with SP-01.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: BCM-01.01B

The basic criterion can (but need not) be fulfilled with a certification of the BCM according to ISO/IEC 22301

Supplementary Information - Complementary Customer Criteria

–

BCM-02 Business Impact Analysis

Basic Criteria

BCM-02.01B

The policies and instructions for business continuity management for the cloud service include the need to perform a business impact analysis. The cloud service provider analyses the impact of disrupting activities to its organisation with respect the development and operations of the cloud service in accordance with applicable policies and instructions with at least the following aspects:

- Possible scenarios based on a risk analysis that includes cyber risks;

- Identification of critical products and services;
- Identification of dependencies, including processes (including resources required), applications, business partners and third parties;
- Capturing threats to critical products and services;
- Identification of effects resulting from planned and unplanned malfunctions and changes over time;
- Determination of the maximum tolerable period of downtime and service degregation;
- Identification of restoration priorities;
- Determination of time targets for the resumption of critical products and services within the maximum acceptable time period (i.e. RTO);
- Determination of time targets for the maximum reasonable period during which cloud service derived data, cloud service provider data, account data and, if its processing is contractually agreed upon, cloud service customer data can be lost and not recovered (i.e. RPO); and
- Estimation of the resources needed for resumption.

BCM-02.02B

The business impact analysis resulting from the applicable policies and instructions is reviewed at regular intervals, at least once a year, or after significant organisational or environment-related changes.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: BCM-02.01B

Scenarios to be considered according to the basic criterion are, for example, the loss of personnel, buildings, infrastructure and service providers.

Supplementary Information - Complementary Customer Criteria

Cloud service 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.

BCM-03 Business Continuity Plans

Basic Criteria

BCM-03.01B

Based on the results of the business impact analysis, business continuity plans are documented in a consistent manner, and in accordance with applicable policies and instructions.

Business continuity 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;
- Consistency over all locations, zones, regions and partitions; and
- Interfaces to Security Incident Management.

BCM-03.02B

The business continuity plans are reviewed at regular intervals, at least once a year, or after significant organisational or environment-related changes.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: BCM-03.01B, BCM-03.02B

Although different partitions do not share a common IAM (and hence no common personnel for BCM), business continuity plans may be shared between different partitions since the same cloud services are provided.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure through suitable controls that the results of their 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 service 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.

BCM-04 Testing Business Continuity

Basic Criteria

BCM-04.01B

Business continuity plans are tested on a regular basis (at least annually) or after significant organisational or environmental changes. Tests involve affected cloud service customers and relevant third parties (e.g. service organisations).

BCM-04.02B

The tests are documented and results are taken into account to review the business continuity plans and for future business continuity measures.

Additional (Sharpening)

–

Additional (Complementing)

BCM-04.01AC

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.

BCM-04.02AC

The cloud service provider has procedures in place to ensure that cloud service customers are timely informed about planned activities related to business continuity tests and exercises that could affect the information security of the cloud service (e.g. regarding its availability). This information includes the scheduled timeframe for the operations as well as a description of the work to be carried out.

BCM-04.03AC

The cloud service provider provide cloud service customers an assessment of the potential impacts concerning the information security of the cloud service and with details for contacting the cloud service provider.

BCM-04.04AC

After a completed exercise, the existing alarm plan is reviewed and (if needed) adapted.

Supplementary Information

About the Criteria

Applicable to: BCM-04.01B, BCM-04.01AC

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.

Relevant third parties are in particular service organisations of the cloud service provider who contribute to the development or operation of the cloud service (cf. basic criteria SSO-02 and SSO-06).

Supplementary Information - Complementary Customer Criteria

Cloud service 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 service 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 service customers ensure that the appropriate measures for coping with the scenario are practiced and tested by means of suitable BCM controls.

BCM-05 Policy for Business Continuity Management

Basic Criteria

BCM-05.01B

Policies and instructions for Business Continuity Management (BCM) are documented, communicated and provided in accordance with SP-01 regarding the following aspects:

- Goals of the BCM;
- Roles and responsibilities, management commitment;
- Scoping of the BCM, identifying relevant business processes;
- Interfaces, in particular to Incident Management;
- Communication with relevant entities and competent authorities;
- Methodology;
- Consideration of Risk;
- Business Impact Analysis (BIA);
- Business Continuity Plan (BCP);
- Resource Planning (usually part of the BCP);
- Testing of Business Continuity Plans and regular updates to BCM documentation; and
- Continuous improvement of the Business Continuity Management.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

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 Criteria

COM-01.01B

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 (Sharpening)

–

Additional (Complementing)

COM-01.01AC

The cloud service provider provides an overview or summary of the procedures described in the basic criterion when requested by a cloud service customer.

Supplementary Information

About the Criteria

Applicable to: COM-01.01B

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 service 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).

The documentation of the identified requirements and the procedures for complying with these requirements may be spread across several documents and does not necessarily have to be recorded in a single register or directory.

Supplementary Information - Complementary Customer Criteria

–

COM-02 Policy for Planning and Conducting Audits

Basic Criteria

COM-02.01B

The cloud service provider documents and implements an audit programme over three years that defines the scope and the frequency of the audits in accordance with the management of change, policies, and the results of the risk assessment (cf. OIS-07).

COM-02.02B

Risk-based policies and instructions for planning and conducting audits that protect the operation of the cloud service from interference by 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 of the cloud service or breaches of contractual requirements are performed during scheduled maintenance windows or outside peak periods;
- Logging and monitoring of activities;
- Review of server and network equipment configurations under the responsibility of the cloud service provider;
- Intrusion testing for external access points; and
- Source code reviews of internally developed security functions.

Additional (Sharpening)

–

Additional (Complementing)

COM-02.01AC

The cloud service provider grants its cloud service customers contractually guaranteed information and audit rights. These rights may be exercised individually or as part of group audits.

Supplementary Information

About the Criteria

Applicable to: COM-02.01B

An audit is a systematic, independent and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled. Audits may be performed as internal audits, sometimes called first party audits, that are conducted by, or on behalf of, the organisation itself. They may also be performed as external audits, generally called second and third party audits. Second party audits are conducted by parties having an interest in the organisation, such as customers, or by other individuals on their behalf. Third party audits are conducted by independent auditing organisations.

An audit programme comprises arrangements for a set of one or more audits planned for a specific time frame and directed towards a specific purpose. It may comprise internal and external audits.

COM-02 is fully applicable to virtual infrastructure and infrastructure as code. Audit activities might still impact operations in a virtual environment. Reviews of configurations might for example be performed as part of code reviews.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure through suitable controls that appropriate responses are made to malfunctions of the cloud service through such audits.

To the extent that contractually guaranteed information and audit rights exist, the cloud service customers ensure through suitable controls that these rights are designed and executed in accordance with their own requirements.

COM-03 Internal Audits of the Information Security Management System

Basic Criteria

COM-03.01B

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) through internal audits. This includes checks regarding:

- Compliance with the policies and instructions (cf. SP-01) within their scope of responsibility (cf. OIS-01); and
- Effectiveness of organisational and operational measures to manage the risks posed to the security of network and information systems (cf. OIS-07).

COM-03.02B

Subject matter experts conducting internal audits are not in the line of authority of the personnel of the area under review. If the size of the cloud service provider does not allow such separation of line of authority, alternative measures to guarantee the impartiality of compliance checks are put in place.

COM-03.03B

Identified vulnerabilities and deviations are subject to risk assessment in accordance with the risk management procedure (cf. OIS-07) and follow-up measures are defined and tracked (cf. OPS-18).

COM-03.04B

The cloud service provider documents specifically deviations that are non-conformities from the applicable legal, regulatory, self-imposed and contractual requirements relevant to the information security of the cloud service, including an assessment of their severity, and keeps track of their remediation.

Additional (Sharpening)

–

Additional (Complementing)

COM-03.01AC

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; and
- Recovery time (time to completion of error handling).

COM-03.02AC

Identified vulnerabilities and deviations are automatically reported to the appropriate cloud service provider's subject matter experts for immediate assessment and action.

COM-03.03AC

The cloud service provider provides interfaces to cloud service customers so that they can check compliance with selected contractual agreements in real time.

Supplementary Information

About the Criteria

Applicable to: COM-03.01B

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, which outlines the requirements for conducting internal audits of an Information Security Management System (ISMS) and for establishing an internal audit program. When establishing the internal audit program(s), the cloud service provider should define the scope and criteria by considering the importance of the processes concerned and the results of previous audits. This approach allows cloud service providers to define the audit scope based on the criticality of complying with relevant legal, regulatory, or contractual requirements (cf. COM-01) and internal policies and instructions (cf. SP-01), without requiring a comprehensive review of all requirements during each audit cycle.

Supplementary Information - Complementary Customer Criteria

–

COM-04 Information on Information Security Performance and Management Assessment of the ISMS

Basic Criteria

COM-04.01B

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. This management review ist performed at least once a year

Additional (Sharpening)

–

Additional (Complementing)

COM-04.01AC

The cloud service provider defines and implements technical and operational metrics that align with the organisation's business objectives, security requirements, and compliance obligations. These metrics are documented and included in the management review of the ISMS to ensure their continued suitability, adequacy, and effectiveness.

Supplementary Information

About the Criteria

Applicable to: COM-04.01B

The top management is a natural person or group of people who take final decisions for the institution and are accountable 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.

Supplementary Information - Complementary Customer Criteria

–

5.16 Dealing with Investigation Requests from Government Agencies (INQ)

Objective: Ensure appropriate handling of government investigation requests for legal review, information to cloud service customers, and limitation of access to or disclosure of data.

INQ-01 Legal Assessment of Investigative Requests

Basic Criteria

INQ-01.01B

Investigation requests from government agencies for cloud service customer data, cloud service derived data and account data are subject to a documented 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 for the given request.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: INQ-01.01B

For evidence purposes, all requests that were completely processed during the specified period shall form the population for testing the operating effectiveness of controls to meet the criteria in this domain. All requests are to be included in the population, irrespective of whether they resulted in cloud service customer data or cloud service derived data being disclosed.

Supplementary Information - Complementary Customer Criteria

Cloud service 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 is only taken up or continued when this risk has been deemed acceptable.

INQ-02 Informing Cloud Service Customers about Investigation Requests

Basic Criteria

INQ-02.01B

The cloud service provider informs the affected cloud service customer(s) without undue delay. Exceptions for this information of the customer need to be justified by the legal basis of this request or because there are clear indications of illegal actions of the customer in connection with the use of the cloud service.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: INQ-02.01B

This does not affect other legal or regulatory requirements that requires earlier information for cloud service customers.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure through suitable controls that such notifications are received and legally checked according to their own specifications and possibilities.

INQ-03 Conditions for Access to or Disclosure of Data in Investigation Requests

Basic Criteria

INQ-03.01B

Access to or disclosure of cloud service customer data, cloud service derived data or account data in response to government investigation requests is only permitted if the cloud service provider has performed a legal assessment. This assessment has to confirm that there is an applicable and valid legal basis and that the request must be granted according to this basis.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: INQ-03.01B

Disclosure of cloud service customer data to government agencies may include handing over encryption keys. The disclosure of keys should also be scrutinised in accordance with the INQ criteria. In particular, with reference to INQ-04, care should be taken to ensure that no other cloud service customer data is compromised by handing over a key.

Supplementary Information - Complementary Customer Criteria

–

INQ-04 Limiting Access to or Disclosure of Data in Investigation Requests

Basic Criteria

INQ-04.01B

The cloud service provider's procedures for granting access to or disclosing cloud service customer data and cloud service derived data in the context of investigation requests from government agencies ensure that the agencies only gain access to or insight into the data that is the subject of the investigation request.

INQ-04.02B

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 service customers who are subject of the investigation request.

Additional (Sharpening)

–

Additional (Complementing)

INQ-04.01AC

The cloud service provider monitors the access and activities performed by or on behalf of investigators as determined by the process described in INQ-01.

INQ-04.02AC

Any deviations identified during monitoring are addressed through timely and appropriate remediation measures.

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

INQ-05 Communication of Technical Procedures for Data Disclosure in Investigation Requests

Basic Criteria

INQ-05.01B

The cloud service provider documents the technical procedures and other relevant technical information regarding the provision or disclosure of cloud service customer data in response to valid investigative requests and provides it to cloud service customers.

INQ-05.02B

The type and scope of the provided information is based on the needs of the cloud service customers' expert personnel to assess risks to the cloud service customer's data confidentiality. At a minimum, the following aspects must be addressed:

- The process for the provision and disclosure of cloud service customer data in response to legitimate investigative requests;
- The technical capabilities and limitations of the cloud service provider regarding disclosure of cloud service customer data;
- Logging mechanisms implemented to records access for disclosure of cloud service customer data;
- Access possibilities for cloud service customers to review such logs;
- Methods for accessing and disclosing cloud service customer data; and
- Laws, regulations, or other legal means and their applicability concerning the cloud service provider's ability to inform its customers about the provision and disclosure of cloud service customer data.

INQ-05.03B

The document is maintained in accordance with SP-01 and aligned with the cloud service provider's guidelines on minimising access to cloud service customer data (cf. DEV-01) to ensure its relevance and accuracy for cloud service customers.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: INQ-05.01B, INQ-05.02B, INQ-05.03B

The criterion is limited to cloud service customer data. The cloud service provider has typically access to other data types such as cloud service derived data and account data such that extending the criterion to those other data types, may not lead to useful information for customers risk management. Technical capabilities and limitations to access cloud service customer data include aspects such as:

- If the cloud service customers stores its cloud service customer data in unencrypted form;
- If the cloud service provider encrypts cloud service customer data in storage and transit;
- Whether the cloud service provider has the ability to decrypt cloud service customer data in case of such requests and how this ability for access or disclosure is used;
- Retention periods for cloud service derived data relating to the cloud service customer and whether such data is stored in encrypted form;
- Possibilities for decrypting cloud service customer data or for extracting cloud service customer data during the decryption process;
- Disclosure of user identities and credentials; and
- Further measures that have been created or can be used for disclosing cloud service customer data.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure through suitable controls that they minimize potential disclosure of their customer data. According to the protection need of the cloud service customer data, the cloud service customer take the decision if the particular cloud service can be used or if the risk of disclosure is to high.

5.17 Product Safety and Security (PSS)

Objective: Provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud service customers, appropriate mechanisms for troubleshooting and logging, as well as authentication and authorisation of users of cloud service customers.

PSS-01 Guidelines and Recommendations for Cloud Service Customers

Basic Criteria

PSS-01.01B

The cloud service provider provides cloud service customers with publicly available guidelines and recommendations for the secure use of the cloud service provided. The information contained therein is intended to assist the cloud service customer in the secure configuration, installation and use of the cloud service, as well as the implementation of complementary customer controls, to the extent applicable to the cloud service and the responsibility of the cloud user.

PSS-01.02B

The type and scope of the information provided will be based on the needs of subject matter experts of the cloud service 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;
- Malware protection for containers or virtual machines;
- Error handling and logging mechanisms;
- Authentication mechanisms;
- Roles and rights concept including combinations that result in an elevated risk;
- Services and functions for administration of the cloud service by privileged users;
- Complementary user entity controls;
- Encryption mechanisms and services;
- Data leakage prevention;
- Secure development and operation of applications on the cloud service;
- Use and configuration of defensive mechanisms;
- Use and configuration of wide-area distributed architecture mechanisms;
- Methods used for client data separation (cf. OPS-28 and OPS-29); and
- How information security risks related to the use of the cloud service can be addressed through proper logging and monitoring mechanisms.

PSS-01.03B

The cloud service provider describes in the user documentation all risks the cloud service customer has to manage on its side.

PSS-01.04B

The information is maintained so that it is applicable to the cloud service provided in the version intended for productive use.

Additional (Sharpening)

–

Additional (Complementing)

PSS-01.01AC

The cloud service provider promptly notifies cloud service customers about any planned modifications to the cloud service that could result in a loss or downgrade of functionality.

Supplementary Information

About the Criteria

Applicable to: PSS-01.01B

In a cloud environment, security responsibilities are shared between the cloud service provider and the customer, varying by service type — Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS). Guidance on the complementary customer controls helps cloud service customers understand their roles and responsibilities within the Shared Responsibility Model, also in terms of security and operational management (cf. OIS-03). By offering detailed guidance, cloud service customers are equipped to understand and implement the necessary controls that fall under their responsibility. The level of detail and length can vary according to the type of cloud service provided.

Examples for defensive mechanisms include payload filtering, traffic shaping, load balancing, load shedding and DDoS defences.

Examples for wide-area distributed architecture mechanisms include replication for fault tolerance, multiple cloud regions to avoid localised outages and disasters and geo-dispersion of service endpoints to reduce user-facing latency.

Supplementary Information - Complementary Customer Criteria

Cloud service 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.

PSS-02 Identification of Vulnerabilities of the Cloud Service

Basic Criteria

PSS-02.01B

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.

PSS-02.02B

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;
- Conducting security checks based on a Software Bill of Materials (SBOM); and
- Obtaining information about confirmed vulnerabilities in software libraries provided by third parties and used in their own cloud service.

PSS-02.03B

The severity of identified vulnerabilities is assessed according to defined criteria and measures are taken to immediately eliminate or mitigate them.

Additional (Sharpening)

–

Additional (Complementing)

PSS-02.01AC

The procedures for identifying such vulnerabilities also include annual code reviews or security penetration tests by qualified external third parties.

Supplementary Information

About the Criteria

Applicable to: PSS-02.01B, PSS-02.02B, PSS-02.03B, PSS-02.01AC

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 criterion OPS-25 (Managing Vulnerabilities, Malfunctions and Errors - Vulnerability Scans).

Supplementary Information - Complementary Customer Criteria

–

PSS-03 Informing Customers about Known Vulnerabilities

Basic Criteria

PSS-03.01B

The cloud service provider ensures that cloud service customers have access to regularly updated information about known vulnerabilities associated with the cloud service. This includes:

- Known-exploited vulnerabilities;
- Known vulnerabilities for which a patch and/or mitigating measures are provided by the cloud

service provider (N-Day vulnerabilities), with appropriate references to the patch/measure; and
- Known vulnerabilities for which a patch and/or mitigating measures are unlikely to be provided by the cloud service provider (Forever-Day vulnerabilities), along with a justification for why they are not provided.

These pertain to the provided cloud service and assets provided by the cloud service provider that the cloud service customers have to install, provide or operate within their own responsibility.

PSS-03.02B

The provided information includes a description of the remediation options for that vulnerability.

PSS-03.03B

These vulnerabilities are also identified based on Software Bill of Materials (SBOM) data.

PSS-03.04B

The vulnerabilities are presented with references to the Common Vulnerabilities and Exposures (CVE) and assessments are based on:

- The Common Vulnerability Scoring System (CVSS),
- The Exploit Prediction Scoring System (EPSS), and
- The Stakeholder-Specific Vulnerability Categorization (SSVC)

in the latest version valid at the time of the execution of the control.

This information is easily accessible to any cloud service customer and forms a suitable basis for risk assessment and possible follow-up actions on the part of the cloud service customers, among other things through references to vulnerability-specific measures in:

- Vulnerability, Exploitability eXchange (VEX), and
- Common Security Advisory Frameworks (CSAF).

PSS-03.05B

The cloud service provider determines when a vulnerability is notified to the cloud service customers as part of Coordinated Vulnerability Disclosure (CVD).

PSS-03.06B

The cloud service provider consults at least daily the vulnerability registers of its service organisations, analyses the potential impact of the published vulnerabilities on the cloud service, and handles them according to the vulnerability handling process (cf. OPS-18).

Additional (Sharpening)

–

Additional (Complementing)

PSS-03.01AC

Assets provided by the cloud service provider, which must be installed, provided or operated by cloud service customers within their area of responsibility, are equipped with automatic update mechanisms. After approval by the respective cloud service customer, software updates are rolled out by the cloud service provider.

PSS-03.02AC

Vulnerabilities are disclosed in accordance with the Common Security Advisory Framework Version 2.0 or higher, and as specified in BSI's Technical Guideline TR-03191.

Supplementary Information

About the Criteria

Applicable to: PSS-03.03B

Although the cloud service provider has to identify the vulnerabilities based on SBOM data to fulfill this criterion, this SBOM data need not be handed over to the customer to fulfill the criterion.

Applicable to: PSS-03.01AC, PSS-03.02AC

Assets provided by the cloud service provider that cloud service 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 information should incorporate or refer to the vulnerabilities of those other cloud services in order for this criterion to be met.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure through suitable controls that the information in this register is incorporated without undue delay into their own risk management, evaluated and, if necessary, taken into account in their own area of responsibility.

PSS-04 Error handling and Logging Mechanisms

Basic Criteria

PSS-04.01B

The cloud service provided is equipped with error handling and logging mechanisms for system components under the responsibility of the cloud service customer. 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.

PSS-04.02B

These mechanisms are designed to address identified security risks related to the use of the cloud service. The cloud service provider identifies and documents these risks in advance, ensuring that the implemented logging mechanisms capture relevant events and activities.

PSS-04.03B

The information is detailed enough to allow cloud users to check the following aspects, insofar as they are applicable to the cloud service:

- Which cloud service customer data and cloud service derived data, services or functions available to the cloud user within the cloud service, have been accessed by whom, when and from where (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.

PSS-04.04B

The logged information is protected from unauthorised access and modification and can be deleted by the cloud service customer.

PSS-04.05B

If the cloud service customer is responsible for the activation or type and scope of logging, the cloud service provider has provide appropriate logging capabilities.

Additional (Sharpening)

–

Additional (Complementing)

PSS-04.01AC

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 Criteria

Applicable to: PSS-04.01B, PSS-04.02B, PSS-04.03B, PSS-04.04B, PSS-04.05B, PSS-04.01AC

Unlike the additional criterion OPS-15, which covers both, system components under the responsibility of the cloud service provider, as well as system components under the responsibility of the cloud service customer, the scope of this criterion is limited to system components under the responsibility of the cloud service customer only.

Supplementary Information - Complementary Customer Criteria

If the cloud service is equipped with error handling and logging mechanisms, cloud service customers

must activate these and configure them according to defined requirements. The cloud service customer must incorporate his own information security management for this purpose.

PSS-05 Authentication Mechanisms

Basic Criteria

PSS-05.01B

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.

PSS-05.02B

For privileged users, IT components or applications, these authentication mechanisms are enforced.

Additional (Sharpening)

–

Additional (Complementing)

PSS-05.01AC

The cloud service offers out-of-band (OOB) authentication, in which the factors are transmitted via different channels (e.g. Internet and mobile network).

Supplementary Information

About the Criteria

Applicable to: PSS-05.01B, PSS-05.02B, PSS-05.01AC

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 e.g. be performed with cryptographic certificates, smart cards or tokens.

Supplementary Information - Complementary Customer Criteria

Cloud service 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.

PSS-06 Session Management

Basic Criteria

PSS-06.01B

To protect confidentiality, availability, integrity and authenticity during interactions with the cloud service, a suitable session management system is used that corresponds to the state-of-the-art and is protected against known attacks.

PSS-06.02B

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 service customer.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: PSS-06.01B

Known attacks include manipulation, forgery, session takeover, Denial of Service attacks, enveloping, replay and null cipher attacks.

Supplementary Information - Complementary Customer Criteria

Cloud service 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.

PSS-07 Confidentiality of Authentication Information

Basic Criteria

PSS-07.01B

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. IAM-09) or the cloud service customer is technically enforced;
- The user is informed about changing or resetting the password. Any password reset procedure is not valid for more than 48 hours and the password shall be changed by the user after the use of the reset procedure; and
- The server-side storage uses hash functions in combination with salt values, both corresponding to the state-of-the-art.

The cloud service provider makes available to the cloud service customers the rules and recommendations that apply to the users under their responsibility, and provides the cloud service customers with tools to manage and enforce these rules.

PSS-07.02B

The cloud service provider distributes credentials using additional security mechanisms to verify the identity of the recipient (e.g. multi-factor authentication), validate the request and protect the credentials.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: PSS-07.01B

The state-of-the-art regarding cryptographic hash functions is described in the current version of the BSI Technical Guideline TR-02102-1 'Cryptographic Mechanisms: Recommendations and Key Lengths'.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure through suitable controls that they use sufficiently secure passwords (cf. IAM-09) according to their own assessment and that the risks of unauthorised access associated with their own choice are borne.

PSS-08 Roles and Rights Concept

Basic Criteria

PSS-08.01B

The cloud service provider provides cloud users with a roles and rights concept. This concept allows users to manage their own access rights. It describes rights profiles for the functions provided by the cloud service. Cloud users can configure certain access control parameters themselves.

PSS-08.02B

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').

PSS-08.03B

The cloud service provider offers a functionality to help cloud service customers review user access rights under their responsibility.

PSS-08.04B

In case the service includes the management of customer identities, for a given customer identity, the cloud service provider is able to provide the list of access rights currently granted to that identity according to the contractual terms.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: PSS-08.01B

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).

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure through suitable controls that:

- they actively utilise the roles and rights concept and accompanying functionalities offered by the cloud service provider;
- 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).

PSS-09 Authorisation Mechanisms

Basic Criteria

PSS-09.01B

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.

PSS-09.02B

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).

PSS-09.03B

If the validation led to vulnerabilities, 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.

PSS-09.04B

Information about known-exploited vulnerabilities and known vulnerabilities for which a patch and/or mitigating measures are unlikely to be provided by the cloud service provider is included in the information provided to cloud service customers about known vulnerabilities (cf. PSS-03).

Additional (Sharpening)

–

Additional (Complementing)

PSS-09.01AC

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 Criteria

–

Supplementary Information - Complementary Customer Criteria

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

PSS-10 Software Defined Networking

Basic Criteria

PSS-10.01B

If the cloud service offers functions for software-defined networking (SDN), the confidentiality of cloud service customer data is ensured by suitable SDN procedures.

PSS-10.02B

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 (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: PSS-10.01B, PSS-10.02B

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.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure through suitable controls that they validate the functionality of SDN features for their individual use cases before using newly introduced capabilities or modifed existing ones.

PSS-11 Images for Virtual Machines and Containers

Basic Criteria

PSS-11.01B

If cloud service customers operate virtual machines or containers with the cloud service, the cloud service provider ensures the following aspects:

- Cloud service customers can restrict the selection of images of virtual machines or containers according to their specifications, so that users of the cloud service customer can only launch the images or containers released according to these restrictions;
- Images made available are labelled with information about their origin;
- If the cloud service provider provides images of virtual machines or containers to the cloud service customer, the cloud service provider appropriately informs the cloud service customer of the changes made to the previous version; and
- In addition, these images provided by the cloud service provider are hardened according to generally accepted industry standards;

Additional (Sharpening)

–

Additional (Complementing)

PSS-11.01AC

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 service customer.

Supplementary Information

About the Criteria

Applicable to: PSS-11.01B, PSS-11.01AC

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-Compendium.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure through suitable controls 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.

PSS-12 Region of Data Processing and Storage

Basic Criteria

PSS-12.01B

The architecture of the cloud service, including the technical design of its infrastructure, ensures that cloud service customer data and eventual data backups thereof are processed and stored only in the region specified in the contractual agreements with the cloud service provider. If the cloud service customer is able to select from multiple regions, processing and storage of the aforementioned data is limited to the selected region.

PSS-12.02B

Processing and storage of cloud service customer data data within the service organisations of the cloud service provider also adheres to the regions selected by the cloud service customer.

PSS-12.03B

The contractual agreements specify the regions in which processing and storage of cloud service customer data, cloud service derived data and account data occurs and the circumstances under which changes may be applied.

PSS-12.04B

Customers are notified beforehand in case of any changes to the regions of data processing or storage. If the cloud service provider has not been granted prior general authorisation by the cloud service customer to do so, such authorisations are obtained in accordance with the requirements specified in the contractual agreements or let the cloud service customer exercise termination rights.

Additional (Sharpening)

PSS-12.01AS, sharpening PSS-12.01B

The basic criterion also applies to all cloud service derived data.

PSS-12.02AS, sharpening PSS-12.02B

The basic criterion also applies to all cloud service derived data.

PSS-12.03AS, sharpening PSS-12.03B

The basic criterion also applies to all cloud service derived data.

PSS-12.04AS, sharpening PSS-12.04B

The basic criterion also applies to all cloud service derived data.

Additional (Complementing)

PSS-12.01AC

The cloud service provider offers partitions selectable by the cloud service customer where partition-specific identity management is enforced for both cloud service customers and all cloud service provider personnel. Identity verification and identity storage are confined to the geographical boundaries of the selected partition.

PSS-12.02AC

Within these partitions, the following operations by the cloud service provider are restricted to occur only within the geographical boundaries of the customer-

selected partitions:

- Privileged access to the production environment by the cloud service provider, including potential access to cloud service customer data and cloud service derived data;
- System logging and event monitoring by the cloud service provider, except for processing event logs specifically for threat intelligence and handling IP addresses for routing purposes;
- Cryptographic key management and storage practices to ensure keys are handled and stored within limits of the partition.

These restrictions considering partitions also apply to any service organisations involved in the operation of the cloud service.

PSS-12.03AC

Monitoring of threat intelligence data, which excludes any cloud service customer data and Account data, and logging of required routing information such as IP addresses are not required to be geographically limited to a single partition.

Supplementary Information

About the Criteria

Applicable to: PSS-12.01B, PSS-12.02B, PSS-12.03B, PSS-12.04B, PSS-12.01AS, PSS-12.01AC, PSS-12.02AC

This criterion supplements the Boundary Condition BC-01. It does not require the cloud service provider to offer multiple partitions. If the cloud service provider offers only one partition for the cloud service(s) in scope, this does not comprise a deviation from the criterion.

If the additional complemental criterion is only applicable for selected partitions in scope of an assurance engagement in accordance with this catalogue, this should be presented in the cloud service provider's description of its system of internal control for the cloud service.

This criterion is a prerequisite for technical service sovereignty.

Supplementary Information - Complementary Customer Criteria

Cloud service 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 partitions and, if there is a choice between different partitions, 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 service customers take the laws of their own jurisdiction applicable to them into account when making their selection (e.g. when processing personal data; compliance with legal retention obligations for business documents, etc.).

6 Legal notice

Published by:
Bundesamt für Sicherheit in der Informationstechnik (BSI)
53175 Bonn

Source:
Federal Office for Information Security (BSI)
Godesberger Allee 87
Phone: +49 (0) 228 999528-0
Fax: +49 (0) 228-999582-5400
Email: cloudsecurity@bsi.bund.de
Internet: www.bsi.bund.de

Last updated:
2025

Content and editing:
Federal Office for Information Security (BSI)

Item number:
t.b.d.