Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Cloud Computing Compliance Criteria Catalogue (C5:2026)

Federal Office for Information Security (BSI)

Contents

Contents **1**

1 Introduction **7**
1.1 Preliminary remarks . . . 7
1.2 Definitions . . . 8
1.2.1 Terms related to Cloud Security . . . 8
1.2.2 Terms related to Audits . . . 14

2 Structure and Content of the Criteria **18**
2.1 Structure . . . 18
2.2 Content of the C5 Criteria . . . 20
2.3 Underlying Standards and Publications . . . 20

3 Providing Conformity through Independent Audits **24**
3.1 Introduction . . . 24
3.2 Audit Standards to be Applied . . . 24
3.3 Relationship to Other Audits . . . 25
3.4 Supplementary Requirements of the BSI . . . 26
3.4.1 Assurance Engagement . . . 26
3.4.2 Qualification of the Auditor . . . 27
3.4.3 Criteria to be Applied . . . 28
3.4.4 Subject Matter and Objective of the Audit . . . 28
3.4.5 Requirements for the Description and the Management Statement . . . 30
3.4.6 Consideration of Service Organisations . . . 33
3.4.7 Obtaining Evidence Regarding the Description . . . 34
3.4.8 Assessing the Fulfilment of the C5 Criteria . . . 34
3.4.9 Obtaining Evidence Regarding Design of Controls . . . 35
3.4.10 Obtaining Evidence Regarding Operating Effectiveness of Controls . . . 35
3.4.11 Considerations for Initial Engagements . . . 35
3.4.12 Deviation Handling . . . 36
3.4.13 Reporting . . . 37
3.5 Dealing with Revisions of this Criteria Catalogue . . . 40

4 Information on the General Conditions of the Cloud Service **42**
GC-01 Information on applicable law, jurisdiction, countries, partitions, regions, zones and locations . . . 42
GC-02 Information on availability and incident handling during regular operation . . . 43
GC-03 Information on recovery parameters in emergency operation . . . 44

GC-04 Information on the approach to ensuring service availability . . . 44
GC-05 Information on how investigation requests from government agencies are handled 45
GC-06 Information on certifications or attestations . . . 46

5 Basic Criteria, Additional Criteria, Supplementary Information 48
5.1 Organisation of Information Security (OIS) . . . 48
OIS-01 Information Security Management System (ISMS) . . . 48
OIS-02 Information Security Policy . . . 49
OIS-03 Interfaces and Dependencies . . . 50
OIS-04 Segregation of Duties . . . 52
OIS-05 Threat Intelligence . . . 53
OIS-06 Contact with Relevant Government Agencies and Interest Groups . . . 55
OIS-07 Risk Management Policy . . . 55
OIS-08 Application of the Risk Management Policy - Risk Assessment . . . 56
OIS-09 Application of the Risk Management Policy - Risk Treatment . . . 59
OIS-10 Information Security in Project Management . . . 61
5.2 Security Policies and Procedures (SP) . . . 62
SP-01 Documentation, Communication and Provision of Policies and Procedures . . . 62
SP-02 Review and Approval of Policies and Procedures . . . 64
SP-03 Exceptions from Existing Policies and Procedures . . . 65
5.3 Personnel (HR) . . . 67
HR-01 Verification of Qualification and Trustworthiness . . . 67
HR-02 Employment Terms and Conditions . . . 70
HR-03 Security Training and Awareness Programme . . . 71
HR-04 Disciplinary Measures . . . 73
HR-05 Responsibilities in the Event of Termination or Change of Employment . . . 74
HR-06 Non-disclosure Agreements . . . 74
HR-07 Remote Working - Policy . . . 75
HR-08 Remote Working - Implementation . . . 76
5.4 Asset Management (AM) . . . 77
AM-01 Asset Management Framework . . . 77
AM-02 Asset Inventory . . . 79
AM-03 Hardware Asset Inventory . . . 80
AM-04 Software Asset Inventory . . . 81
AM-05 Policy for the Proper and Secure Use of Assets . . . 82
AM-06 Commissioning of Hardware . . . 83
AM-07 Decommissioning of Hardware . . . 84
AM-08 Commitment to Proper Use, Safe and Secure Handling and Return of Assets . . . 85
AM-09 Asset Classification and Labelling . . . 86
AM-10 Protection of Hardware on Hold . . . 88
AM-11 Transfer of Hardware . . . 89
AM-12 Removable Media and Endpoint Devices . . . 89
5.5 Physical Security (PS) . . . 91
PS-01 Physical Security and Environmental Control Requirements . . . 91
PS-02 Redundancy Model . . . 94
PS-03 Perimeter Protection . . . 95
PS-04 Physical Site Access Control . . . 97
PS-05 Protection against Threats from Outside and from the Environment . . . 98

PS-06 Protection against Interruptions caused by Power Failures and similar Risks to Supply Facilities . . . 100
PS-07 Surveillance of Operational and Environmental Parameters . . . 102
PS-08 Workplace Security Requirements . . . 103
5.6 Operations (OPS) . . . 104
OPS-01 Capacity Management - Planning . . . 104
OPS-02 Capacity Management - Monitoring . . . 105
OPS-03 Capacity Management - Controlling of Resources . . . 106
OPS-04 Protection Against Malware - Policies and Procedures . . . 107
OPS-05 Protection Against Malware - Implementation . . . 108
OPS-06 Data Backup and Recovery - Policies and Procedures . . . 109
OPS-07 Data Backup and Recovery - Monitoring . . . 111
OPS-08 Data Backup and Recovery - Regular Testing . . . 112
OPS-09 Data Backup and Recovery - Storage . . . 113
OPS-10 Logging and Monitoring - Policies and Procedures . . . 115
OPS-11 Logging and Monitoring - Policies and Procedures for Handling Cloud Service Derived Data and Account Data . . . 116
OPS-12 Logging and Monitoring - Access, Retention and Deletion . . . 117
OPS-13 Logging and Monitoring - Security Information and Event Management . . . 118
OPS-14 Logging and Monitoring - Retention of the Logging Data . . . 119
OPS-15 Logging and Monitoring - Accountability . . . 120
OPS-16 Logging and Monitoring - Configuration . . . 121
OPS-17 Logging and Monitoring - Availability of the Monitoring Software . . . 121
OPS-18 Managing Vulnerabilities - Policies and Procedures . . . 122
OPS-19 Managing Incidents and Crashes - Policies and Procedures . . . 124
OPS-20 Managing Incidents - Implementation . . . 126
OPS-21 Managing Crashes - Implementation . . . 126
OPS-22 Managing Vulnerabilities, Incidents and Crashes - Penetration Tests . . . 127
OPS-23 Managing Vulnerabilities, Incidents and Crashes - Measurements, Analyses and Assessments of Procedures . . . 130
OPS-24 Involvement of Cloud Service Customers in the Event of Incidents . . . 131
OPS-25 Managing Vulnerabilities, Incidents and Crashes - Vulnerability Scans . . . 132
OPS-26 Managing Vulnerabilities, Incidents and Crashes - System Hardening . . . 134
OPS-27 Managing Vulnerabilities - Patch Management Policies and Procedures . . . 135
OPS-28 Managing Vulnerabilities - Patch Management Implementation . . . 137
OPS-29 Managing Vulnerabilities, Incidents and Crashes - Externally Sourced Components . . . 137
OPS-30 Separation of Datasets - Policies and Procedures . . . 138
OPS-31 Separation of Datasets - Implementation . . . 139
OPS-32 Confidential Computing - Policies and Procedures . . . 140
OPS-33 Confidential Computing - Remote Attestation . . . 142
OPS-34 Container Management - Policies and Procedures . . . 143
OPS-35 Container Management - Implementation . . . 145
5.7 Identity and Access Management (IAM) . . . 145
IAM-01 Policy for Identities and Access Rights . . . 145
IAM-02 Granting and Change of Identities and Access Rights . . . 148
IAM-03 Risk-Based Procedure for Locking and Withdrawal of Identities . . . 149
IAM-04 Withdrawal or Adjustment of Access Rights as the Task Area Changes . . . 150
IAM-05 Regular Review of Access Rights . . . 151

IAM-06 Privileged Access Rights . . . 153
IAM-07 Access to Cloud Service Customer Data . . . 155
IAM-08 Authentication Mechanisms . . . 158
IAM-09 Confidentiality of Authentication Information . . . 160
5.8 Cryptography and Key Management (CRY) . . . 162
CRY-01 Policy for the Use of Cryptographic Mechanisms . . . 162
CRY-02 Cryptographic Change Management . . . 165
CRY-03 Review of Cryptography Practices . . . 165
CRY-04 Protection of Data for Transmission (Transport Protection) . . . 166
CRY-05 Encryption of Sensitive Data at Rest . . . 167
CRY-06 Secure Key Generation . . . 169
CRY-07 Rotation of Cryptographic Keys . . . 169
CRY-08 Public-Key Certificate Issuance . . . 170
CRY-09 Secure Key Provisioning . . . 171
CRY-10 Secure Storage of Keys . . . 171
CRY-11 Cryptographic Key Archival . . . 172
CRY-12 Cryptographic Key Transition Management . . . 173
CRY-13 Handling of Compromised Keys . . . 173
CRY-14 Secure Deactivation of Cryptographic Keys . . . 174
CRY-15 Requirements for Pre-Shared Keys . . . 175
CRY-16 Operational Continuity for Key Management . . . 175
CRY-17 Cryptographic Key Lifecycle Management . . . 176
CRY-18 Usage of External Key Management Systems . . . 177
CRY-19 Secure Handling of Customer Managed Keys . . . 178
5.9 Communication Security (COS) . . . 179
COS-01 Technical Safeguards . . . 179
COS-02 Security Requirements for Connections in the Cloud Service Provider's Network . . . 180
COS-03 Monitoring of Connections in the Cloud Service Provider's Network . . . 181
COS-04 Cross-Network Access . . . 182
COS-05 Networks for Administration . . . 183
COS-06 Separation of Data Traffic in Jointly Used Network Environments . . . 184
COS-07 Documentation of the Network Topology . . . 184
COS-08 Policies for Data Transmission . . . 186
5.10 Portability and Interoperability (PI) . . . 187
PI-01 Safety of Input and Output Interfaces . . . 187
PI-02 Contractual Agreements for the Provision of Data . . . 188
PI-03 Secure Deletion of Data . . . 190
5.11 Procurement, Development and Modification of Information Systems (DEV) . . . 191
DEV-01 Policies for the Development/Procurement of System Components . . . 191
DEV-02 Outsourcing of the Development . . . 193
DEV-03 Policies for Changes to System Components . . . 195
DEV-04 Safety Training and Awareness Programme Regarding Continuous Software Delivery and Associated Systems, Components or Tools . . . 197
DEV-05 Design Documentation for Security Features . . . 197
DEV-06 Risk Assessment, Categorisation and Prioritisation of Changes . . . 198
DEV-07 Testing Changes . . . 199
DEV-08 Logging of Changes . . . 200
DEV-09 Version Control . . . 201

DEV-10 Approvals for Provision in the Production Environment . . . 202
DEV-11 Protection of Development and Test Environments . . . 203
DEV-12 Separation of Environments . . . 204
DEV-13 Transparency about Software Components . . . 204
DEV-14 Secure Use of Third Party Hardware and Software . . . 205
DEV-15 Exceptions to the Change Management Process . . . 206
5.12 Control and Monitoring of Service Providers and Suppliers (SSO) . . . 207
SSO-01 Policies and Procedures for Controlling and Monitoring Service Organisations 207
SSO-02 Risk Assessment of Service Organisations . . . 208
SSO-03 Data Processing of Service Organisations . . . 210
SSO-04 Directory of Service Organisations . . . 210
SSO-05 Monitoring of Compliance with Requirements . . . 211
SSO-06 Contract Termination Strategy for Service Organisations . . . 214
SSO-07 Ensuring Transparency within Service Organisations . . . 216
SSO-08 Controlling Exchanges with Suppliers of Functional Components . . . 217
5.13 Security Incident Management (SIM) . . . 218
SIM-01 Policy for Security Incident Management . . . 218
SIM-02 Security Incident Response Plans . . . 219
SIM-03 Processing of Security Incidents . . . 219
SIM-04 Documentation and Reporting of Security Incidents . . . 221
SIM-05 Duty of the Personnel to Report Security Incidents to a Central Body . . . 222
SIM-06 Evaluation and Learning Process . . . 223
5.14 Business Continuity Management (BCM) . . . 224
BCM-01 Business Continuity and Emergency Management System . . . 224
BCM-02 Business Impact Analysis . . . 225
BCM-03 Business Continuity Plans . . . 226
BCM-04 Testing Business Continuity . . . 227
5.15 Compliance (COM) . . . 229
COM-01 Identification of Applicable Legal, Regulatory, Self-imposed or Contractual Requirements . . . 229
COM-02 Policy for Planning and Conducting Audits . . . 230
COM-03 Internal Audits of the Information Security Management System . . . 232
COM-04 Information on Information Security Performance and Management Assessment of the ISMS . . . 233
5.16 Dealing with Investigation Requests from Government Agencies (INQ) . . . 235
INQ-01 Legal Assessment of Investigation Requests . . . 235
INQ-02 Informing Cloud Service Customers about Investigation Requests . . . 236
INQ-03 Limiting Access to or Disclosure of Data in Investigation Requests . . . 236
INQ-04 Communication of Technical Procedures for Data Disclosure in Investigation Requests . . . 237
5.17 Product Safety and Security (PSS) . . . 239
PSS-01 Guidelines and Recommendations for Cloud Service Customers . . . 239
PSS-02 Identification of Vulnerabilities of the Cloud Service . . . 241
PSS-03 Informing Customers about Known Vulnerabilities . . . 242
PSS-04 Error handling and Logging Mechanisms . . . 244
PSS-05 Authentication Mechanisms . . . 246
PSS-06 Session Management . . . 247
PSS-07 Confidentiality of Authentication Information . . . 247
PSS-08 Roles and Rights Framework . . . 249

PSS-09 Authorisation Mechanisms 250
PSS-10 Software Defined Networking 251
PSS-11 Images for Virtual Machines and Containers 251
PSS-12 Region of Data Processing and Storage 253

6 Legal notice **256**

1 Introduction

1.1 Preliminary remarks

Cybersecurity is a whole-of-society task that can only be addressed collectively. The BSI fulfils its responsibility as an integral part of the German, European and global cybersecurity architecture and works in open, collaborative cooperation at eye level with all stakeholders towards the vision of Cybernation Germany. Information security is a prerequisite for successful digitalisation, as this can only succeed if users develop trust in (new) technologies and are able to use them safely for their benefit.

Cloud computing is the basis of modern industrialised IT and therefore essential for the digitalisation of economy, administration and society. However, in order to securely utilise the potential of this development and implement the vision of the Cybernation Germany, industry-compatible security standards are required: they make cloud services comparable, create trust and thus support the unison of cyber security and digitalisation.

Making sovereign decisions on the use of cloud services requires having options and being able to evaluate them on a sound basis. This demands a thorough understanding of the available offerings and their security properties - to assess their effectiveness, evaluate risks to information security, appraise achievable resilience, analyse complex supply chains and associated dependencies, and to derive clear and binding requirements from these insights. The Cloud Computing Compliance Criteria Catalogue (C5) makes a decisive contribution in this regard: as a technical and procedural standard of high professional quality, it creates the transparency about the security properties of cloud services that is necessary for strategic decisions to be made on a technically sound and substantiated basis.

Since 2016, the BSI has provided an established pillar for the security of cloud computing with the C5. The C5 directly contributes to the achievement of the strategic objectives of Cybernation Germany: it places cybersecurity as a binding standard on the agenda of cloud service providers and their customers, substantially increases the cyber resilience of companies and institutions, promotes consistent digitalisation through reliable security requirements, and strengthens the German, European and global cyber market as the foundation for a trustworthy cloud ecosystem. With the C5:2026, the BSI now presents the second substantive revision of this criteria catalogue. The C5:2026 builds on the foundation of the C5:2020 and carries forward its proven criteria, while supplementing them with significant new requirements to account for the wide range of technological and regulatory developments of recent years.

A significant development in this context is the work of ENISA on the European cloud certification scheme EUCS. The C5:2020, a widely used and globally adopted standard for cloud security, served

as the basis for the development of the security requirements of the planned EUCS Substantial level. The requirements developed in this process and by the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation (CEN/CENELEC) form the substantive basis of the C5:2026. The BSI thus responds to the pace of technological change while simultaneously ensuring compatibility with EUCS Substantial.

In addition to the EUCS, the current versions of other relevant documents were taken into account in the development of the C5:2026, including Version 4 of the CSA Cloud Controls Matrix, the 2022 edition of the ISO/IEC 27001 standard, and the NIS2 Directive. Furthermore, practical experience from cloud providers, auditors, and consultants has been incorporated into this current revision.

The following aspects represent the key changes compared to the previous version of this criteria catalogue:

- Inclusion of new criteria addressing current technical developments and advances, in particular regarding container management, supply chain management, post-quantum cryptography, and confidential computing;
- More detailed consideration of multi-tenancy and the technical implementation of sovereignty, to provide users with a sound basis for making sovereign decisions on the use of cloud services;
- Sharpening which types of data individual criteria apply to, based on frequently received feedback on the C5:2020;
- Structural revision of the criteria in line with EUCS: C5 criteria now consist of sub-criteria that are clearly delineated from one another in terms of content, enabling more precise mapping to controls within cloud providers' service organisation control systems and greater clarity in auditing; and
- Explicit classification of additional criteria according to whether they sharpen the existing basic criteria with stricter requirements ('additional sharpen') or complement them with new requirements ('additional complement').

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

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 (cf. below) that is required to administer the cloud service (cf. below). Account data (e.g. payment information, contact information, etc.) is typ-

ically generated when a cloud service is purchased and is under the control of the cloud service provider (cf. below).

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 property that information, services, and functions of an IT system, IT applications or IT networks are accessible and usable on demand by an authorised entity.

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 broker

A cloud service broker is a natural or legal person, or a group of either (whether or not incorporated), that performs a set of specified tasks supporting or auxiliary to the cloud service provider, one or more cloud service customer, or both — with the specific function of negotiating relationships between cloud service customers and cloud service providers.

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 service 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

Natural or legal person providing a cloud service.

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.

Cloud service user

Natural person, or entity acting on their behalf, associated with a cloud service customer that uses cloud services.

Confidentiality

The property that information is not made available or disclosed to unauthorised individuals, entities, or processes.

Cybersecurity risk

Cybersecurity risks are effects of uncertainty associated with information and technology. Cybersecurity risks relate to the loss of confidentiality, authenticity, integrity (cf. below), 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.

Framework

A framework is a structured set of policies, procedures, guidelines and accompanying documents that provide an organised approach for archieving specific objectives.

Functional component

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

Guideline

A guideline provides recommendations, orientation and good practice about a specific topic. They are less formal than policies or procedures (both cf. below) and do in general not exhibit requirements. They often serve as explanations for policies and help to set procedures.

Hardware components

System components (cf. below) that are classified as hardware.

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).

ICT service

A service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems.

Incident

Unplanned interruption to the cloud service, a reduction in the quality of the cloud service or an event that has not yet impacted the cloud service to the cloud service customer.

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 property that information is 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.

Log

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.

Maximal tolerable period of disruption (MTPD)

Time limit until which a business process may be unavailable before intolerable consequences arise for an organisation. The time limit is determined based on a damage assessment of the affected business process.

Minimum business continuity objective (MBCO)

Capacity required in an emergency to ensure adequate business operations. The MBCO is determined individually for each business process or resource.

Partition

A partition is an overarching grouping of regions (cf. below) that share a unified identity and access management (IAM) system for both cloud service provider personnel 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.

Policy

Intentions and directions of an organisation that are formally expressed by its top management.

Procedure

A procedure is often connected to a policy and describes how a policy, process or task is put into concrete action; i.e. it operationalises the expectations that policies lay out.

Protection need

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 for 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.

Recovery point objective (RPO)

Maximum age that available data may have in order to enable the adequate operation of time-critical business processes after a disruption. The RPO is usually specified as the required frequency of data backups per application, IT system or business process.

Recovery time objective (RTO)

The period of time following an incident within which a product, service or activity must be resumed, or resources must be recovered, to a predefined level, in order to limit the impact of the interruption to an acceptable level.

Redundancy

Availability of alternate components, systems, or processes to assume the intended function following the failure of one or more components, in order to maintain the required level of service.

Region

A region comprises one or more zones (cf. below), 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.

Resilience

Ability to resist, adapt to, or quickly recover from potentially disruptive events or conditions, whether natural or anthropogenic, in order to maintain or restore the intended service.

Risk Owner

Person or entity with the accountability and authority to manage a risk.

Security 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 materialised cybersecurity risk. A security incident is a strict subset of incidents.

Significant change

Addition, modification, or removal of system components (cf. below) that could reasonably be expected to materially impact information security risks, control effectiveness or contractual obligations of the cloud service provider. Exemplary events that could represent a significant change are listed in the supplementary information for criterion OPS-22.

Software components

System components (cf. below) that are classified as software.

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.

Timely

Done or occurring sufficiently early, without unreasonable delay, considering the nature of the matter and the potential harm it could cause, including the cloud service provider's ability to meet the C5 criteria.

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.

Zone

A zone is a logical group consisting of at least two locations in close proximity to each other. Zones are physically segregated with separate power supply, cooling, networking and environmental risk profiles, such as separate fire compartments, to minimise the risk that disruptions at one zone impact the availability of other zones within a region.

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 assurance engagement in which a party other than the practitioner (cf. below) measures or evaluates the underlying subject matter against the criteria. A party other than the practitioner also often presents the resulting subject matter information in a report or statement and concludes whether or not the subject matter information is free from material misstatement (cf. below). Please note: In general usage, assurance engagements are called audits, whereas public accountants use the term audit for financial statement audit engagements, only. To ease understanding also for general readers, we use the term audit in the description to refer to general usage although it is not an audit engagement of a financial statement but an attestation engagement.

C5 criteria

The criteria applied to assess the information security of the cloud service and defined in this catalogue.

Carve-out method

Method of addressing the services provided by a subservice organisation (cf. below) in which the components of the subservice organisation's system of internal control (cf. below) 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. Consequently, no information provided about the subservice organisation beyond the information obtained by the cloud service provider for the operation of its controls to meet the criteria of the SSO domain is considered in the audit. However, the description of the system of internal control 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 (cf. below) that a cloud service provider assumed, in the design of its system of internal control (cf. below) 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 provide reasonable assurance that the applicable C5 criteria are met.

Complementary subservice organisation controls (CSOC)

Controls (cf. below) that cloud service provider assumed, in the design of its system of internal control (cf. below) relevant to the development and operation of the cloud service, would be implemented by the subservice organisation (cf. below). 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 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 (cf. below) in which the description of the cloud service provider's system of internal control (cf. below) 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.:

1. Information does indicate that controls are not suitably designed, not implemented or not operating effectively to meet the C5 criteria with reasonable assurance;
2. 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
3. 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.

Practitioner

The individual(s) conducting the audit, also referred to as the 'auditor'.

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:

1. 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.
2. 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 so-called 'General Conditions' (cf. section 4) and criteria regarding the information security of cloud services (cf. section 5).

The so-called 'General Conditions' (cf. section 4) 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 3.4.4.2; this section also provides guidance for obtaining evidence about 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. These further criteria also serve to 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.

Section 5 contains 17 objectives regarding the information security of cloud services. Each objective has its own subsection where the particular criteria are found that are required to achieve the objective.

The criteria themselves are divided into basic criteria and additional criteria (C5 criteria). If the criteria address several aspects for achieving the objective, they are broken down into subcriteria. This is done

1. to ease the mapping of controls of
    1. the cloud service provider's internal control system controls,
    2. Complementary User Entity Controls to cloud service provider controls; and
2. to ease the documentation of testing procedures for auditors.

The set of all basic subcriteria of one criterion (e.g. OIS-01.01B, OIS-01.02B and OIS-01-03B) is hence called the basic criterion (in this case OIS-01). Definitions and context are to be understood across the entire criterion; that is, the subcriteria belonging to the same criterion are not to be considered in isolation, but in combination with one another.

The additional criteria are further divided into sharpening and complementing additional subcriteria (also refered to as 'additional (sharpening)' and 'additional (complementing)'). The set of all additional sharpening and complementing subcriteria of one criterion is called the additional criterion (e.g. the notion 'additional criterion of OIS-01' refers to the set of OIS-01.01AS and OIS-01.01AC).

A sharpening additional subcriterion always sharpens a particular basic subcriterion. It does so by addressing the same aspect for achieving the criterion's objective as the basic subcriterion, but with sharper security requirements. A sharpening additional subcriterion thus acts as stricter replacement for the basic subcriterion it sharpens. A complementing additional subcriterion, on the other hand, complements the basic criterion by introducing new aspects for achieving the criterion's objective that were not yet addressed by any of the basic subcriteria. A complementing additional subcriterion thus acts as an addition to the entire set of basic subcriteria of its criterion. The definitions and context from the basic criterion extend to the additional criterion.

According to the BSI, the basic criteria reflect the minimum level of information security that a cloud service has to 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 protection need, the additional criteria can provide a starting point to address this protection need together with a solid architecture of their cloud workload. The identification of the particular additional criteria required to meet this protection need is one possible result of the cloud service customer's 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:

1. The criteria support cloud service providers with identifying those C5 criteria that typically require complementary user entity controls (CUEC) which must be set up together with the controls of the cloud service provider in order to meet the C5 criteria;
2. The criteria support auditors with assessing the system description regarding the appropriateness of the information provided about the CUEC; and
3. The criteria support cloud service customers in better understanding the information provided about the CUEC 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 shall 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 grouped into 17 areas based on the structure of the objectives in ISO/IEC 27001:2013 Annex A (cf. Table 2.1). However, for the content of the criteria, ISO/IEC 27001:2022 was considered instead (cf. 2.3).

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 Procedures (SP)	Provide policies and procedures regarding security requirements and to support business requirements.
3	Personnel (HR)	Ensure that personnel understands its responsibilities, is aware of its 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 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 (service organisation) 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:

1. ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection - Information security management systems - Requirements
2. ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection - Information security controls
3. ISO/IEC 27017:2015 - Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services
4. BSI - IT-Grundschutz-Compendium, 2023
5. 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)
6. 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)
7. ANSSI (Agence nationale de la sécurité des systèmes d'information, National Cybersecurity Agency of France) - Providers of cloud computing services v. 3.2 (SecNumCloud)
8. IDW (Institut der Wirtschaftsprüfer, the German Institute of Certified Public Accountants) RS FAIT 5 - 'Principles of Orderly Accounting for the Outsourcing of Financial Reporting-Related Services including Cloud Computing', as of November 4, 2015
9. ANNEX 'Technical and methodological requirements', C(2024)7151, Implementing Regulation to the NIS2-Directive (2022/2555)
10. CEN/TS 18026:2024, 'Three-level approach for a set of cybersecurity requirements for cloud services', 2024
11. 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 principles, procedures and measures on one or more of these standards and publications can map them to the C5 criteria to assess compliance. Please note that CEN/TS 18026:2024 is the technical specification that was created for the European Cybersecurity Certification Scheme for Cloud Services (EUCS), for which C5:2020 was the basis for the level 'Substantial' and which was an important intermediate step for the present C5.

A cross-reference table of the BSI supports the mapping and is available on its website (https://www.bsi.bund.de/C5). Cloud service providers should consider the table as an aid when assessing compliance. Notwithstanding the information contained in the cross-reference table, cloud service providers and auditors shall determine to what extent existing principles, 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 principles, 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. The BSI published an Excel-based evaluation guideline to help cloud service customers evaluate C5 reports in a structured manner. 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. For cloud service customer on the federal level of the German public sector, the 'Mindeststandard des BSI zur Nutzung externer Cloud-Dienste' is applicable.

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 usually 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. These are:

1. The International Standard on Assurance Engagements (ISAE) 3000 (Revised) 'Assurance Engagements Other than Audits or Reviews of Historical Financial Information',
2. 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),
3. or other national equivalents to ISAE 3000 (Revised).

Auditors shall 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:

1. ISAE 3402 'Assurance Reports on Controls at a Service Organization',
2. the German IDW PS 951 n.F. 'Die Prüfung des internen Kontrollsystems bei Dienstleistungsunternehmen', which is in line with ISAE 3402,
3. or other national equivalents to ISAE 3402.

The scope of audits in accordance with these standards comprises the principles, procedures and measures 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 objectives 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'.

3.3 Relationship 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 catalogue, both in terms of organisation and timing. This enables auditors and cloud service providers to use records simultaneously 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 to a certain extent. A cross-reference table of the BSI can be used for this purpose. It is available on the BSI's website (https://www.bsi.bund.de/C5).

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 cross-reference table, the C5 criteria are mapped to the criteria defined in other standards. It should be noted that the 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 table is 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 fulfillment of the C5 criteria by priciples, procedures and measures implemented by a cloud service provider solely from the mapping given in the cross-reference table. This applies even if the established principles, procedures and measures have already been audited against one or more of the standards contained in the cross-reference table. According to the BSI, it shall always be assessed individually and specifically to what extent the principles, 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 cross-reference table 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 BSI's supplementary requirements for conformity assessments in accordance with this criteria catalogue. These requirements were derived from ISAE 3000 and ISAE 3402. In addition, the auditing standards 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 considered. These standards supplement ISAE 3402 and IDW PS 951 especially with requirements for the consideration of subservice organisations. These supplementary requirements shall be adhered to by cloud service providers and auditors when performing conformity assessments based on this criteria catalogue.

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.

3.4.1 Assurance Engagement

Conformity assessments shall always 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 'reasonable 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 a conclusion on the cloud service provider's controls to meet the C5 criteria throughout a specified period. Assurance engagements on the suit-

ability 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 one or several cloud services, when there is not yet sufficient evidence to issue a conclusion about the operating effectiveness throughout a specified period (e.g. when a new cloud service is supposed to be made available to cloud service customers). As such, assurance engagements only on the suitability of the design shall not 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 Management (ISQM) 1 'Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements' or the German IDW quality management assurance standard 'Anforderungen an das Qualitätsmanagement in der Wirtschaftsprüferpraxis' (IDW QMS 1 (09.2022)) or other national equivalents of ISQM 1, supervise the execution and review the results of the engagement (including evaluation of the work performed, review of the documentation and the planned reporting):

1. 3 years relevant professional experience with IT audits in a public audit firm

or one of the following professional examinations/ certifications:

1. 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)
2. ISO/ IEC 27001 Lead Auditor or BSI certified ISO 27001 Auditor for audits based on BSI IT-Grundschutz
3. Cloud Security Alliance (CSA) – Certificate of Cloud Security Knowledge (CCSK)
4. $(ISC)^2$ – Certified Cloud Security Professional (CCSP)
5. $(ISC)^2$ - Certified Information Systems Security Professional (CISSP)

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

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 protection need, the additional criteria can provide a starting point to address this protection need together with a solid architecture of their cloud workload. The identification of the particular additional criteria required to meet this protection need is one possible result of the cloud service customer's assessment.

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. The cloud service provider may also include individual additional subcriteria of a criterion in the scope of the audit without having to include the entire set of the criterion's additional subcriteria. 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 or subcriteria to the scope, these criteria or subcriteria should be included. If the cloud service provider includes only certain of the additional criteria or subcriteria, 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 sharpening additional subcriterion is included in the audit and presented in the description of the cloud service provider's system of internal control for the cloud service, the basic subcriterion that it sharpens is not presented in the description, but only the sharpening additional subcriterion. The basic subcriterion is replaced by the sharpening additional subcriterion. If a complementing additional subcriterion is included in the audit, the subcriteria of the basic criterion that it complements are presented in the description in combination with the complementing additional subcriterion.

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 include this justification as well when presenting the applicability of the criterion.

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 suitabil-

ity 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 a conclusion with reasonable assurance as to whether:

1. 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 3.4.13 of this catalogue;
2. 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
3. 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 shall be mandated for initial engagements only. Subsequent engagements shall mandate a type 2 report. If a type 2 report is mandated, the minimum period should cover at least three 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 twelve months. In exceptional cases, the specified period may be extended beyond twelve months, for example to better align with other audits. In general, consistency in the specified period is recommended.

The auditor's conclusion 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 personnel that belongs 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. For the consideration of controls at subservice organisations, see also section 3.4.6.

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 (cf. section 3.4.5.1 '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 a conclusion with reasonable assurance as to whether

1. 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
2. if mandated (type 2 report), the principles, procedures and measures applied by the cloud service provider operated effectively to provide reasonable assurance that the applicable criteria were met throughout the specified period.

Type 1 reports shall be mandated for initial engagements only. Subsequent engagements shall mandate a type 2 report. If a type 2 report is mandated, the minimum period should cover at least three 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 twelve months. In exceptional cases, the specified period may be extended beyond twelve months, for example to better align with other audits. In general, consistency in the specified period is recommended.

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. Please note that, in case of a direct engagement, it is the responsibility of the auditor to ensure that the information listed in the section 'Information on the General Conditions of the Cloud Service' (cf. section 4) is obtained.

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 (the 'Description Criteria').

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

1. Name, type and scope of cloud services provided;
2. Description of the system components for providing the cloud service;
3. 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;
4. 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';

5. 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;
6. Dealing with significant events and conditions that represent exceptions to normal operation, such as security incidents or the failure of system components;
7. Complementary customer controls (also called complementary user entity controls (CUEC)) assumed in the design of the cloud service provider's controls; and
8. 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 accordance with criterion SSO-05.

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

1. 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;
2. Details on significant events and conditions that are exceptions to normal operation, that have occurred throughout the specified period and have resulted in:

    1. contractual agreements regarding the availability of the cloud service not being fulfilled, or
    2. unauthorised third parties having gained access to cloud service customer data, or
    3. the integrity of the cloud service customer data was compromised or the protective measures put in place (e.g. data backup) were not effective,

3. as well as the measures initiated by the cloud service provider to prevent such events and conditions in the future.

Events and conditions are typically significant when they affect multiple cloud service customers, and the cloud service provider informs the affected parties or the public. The information about the events and conditions 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 events and conditions.

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:

1. 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;
2. 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.
3. 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 twelve 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 Service 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' (cf. 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:

1. The services provided by the service organisation are likely to be relevant to the cloud service customers' understanding of the architecture of the cloud service and how the cloud service provider addresses the applicable C5 criteria. A service is likely relevant, if the service organisation contributes and/or has access to system components of the cloud service and may access confidential information or transmit information between themselves and the cloud service.
2. 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, the service organisation 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 characteristic of relevance to the cloud service customer's understanding, 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 accountable 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
    1. Name of the company with which a contractual relationship exists for the services performed;

   2. Location of processing and storage of data (Country-level information is sufficient);
   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 (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 accordance with criterion SSO-05.

In the case of a direct engagement, where there is no Description prepared by the cloud service provider, the auditor shall 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 to 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 each criterion and how these fulfil the corresponding subcriteria. 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:

1. Whether the control (and if applicable, considered with other controls) addresses the elements of the C5 criteria to which it relates on the level of the subcriteria (the control is commensurate with the measures specified in the subcriteria).
2. 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.
3. The frequency or timing of the occurrence or performance of the control.
4. 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).
5. 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).
6. Whether the information used in the operation of the controls is reliable.
7. Whether the control is adequately adapting and and evolving, e.g., when the cloud service provider's organisation changes or new risks, threats and vulnerabilities need to be addressed.
8. 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:

1. 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.
2. If controls 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 shall be limited to the initial engagement only and shall not be mandated for consecutive engagements. If a type 2 report is mandated, the minimum period should cover at least three 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 twelve months. In exceptional cases, the specified period may be extended beyond twelve months, for example to better align with other audits. In general, consistency in the specified period is recommended.

3.4.12 Deviation Handling

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

1. The cloud service provider's Description does not fairly present, in all material respects, the System as designed and implemented;
2. The applicable C5 criteria were not fully met by controls, which is to be assumed if one of the subcriteria belonging to a criterion is not met;
3. The controls related to the applicable C5 criteria were not suitably designed, in all material respects;
4. In the case of a type 2 report, the controls tested did not operate effectively, in all material respects; or
5. The auditor is unable to obtain sufficient appropriate evidence,

the auditor's conclusion 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 conclusion needs to be modified:

1. Inquiry of management of the cloud service provider regarding the root cause analysis of the identified deviation;
2. Assessment of the cloud service provider's handling of the identified deviation;
3. 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
4. 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 conclusion 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:

1. If the deviation was detected by the cloud service provider itself, when and in the course of which measures the deviation was detected.
2. 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.
3. 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 a conclusion 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 organisations, 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:

1. preparing the Description of its System and the management statement, including the completeness, accuracy, and method of presentation of the Description and the statement;
2. providing the cloud services covered by the Description;
3. selecting the applicable C5 criteria stated in the Description;
4. identifying the risks that threaten the applicable C5 criteria from being met; and
5. 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:

   1. complies with the independence and other ethical requirements of the International Code of Ethics for Professional Accountants (including International 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;
   2. 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
   3. 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 a conclusion 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 conclusion 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:

   1. Name, type and scope of cloud services provided;
   2. The nature of the cloud services provided;
   3. How the cloud service provider's System interacts with user entities, subservice organisations, and other parties;
   4. Internal control and its limitations;

5. Complementary controls of user entities and how they interact with related controls at the cloud service provider to meet the applicable C5 criteria;
6. User entity responsibilities and how they may affect the user entity's ability to effectively use cloud services;
7. The criteria set out in this catalogue; and
8. 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 pre-formulated 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 service 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:

   1. 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.
   2. 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 (cf. 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 a conclusion 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 in engagements with specified dates (type 1 reports) as of or after June 1st, 2027, or specified periods (type 2 reports) beginning on or after June 1st, 2027. Earlier adoption is permitted.

In a Type 2 engagement, if the specified period begins before June 1st, 2027 and ends after that date, the engagement should comprise the criteria of the previous revision of this catalogue only (C5:2020). There should be no combinations of the previous revision (C5:2020) and the current revision (C5:2025) in the same engagement, because this could lead to confusion about the applicability of criteria.

Cloud service providers that have a System of internal control addressing C5:2020 are required to adjust their controls so these address the criteria set out in this revised catalogue. Adjustments of controls might include, e.g., expansions of a control's scope or activity to address an additional aspect required by a revised criterion. Hence, there might be evaluations of the suitability of the design or operating effectiveness of controls that encompass the controls' status both before and after the cloud service provider has adjusted them to the revised catalogue.

Adjustments that the cloud service provider applies to its System of internal control relevant to the development and operation of the cloud service shall be considered to be significant changes. Therefore, the cloud service provider shall include information on these changes in the system description (cf. section 'Description Criteria' of this catalogue). In the case of a direct engagement, the auditor shall obtain and disclose this information.

Adjusting controls is a process and cloud service providers might not have completed all adjustments required to meet the new and revised criteria in this catalogue ahead of an audit. Thus, if the specified period ends on or after Februry 28th, 2027, the cloud service provider shall provide additional information on planned changes to controls in the Description of its System of internal control relevant

to the development and operation of the cloud service. This is to provide transparency to customers about the cloud service provider's general ability to comply with the criteria of this catalogue going forward.

The cloud service provider should include the following aspects on planned changes, as applicable:

1. ID/Title of the revised criterion to be met with the change
2. Nature of the change
3. Implementation status (e.g. implemented/not implemented)
4. Implementation date.

As the information is part of the cloud service provider's Description, the auditor shall perform procedures to determine whether the information is fairly presented. However, the auditor shall not yet evaluate the suitability of the design or operating effectiveness of such changes to controls.

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 'General Conditions' or 'GC' for short - serves to provide cloud service 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 cloud service customers to compare several cloud service 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 shall document details of the general conditions in accordance with the information provided by the cloud service provider (cf. section 3.4).

The information is prepared to meet the common needs of a broad range of subject matter experts of the cloud service customers who define or implement information security requirements, validate their effectiveness or assess the suitability of the cloud service from a legal and regulatory perspective (e.g. IT, compliance, internal audit).

GC-01 Information on applicable law, jurisdiction, countries, 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:

1. Its applicable law;
2. Its jurisdiction (courts that will hear disputes);
3. The country in which the cloud service provider's entity or entities that prepared the description is/are registered as a legal entity;
4. The country in which the cloud service provider's headquarters (ultimate parent) is registered as a legal entity;
5. The partitions, regions, zones and locations that are provided to cloud service customers for the operation of the cloud service, where the cloud service customer data, cloud service derived data and account data is processed, stored and backed up, based on service offering type (SaaS, PaaS, IaaS); and

6. If certain of these partitions, regions, zones and locations are not in scope of the assurance engagement, an indication for their exclusion.

The information is prepared to meet the common needs of a broad range of subject matter experts of the cloud service customers who define or implement information security requirements, validate their effectiveness or 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

For definitions of the terms partitions, regions, zones, locations and the data types cf. section 1.2. If the processing, backup and storage of customer data take place in different partitions, regions, zones and locations, this has to be described comprehensibly and transparently in the system description.

GC-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 presents comprehensible, binding and transparent information on:

1. Availability of the cloud service;
2. Categorisation and prioritisation of incidents;
3. Response times for disruptions of regular operation according to the categorisation (time elapsed between the reporting of the disruption and the first response by the cloud service provider);
4. Recovery time (time elapsed until the incident has been resolved); and
5. Contractual consequences of non-compliance.

The information is based on definitions that allow subject matter experts of the cloud service customers to assess the cloud service against their business requirements. Contractual agreements may refer to operational documentation (e.g. service documentation, technical specifications, or other publicly accessible resources) that can be regularly updated. The description of the cloud service provider's system of internal control relevant to the development and operation of the cloud service indicates where this information can be found. References relate precisely to the individual aspects specified above, allowing readers who are not familiar with the contractual agreement or the operational documentation to find the information in a timely manner.

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.

GC-03 Information on recovery parameters in emergency operation

Information on the General Conditions of the Cloud service

Upon request by subject matter experts of the cloud service customers, the cloud service provider shares comprehensible and transparent information about the following recovery parameters of the cloud service:

1. Maximum tolerable period of downtime (MTPD) and Recovery Time Objective (RTO);
2. Maximum allowable data loss / Recovery Point Objective (RPO);
3. Recovery time to start emergency operation;
4. Minimum business continuity objective (MBCO) (capacity related to regular operation); and
5. 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 indicates where this information can be found. References relate precisely to the individual aspects specified above, allowing these subject matter experts to find the information in a timely manner.

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.

GC-04 Information on the approach to ensuring service availability

Information on the General Conditions of the Cloud service

The cloud service provider shares comprehensible and transparent information subject matter experts of cloud service customers with on its approach to ensuring service availability, including relevant availability metrics and architecture design principles for both, datacentre-infrastructure and cloud services. This information addresses both, physical infrastructure resilience and logical service resilience, enabling cloud service customers to perform their business impact analysis effectively and understand how the cloud service provider's multi-layered resilience approach aligns with their own business continuity requirements at both, the infrastructure and service levels.

Supplementary Information - Notes on the General Conditions

The information may outline resilience capabilities, such as regional deployment strategies, datacentre redundancy configurations, service-level commitments, historical performance data, or architectural resilience patterns.

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

1. Tier I: 99.671 %; up to 28.8 hours cumulative downtime per year;
2. Tier II: 99.741 %; up to 22.7 hours cumulative downtime per year;
3. Tier III: 99.982 %; up to 1.6 hours cumulative downtime per year; and
4. Tier IV: 99.995 %; up to 25 minutes cumulative downtime per year.

An alternative definition of availability classes (AC) is provided by the BSI in the 'HV-Benchmark kompakt' (German for: 'High Availability Benchmark Compact', document only available in German):

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

GC-05 Information on how investigation requests 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 presents 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:

1. Procedures to verify the legal basis of such requests;
2. Procedures for informing and involving the affected cloud service customers upon receipt of such requests;
3. The ability of the affected cloud service customers to object;
4. Whether the cloud service provider stores cloud service customer data or cloud service derived data in unencrypted form;

5. 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;
6. The number of investigation requests for cloud service customer data or cloud service derived data and the countries from which these requests originate; and
7. 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-04. In case the description of the cloud service provider's system of internal control addresses multiple cloud services, differences in technical procedures between each service are to be detailed within the provided information.

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.

Further regulation applicable within the EU are, e.g., the Budapest Convention on Cybercrime (ETS No. 185) as well as the EU directives 2023/1543 and 2023/1544 to establish a legal framework for obtaining and securing electronic evidence in criminal proceedings across EU Member States.

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.

GC-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 presents comprehensible and transparent information on existing and valid certifications or attestations by independent third parties relating to the following aspects of the cloud service:

1. Compliance of the management systems for information security, business continuity and quality with applicable international standards;
2. Compliance with the European General Data Protection Regulation (GDPR);
3. Suitability of the design and operating effectiveness of the internal control system in relation to the applicable criteria;
4. Certifications or attestations (assurance reports) according to industry specific requirements of cloud service customers; and
5. Certifications or attestations (assurance reports) related to environmental, social and governance standards (ESG).

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

1. Date of issuance;
2. Issuing organisation;
3. Applicable scope; and
4. 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.

Compliance of the management systems for information security, business continuity and quality may be demonstrated, for example, with certificates in accordance with ISO/IEC 27001, ISO 22301 and ISO 9001.

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

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 maintains an ISO/IEC 27001-compliant information security management system (ISMS). 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:

1. Context of the cloud service provider;
2. Scope of the ISMS (section 4.3 of ISO/IEC 27001);
3. Statement of applicability (section 6.1.3 of ISO/IEC 27001);
4. Overview of how activities in the ISMS cover the cloud service;
5. Description of how the cloud service provider maintains and improves the cloud service's security; and
6. Results of the last management review (section 9.3 of ISO/IEC 27001).

OIS-01.03B

Additionally, the cloud service provider documents the scope and boundaries of the cloud service under its operational control, including any exclusions or shared-responsibility areas.

Additional (Sharpening)

OIS-01.01AS, sharpening OIS-01.01B

The Information Security Management System (ISMS) has a valid certification according to ISO/IEC 27001 or ISO 27001 based on BSI IT-Grundschutz. The scope of the certification covers the cloud service provider's organisational units, locations, zones, regions, and procedures relevant to the development and operation of the cloud service.

Additional (Complementing)

OIS-01.01AC

Existing valid certifications according to ISO/IEC 27001 are issued and recognised by an accredited certification body.

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 BSI 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 established to cover both, cloud service-specific internal control systems and organisation-wide/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 personnel as well as cloud service customers.

OIS-02.03B

The information security policy describes:

1. The importance of information security, based on the requirements of cloud service customers in relation to information security;
2. 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;
3. The cloud service provider's commitment to implement the necessary security measures for fulfilling the established security objectives;
4. The most important aspects of the security strategy to achieve the security objectives set; and
5. The organisational structure for information security in the scope of the ISMS.

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 organisation 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 a 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 cloud service customers.

OIS-03.02B

The SSRM documentation clearly defines the responsibilities between both parties for handling vulnerabilities, security incidents, and incidents. 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 in accordance with SP-02 to ensure its accuracy and relevance for all cloud service offerings.

OIS-03.04B

The cloud service provider implements, operates, and reviews 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.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: OIS-03.01B

Third parties in the sense of this basic criterion are, e.g. cloud service customers and service organisations (including cloud service broker). A SSRM provides a consolidated view of the key interfaces and dependencies between the cloud service provider and third parties. Detailed information on interfaces and dependencies can be defined in separate documents that are referenced in the SSRM, such as guidelines and procedures. 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 procedures to help cloud service customers understand their roles and responsibilities in terms of security and operational management.

If cloud services are delivered through a cloud service broker, the SSRM should clearly delineate responsibilities among the cloud service provider, the cloud service broker and the cloud service customer, in particular:

1. Data ownership and processing boundaries;
2. Security control implementation by each party;
3. Incident notification and escalation paths; and

4. Compliance attestation scope.

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

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

The cloud service provider can leverage existing documentation, such as guidelines, contractual agreements or procedures to present the underlying Shared Responsibility Model of their cloud service, thereby clarifying cloud service customers' security and operation responsibilities.

Applicable to: OIS-03.03B, OIS-03.05B

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.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure with 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:

1. Administration of a role, rights and authorisation framework based on role-based access control and the business and security requirements of the cloud service provider (cf. IAM-01);
2. Development, testing and release of changes (cf. DEV-01);
3. Risk management (cf. OIS-07); and
4. Operation of the system components.

OIS-04.02B

Mitigating measures are outlined in the risk treatment plan (cf. OIS-09) and implemented by the cloud service provider in a way that prioritises the segregation of duties.

OIS-04.03B

If segregation of duties cannot be implemented due to organisational or technical constraints, the cloud service provider establishes and operates compensating controls to monitor relevant activities. These controls are designed to detect unauthorised or unintended changes, misuse of data, or violations of operational policies, and enable timely and appropriate response actions.

OIS-04.04B

An inventory consisting of conflicting tasks, responsibilities and resolving measures is established and maintained by the cloud service provider. For the assignment, change or revocation of roles, rights and authorities, the cloud service provider enforces the segregation of duties.

Additional (Sharpening)

–

Additional (Complementing)

OIS-04.01AC

To resolve conflicting roles, measures associated with the segregation of duties are monitored and enforced by the cloud service provider.

OIS-04.02AC

Timely and appropriate remediation measures address any deviations identified during monitoring.

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. The area of risk management in the context of segregation of duties refers to the so-called different lines of defense, i.e. roles that review risks (2nd line of defense) are different from roles that own risks (1st line of defense).

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 cloud service provider integrates threat intelligence insights into its risk management process (cf. OIS-07, OIS-08 and OIS-09).

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: OIS-05.01B

Internal sources that can be used to collect information include, for example, the cloud service provider's internal security monitoring. External sources that can be used to collect information include, for example, threat intelligence feeds from government agencies, commercial threat intelligence providers or industry consortiums. Threat intelligence generally includes different areas like cybersecurity risk intelligence gathering (e.g. monitoring relevant internal or external sources), threat modelling and risk management.

Applicable to: OIS-05.02B

This process can, for example, include correlating threat intelligence with organisational assets, vulnerabilities, and business processes to identify relevant and actionable threats. The results can be used to provide regular threat briefings to cloud service provider's management and security teams.

Applicable to: OIS-05.03B

If a threat model is used for this process, the cloud service provider can, for example:

1. Use structured methodologies (e.g., STRIDE, PASTA, LINDDUN) appropriate to the cloud service architecture;
2. Map current threat landscape intelligence to specific system components, data flows, and trust boundaries;
3. Incorporate real-time threat intelligence to update threat models dynamically rather than relying on static annual assessments;
4. Consider emerging attack vectors, techniques, and procedures (TTPs) documented in frameworks such as MITRE ATT&CK; and
5. Account for supply chain and third-party risks through extended threat modelling.

The aim of threat modelling is to ensure that the current internal and external threats are reflected

in risk handling measures.

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 as appropriate.

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. If the cloud service provider does not have customers in the public sector, this criterion is not applicable.

As appropriate means that contacts are established when there is an actual need to do so. For instance, establishing contact with CERT typically involves the reporting of security incidents to CERT and following CERT's communication channels to stay informed about current threats, vulnerabilities and security guidance. Maintaining contact in the sense of OIS-06.01B does in this instance not require the cloud service provider to proactively communicate with CERT unprompted.

For KRITIS (critical infrastructure), as defined in section 2(10) of the BSI Act (BSIG), similar requirements to maintain contact with government agencies and stakeholders may apply under German national law.

Supplementary Information - Complementary Customer Criteria

–

OIS-07 Risk Management Policy

Basic Criteria

OIS-07.01B

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

1. 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;
2. Analysis of the probability and impact of occurrence and determination of the level of risk;
3. Evaluation of the risk assessment based on defined criteria for risk acceptance and prioritisation of risk management;
4. Treatment of risks through measures, including approval of authorisation and acceptance of residual risks by risk owners;
5. Documentation of the activities implemented to enable consistent, valid and comparable results; and
6. Evaluation of the risk assessment and the status of risk treatment plans by the level of 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, semiquantitative and quantitative methods (cf. ISO 31010) based on the likelihood and impact of the risks.

For identifying, evaluating, and prioritising potential threats and vulnerabilities associated with processes, systems, and data flows, threat modelling can provide a structured methodology: The cloud service provider can systematically analyse attack vectors and possible impacts to support auditors and stakeholders in validating the suitability of the design of implemented controls, highlight gaps in existing security measures, and ensure alignment with best practices for proactive risk mitigation.

Supplementary Information - Complementary Customer Criteria

–

OIS-08 Application of the Risk Management Policy - Risk Assessment

Basic Criteria

OIS-08.01B

The cloud service provider performs the risk management process specified by OIS-07 as needed and at least annually.

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:

1. Processing, storage or transmission of cloud service customer data and cloud service derived data with different protection needs;
2. Occurrence of vulnerabilities and incidents in technical protective measures for separating shared resources;
3. Attacks via access points, including interfaces accessible from public networks and accidentally exposed interfaces;
4. Dependencies on service organisations;
5. An encryption and key management risk programme which addresses the risks of unauthorised disclosure, modification, destruction, or information loss of cryptographic keys; and
6. Separation of cloud service customers and their data within systems, networks and storage.

OIS-08.03B

Policies and procedures covering risk assessments relevant for the delivery and operation of the cloud service are implemented by the cloud service provider.

OIS-08.04B

The risk assessment's results are provided to relevant internal parties.

OIS-08.05B

Relevant external parties are provided with information, specific to the parties' purposes, resulting from the risk assessments.

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. In addition, in case of significant changes to the cloud service, a review is carried out focusing on the parts of the risk assessment relevant to the change.

Additional (Sharpening)

OIS-08.01AS, sharpening OIS-08.01B

The cloud service provider performs the risk management process as specified by OIS-07 as needed and at least annually. The evolution of the risks is monitored and the risk assessments are reviewed correspondingly.

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:

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

OIS-08.02AC

When identifying risks, the cloud service provider also takes into account the detection of unusual and harmful actions of internal threat actors, insofar as it is applicable to the cloud service provided and is within the area of responsibility of the cloud service provider.

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-08.01AS, OIS-08.01AC, OIS-08.02AC

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 service 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)'.

Cloud service providers may leverage established risk management standards, such as ISO 27005 or the ISO 31000 family of standards to address risks related to the cloud service. Risk management procedures already implemented at the cloud service provider may be leveraged for OIS-08 where possible to reduce redundancies. Documentation of risks, treatment plans and risk acceptance in the sense of this criterion does not require specific formal frameworks; lean forms of documentation can be leveraged wherever appropriate to address the OIS-08 subcriteria.

Applicable to: OIS-08.01B

Examples of scenarios in which the risk management process may be executed 'as needed' include, but are not limited to, the following:

1. Changes to the threat landscape (cf. OIS-05);
2. Security incidents or business disruptions;
3. Changes to the cloud service provider's legal, regulatory, self-imposed and contractual requirements relevant to the information security of the cloud service (cf. COM-01);

4. Changes to the cloud service provider's organisational structure with impact on roles, responsibilties or procedures for provisioning the cloud service;
5. Changes to the achitecture of the cloud service (cf. OPS-31);
6. Events related to the cloud service provider's service organisations (cf. SSO-05);
7. Exceptions to policies or procedures (cf. SP-03); and
8. Identification of critical vulnerabilities (cf. OPS-22) or compliance deviations (cf. COM-03).

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.

Applicable to: OIS-08.04B

Relevant internal parties can include the cloud service provider's management and security teams.

Applicable to: OIS-08.05B

Relevant external parties can include cloud service customers, subservice organisations and regulatory agencies.

Information that can be relevant in this context includes information about identified vulnerabilities, security incidents and threat intelligence.

The cloud service provider can choose to make this information accessible through its SSRM (cf. OIS-03), its documentation and guidelines (cf. PSS-01) or its processes for informing cloud service customers about known vulnerabilities (cf. PSS-03).

Supplementary Information - Complementary Customer Criteria

–

OIS-09 Application of the Risk Management Policy - Risk Treatment

Basic Criteria

OIS-09.01B

The risk treatment is prioritised corresponding to the level of cybersecurity risks associated with the cloud service.

OIS-09.02B

A risk treatment plan according to the risk assessment (cf. OIS-08) is documented and implemented.

OIS-09.03B

Actions defined in the risk treatment plan reduce the risk level to a residual risk that risk owners are

able to accept.

OIS-09.04B

The risk treatment plan, as well as suitably summarised and abstracted versions, is provided to relevant internal parties.

OIS-09.05B

Based on contractual agreements and relevant legal and regulatory requirements, the cloud service provider determines which relevant external parties are provided with information, specific to the parties' purposes, about the risk treatment plan. The cloud service provider also determines the extent to which this should happen.

OIS-09.06B

The selected options for risk treatment are reviewed by the risk owners every time the risk assessment is modified. The review considers the criteria for risk acceptance and prioritisation of risk treatment.

OIS-09.07B

In case of the cloud service provider sharing risks with the cloud service customers, the cloud service provider maps shared risks to complementary customer controls and describes them in the user documentation (cf. PSS-01).

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: OIS-09.01B, OIS-09.02B, OIS-09.03B, OIS-09.04B, OIS-09.05B, OIS-09.06B, OIS-09.07B

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)'.

Cloud service providers may leverage established risk management standards, such as ISO 27005 or the ISO 31000 family of standards to address risks related to the cloud service. Risk management procedures already implemented at the cloud service provider may be leveraged for OIS-09 where possible to reduce redundancies. Documentation of risks, treatment plans and risk acceptance in the sense of this criterion does not require specific formal frameworks; lean forms of documentation can

be leveraged wherever appropriate to address the OIS-09 subcriteria.

Applicable to: OIS-09.01B

The priorisation can, for example, be performed by setting appropriate time limits for the treatment of the risks.

Applicable to: OIS-09.06B

Options for risk treatment may involve one or more of the following:

1. Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
2. Taking or increasing the risk in order to pursue an opportunity;
3. Removing the risk source;
4. Changing the likelihood;
5. Changing the consequences;
6. Sharing the risk (e.g. through contracts, buying insurance); and
7. Retaining the risk by informed decision.

Applicable to: OIS-09.07B

Risks that the cloud service provider shares with the cloud service customer are described as part of the SSRM (cf. OIS-03).

Supplementary Information - Complementary Customer Criteria

–

OIS-10 Information Security in Project Management

Basic Criteria

OIS-10.01B

Information security is integrated into project management. Risks are assessed by the cloud service provider according to OIS-07, and the risk treatment is performed if necessary. Risks are treated in all projects that may have a direct or significant impact on the provision, operation, or security of the cloud service.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: OIS-10.01B

Risks with a significant impact are those that, if they were to occur, would cause a damage of such a scale as to materially affect the information security of the cloud service, control effectiveness or service commitments of the cloud service provider.

Supplementary Information - Complementary Customer Criteria

–

5.2 Security Policies and Procedures (SP)

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

SP-01 Documentation, Communication and Provision of Policies and Procedures

Basic Criteria

SP-01.01B

Policies and procedures (incl. frameworks and guidelines) are derived from the information security policy and are documented according to a uniform structure. The policies and procedures describe at least the following aspects:

1. Objectives;
2. Scope;
3. Roles and responsibilities, including personnel qualification requirements and the establishment of substitution rules;
4. Roles and dependencies on other organisations (especially cloud service customers and subservice organisations);
5. Steps for the execution of the security strategy; and
6. Applicable legal and regulatory requirements.

SP-01.02B

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

SP-01.03B

The policies and procedures are subject to version control.

SP-01.04B

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

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: SP-01.01B

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

1. Information Security Policy (OIS-02)
2. Risk Management Policy (OIS-07);
3. Remote Working - Policy (HR-07);
4. Asset Management Framework (AM-01);
5. Policy for the Proper and Secure Use of Assets (AM-05);
6. Physical Security and Environmental Control Requirements (PS-01);
7. Physical Site Access Control (PS-04);
8. Workplace Security Requirements (PS-08);
9. Protection Against Malware - Policies and Procedures (OPS-04);
10. Data Backup and Recovery - Policies and Procedures (OPS-06);
11. Logging and Monitoring - Policies and Procedures (OPS-10);
12. Logging and Monitoring - Policies and Procedures for Handling Cloud Service Derived Data and Account Data (OPS-11);
13. Managing Vulnerabilities - Policies and Procedures (OPS-18);
14. Managing Incidents and Crashes - Policies and Procedures (OPS-19);
15. Managing Vulnerabilities - Patch Management Policies and Procedures (OPS-27);
16. Separation of Datasets - Policies and Procedures (OPS-30);
17. Confidential Computing - Policies and Procedures (OPS-32);
18. Container Management - Policies and Procedures (OPS-34);
19. Policy for Identities and Access Rights (IAM-01);
20. Authentication Mechanisms (authentication policy) (IAM-08);
21. Policy for the Use of Cryptographic Mechanisms (CRY-01);
22. Technical Safeguards (COS-01);
23. Policies for Data Transmission (COS-08);
24. Policies for the Development/Procurement of System Components (DEV-01);
25. Policies for Changes to System Components (DEV-03);
26. Secure Use of Third Party Hardware and Software (policies and procedures for the use of third party and open source software) (DEV-14);
27. Policies and Procedures for Controlling and Monitoring Service Organisations (SSO-01);
28. Controlling Exchanges with Suppliers of Functional Components (SSO-08);
29. Policy for Security Incident Management (SIM-01);
30. Business Continuity and Emergency Management System (BCM-01);
31. Policy for Planning and Conducting Audits (COM-02); and
32. Communication of Technical Procedures for Data Disclosure in Investigation Requests (INQ-04).

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:

1. Integration of guidelines and procedures in the onboarding of new personnel;
2. Training and information campaigns when adopting new or revising existing policies and procedures; and
3. Form of provision.

Supplementary Information - Complementary Customer Criteria

–

SP-02 Review and Approval of Policies and Procedures

Basic Criteria

SP-02.01B

Information security policies and procedures are reviewed for adequacy by the cloud service provider's subject matter experts at least annually, and in case of significant changes to the cloud service. The review shall consider at least the following aspects:

1. Organisational and technical changes in the procedures for providing the cloud service; and
2. Legal and regulatory changes in the cloud service provider's environment.

SP-02.02B

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

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: SP-02.01B

During an ISO 27001 certification audit, the controls to this criteria are most likely also tested. If it is a joint audit (C5 and ISO), efficiency of audit-once-certify-many may be gained here. If it is a

separate audit, the auditor of the C5 attestation engagement can choose to inspect the ISO report instead of testing the control again, if the provided evidence is conclusive enough.

Applicable to: SP-02.02B

Significant changes include, but are not limited to, any circumstances or events that materially affect the scope, effectiveness, or objectives of the information security policy. Specifically, significant changes are e.g.:

1. Major technical or architectural changes to the cloud platform (e.g., adoption of new infrastructure services, cloud migration, introduction of a new service offering);
2. Substantial updates to national or international laws, regulations, or sector-specific standards (e.g., NIS2, DORA, GDPR) that impact information security obligations;
3. Reorganisation or merger/acquisition of organisational units that affect leadership, decision-making, or key responsibilities related to security;
4. Significant changes in contractual requirements, risk assessments, operational processes, or threat landscape (e.g., new threat intelligence indicating emerging risks, supply chain incidents);
5. Major security incidents or breaches requiring incident response revision;
6. Launch or decommissioning of service components impacting customer data or trust boundaries; and
7. Changes in the composition or responsibilities of top management or the information security steering committee.

For an efficient review the cloud service provider can document the nature of each significant change, the rationale for review, and the result of policy adjustments. Automated tracking of policy changes and manual verification of content can also be integrated into the review workflow.

The top level management is an appropriate level of management for approving the information security policy.

Supplementary Information - Complementary Customer Criteria

–

SP-03 Exceptions from Existing Policies and Procedures

Basic Criteria

SP-03.01B

All exceptions to policies and procedures for information security are maintained in a list, including also the controls associated with the exceptions.

SP-03.02B

Exceptions to the policies and procedures 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 risk management procedures in accordance with OIS-07, also take into account the aggregated risk from a combination of single exceptions.

SP-03.04B

The approvals of exceptions are documented, with a defined validity and reviewed for appropriateness at least annually by the risk owners or by the top management. This review also takes into account the aggregated risk from a combination of single exceptions.

SP-03.05B

Exceptions in information security policies and procedures that would result in a deviation (cf. 3.4.12) from any applicable C5 criterion within the scope of an assurance engagement (cf. 3.4.1) are not permitted.

Additional (Sharpening)

–

Additional (Complementing)

SP-03.01AC

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

SP-03.02AC

The cloud service provider monitors the list of exceptions to prevent the expiration of approved exceptions and ensure the up-to-dateness of all reviews and approvals.

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

During an ISO 27001 certification audit, the controls to this criteria are most likely also tested. If it is a joint audit (C5 and ISO), efficiency of audit-once-certify-many may be gained here. If it is a separate audit, the auditor of the C5 attestation engagement can choose to inspect the ISO report instead of testing the control again, if the provided evidence is conclusive enough.

Applicable to: SP-03.05B

This criterion addresses policies and procedures and demands that on this level, no codified deviations from applicable C5 criteria are permitted.

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

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

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

Applicable to: SP-03.01AC

Appropriate level of management for approval are in most cases either the level of management that approved the policies or procedures or the level of management to whom this task is delegated.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure with suitable controls that they obtain information from the cloud service provider about exceptions to information security policies and procedures in order to assess and appropriately manage the associated risks to their own information security.

5.3 Personnel (HR)

Objective: Ensure that personnel understands its responsibilities, is aware of its 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 for the production environment 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.

HR-01.02B

The competency and integrity of all internal and external personnel 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:

1. Verification of the person's identity via identity card or passport;
2. Verification of professional experience through the CV;
3. Verification of academic titles and degrees;
4. Request for a certificate of good conduct, police clearance or other national equivalents; and

5. Evaluation of susceptibility to blackmail.

HR-01.03B

The cloud service provider considers changes in personnel roles or employment status that may impact access rights, responsibilities, or risk exposure, and identifies and mitigates related risks.

HR-01.04B

The cloud service provider classifies security-sensitive positions according to their level of risk, including IT administration roles and any positions with access to cloud service customer data or to system components used to provide the cloud service in the production environment.

HR-01.05B

The cloud service provider assesses the competence and integrity of its personnel before transfer or promotion into a role with a higher risk classification.

HR-01.06B

The intensity of the assessment defined in this criterion is in proportion to the business context, the sensitivity of the information that the personnel will access, and the associated risks.

Additional (Sharpening)

–

Additional (Complementing)

HR-01.01AC

The cloud service provider defines in the human resource policy positions with levels and risk classification that require regular assessment of competence and integrity. The cloud service provider annually reviews their assessment of competence and integrity for personnel belonging to the defined positions.

Supplementary Information

About the Criteria

Applicable to: HR-01.01B

This criterion applies to both existing and newly hired personnel. Roles with access to these data types or system components can, depending on their access rights, include, but are not limited to:

1. Cloud software engineers and developers;
2. Cloud architects and cloud infrastructure engineers;
3. Cloud platform engineers and DevOps engineers;
4. System operations engineers and managers;
5. Cloud operations engineers and managers;
6. Cloud network engineers and architecture leads;

7. Cloud security engineers, administrators and security architects;
8. Cloud security operations specialists and analysts;
9. Storage and database engineers;
10. Technical account managers and customer account managers;
11. Customer support engineers;
12. IAM administrators and access management specialists;
13. Cloud compliance managers and risk and compliance analysts; and
14. Information security officers and data protection officers.

Personnel refers to both internal and external personnel.

Applicable to: HR-01.02B

This criterion applies to both existing and newly hired personnel. External personnel in the sense of the criterion is that which performs activities in accordance with the processes and procedures of the cloud service provider and that has potential access to cloud service customer data or cloud service derived data. Personnel of service organisations that performs activities according to the service organisation's own processes and procedures is not covered by this criterion.

Permissible verifications of competency and integrity are governed by applicable local laws and the roles of the personnel. In some jurisdictions, the collection, processing, or disclosure of such information is fundamentally restricted or even prohibited, meaning they may be unable to be obtained at all or only in a very limited form. Where permitted, explicit consent by the personnel may be required depending on the nature and scope of the checks. These legal constraints also apply to any analyses concerning blackmailing.

The verification of qualification and trustworthiness can be supported by specialised service providers or be based on voluntary self-disclosure of the personnel. Depending on national legislation, national equivalents of the German certificate of good conduct ('Führungszeugnis') may also be permitted. Assessing the vulnerability of potential personnel 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.

Applicable to: HR-01.01AC

Cloud service providers can implement various methods to assess competence and integrity of personnel in high risk positions, such as:

1. Self-disclosure of significant financial interests to determine conflicts of interest and susceptibility to blackmail;
2. Regular checking of certificates of good conduct, police clearance or other national equivalents;
3. Regular self-declaration of commitment with applicable policies and obligations;

4. Enforcing regular ethics and compliance trainings, including certification and testing of the personnel's understanding of applicable requirements and policies;
5. Enforcing regular participation in assessment centers to evaluate personnel's competence and integrity; and
6. Regular checks of personnel against national and international sanctions lists.

Supplementary Information - Complementary Customer Criteria

–

HR-02 Employment Terms and Conditions

Basic Criteria

HR-02.01B

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

HR-02.02B

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

HR-02.03B

The cloud service provider ensures that a non-disclosure provision is included in the terms for all internal and external personnel. The non-disclosure provision covers any information, including anonymised and decontextualised information, that the personnel obtains or generates as part of the cloud service.

HR-02.04B

The cloud service provider instructs its personnel on the code of ethics and the information security policy, as well as the policies, procedures and instructions based on it, 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.

HR-02.05B

Additionally, the cloud service provider requires the code of ethics and the information security policy, as well as the policies, procedures and instructions based on it, to be acknowledged by the internal and external personnel in a documented form before access is granted to any of the aforementioned data or system components.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: HR-02.03B

These agreements are prescribed in more detail in HR-06.

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 personnel of the cloud service provider undergoes a role-based training programme regularly and when changing job function, taking into consideration at least the risk classification and technical responsibilities of their position.

HR-03.03B

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

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

HR-03.04B

The learning outcomes achieved through the awareness and training programme are measured and evaluated.

Additional (Sharpening)

HR-03.02AS, sharpening HR-03.02B

All internal and external personnel of the cloud service provider undergoes a role-based training programme at least annually and when changing job function, taking into consideration at least the risk classification and technical responsibilities of their position.

Additional (Complementing)

HR-03.01AC

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

HR-03.02AC

Timely and appropriate remediation measures address any deviations identified during monitoring.

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-03.01B

The target groups may be defined considering job function, job position and the associated risk classification. Target groups serve to simplify and systematise the security training and awareness programme.

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 member of the personnel 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 the personnel's privacy requirements.

Supplementary Information - Complementary Customer Criteria

–

HR-04 Disciplinary Measures

Basic Criteria

HR-04.01B

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

HR-04.02B

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

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

HR-04.03B

The internal and external personnel of the cloud service provider is informed about possible disciplinary measures.

HR-04.04B

The use of disciplinary measures is appropriately documented.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

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 personnel has been informed about which responsibilities, arising from employment terms and conditions relating to information security, will remain in place when the employment is terminated or changed and for how long.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

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 personnel and service organisations 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 service organisations when the contract is agreed.

HR-06.03B

The agreements are to be accepted by internal personnel 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), as well as in case of significant changes to the cloud service. 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 personnel and service organisations and obtains confirmation of the updated confidentiality or non-disclosure agreement.

HR-06.06B

In instances where an agreement on the updates cannot be reached, the cloud service provider assesses 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 (NDA) is a legal document and has content required by both parties to protect confidential information. Processes and procedures around media handling can be managed separately outside of the NDA. An NDA should cover:

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

These agreements are described in general in HR-02.

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 Remote Working - Policy

Basic Criteria

HR-07.01B

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

1. Establishing guidelines for the personnel for the safe handling and storage of sensitive information and data types;
2. Definition of remote access security requirements;
3. Utilisation of secure communication methods and enforcement of secure network use (e.g., VPN usage, endpoint protection, multi-factor authentication, secure communication channels); and
4. Provision of organisation-approved equipment and prohibition of unregulated personal devices.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: HR-07.01B

Please note that this criterion refers to off-site working places whereas PS-08.01B addresses security requirements for on-site office workplaces.

The guidelines for the personnel for safe handling and storage of sensitive information and data types refer to organisational measures the personnel is obligated to follow. Remote access security requirements refer to technical measures like e.g. MFA and VPN and also rules for the particular work place that follow from general considerations about working e.g. in public places where the screen can be spied on.

Supplementary Information - Complementary Customer Criteria

–

HR-08 Remote Working - Implementation

Basic Criteria

HR-08.01B

The cloud service provider designs, implements and maintains the technical and organisational measures required to enable its personnel to comply with the policies and procedures for remote work (cf. HR-07).

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: HR-08.01B

Please note that this criterion refers to off-site working places whereas PS-08.01B addresses security requirements for on-site office workplaces.

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 Framework

Basic Criteria

AM-01.01B

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

1. Identification of assets which are used to provide the cloud service in the production environment;
2. Definition of a scheme for identifying protection needs based on information processed, stored or transmitted on the asset;
3. Definition of asset types, considering at a minimum the differentiation of hardware and software objects;
4. Definition of asset lifecycles based on the asset type; and
5. 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:

1. Identify the impact on cloud services and functions in case of events that could lead to a breach of protection objectives; and
2. Support information provided to affected cloud service customers in accordance with contractual agreements.

AM-01.02AC

The cloud service provider assures that the inventory of assets is up-to-date by implementing monitoring measures to the process that is maintaining it.

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 include, but are not limited to:

1. Physical and virtual infrastructure resources (e.g. servers, storage systems, network components); and
2. 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 include, but are not limited to, hypervisors, containers, operating systems, databases, microservices and application programming interfaces (APIs).

The lifecycle of an asset includes, depending on the asset type:

1. Acquisition;
2. Commissioning;
3. Maintenance;
4. Decommissioning; and
5. 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 framework (cf. AM-01).

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 of an asset are logged.

AM-02.05B

The cloud service provider maintains lists of all users under its responsibility 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 service organisation (e.g. virtual machines or containers) may use tools provided by the service organisation to inventory those assets, insofar as the cloud service provider deems these suitable based on their asset management framework.

In practice, the implementation of the asset inventory can vary greatly depending on the number, size and complexity of provided cloud services.

Applicable to: AM-02.05B

These lists can be, but do not have to be, provided by the inventory system established through the criteria AM-02, AM-03 and AM-04.

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 (cf. AM-02) includes information for each entry that:

1. Enables the identification of the hardware asset;
2. Provides visibility into the lifecycle of the hardware asset; and
3. Enables the cloud service provider to control the hardware asset, perform a risk assessment and protect its information security.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: AM-03.01B

This basic criterion can, but does not have to, be fulfilled by including the following details for each entry of the hardware asset inventory:

1. Identification details (such as name, IP address, MAC address, etc.);
2. The function of the asset;
3. The model of the asset;
4. The location of the asset;
5. The owner of the asset; and
6. Information security requirements for the asset.

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 inventories the containers and document their life cycle (cf. OPS-34).

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 (cf. AM-02). This inventory includes information for each entry that:

1. Enables the identification of the software asset;
2. Provides visibility into which other assets use the software asset for the provision of the cloud service; and
3. Enables the cloud service provider to control the software asset, perform a risk assessment and protect its information security.

Additional (Sharpening)

–

Additional (Complementing)

AM-04.01AC

The inventory also includes information for each entry that provides visibility into how long the software asset will receive security updates from its supplier, if such a time frame has been communicated by the supplier.

Supplementary Information

About the Criteria

Applicable to: AM-04.01B

This basic criterion can, but does not have to, be fulfilled by including the following details for each entry of the software asset inventory:

1. Identification details (such as name, IP address, MAC address, etc.);
2. The version of the software; and
3. The parent resource (hardware asset or software asset) on which the software is installed.

Applicable to: AM-04.01AC

This additional criterion can, but does not have to, be fulfilled by including license information, including communicated end-of-support dates related to the licensed software, for each entry of the software asset inventory.

Supplementary Information - Complementary Customer Criteria

–

AM-05 Policy for the Proper and Secure Use of Assets

Basic Criteria

AM-05.01B

Policies and procedures 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:

1. Approval procedures for acquisition, commissioning, maintenance, decommissioning, and disposal by authorised personnel or system components;
2. Classification and labelling based on the protection need 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;
3. Secure configuration of mechanisms for error handling, logging, encryption, authentication and authorisation;
4. Requirements for versions of software and images as well as application of patches;
5. Handling of software for which support and security patches are not available anymore;
6. Restriction of software installations or use of services;
7. Protection against malware;
8. Remote deactivation, deletion or blocking;
9. Physical delivery and transport;
10. Dealing with incidents and vulnerabilities;
11. Deletion of cloud service customer data, cloud service derived data, cloud service provider data and account data; and
12. 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 framework (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, logging, 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 either:

1. The complete and permanent deletion of all cloud service customer data, cloud service derived data, cloud service provider data and account data; or
2. The proper destruction of the media.

Account data needs to be deleted at least in cases where the data is located in the production environment for the operation of system components.

Additional (Sharpening)

AM-07.01AS, sharpening 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, development, test or staging 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.

Additional (Complementing)

AM-07.01AC

The destruction of data on hardware components is carried out in such a manner that data recovery can be reasonably considered to be impossible.

Supplementary Information

About the Criteria

Applicable to: AM-07.01B

The decommissioning procedure typically includes:

1. Verification that the asset is no longer required for operational use;
2. Assessment of associated risks and dependencies;
3. Approval by authorised personnel based on internal policies;

4. Execution of secure data deletion or sanitization processes;
5. Updating the asset inventory to reflect decommissioning status; and
6. Disposal or repurposing of the hardware in accordance with environmental and security guidelines.

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

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.

Applicable to: AM-07.01AC

This approval process ensures that disposal activities conducted offsite adhere to the organisation's security, compliance, and environmental policies. It typically includes:

1. Verification of asset ownership and usage history;
2. Assessment of data sanitisation requirements;
3. Selection of approved disposal vendors or methods;
4. Documentation of disposal actions and approvals; and
5. Confirmation of secure data deletion or destruction.

Applicable to: AM-07.01B, AM-07.02B, AM-07.01AS, AM-07.01AC

This criterion is not applicable for hardware components that do not store cloud service customer data, cloud service derived data, cloud service provider data or account data (e.g. monitors, routers or keyboards).

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 personnel is provably committed to the policies and procedures 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.

AM-08.03B

If assets cannot be returned prior to or on the day of the termination, the cloud service provider removes the access rights of the personnel no later than the date of termination

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: AM-08.01B, AM-08.02B, AM-08.03B

The criterion essentially concerns mobile devices (e.g. notebooks, tablets, smartphones, FIDO2 security keys, 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).

Applicable to: AM-08.03B

The removal of access rights of terminated personnel can be implemented by e.g. disabling their identity on the device.

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 in case of significant changes to the cloud service. Based on the review, the classification levels are updated where appropriate.

AM-09.03B

The protection need 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

The unique identification of physical 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 protection need.

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 categorise the assets specifically, then all assets may be treated as requiring the highest level of protection needs.

Applicable to: AM-09.02B

If a review is caused by significant changes to the cloud service, only the classification levels affected by the changes need to be included in the review.

Applicable to: AM-09.01AC

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

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

Applicable to: AM-09.02AC

Integrating device identification ensures that each asset is uniquely recognised and appropriately classified based on its protection needs. This is particularly important for mobile and endpoint devices, which may carry sensitive data or serve as access points to cloud services. Proper labeling supports traceability, risk assessment, and enforcement of security controls throughout the asset lifecycle.

Supplementary Information - Complementary Customer Criteria

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

Cloud service customers ensure with 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

Based on a risk assessment (cf. OIS-07), the cloud service provider has documented and implemented a procedure for protecting hardware components of the cloud service's production environment that are temporarily not in use. The procedure supports the secure storage and protection against unauthorised access or damage of inactive hardware until it is needed again.

Additional (Sharpening)

AM-10.01AS, sharpening AM-10.

Based on a risk assessment (cf. OIS-07), the cloud service provider has documented and implemented a procedure for protecting any hardware components that are temporarily not in use. The procedure supports the secure storage and protection against unauthorised access or damage of inactive hardware until it is needed again.

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

AM-11 Transfer of Hardware

Basic Criteria

AM-11.01B

Based on a risk assessment (cf. OIS-07), the cloud service provider ensures the secure and controlled transfer of hardware objects 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 cloud service provider ensures that all transfers of hardware objects used in the cloud service production environment are conducted using secure, documented methods designed to prevent unauthorised access, tampering, data leakage, or loss during transit. These methods include physical protection, chain-of-custody tracking, and verification upon receipt.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: AM-11.02B

Authorisation ensures that hardware object transfers, whether internal or external, are controlled, traceable, and compliant with organisational policies. This is particularly important for assets containing sensitive data or used in production environments. The process typically includes:

1. Verification of asset ownership and classification;
2. Assessment of associated risks;
3. Documentation of the transfer request and approval; and
4. Confirmation of secure handling during transit.

Supplementary Information - Complementary Customer Criteria

–

AM-12 Removable Media and Endpoint Devices

Basic Criteria

AM-12.01B

Based on a risk assessment (cf. OIS-07), the cloud service provider designs, implements and maintains controls for endpoint devices and removable storage media regarding the following aspects:

1. Except for system administrative tasks for which no other method is available, the use of removable media is forbidden;
2. Removable media is used for dedicated, specific purposes only;
3. Storage encryption is enabled on managed endpoints and removable storage media (except those used for unavoidable system administration actions) to protect information from unauthorised disclosure;
4. Managed endpoints are configured with anti-malware detection and prevention technology and services;
5. Self-execution from removable storage is disabled and storage media is scanned before use on the cloud service provider's systems;
6. Measures are to be taken by users to protect mobile endpoints and removable storage in transit and in storage;
7. Protection in terms of confidentiality and integrity of any equipment containing cloud service customer data during the transfer off-site for disposal is equivalent to that on the site;
8. Cloud service customer data and cloud service derived data stored on shareable equipment is encrypted in accordance with CRY-05 or destroyed using a secure deletion mechanism before the equipment is shared with a third party;
9. Users are to use mobile endpoints and removable storage in a secure manner, this includes for example not leaving media openly accessible in public spaces, using screen locks and screen privacy films; and
10. 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 procedures for endpoint devices and removable storage media furthermore contain the following aspects:

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

Supplementary Information

About the Criteria

Applicable to: AM-12.01B, AM-12.01AC

A removable medium is a portable data storage medium that can be added to or removed from a computing device or network. Examples include, but are not limited to, optical discs (e.g., CD, DVD, Blu-ray), external or removable hard drives or solid state disk drives, magnetic or optical tapes and flash memory devices (e.g., USB, eSATA, flash drive, thumb drive).

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 and one public area. A sensitive area covers the buildings and premises in which sensitive activities take place, such as hosting the system components used for providing the cloud service. A public area covers all buildings and premises not otherwise covered by a security area.

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, protection needs identified for the cloud service and a risk assessment regarding physical and environmental security. The security requirements are documented, communicated and provided in a policy or framework 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:

1. Faults in planning;
2. Unauthorised access (including access to the premises by drones);
3. Insufficient surveillance;
4. Lightning and overvoltage (aligned with the internationally harmonised standards of IEC 62305);
5. Fire and smoke;
6. Unwanted water;
7. Failures and/or unavailable telecommunications;

8. Power failure; and
9. Insufficient 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:

1. The complementary subservice organisation controls (CSOC) expected at the service organisations; and
2. 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

If the cloud service provider operates the cloud service in data centres operated by service organisations, the cloud service provider performs a verification of the implementation of suitable CSOC in accordance with the criteria for controlling and monitoring service organisations (cf. SSO-05).

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 security requirements include time limits in order to provide self-sufficient operation of a location for at least 72 hours in the event of a failure of the external power supply, or until all services are transferred to another location.

PS-01.03AC

The security requirements for a self-sufficient operation during a heat period are based on the highest outside temperatures that can reasonably be estimated to occur at the locations of the premises and buildings within the lifespan of the cooling supply system. The cloud service provider determines these temparatures with an appropriate safety margin.

PS-01.04AC

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

PS-01.05AC

The security requirements take into account that if water is taken from a body of water (e.g., river or lake) 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

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 time frame 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).

Applicable to: PS-01.03AC

A reasonable estimation of the highest outside temperatures can be based on information supplied by official measurement station such as Deutscher Wetterdienst (DWD) or other reliable resources, such as e.g. American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE).

These estimations should take the effects of global warming into account.

What constitutes an appropriate safety margin depends on the location of the premises and buildings. In Germany, 3 Kelvin can generally be considered appropriate.

Supplementary Information - Complementary Customer Criteria

–

PS-02 Redundancy Model

Basic Criteria

PS-02.01B

The cloud service is provided from at least two locations. 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 and resilience.

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 effectiveness 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. The locations meet the security requirements of the cloud service provider (cf. PS-01) and are located sufficiently far apart to achieve georedundancy and resilience. 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 3.4.12) 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' (German for: 'Criteria for selecting the location of data centres', document only available in German) provides recommendations in this regard.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure with 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 so that their combined resistance time withstand a break-in attempt for at least ten minutes in total. This time period applies from the moment an external intruder is detected (e.g. by perimeter surveillance).

PS-03.04B

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

PS-03.05B

If the construction elements as a whole do not fully meet the associated requirements, compensating controls are implemented to restore the appropriate security level.

PS-03.06B

Data centre personnel are trained on how to respond effectively to 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 anti-burglary 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. However, fulfilling the objective of this criteria does not necessarily imply that those standards have to be fulfilled.

Additionally, the subcriterion demands that all construction elements as a whole lead to a resistance time to break-in attempts for at least ten minutes. Consequently, it does not necessarly demand that all individual construction elements have to fulfil this requirement on their own, provided the combined measures effectively delay an external attack for the required time.

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 framework in accordance with SP-01 and include the following aspects:

1. Specified procedure for the granting and modifying of user accounts and access rights (cf. IAM-02) based on the 'least-privilege-principle' and the 'need-to-know-principle';
2. Revocation of access authorisations if they have not been used for a period of two months. Exceptions are only made for well-founded individual cases and follow a defined exception process according to SP-03;
3. Authentication with at least one factor for access to any non-public area;
4. Multi-factor authentication for access to areas hosting system components that process cloud service customer data;
5. 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;
6. Physical access control exceptions applicable in case of emergency, including an analysis procedure following every use of these exceptions; and
7. For visitors and external personnel, measures that ensure identification and tracking of every individual such that their activities are traceable and - in case of activities that infringe information security - stoppable in an appropriate reaction time. These measures are appropriate and proportional to the sensitivity of the zone the visitors or external personnel are in. The appropriate reaction time frame is determined based on a risk assessment (cf. OIS-07).

PS-04.02B

The cloud service provider displays a warning at the entrance of each applicable non-public area regarding its limits and access conditions.

PS-04.03B

Physical access control to the site is managed by an electronic access control system that supports authentication, authorisation, and logging of entry and exit events.

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 framework can be deployed with each on-premises area having separate access permissions. If a zoning framework is implemented, each on-premises area should be physically separated with its own access control system. Examples for zoning on-premises can be:

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

Examples for reasonable exceptions to the revocation of access authorisations after two months of inactivity are e.g. cases where personnel with specific roles, such as management positions or supervisors, requires only occasional but crucial entry. The rationale for the exceptions should be documented and during the review critically assessed if they are still necessary.

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:

1. 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. If compensating measures are taken into account, the fire resistance of structural parts has to be at least 60 minutes;
2. Effective implementation of measures to protect against lightning and overvoltage damage; and
3. Effective implementation of measures to protect against flooding, unless critical facilities are located significantly above the highest flood level at the location of the cloud data centre. Additionally, appropriate measures to mitigate the effects of heavy rain are implemented, unless critical facilities are located significantly above the backwater level at the location of the cloud data centre.

PS-05.03B

Technical Measures include the following aspects:

1. 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;
2. Extinguishing system or oxygen reduction; and
3. Fire alarm system with reporting to the local fire department.

PS-05.04B

Organisational Measures include the following aspects:

1. Regular fire protection inspections to check compliance with fire protection requirements; and
2. 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:

1. Partitioning and layout of fire sections;
2. Extinguishing systems within the fire sections;
3. Early and very early fire detection mechanisms;
4. Redundancy of systems and supply facilities within the premise; and
5. Period of time the locations and premises can withstand a fire impairing a data hall without a second data hall catching fire.

The cloud service provider should describe the measures taken to protect its premises and buildings against fire as part of the system description.

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 containing 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:

1. Operational redundancy (N+1) in power and cooling supply;
2. Use of appropriately sized uninterruptible power supplies (UPSes) and emergency power supplies (EPSes), designed to ensure that all data remains undamaged in the event of a power failure. The functionality of UPSes and EPSes is checked at least annually by suitable tests and exercises (cf. BCM-04);
3. Maintenance (servicing, inspection, repair) of the utilities in accordance with the manufacturer's recommendations; and
4. Protection of power supply and telecommunications lines against interruption, interference, damage and eavesdropping.

PS-06.02B

Uninterruptible Power Supplies (UPSes) and Emergency Power Supplies (EPSes) are implemented to comply with the availability requirements defined in the Service Level Agreement.

PS-06.03B

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:

1. Traces of violent attempts to open closed distributors;
2. Up-to-dateness of the documentation within the distributor;
3. Conformity of the actual wiring and patching with the documentation;
4. The short-circuits and earthing of unneeded cables and wires are intact; and
5. Impermissible installations and modifications.

Additional (Sharpening)

–

Additional (Complementing)

PS-06.01AC

The cooling supply system 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 that can reasonably be estimated to occur at the locations of the premises and buildings within the lifespan of the cooling supply system, with an appropriate safety margin.

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

The cloud service provider implements measures to ensure the compatibility of the conditions for installation, maintenance and servicing of the related technical equipment (e.g., electrical power, air conditioning, fire protection) with the cloud service's availability and security requirements.

PS-06.04AC

The cloud service provider ensures that maintenance agreements for equipment used for the hosting of the cloud service enable the timely installation of security updates 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.

Applicable to: PS-06.03B

The subcriterion requires the check to be performed at least every two years. If no check was performed during the specified period of a Type 2 engagement, the auditor shall note in the test result that there was 'no occurrence' provided that the previous check was performed within the two years required by the criterion. For the evaluation of the design of the control, the auditor may obtain evidence regarding the previous check, even if this check did not occur within the specified period of the engagement. If there was no check performed for two years, the auditor shall note a deviation.

Applicable to: PS-06.01AC

This subcriterion demands the implementation of concrete measures to fulfil the policy required by PS-01.03AC. The cloud service provider also determines the highest outside temperatures that can reasonably be estimated to occur at the locations of the premises and buildings within the lifespan of the cooling supply system as part of PS-01.03AC.

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 timely initiate the necessary measures for return to the control range.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: PS-07.01B

These measures typically include but are not limited to:

1. Environmental monitoring systems (e.g., temperature and humidity sensors);
2. Fire suppression systems;
3. Climate control (HVAC) systems; and
4. Leak detection and alarms.

Supplementary Information - Complementary Customer Criteria

–

PS-08 Workplace Security Requirements

Basic Criteria

PS-08.01B

Based on a risk assessment according to OIS-07, security requirements for office environments are documented, communicated and provided in accordance with SP-01. The security requirements for rented offices take into account proportionality and appropriateness, potentially being less extensive than those in own office environments. These security requirements encompass various aspects for a safe and secure working environment, including at least:

1. Physical access controls, such as key cards and biometric scanners, for office buildings;
2. Use of screen locks and privacy screens for workstations;
3. No openly visible confidential data at temporarily unattended workstations;
4. Disposal of all company documents that are no longer required within the company premise;
5. Prohibition of the use of third party equipment; and
6. Securing the entrances of office premises with alarm systems and surveillance cameras.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: PS-08.01B

As a result of the risk assessment in accordance with OIS-07, not every aspect listed in the criterion may need to be addressed by corresponding security requirements. For example, if there are no assets related to the development or operation of the cloud service in an office building, alarm systems and surveillance cameras may not be required.

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 system components) follows an established procedure in order to avoid possible capacity restrictions.

OPS-01.02B

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

OPS-01.03B

The cloud service provider takes 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 restrictions or outages regarding personnel and system components. 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 system components (CPU, RAM, storage space, network). In multi-tenant environments, existing resources should still be shared between cloud service customers (clients) in such a way that service level agreements are adhered to. In this respect, proper planning and monitoring of system components 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 restrictions 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 with 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

Procedures and technical safeguards for the monitoring, 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 restrictions that result in breaches of contractual obligations are to be reported to cloud service customers in accordance with 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:

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

Applicable to: OPS-02.02B

Cloud service providers may provide a health dashboard to the cloud service customer. This subcriterion can be fulfilled by the provision of such a health dashboard if the health dashboard informs the cloud service customer about breaches of contractual obligations, such as SLAs.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure with 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 system components assigned to the customer for administration/use in order to avoid overcrowding of resources and to achieve sufficient performance.

OPS-03.02B

If there are significant security changes, or planned significant security changes, in the system components provided as part of the cloud service and allocated by the cloud service customer, the cloud service provider informs the cloud service customer about them.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: OPS-03.01B

System components to be allocated and managed by the cloud service customer can include, according to the possibilities of the service model:

1. Computing capacity;
2. Storage capacity;
3. Configuration of network properties;
4. Application Programming Interfaces (APIs); and
5. Databases.

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

Applicable to: OPS-03.02B

Significant security changes in this context can include the change of the security feature itself, such as when changing the service architecture. Non-significant changes can include the change of the implementation of a security feature in a way that does not alter its functionality or reduce its security level, such as when replacing a used cryptographic primitive with another, equivalent one.

Supplementary Information - Complementary Customer Criteria

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

OPS-04 Protection Against Malware - Policies and Procedures

Basic Criteria

OPS-04.01B

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

1. Use of system-specific protection mechanisms;
2. Operating protection programmes on system components under the responsibility of the cloud service provider;
3. Operation of protection programmes for personnel's terminal equipment; and
4. Operation of protection programmes on flows coming in over cloud service provider end-devices, as well as all other incoming flows.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: OPS-04.01B

Protection programmes for personnel 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 procedures.

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 they are available, at least on a daily basis.

OPS-05.03B

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

Additional (Sharpening)

OPS-05.02AS, 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 they are available, at the highest frequency that the vendor(s) offer(s) where applicable.

Additional (Complementing)

OPS-05.01AC

Policies and procedures 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-05.02AC

The configuration of the protection mechanisms is monitored automatically.

OPS-05.03AC

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-05.02AS

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 service 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.

Applicable to: OPS-05.01B

For end-devices used by the personnel of the cloud service provider, the applicability of this subcriterion is determined based on the risk assessment performed according to AM-08.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure with 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 - Policies and Procedures

Basic Criteria

OPS-06.01B

Policies and procedures for regular backup or replication and regular 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:

1. 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);
2. Data is backed up in encrypted, state of the art form;
3. Secure storage, transfer, management and disposal of backup data;
4. Access to the backed-up data and the execution of restores is performed only by authorised persons;

5. Tests of data restore procedures by the cloud service provider (cf. OPS-08); and
6. If part of the contractual agreement: Execution of actual data restore requests or restore tests initiated by the cloud service customer.

The policies and procedures include conditions for those parts of cloud service provider data that do not require a backup. For those parts of cloud service provider data, this subcriterion is not applicable.

Additional (Sharpening)

OPS-06.01AS, sharpening OPS-06.01B

Policies and procedures for at least daily backup or replication and at least daily 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:

1. 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);
2. Data is backed up in encrypted, state of the art form;
3. Secure storage, transfer, management and disposal of backup data;
4. Access to the backed-up data and the execution of restores is performed only by authorised persons;
5. Tests of data restore procedures by the cloud service provider (cf. OPS-08); and
6. If part of the contractual agreement: Execution of actual data restore requests or restore tests initiated by the cloud service customer.

The policies and procedures include conditions for those parts of cloud service provider data that do not require a backup. For those parts of cloud service provider data, this subcriterion is not applicable.

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: OPS-06.01B, OPS-06.01AS

Particularly within IaaS and PaaS service models, responsibility for backup and recovery of cloud service customer data often remains with the customer and is therefore not part of the contractual agreements between cloud service provider and cloud service customer.

If the data backup of cloud service customer data is not part of the contract, 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 policies and procedures specifiy which type of data backup is to be carried out (e.g. scope, frequency and duration) and specify 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 are 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.

Applicable to: OPS-06.01B

Parts of cloud service provider data that do not require a backup include, but are not limited to, parts of cloud service provider data than can be built from scratch without a backup.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure with 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 procedures for data backup and recovery (cf. OPS-06).

OPS-07.02B

Incidents are investigated by qualified personnel and rectified timely 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 with 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 provider data and, if contractually agreed upon, cloud service customer data and cloud service derived data.

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

Performed restore tests are thoroughly documented. This also includes the documentation of the safe disposal of the restored data.

OPS-08.05B

Deviations from the specifications are reported to the responsible personnel or system components

so that these can timely assess the deviations and initiate the necessary actions.

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 restore tests.

OPS-08.02AC

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

Supplementary Information

About the Criteria

Applicable to: OPS-08.01B, OPS-08.02B, OPS-08.03B, OPS-08.04B, OPS-08.05B, OPS-08.01AC, OPS-08.02AC

If the data backup has not been contractually agreed between the cloud service provider and the cloud service customer, this criterion is not applicable. The cloud service provider transparently presents this situation in the system description.

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 with suitable controls that they actively request information on the results of restore 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 protection needs resulting from the data classification of the original data (e.g., encryption, access control) are also 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 (cf. CRY-04).

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 equivalent to those at the main site.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: OPS-09.01B, OPS-09.02B, OPS-09.03B, OPS-09.04B, OPS-09.05B

If the data backup has not been contractually agreed between the cloud service provider and the cloud service customer, this criterion is not applicable. The cloud service provider transparently presents this situation in the system description.

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 - Policies and Procedures

Basic Criteria

OPS-10.01B

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

1. Definition of events that could lead to a violation of the protection goals;
2. Specifications for activating, stopping and pausing the various logs;
3. Information regarding the purpose and retention period of the logs;
4. Definition of roles, responsibilities and authorities for setting up and monitoring logging;
5. Definition of log data allowed for transfer to cloud service customers and technical requirements of such a transfer;
6. Information regarding timestamps used in event creation;
7. Time synchronisation of system components with at least one approved time source that the cloud service provider considers to be reliable based on defined criteria. If several time sources are used, they are consistent with each other. The time sources can also be synchronised to several external reliable sources, except when used for isolated networks; and
8. 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 with 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 - Policies and Procedures for Handling Cloud Service Derived Data and Account Data

Basic Criteria

OPS-11.01B

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

1. 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;
2. No commercial use beyond the aforementioned purpose to administer and operate the cloud service;
3. Storage for a fixed period reasonably related to the purposes of the collection;
4. The confidentiality and integrity of the logs is protected through appropriate security controls;
5. 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;
6. 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
7. Provision to cloud service customers according to contractual agreements.

OPS-11.02B

The cloud service provider specifies in the contractual agreements with cloud service customers all purposes for which cloud service derived data are collected and used, except for those purposes that are inherent to the general operation of 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, particularly log data, is included in regulatory compliance assessments.

Supplementary Information

About the Criteria

Applicable to: OPS-11.01B

The collection and use of cloud service derived data and account data for the administration and operation of the cloud service also includes the analysis of the aforementioned data to the purpose of improving the provided cloud service, unless this improvement only serves the economic interests of the cloud service provider. If the cloud service provider acts as a cloud service broker, the policies and procedures should give special consideration to the complexities of handling cloud service derived data and account data as part of this role.

Applicable to: OPS-11.02B

Purposes that are inherent to the general operation of many cloud services are:

1. Capacity planning and resource management;
2. Security monitoring and incident response;
3. Compliance with regulatory requirements; and
4. Service performance and reliability.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure with 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, Retention 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 (cf. OPS-10, OPS-11) are implemented by technically supported procedures with regard to the following restrictions:

1. Access only for authorised users and systems;
2. Retention for the specified period; and
3. 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 Logging and Monitoring - 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 is deployed within the cloud environment or externally and includes the following capabilities:

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

Additional (Sharpening)

–

Additional (Complementing)

OPS-13.01AC

The cloud service provider validates the correct operation of event detection processes on appropriate assets. The appropriateness of the assets is identified in accordance with the asset classification schema (cf. AM-09).

OPS-13.02AC

Timely and appropriate remediation measures address any deviations identified during validation.

OPS-13.03AC

If an event that can lead to security incidents is identified, incident handling activities by the cloud service provider are triggered without undue delay.

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

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

Basic Criteria

OPS-14.01B

The cloud service provider retains the generated log data, including SIEM 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)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure with suitable controls that they determine whether they require access to the customer-specific portion of the cloud service derived data that consists of log data, and if so, actively request it.

OPS-15 Logging and Monitoring - Accountability

Basic Criteria

OPS-15.01B

The log data generated - compromising both cloud service derived data and cloud service provider data - enables unambiguous identification of user access at the tenant level, supporting effective forensic analysis in the event of a security incident.

OPS-15.02B

Each logged event includes 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 hardware objects 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

The aforementioned logs are collected and maintained using controls and processes that preserve their integrity and reliability for security monitoring and incident investigation purposes. This implies, but is not limited to:

1. Records are complete and have not been tampered with in any way;
2. Logging systems are clock synchronised, logs include accurate timestamps;
3. Copies of electronic evidence are provably identical to the originals; and
4. 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-15.01AC

The additional criterion also refers to logs of system components under the 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-03). For logging of system components under the responsibility of the cloud service provider cf. PSS-04.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure with 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 timely 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 cloud service provider provides resilience for the logs and the associated infrastructure by defining, documenting and implementing measures to protect their integrity, availability and confidentiality.

OPS-17.02AC

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

Supplementary Information

About the Criteria

Applicable to: OPS-17.02AC

Individual components that might restrict the overall functionality are single points of failure. Such restrictions can be avoided by identifying potential single points of failure and adressing them through redundancy or the design and implementation of a resilient architecture.

Supplementary Information - Complementary Customer Criteria

–

OPS-18 Managing Vulnerabilities - Policies and Procedures

Basic Criteria

OPS-18.01B

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

1. Regular (proactive) identification of vulnerabilities through suitable measures, including vulnerability scans and penetration tests, considering typical vulnerability classes and Common Weaknesses (CWEs);
2. Assessing the severity of identified vulnerabilities using the Common Vulnerability Scoring System (CVSS);

3. Prioritising and implementing measures considering existing standards for timely remediation and/or mitigation of identified vulnerabilities based on severity according to defined time frames and with reference to commonly used scoring systems like the Exploit Prediction Scoring System (EPSS) and the Stakeholder-Specific Vulnerability Categorisation (SSVC);
4. Deployment of Security Patches;
5. Handling system components for which no measures for timely remediation or mitigation of vulnerabilities are initiated based on a risk assessment;
6. Interfaces to incident management in case vulnerabilites become incidents;
7. 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
8. 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 policies and procedures for the timely identification and addressing of vulnerabilities define that for vulnerabilities assessed to be 'critical', engagement has to begin in a timely manner after identification, even if this occurs outside regular working hours. They also define how such a vulnerability is engaged with.

OPS-18.03B

The policies and procedures for the timely identification and addressing of vulnerabilities also define that for vulnerabilities assessed to be 'high', engagement has to begin within one working day after their identification. They also define how such a vulnerability is engaged with.

OPS-18.04B

The engagement with a vulnerability according to the policies and procedures for the timely identification and addressing of vulnerabilities includes regular follow-up of the vulnerability until its remediation.

OPS-18.05B

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 reviewed regularly and in case of significant changes to the cloud service.

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:

1. Low: 0.1 - 3.9;
2. Medium: 4.0 - 6.9;
3. High: 7.0 - 8.9; and
4. 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, but are not limited to:

1. Software Bill of Materials (SBOM),
2. Common Vulnerabilities and Exposures (CVE) or European Vulnerability Database (EUVD),
3. Vulnerability, Exploitability eXchange (VEX); and
4. 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 with 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 - Policies and Procedures

Basic Criteria

OPS-19.01B

Policies and procedures with technical and organisational measures are documented, communicated, and provided in accordance with SP-01 to govern 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 policies and procedures include specifications regarding the following aspects:

1. Classification and prioritisation of incidents and crashes;
2. Standardised incident-handling procedures for addressing known issues;
3. Escalation rules and procedures, including criteria for triggering Security Incident Management (SIM) processes in accordance with SIM-02 or internal incident management procedures;
4. Knowledge sources for incidents and crashes;
5. Criteria for determining when crashes are classified as incidents and when they trigger incident management processes;
6. Mechanisms ensuring that access to crash files is restricted to authorised personnel only;
7. Safeguards to prevent exposure of sensitive, personal, or confidential data within crash files;
8. Encryption of crash files for storage and during transmission;
9. Access management, logging, and review processes for access logs of crash files; and
10. 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 an incident that leads to a sudden and complete failure of a system or system component. It can be indicative of a larger problem, such as an attempted DDoS attack or an unmitigated vulnerability.

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).

Criteria for determining when an incident or crash triggering Security Incident Management (SIM) processes can include, but are not limited to, the incident or crash resulting in one or more of the following:

1. Failure to uphold internal security policies, contractual agreements or relevant legal and regulatory requirements;
2. Unauthorised access to cloud service customer data or system components used to provide the cloud service in the production environment;
3. Loss or exfiltration of cloud service customer data;
4. Unauthorised changes to system components used to provide the cloud service in the production environment; and
5. Failure to uphold the availability requirements contained in the service level agreement.

Supplementary Information - Complementary Customer Criteria

–

OPS-20 Managing Incidents - Implementation

Basic Criteria

OPS-20.01B

The cloud service provider identifies, records, classifies, prioritises, and addresses incidents according to the policies and procedures for the identification and management of incidents and crashes (cf. OPS-19).

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 procedures for the identification and management of incidents and crashes (cf. OPS-19).

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

OPS-22 Managing Vulnerabilities, Incidents and Crashes - 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 in accordance with the policies for managing vulnerabilities (cf. OPS-18).

OPS-22.02B

Penetration tests are carried out in accordance with a documented framework for penetration tests that outlines the number and types of penetration tests to be performed and the requirements for the qualification and competence of the personnel to perform such tests. The number and types of penetration tests to be performed are determined based on a risk assessment (cf. OIS-07).

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-year test plans, each relevant system component is 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 assessment.

OPS-22.07B

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

OPS-22.08B

The vulnerabilities discovered through penetration testing are subject to a root cause analysis. The root cause analysis enables an assessment of the extent to which similar vulnerabilities may be

present in the cloud service.

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 in accordance with the policies for managing vulnerabilities (cf. OPS-18). 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 framework for penetration tests that outlines the number and types of penetration tests to be performed and the requirements for the qualification and competence of the personnel to perform such tests. The number and types of penetration tests to be performed are determined based on a risk assessment (cf. OIS-07).

OPS-22.03AS, sharpening OPS-22.03B

Penetration tests target 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 incorporating, where applicable, threat modelling.

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 designs a multi-year test plan for its penetration testing activities.

OPS-22.03AC

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

OPS-22.04AC

The cloud service provider uses the threat modelling process to prioritise system components with the highest risk exposure for penetration testing by systematically analysing cloud components, services, data flows, trust boundaries and assets critical to the cloud service to enumerate potential threats, vulnerabilities, and attack vectors.

OPS-22.05AC

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.

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-22.01AS, OPS-22.02AS, OPS-22.03AS, OPS-22.01AC, OPS-22.02AC, OPS-22.03AC, OPS-22.04AC, OPS-22.05AC

See section '1.2 Definitions' for the terms 'penetration test' and 'significant change'.

In contrast to vulnerability scans, which analyse code, penetration tests as referred to in this criterion mainly aim at probing the live system to uncover real-world vulnerabilities or weaknesses that only show up in the actual operation of the cloud service, thus creating the connection to criterion OPS-18.

There are three types of penetration tests:

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

It can further be distinguished between

1. 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
2. Post-launch penetration testing: Testing carried out during the regular operations of the cloud service.

Significant changes may include, but are not limited to, the following events:

1. Replacing core cloud infrastructure technologies or performing major version upgrades;
2. Moving between service organisations, such as switching to a new IaaS or data centre provider;
3. Material changes in the way cloud service customer data is processed and stored, such as new backup technologies or new regions from which the service is operated;
4. Replacing or performing major upgrades on security technologies such as authentication workflows, network security mechanisms or monitoring mechanisms; and
5. Material changes to the cloud service model or of functionality made available to the cloud service customer.

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-22.02B, OPS-22.02AS

How many penetration tests should be performed within a year depends on factors such as the size and complexity of the provided cloud service. If penetration tests follow multi-year test plans, these should be considered when determining the number and types of penetration tests to be performed within a year.

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

The risk assessment should be used to identify the system components that are most critical for the provision of the cloud service or most relevant for penetration testing.

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.

Applicable to: OPS-22.04AC

This subcriterion is only applicable if subcriterion OPS-22.03AS is applied as well.

The risk-based scoping ensures that penetration tests focus on the areas most susceptible to security threats, improves business alignment and collaboration, and provides clear technical insight into which components require testing beyond standard risk evaluation.

For the threat modelling process, a structured threat modelling approach such as STRIDE, DREAD, PASTA, or hybrid methodologies tailored for cloud environments can be used.

Supplementary Information - Complementary Customer Criteria

–

OPS-23 Managing Vulnerabilities, Incidents and Crashes - 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 effec-

tiveness.

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 (Key Performance Indicators) that are volume, time-based or resolution/quality-based;
2. Customer complaints or the results of customer surveys about their satisfaction with the procedures; and
3. Results of internal or external audits.

KPIs for vulnerabilities include, for example: 1. Mean Time to Detect (MTTD, average time it takes to discover a vulnerability from its disclosure or creation); 2. Mean Time to Remediate (MTTR, average time it takes to fix or patch a vulnerability after it has been detected); 3. Number of open vulnerabilities at each severity level; and 4. Percentage of vulnerabilities that have been patched within a set period.

KPIs for incidents include, for example: 1. Number of incidents reported over a set period and how this evolved over the time; 2. Average response and resolution time; 3. Percentage of incidents resolved within the agreed-upon service level agreement; and 4. Percentage of incidents resolved during the first attempt for resolution.

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.

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 with 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, Incidents and Crashes - 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 software component 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 frame.

OPS-25.04B

The results of the vulnerability scans are used to update the cloud service provider's SIEM system (cf. OPS-13) rules, enabling the system to detect when known vulnerabilities are being actively ex-

ploited.

Additional (Sharpening)

OPS-25.01AS, sharpening 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 day in accordance with the policies for handling vulnerabilities (cf. OPS-18). These vulnerability scans include a comparison of software component data against up-to-date vulnerability databases (e.g., CVE, EUVD, etc.) to identify known vulnerabilities.

OPS-25.02AS, 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 assessment.

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, OPS-25.01AS

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.

Definitions of the terms 'CVE' and 'EUVD', as well as other vulnerability-related terms, can be found in the supplementary information of criterion OPS-18.01B.

The software component data to be compared against up-to-date vulnerability databases can be, but does not have to be, obtained using a Software Bill of Materials (SBOM).

Applicable to: OPS-25.01AC

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

1. Critical (CVSS = 9.0 - 10.0): 24 - 48 hours;
2. High (CVSS = 7.0 - 8.9): 48 - 72 hours;
3. Medium (CVSS = 4.0 - 6.9): 5 days; and
4. Low (CVSS = 0.1 - 3.9): 1 month.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure with 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) provided by either the cloud service provider or the cloud service customer themselves are used.

OPS-26 Managing Vulnerabilities, Incidents and Crashes - 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 aforementioned immutable images are retained.

OPS-26.05B

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

OPS-26.06B

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

Additional (Sharpening)

OPS-26.05AS, 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-26.05AS

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-26.01B

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-26.04B

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

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

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

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

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure with 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 - Patch Management Policies and Procedures

Basic Criteria

OPS-27.01B

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

1. Software is kept up-to-date, including timely deployment of security patches;

2. Patches are scheduled within maintenance windows, where applicable, to minimise service disruption; and
3. 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-27.02B

Patch management procedures are harmonised with the cloud service provider's overall software change management process (cf. DEV-03).

OPS-27.03B

According to the measures and procedures of the overall change management, patches provided by third parties are identified, tested and deployed.

OPS-27.04B

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

Additional (Sharpening)

OPS-27.03AS, sharpening OPS-27.03B

According to the measures and procedures of the overall change management, 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-27.01B, OPS-27.02B, OPS-27.03B, OPS-27.04B, OPS-27.03AS

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

Applicable to: OPS-27.01B

What constitutes as timely in the sense of this subcriterion depends on the criticality of the patched issue, vulnerability or exploit.

Applicable to: OPS-27.04B

The scans performed after the application of a patch can, but do not have to be, restricted to the system components to which the patch was applied.

Supplementary Information - Complementary Customer Criteria

–

OPS-28 Managing Vulnerabilities - Patch Management Implementation

Basic Criteria

OPS-28.01B

The cloud service provider designs, implements and maintains technical and organisational measures for the deployment of patches on the systems and applications under its responsibility according to the patch management policies and procedures (cf. OPS-27).

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

OPS-29 Managing Vulnerabilities, Incidents and Crashes - Externally Sourced Components

Basic Criteria

OPS-29.01B

The cloud service provider designs, implements and maintains technical and organisational measures to manage updates to system components used to provide the cloud service that incorporate third-party or open-source libraries. This includes:

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

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

OPS-30 Separation of Datasets - Policies and Procedures

Basic Criteria

OPS-30.01B

Based on a risk assessment (cf. OIS-07), the cloud service provider established policies and procedures 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 policies and procedures are documented, communicated and provided in accordance with SP-01 and contain specifications regarding the client separation based on a documented cloud layer model and include the following:

1. Illustration of which cloud layers are used for the particular cloud service. The used cloud layers should be appropriate to enable client separation;
2. 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;
3. Monitoring and compliance with these measures; and
4. Initiation of suitable measures in the event of deviations.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: OPS-30.01B

The policies and procedures 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 resources 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 policies, procedures and the corresponding measures. The systematic approach of the policies and procedures 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 Reference Architecture*. The layers provided in version 2.0 of this document include identity, credential and access management, data, networking, applications, runtime, middleware, operating systems, virtualisation, servers, storage and physical security. The cloud service provider may use its own categorisation of cloud layers as appropriate for the provided cloud service.

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 policy for every possible combination of prevention, detection and reaction as well as confidentiality, integrity and availability. Those cases should be comprehensibly documented in the policies and procedures.

Supplementary Information - Complementary Customer Criteria

–

OPS-31 Separation of Datasets - Implementation

Basic Criteria

OPS-31.01B

The cloud service provider designs, implements and maintains measures and procedures against threats to the separation of data sets according to the policies and procedures of OPS-30. The measures address prevention against, detection of and reaction to any incidents infringing the separation.

OPS-31.02B

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

OPS-31.03B

The risk assessment is reviewed as needed, especially in case of changes to the architecture of the cloud service, and at least annually. Measures are adjusted or improved as appropriate to ensure they remain commensurate with the risks.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: OPS-31.02B

Shared resources include CPU, RAM, storage space and 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 Technical Reference Architecture*. The separation on each shared resource is implemented as deemed appropriate based on the conducted risk assessment, which might also include not implementing a cryptographic separation for certain shared resources.

Where the adequacy and effectiveness of separation 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 policies and procedures).

The separation of transmitted data is subject to criterion COS-06.

Supplementary Information - Complementary Customer Criteria

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

OPS-32 Confidential Computing - Policies and Procedures

Basic Criteria

OPS-32.01B

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

1. Purpose and scope, including which information security risks on the cloud service provider's side are to be mitigated through the use of confidential computing (cf. OIS-07) and how the cloud service customers can use the provided features to manage information security risks on their side;
2. Available confidential computing technologies;
3. Determination of which parts of the cloud stack are protected with each technology and where third-party access is possible;
4. Listing of involved suppliers/service organisations; and
5. Utilisation of Trusted Execution Environments (TEEs) or secure enclaves.

OPS-32.02B

The cloud service provider provides its customers with information on the aspects specified in OPS-32.01B according to PSS-01.

OPS-32.03B

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

1. Responsibilities for the implementation and monitoring of confidential computing measures;
2. Security requirements to ensure the confidentiality, integrity, and authenticity of the data during processing; and
3. Relevant legal and regulatory requirements applicable to confidential computing.

These security requirements to ensure the confidentiality, integrity, and authenticity of the data during processing include that:

1. 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
2. Cryptographic algorithms that comply with the cloud service provider's policy for the use of cryptographic mechanisms (cf. CRY-01) are used.

Additional (Sharpening)

–

Additional (Complementing)

OPS-32.01AC

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

1. Usage of Trusted Execution Environments (TEEs) or secure enclaves to process sensitive data (data in use) in a protected environment;
2. Documentation of all associated interfaces;
3. Consideration of available hardware attestations;
4. Utilisation of encryption techniques to secure data during processing, including secure key management;
5. Remote attestation to verify the identity and measured state of the TEE as well as code executed within the TEE;
6. Implementation of monitoring and logging mechanisms to detect and respond to security incidents;
7. Conducting security reviews and penetration tests (cf. OPS-22) regularly as well as on an event-driven basis to verify the effectiveness of confidential computing measures; and

8. Performing regular updates on the Trusted Computing Base of the TEE.

Supplementary Information

About the Criteria

Applicable to: OPS-32.01B, OPS-32.02B, OPS-32.03B, OPS-32.01AC

Confidential computing as defined by the Confidential Computing Consortium and within the meaning of this criterion is the protection of data 'in use' by performing computation in a hardware-based, attested Trusted Execution Environment (TEE).

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). Generally, a TEE enforces that only authorised code can execute within the TEE and data used by that code cannot be read or tampered with by code outside the TEE. The attestation of the TEE and the application running within the TEE serve to validate the trustworthiness of the processing.

Confidential computing measures include the implementation and monitoring of technical and organisational controls to ensure the secure deployment and operation of confidential computing technologies. Such measures may include the validation of TEE configurations, continuous attestation processes, monitoring for unauthorised code changes, and lifecycle management of attested environments.

Supplementary Information - Complementary Customer Criteria

–

OPS-33 Confidential Computing - Remote Attestation

Basic Criteria

OPS-33.01B

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

OPS-33.02B

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

OPS-33.03B

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

Additional (Sharpening)

–

Additional (Complementing)

OPS-33.01AC

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

OPS-33.02AC

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

Applicable to: OPS-33.03B

The attestation interface allows customers to securely retrieve attestation evidence from the confidential computing environment. Verification of this evidence may be performed by the customer or by trusted third-party services.

Applicable to: OPS-33.01AC

Remote attestation can be performed at different locations and with different trust levels:

1. Cloud service customers retrieve evidence from TEEs and perform verification in an environment fully trusted by them. This scenario is generally assumed to provide a very strong attestation;
2. Cloud service providers retrieve evidence from TEEs, perform verification in verification services they control and provide verification results and evidence to the cloud service customer. Cloud service customers verify the attestation evidence in an environment fully trusted by them. This scenario is generally assumed to provide a very strong attestation;
3. Cloud service customers retrieve evidence from TEEs and send it to an evidence verification service they trust. This scenario is generally assumed to provide a strong attestation; and
4. Cloud service providers retrieve evidence from TEEs, send it to a verification service in their control and only return verification result to cloud service customers. This scenario is generally assumed to provide a weak attestation.

Supplementary Information - Complementary Customer Criteria

–

OPS-34 Container Management - Policies and Procedures

Basic Criteria

OPS-34.01B

Policies and procedures with technical and organisational measures for the planning and management of containers are documented, communicated and provided in accordance with SP-01. These

policies and procedures contain specifications for the entire container life cycle regarding at least the following aspects:

1. Image creation, testing, and validation;
2. Image storage and retrieval;
3. Container deployment and management;
4. Container operations; and
5. Decommissioning of images and container.

OPS-34.02B

The policies and procedures describe measures along the life cycle of containers and address at least the following aspects:

1. Containers are inventoried according to a documented process (cf. AM-02, AM-03, AM-09);
2. The need for malware protection is assessed and, if necessary, ensured (cf. OPS-05);
3. Logging and monitoring of events takes place along the container lifecycle and is executed according to a defined logging framework (cf. OPS-10, OPS-12);
4. Cloud service customer data is separated based on a risk assessment (cf. OPS-30);
5. Access to the container host should take place in accordance with a roles and rights framework and a policy for managing access and access authorisations (cf. IAM-01, IAM-06);
6. 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);
7. 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;
8. Changes to containers and images follow a regulated process (cf. DEV-03); and
9. 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)

OPS-34.01AC

The policies and procedures additionally describe measures along the life cycle of containers that address at least the following aspects:

1. Container images are cryptographically signed and the signing key securely stored (cf. CRY-10) to ensure their authenticity and integrity;
2. Container behaviour is monitored and restricted using runtime security controls; and
3. Software products used for the provision of container images are, where possible, regularly scanned for known vulnerabilities or malicious components in container images and dependencies.

Supplementary Information

About the Criteria

Applicable to: OPS-34.01AC

In case of third-party and open source software products used for the provision of container images, scanning procedures comply with the policies and procedures defined in DEV-14.

Supplementary Information - Complementary Customer Criteria

–

OPS-35 Container Management - Implementation

Basic Criteria

OPS-35.01B

The cloud service provider designs, implements and maintains technical and organisational measures for the planning and management of containers along their life cycle according to the container management policies and procedures (cf. OPS-34).

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

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 to prevent unauthorised access.

IAM-01 Policy for Identities and Access Rights

Basic Criteria

IAM-01.01B

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

1. An authorisation framework based on role-based access control and the business and security requirements of the cloud service provider; and
2. A policy for managing identities and access rights for internal and external personnel of the cloud service provider and system components that have a role in automated authorisation processes of the cloud service provider.

IAM-01.02B

For the purpose of the business and security requirements these documents address at least the following aspects:

1. Aspects that are relevant for making access control decisions;
2. Assignment of unique usernames;
3. Granting and modifying identities and access rights based on the 'least-privilege-principle' and the 'need-to-know-principle';
4. Application of a role-based mechanism for assigning access rights;
5. Definition of the supported identity and role-based access types, including an assignment of access control parameters and roles to be considered for each type;
6. Segregation of duties between operational and monitoring functions ('Segregation of Duties');
7. Assigning and monitoring privileged access rights;
8. Approval by authorised individual(s) or system(s) for granting or modifying identities and access rights before cloud service customer data, cloud service derived data and cloud service provider data can be accessed;
9. Regular review of assigned identities and access rights;
10. Blocking and removing identities or limiting access in the event of inactivity;
11. Specific measures for managing identities whose use is restriced to emergency recovery and similar scenarios;
12. Time-based or event-driven removal or adjustment of access rights in the event of changes to job responsibility;
13. Multi-factor authentication for users with privileged access;
14. Remote access and access across geographic boundaries;
15. Requirements for approving and documenting the management of identities and access rights; and
16. Measures to be taken upon the detection of a potential identity compromise, such as disabling and removing the affected identities.

IAM-01.03B

The cloud service provider is capable of producing a list of the currently granted cloud-based access rights for each identity under its responsibility.

Additional (Sharpening)

–

Additional (Complementing)

IAM-01.01AC

Access logs are reviewed at least every month in order to detect attempts of unauthorised access or suspicious access patterns.

Supplementary Information

About the Criteria

Applicable to: IAM-01.01B

External personnel includes 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 identities and access rights based on approved requests.

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

If a cloud service provider uses alternative access methods for which it is not possible or feasible to block and remove identities (such as time-bounded access methods), limiting the access to an identity is an another solution for handling inactivity that fulfils this subcriterion.

Applicable to: IAM-01.01B, IAM-01.02B

Requirements for physical access control in accordance with the policy for identities and access rights are specified in more detail in the physical access control policy (cf. PS-04).

If the cloud service provider offers federated identity services, in particular if the cloud service provider offers these services as a cloud service broker, the documents defined in these subcriteria should recognise the complexity of the particular cloud service architecture. This can include, but is not limited to, the following aspects:

1. Management of the trust boundaries between the different parties involved in the authentication process of a federated identity;
2. Propagation of identity management-related events across all parties involved in the authentication process of a federated identity;
3. Logging of events related to the authentication process of a federated identity; and
4. Notification of cloud service customers in case of a federation credential being compromised or a trust boundary being violated.

Applicable to: IAM-01.03B

Based on this list, the cloud service provider is able to review the cloud-based access rights of the given identity.

'Cloud-based' in this case refers to all of the access rights that are within the scope of the cloud service provider's system of internal control.

Applicable to: IAM-01.01AC

A review can be carried out manually or via automated manners. In a monthly review, suspicious behaviours like e.g. access failures over a larger time frame (e.g. once a day) or consecutive logins from different countries may show up that a SIEM that only analyses real-time login attemps may overlook.

Supplementary Information - Complementary Customer Criteria

–

IAM-02 Granting and Change of Identities and Access Rights

Basic Criteria

IAM-02.01B

Specified procedures for granting and modifying identities and access rights for internal and external personnel 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 policies and procedures as well as the policy for managing identities and access rights.

IAM-02.02B

The aforementioned procedures include, but are not limited to:

1. Processes and technical controls to restrict access to the cloud service provider's data and system functions to authorised personnel; and
2. Processes and technical controls to manage and verify access permissions within the cloud service provider's systems.

IAM-02.03B

If the cloud service provider defines break glass accounts for use in case of a non-availability of the main procedure for authentication, specific requirements and procedures for the secure usage of those accounts are defined and implemented.

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 Identities

Basic Criteria

IAM-03.01B

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

IAM-03.02B

As part of this procedure, specific parameters for automatically locking and withdrawing access due to inactivity or indications of brute force attacks are defined, with exceptions for the identities whose use is restriced to emergency recovery and similar scenarios.

IAM-03.03B

The cloud service provider documents and implements a process for monitoring stolen and compromised credentials, which also includes disabling any identity for which an issue is identified. This process is implemented on all identities under the responsibility of the cloud service provider that have privileged access rights.

IAM-03.04B

The aforementioned process includes an exception mechanism to be applied if all identities needed to manage the situation are potentially compromised.

Additional (Sharpening)

IAM-03.03AS, sharpening IAM-03.03B

The cloud service provider documents and implements a process for monitoring stolen and compromised credentials, which also includes disabling any identity for which an issue is identified. This process is implemented on all identities under the responsibility of the cloud service provider.

Additional (Complementing)

IAM-03.01AC

The context of authentication attempts is monitored and suspicious events are, as relevant, flagged to authorised persons.

IAM-03.02AC

The effectiveness of the procedures for locking and withdrawing identities is validated.

IAM-03.03AC

Timely and appropriate remediation measures address any deviations identified during validation.

Supplementary Information

About the Criteria

Applicable to: IAM-03.01B, IAM-03.02B, IAM-03.03B, IAM-03.04B, IAM-03.03AS, 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 personnel, for example, due to illness, parental leave, or sabbatical. Multiple failed login attempts can be indications of brute force attacks.

Applicable to: IAM-03.03B, IAM-03.03AS

This process can be performed automatically, or manually by authorised personnel.

Applicable to: IAM-03.04B

This exception mechanism should be implemented as part of the business continuity and emergency management system (cf. BCM-01), as cases where all identities needed to manage the situation described in IAM-03.03B are potentially compromised constitute an emergency.

Applicable to: IAM-03.01AC

The context of an authentication attempt can, but does not have to, include IP addresses, the date and time, or the device used.

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 timely adjusted or revoked if the job responsibilities of the cloud service provider's internal or external personnel 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 identities and access rights (cf. IAM-02) is repeated.

IAM-04.05B

In cases of role changes where temporary access may need to be granted, these access rights are approved, time-limited and documented.

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

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 personnel 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 personnel 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 and in case of significant changes to the cloud service 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 personnel or system components.

IAM-05.03B

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

IAM-05.04B

When revoking identities, the system ensures that all production associated system components (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.

IAM-05.05B

For system components that are not production associated, the cloud service provider designs, implements and maintains appropriate controls for the prevention of orphan resources based on a risk assessment (cf. OIS-07).

Additional (Sharpening)

–

Additional (Complementing)

IAM-05.01AC

Privileged access rights are reviewed at least every six months, and in case of significant changes to the cloud service.

Supplementary Information

About the Criteria

Applicable to: IAM-05.01B, IAM-05.02B, IAM-05.03B, IAM-05.04B, IAM-05.05B

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.

Applicable to: IAM-05.01B, IAM-05.01AC

If a review is caused by significant changes to the cloud service, only the identities and access rights affected by the change need to be included in the review.

Applicable to: IAM-05.05B

The system components meant here are system components in development, test or any other non-productive environments. Orphan resources are system components that have no assigned owner.

Supplementary Information - Complementary Customer Criteria

–

IAM-06 Privileged Access Rights

Basic Criteria

IAM-06.01B

Privileged access rights for internal and external personnel as well as technical users of the cloud service provider are assigned and changed in accordance with the policy for managing identities 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

Anonymous technical users are only accessed through authentication with a personalised identitiy.

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 timely 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 containers and images, activities of users with privileged access are logged according to OPS-10.

IAM-06.09B

Access to the cloud service provider's administration interfaces requires the use of multi-factor authentication.

Additional (Sharpening)

–

Additional (Complementing)

IAM-06.01AC

The cloud service provider maintains an inventory of the identities with privileged access rights under its responsibility. This inventory is kept up-to-date.

IAM-06.02AC

The cloud service provider maintains a list of the personnel that is responsible for an identity assigned to a non-human entity within the cloud service provider's scope of responsibility. This list is reviewed every six months and in case of significant changes to the cloud service.

IAM-06.03AC

For privileged users, phishing-resistant multi-factor authentication such as FIDO2 security keys or comparable mechanisms using public key cryptography and domain binding are implemented.

IAM-06.04AC

Privileged access rights are enforced through a privileged access management (PAM) solution with support for 'just-in-time' elevation and 'just-enough' access.

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, IAM-06.03AC, IAM-06.04AC

Privileged access rights in the sense of the criterion are those that enable personnel of the cloud service provider to perform any of the following activities:

1. 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
2. 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 cloud service customers data (also indirectly, e.g. by deactivating the logging and monitoring of security-relevant events).

Applicable to: IAM-06.06B

Responsible personnel for events that may indicate misuse can be e.g. the personnel of the cloud service provider's security operations centre.

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

Applicable to: IAM-06.02AC

If a review is caused by significant changes to the cloud service, only the parts of the list that are affected by the change need to be included in the review.

Supplementary Information - Complementary Customer Criteria

–

IAM-07 Access to Cloud Service Customer Data

Basic Criteria

IAM-07.01B

The cloud service provider implements partitioning measures that are:

1. Sufficient for separating the system components for providing the cloud service from the system components of the cloud service provider's other information systems; and
2. Suitable for separating different cloud service customers from each other (cf. OPS-30 and OPS-31).

IAM-07.02B

The partitioning measures of the cloud service provider ensure that security incidents, if they compromise the system components storing the cloud service customer data, do not also compromise the system components that manage the access to them.

IAM-07.03B

Unless prohibited by applicable law, the cloud service customer is informed by the cloud service provider whenever internal or external personnel of the cloud service provider reads or writes to the cloud service customer data processed, stored or transmitted in the cloud service or has 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 provided about the access 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 discloses, through contractual agreements and before offering its services, all instances where the cloud service provider may access cloud service customer data in unencrypted form while it is processed, stored or transmitted in the cloud service.

Additional (Sharpening)

IAM-07.03AS, sharpening IAM-07.03B

Access to cloud service customer data and cloud service derived data by internal or external personnel 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-07.04AS, sharpening IAM-07.04B

Unless contractually agreed otherwise, the information provided for the consent 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. In addition to the provided information, the cloud service provider specifies a time frame within which the cloud service customer shall respond to the access request.

IAM-07.06AS, sharpening IAM-07.06B

The cloud service provider discloses, through contractual agreements and before offering its services, all instances where the cloud service provider may access cloud service customer data or cloud service derived data in unencrypted form while it is processed, stored or transmitted in the cloud service.

Additional (Complementing)

IAM-07.01AC

If the cloud service provider might access the cloud service customer data transmitted, handled or stored in the cloud service in a non-encrypted way, the cloud service provider includes provisions through contractual agreements for cases in which seeking prior consent for such an access is not feasible.

IAM-07.02AC

In order to be able to directly or indirectly access cloud service customer data, any internal or external personnel of the cloud service provider has to pass an appropriate assessment, or has to instead be supervised by personnel who has passed an appropriate assessment (cf. HR-01). The cloud service provider verifies that one of these conditions is met before the access is granted. This applies to support operations as well.

IAM-07.03AC

If the performed access is supervised, the cloud service provider ensures that:

1. The mechanisms used to perform the supervised access allow the supervising personnel to authorise or deny individual actions of the supervisee and ask for explanations in real time;
2. Any access rights that are granted as part of the supervised access are revoked at the end of the operation;
3. All operations that are performed as part of the supervised access are logged as administration actions;
4. The supervisee and the device used to perform the supervised access are authenticated by the supervision solution;
5. The operations that the supervisee proposes and the actions of the supervising personnel are logged by the supervision solution, including operations that were denied; and
6. Information flows towards the device of the supervisee are prevented by the supervision solution.

IAM-07.04AC

If the cloud service customer is given access to interfaces for administrators and for end users as part of the cloud service, the cloud service provider separates these interfaces from one another and ensures that access paths for customer administrators differ from those for end users.

Supplementary Information

About the Criteria

Applicable to: IAM-07.01AC

This subcriterion is only applicable if subcriterion IAM-07.03S is also applied.

Seeking prior consent might, for example, not be feasible where the cloud service needs to be troubleshot to preserve the confidentiality, integrity and availability of cloud service customer data.

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

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-07.03AS, IAM-07.04AS, 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-03. These are to be communicated to cloud service customers as far as it is legally not forbidden.

The criterion aims at minimising the cloud service provider's capability to access cloud service customer data. Minimisation of the cloud service provider's possibility to access cloud service customer data is often a question related to the radius of the collusion circle. For example, if the four-eyes principle for access is applied and the access is being logged, then three people make up the collusion

circle. In order to build trust into such access statements, the cloud service provider should describe in the system description the measures taken to enlargen the collusion circle.

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

The geographic location of the access provided to the cloud service customer need not be a GPS location, but should at least be as precise as the country from which the access has been or is meant to be performed.

Applicable to: IAM-07.02AC, IAM-07.03AC

The cloud service provider should make details about how the supervised access is performed accessible to cloud service customers.

Applicable to: IAM-07.04AC

The separation should be designed and implemented such that customer administrators can access the cloud service even when the end user interfaces are unavailable.

Supplementary Information - Complementary Customer Criteria

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

IAM-08 Authentication Mechanisms

Basic Criteria

IAM-08.01B

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 personnel as well as system components that are involved in the cloud service provider's automated authorisation processes.

IAM-08.02B

The cloud service provider enforces multi-factor authentication (MFA) for all access to the production environment. This requirement applies to both human users and automated processes, ensuring that only authorised entities can access systems and data in the production environment.

IAM-08.03B

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 policies and procedures for the use of cryptographic mechanisms (cf. CRY-01).

IAM-08.04B

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:

1. The selection of appropriate mechanisms for every level of risk and each identity type;
2. The protection of credentials that the authentication mechanisms use, including the confidentiality of personal or shared authentication information and non-sharing of credentials;
3. The generation and distribution of credentials for any new identity;
4. The non-reuse of credentials;
5. Rules on the storage of credentials;
6. Rules for renewing credentials, including periodic renewals and renewals in case a credential is lost or compromised; and
7. Rules on the required strength of credentials, including trade-offs between entropy and ability to memorise where applicable, as well as mechanisms for communicating and enforcing these rules.

IAM-08.05B

The cloud service provider determines by means of a risk assessment (cf. OIS-07) the risk that the authentication mechanisms integrated into the system components under its responsibility used to provide the cloud service become outdated. Based on the results of the risk assessment, the cloud service provider implements appropriate measures for exchanging outdated authentication mechanisms or the system components into which they are integrated.

IAM-08.06B

Any authentication mechanism integrated into the system components used to provide the cloud service has a mechanism for disabling an identity after a predefined number of unsuccessful authentication attempts.

IAM-08.07B

The cloud service provider implements measures which require that users can only access non-personal identities assigned to multiple persons after they have already been authenticated with their identity assigned to a single person.

Additional (Sharpening)

IAM-08.02AS, sharpening IAM-08.02B

The cloud service provider enforces multi-factor authentication (MFA) for all access to any environment. This requirement applies to both human users and automated processes, ensuring that only authorised entities can access systems and data in all of the environments.

IAM-08.03AS, sharpening IAM-08.03B

Within an 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 policies and procedures for the use of cryptographic mechanisms (cf. CRY-01).

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: IAM-08.02B

Multi-factor authentication implies that different sources for identity verification are used. This applies both to human users and automated processes. Human users may use different factors like a password and a hardware token. Multi-factor authentication for automated processes implies using independent sources for identity verification like e.g. cryptographic keys and a short term token from another source.

Applicable to: IAM-08.02AS, IAM-08.03AS

These environments include production, development, test and staging environments.

Supplementary Information - Complementary Customer Criteria

–

IAM-09 Confidentiality of Authentication Information

Basic Criteria

IAM-09.01B

The allocation of authentication information to access system components used to provide the cloud service to internal and external users of the cloud service provider and system components that are involved in automated authorisation processes of the cloud service provider is done in an orderly manner that ensures the confidentiality of the information.

IAM-09.02B

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

IAM-09.03B

If passwords are used as authentication information, their confidentiality is ensured by the following procedures, as far as technically possible:

1. 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;
2. When creating passwords, compliance with the authentication policy (cf. IAM-08) is enforced as far as technically possible;
3. The user is informed about changing or resetting the password; and
4. The server-side storage takes place using state of the art cryptographic hash functions, with the exception of passwords that are stored in the plain text form for later use, for example in a password manager. In this case, state of the art cryptographic mechanisms are used to protect the passwords.

IAM-09.04B

Deviations are evaluated by means of a risk assessment according to OIS-07 and mitigating measures derived from this are implemented.

IAM-09.05B

Rules and recommendations for managing credentials in accordance with the authentication policy (cf. IAM-08) are documented, communicated and made available to all users under the responsibility of the cloud service provider. They include recommendations on password managers and recommendations to specifically address classical attacks such as phishing, social attacks, and whaling.

IAM-09.06B

Used cryptographic mechanisms comply with the policies and instructions for cryptographic mechanisms (cf. CRY-01).

IAM-09.07B

Password reset procedures are valid for at most 24 hours. After the reset procedure has been used, the password is to be changed by the user.

Additional (Sharpening)

–

Additional (Complementing)

IAM-09.01AC

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-09.01B, IAM-09.02B, IAM-09.03B, IAM-09.01AC

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

Applicable to: IAM-09.07B

This subcriterion is only applicable to password-based authentication schemes.

Applicable to: IAM-09.01AC

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

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

1. Usage of encryption procedures and secure network protocols that correspond to the state of the art;
2. Usage of hash functions and salt values, that both correspond to the state of the art;
3. Usage of signature schemes that correspond to the state of the art;
4. 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;
5. Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal, backup, restoration and deletion of the keys;
6. Requirements for the rotation of cryptographic keys that follow industry best practices and consider the potential risk of information exposure;
7. Consideration of relevant legal and regulatory obligations and requirements;
8. Documentation of a change management process for managing cryptographic, encryption, authentication and key management technology changes; and
9. Consideration of crypto-agility to allow for efficient substitution of implemented cryptographic mechanisms during their intended lifetimes.

CRY-01.02B

Reviews of policies and procedures regarding cryptographic mechanisms include checks that the policies and procedures are up to date and comply with the BSI technical guideline (BSI TR-02102)

or suitable NIST guidelines (e.g. FIPS 140 series and SP 800 series). Deviations are analysed and documented in a risk assessment for cryptographic mechanisms valid at the given time. 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 service provider's PQC strategy is aligned with cryptography policies and procedures and includes the following aspects:

1. 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;
2. Staying informed about encryption measures that are deemed state of the art and secure against adversaries who possess a quantum computer;
3. Usage of hybrid cryptography models to ensure security for both quantum and non-quantum computing based attacks; and
4. 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:

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

4. BSI TR-02102-4 Cryptographic Mechanisms: Recommendations and Key Lengths – Use of Secure Shell (SSH).

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.

Applicable to: CRY-01.01B

Crypto-agility refers to the ability to change the used cryptographic mechanisms or implementation of such mechanisms, e.g. in such a way that a transition to larger key lengths and stronger cryptographic mechanisms is possible. For further information, please refer to BSI TR-02102-1.

Applicable to: CRY-01.01AC, CRY-01.02AC, CRY-01.03AC

Recommendations for the migration to PQC and future-proof use of cryptography are provided, for example, in:

1. The BSI guideline 'Quantum-safe cryptography – fundamentals, current developments and recommendations';
2. The roadmap 'A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography' published by the European Commission; and
3. The preliminary drafts for the NIST publication 'NIST SP 1800-38: Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography'.

Applicable to: CRY-01.02AC

Hybrid cryptography models, as defined in the context of post-quantum cryptography (PQC), combine classical and quantum-safe mechanisms to ensure that the system remains secure even if one component is compromised. The purpose of such models is to provide long-term protection against threats such as 'store now, decrypt later' and other attacks based on classical or quantum computing.

Applicable to: CRY-01.03AC

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

1. The threat landscape posed by advancements in quantum computing;
2. Advancements in cryptographic mechanisms that are deemed secure against attackers in possession of a quantum computer;
3. Vulnerabilities inherent to the cryptographic mechanism; and
4. 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 in accordance with DEV-06. This process includes an analysis of the cloud infrastructure of the cloud service, as well as an analysis of potential disruptions to cloud service customer-managed workloads and the evaluation of residual risks, cost implications, and integration benefits. The cloud service provider informs cloud service customers of these downstream effects to prevent unforeseen failures within the cloud service customer's specific cryptographic implementations.

CRY-02.02B

All changes and adjustments to cryptographic systems are documented and traceable.

CRY-02.03B

The personnel responsible for cryptographic systems is regularly trained and informed about respective changes.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: CRY-02.01B

When performing the evaluation of the potential impact of changes, the cloud service provider should consider the complexity of the distributed architecture of its cloud service.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure with 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 and COM-03 to identify and address potential vulnerabilities. At a minimum, reviews are performed annually and immediately following security incidents involving cryptographic components.

CRY-03.02B

As part of the reviews, the cloud service provider determines if the cryptographic practices align with the state of the art and updates them as needed.

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

Applicable to: CRY-03.02B

The cloud service provider applies the cryptographic change management process (cf. CRY-02) when updating the cryptographic practices to align with the state of the art.

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 safeguards for state of the art encryption and authentication for the transmission of cloud service customer data and cloud service derived data over public networks.

CRY-04.02B

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

Additional (Sharpening)

CRY-04.01AS, sharpening CRY-04.01B

The cloud service provider has established procedures and technical safeguards 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-04.02B, CRY-04.01AS

When transmitting data with normal protection needs 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, wildcard certificates should not be used.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure with 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 needs.

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

In general, the private keys (for asymmetric algorithms) or secret keys (for symmetric algorithms) used for encryption are accessible only by the cloud service customer in accordance with applicable legal and regulatory obligations and requirements. If due to the nature of the cloud service, the cloud service provider has to access the private or secret keys of the customer in order to provide the cloud service, this access is performed in accordance with IAM-07. Exceptions follow a specified procedure.

CRY-05.03B

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

CRY-05.04B

If any changes of these procedures and technical safeguards may affect the confidentiality of the cloud service customer data, the cloud service provider communicates these changes to the cloud service customers.

CRY-05.05B

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.

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

The requirement of 'accessible only by the cloud service customer' 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.

Applicable to: CRY-05.02B

Scenarios in which the cloud service provider has to access the secret or private keys of the customer include, but are not limited to, the use of provider-managed keys in a SaaS service.

Applicable to: CRY-05.02B, CRY-05.05B

The use of a master key by the cloud service provider may be an exception to the requirement that keys are accessible only by the cloud service customers.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure with 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 needs.

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 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 assessment, the cloud service provider does not perform key rotation, 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:

1. Verification of identity before issuing public-key certificates that are issued by or on behalf of the cloud service provider for its own system components or personnel to ensure they are granted to legitimate entities;
2. Secure methods for issuing certificates that are issued by or on behalf of the cloud service provider for its own system components or personnel to prevent unauthorised access; and
3. Procedures for obtaining public-key certificates from trusted Certificate Authorities to ensure the authenticity of the certificates used by the cloud service provider.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: CRY-08.01B

The first two bullet points apply to certificates issued by or on behalf of the cloud service provider for its own system components and personnel. If the cloud service provider offers certificate authority services for cloud service customers, the shared responsibility principle applies, i.e. the cloud service provider should ensure that the cloud service provides adequate technical measures to enable cloud service customers to perform adequate identity verification (cf. also the Complementary Customer Criteria). The third bullet point applies to certificates that the cloud service provider obtains from external Certificate Authorities for use in its own cloud services and system components. The cloud service provider should ensure that certificates are obtained only from trusted Certificate Authorities and that the authenticity of received certificates is verified before use. This criterion does not

necessarily extend to certificates that cloud service customers obtain from external Certificate Authorities for their own purposes; the selection and validation of external Certificate Authorities by customers falls under customer responsibility within the shared responsibility model.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure with suitable controls that, where they use certificate authority services provided by the cloud service provider, identity verification procedures appropriate to the certificates being issued are implemented and the technical controls provided by the cloud service are configured to enable and enforce identity verification. Cloud service customers ensure with suitable controls that, where they obtain certificates from external Certificate Authorities for their own use, procedures are established for selecting trusted Certificate Authorities and validating the authenticity of obtained certificates.

CRY-09 Secure Key Provisioning

Basic Criteria

CRY-09.01B

The cloud service provider has documented and implemented procedures and technical safeguards 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 safeguards 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 contractual, legal, regulatory, and security requirements.

Additional (Sharpening)

–

Additional (Complementing)

CRY-10.01AC

Based on a risk assessment (cf. OIS-07), the cloud service provider uses a suitable software or hardware security module for the secure storage of cryptographic keys.

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 safeguards for the secure archiving of cryptographic keys. These include:

1. Storage of archived keys in a repository to prevent unauthorised access;
2. Restriction of access to archived keys to authorised personnel based on the principle of least privilege;
3. Support of later recovery of information through archived keys;
4. Retention of archived keys only for as long as needed and secure destruction afterwards; and
5. 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 comply with applicable laws and regulations.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: CRY-12.01B

Suspension of a cryptographic key refers to a temporary state in which the key is disabled and cannot be used for cryptographic operations but may later be reactivated. Deactivation of a cryptographic key, in contrast, represents a permanent state in which the key is withdrawn from use and cannot be reactivated.

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 complying with legal and regulatory requirements.

CRY-13.02B

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

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. These procedures ensure that:

1. Expired keys are no longer used for encryption purposes, but may still be used for decryption if necessary;
2. Expired keys are no longer used for signature creation, but may still be used for signature verification;
3. Deactivated keys are eventually destroyed when they are no longer required, with relevant metadata retained for auditing; and
4. 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 safeguards 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 contractual, 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:

1. 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 assessment.
2. 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 safeguards to monitor and document the lifecycle of cryptographic keys and materials.

CRY-17.02B

For all keys except for ephemeral keys, the aforementioned safeguards 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 safeguards for the usage of external key management systems (KMS) are established. The following aspects are taken into account:

1. The external KMS have recognised security certifications that reflect the state of the art to comply with legal, regulatory and contractual requirements;
2. The integration of the external KMS into the cloud infrastructure is secure to ensure the confidentiality, integrity, and availability of the keys;
3. Strict access control are implemented to ensure that only authorised users and systems can access the keys (cf. IAM-01);
4. Procedures for the regular rotation and renewal of keys are defined and implemented to ensure the security of the keys (cf. CRY-07);
5. All accesses and operations on the external KMS are logged and monitored to detect and respond to suspicious activities; and
6. The cloud service provider ensures that the external KMS is regularly checked for vulnerabilities (cf. OPS-25) and updated (cf. OPS-28) 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:

1. Secure integration of customer-generated keys ('Bring-Your-Own-Key'; BYOK) into the cloud environment;
2. Logging of all activities related to customer-managed keys; and
3. 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 with 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.

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 assessment carried out according to OIS-07, the cloud service provider has implemented technical safeguards which are suitable to timely detect and respond to attacks on the network of system components used for provisioning of the cloud service.

COS-01.02B

For these technical safeguards, preventive and protective measures are implemented at multiple tiers (defence in depth) within the cloud service to mitigate the risk of breaching the deployed defensive system. This includes network-based cyber attacks such as:

1. Attacks on the basis of irregular incoming or outgoing traffic patterns;
2. Distributed Denial-of-Service (DDoS) attacks;
3. Spoofing attacks;
4. Code injection attacks;
5. DNS tunneling; and
6. 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 safeguards 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 safeguards 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 with 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, documented 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:

1. In which cases the security zones are to be separated and in which cases cloud service customers are to be logically or physically separated;
2. Which communication relationships and which network and application protocols are permitted in each case;
3. How the data traffic for administration and monitoring is separated from each on network level;
4. How office networks are secured with firewalls and secure WIFI configurations as well as VPN for remote access;
5. Which internal, cross-partition communication is permitted; and
6. Which cross-network communication is allowed.

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 distinguishes 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 (cf. COS-02).

COS-03.03B

The cloud service provider ensures that the configuration of networks matches the security requirements (cf. COS-02). The cloud service provider reviews at least annually and in case of significant changes to the cloud service the design and implementation of the 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.

Applicable to: COS-03.03B

If the review is caused by significant changes to the cloud service, only the design and implementation of configuration of the connections affected by these changes need to be included in the review.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure with 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.

COS-04.02B

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-04.02B

A security gateway is a stack of chained filtering and firewall components that restrict communication to explicitly permitted traffic. Security gateways can, for example, employ a P-A-P structure, consisting of an outer packet filter, an application-level gateway acting as a deep-inspection proxy, and an inner packet filter. The stack may be further enriched with an intrusion detection system, intrusion prevention system, or antivirus scanner. However, this structure is not mandatory. It serves

to keep filtering and inspection functionally independent of each other, so that a failure of one does not automatically lead to a failure of the other.

Applicable to: COS-04.02B

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 with 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-08).

COS-05.02B

Networks used by the cloud service provider to create, migrate or orchestrate compute workloads (e.g. virtual machines, containers, functions) are physically or logically separated from tenant networks.

Additional (Sharpening)

–

Additional (Complementing)

COS-05.01AC

If there is no physical separation between the administration networks and other networks, the administration network traffic uses state of the art encryption (cf. CRY-01).

Supplementary Information

About the Criteria

Applicable to: COS-05.01B

The separation can be physical or logical (e.g. VLAN, SDN, VRF).

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 framework 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 encryption in combination with logical network separation or encapsulation.

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 framework). The separation of stored and processed data is subject of the criteria OPS-30 and OPS-31. After successful authentication 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 encryption of the networks that corresponds to the state of the art. For the definition of state of the art encryption, the BSI Technical Guideline TR-02102 should be considered (cf. CRY-01).

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure with 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 incidents in accordance with contractual obligations. The documentation shows:

1. How the subnets are allocated;
2. How the network is zoned and segmented;
3. How the network connects with third party and public networks; and
4. How the data flows between different subnets and system components within the network to support the management, monitoring and analysis of the network.

COS-07.02B

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

COS-07.03B

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 the network topology documentation and the asset inventory (cf. AM-02). The documentation includes the system components that provide security functions and the system components that host the corresponding cloud service customer data and cloud service derived data, or provide sensitive functions.

COS-07.04B

The network topology documentation is reviewed at least once a year. Timely and appropriate remediation measures address any deviations identified during the review.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: COS-07.01B, COS-07.02B, COS-07.03B

The network documentation can follow a hierarchical or grouped approach based on the scale of operations.

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 procedures 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 procedures establish a reference to the asset classification and labelling (cf. AM-09) and cryptographic mechanisms (cf. CRY-01).

COS-08.02B

Technical safeguards outlined in the documented policies and procedures to protect the transmission of data are implemented and reviewed regularly, as well as in case of significant changes to the cloud service.

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.

Applicable to: COS-08.02B

If a review is caused by significant changes to the cloud service, only the technical safeguards affected by these changes need to be included in the review.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure with suitable controls that the 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 Safety of Input and Output Interfaces

Basic Criteria

PI-01.01B

For inbound and outbound interfaces through which the cloud service can be accessed by other cloud services or IT systems of cloud service customers, the cloud service provider designs, implements and maintains controls regarding the following aspects:

1. 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 needs, and the adequate authentication of the user;
2. The use of encryption according to CRY-02 in case of communication over untrusted networks;
3. The use of standardised data formats and common data processing standards to facilitate information processing interoperability;
4. 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; and
5. The provision of up-to-date information about the available communication protocols, as well as applicable data formats and data processing standards.

PI-01.02B

The cloud service provider provides suitable technical means for extracting cloud service customer data in accordance with the aforementioned policies and procedures to the cloud service customer. Where data volume, format, or architecture make a customer-driven extraction infeasible, the cloud service provider provides appropriate extraction services to the cloud service customer.

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 the authentication information of users under the responsibility of the cloud service cus-

tomer. 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 service customer 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.

Those interfaces and their documentation should include sufficient information on the cloud service to enable the development of software to communicate with it for the purposes of data portability and interoperability. However, the cloud service provider is not required to develop new technologies to this purpose or share information that is protected by intellectual property rights or that constitutes a trade secret.

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 with suitable controls that the interfaces provided (and their security) are adequate for its protection needs 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 cloud service customer data following termination of the contractual relationship, insofar as these are applicable to the cloud service:

1. Type, scope and format of the cloud service customer data the cloud service provider provides to the cloud service customer;
2. Methods for delivering the data to the cloud service customer;
3. Conditions and time frames for cloud service customer data provisioning throughout the duration of the contractual relationship;
4. Right of termination of the contract and definition of the time frame within which the cloud service provider makes the cloud service customer data available to the cloud service customer after termination of the contract;
5. 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;
6. The cloud service customers' responsibilities and obligations to cooperate for the provision of the cloud service customer data; and
7. 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.

Legal requirements can, for example, include the EU Data Act. In Germany, legal requirements for retention in particular 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, and these are applicable due to the service model, the criterion is not met and a deviation is to be noted by the auditor.

Applicable to: PI-02.01B

If the cloud service provider acts as a cloud service broker, special consideration should be given to contractual data-portability clauses that recognise the complexity of the particular cloud service broker scenario. This can include, but is not limited to, the definition of:

1. Responsibility for the export of cloud service customer data;
2. If there are multiple underlying cloud service providers, the export scope, the consolidated format, any completeness limits, and how cloud service broker generated artifacts such as aggregated logs are handled;
3. Whether cloud service customers can access the cloud services of underlying cloud service providers directly via APIs or have to rely on the cloud service broker's export interface, and whether there are any timing or usage restrictions; and
4. Time frames for the delivery of cloud service customer data exports to the cloud service customer.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure with 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). Exceptions are only made if they are required by a valid court order or needed for the fulfilment of known future financial and legal obligations.

PI-03.02B

The deletion procedures prevent recovery by forensic means that comply with the established rules of technology.

PI-03.03B

The deletion of the cloud service customer data, cloud service derived data and account data is documented 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 with 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 procedures 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 procedures 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:

1. 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;
2. Security and quality in software deployment (including continuous delivery);
3. Security and quality in operation (reaction to identified faults and vulnerabilities); and
4. Secure coding standards and practices (reduction of vulnerabilities being introduced to the 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 cloud service provider defines measures to enforce the specified standards and guidelines as part of the policies and procedures for the secure development of system components of the cloud service.

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 instead of 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:

1. ISO/IEC 27034; and
2. 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:

1. 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;
2. Design phase: Carrying out design reviews and inspections of the cloud service to ensure that the design meets the quality requirements;
3. 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;
4. 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;
5. 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;
6. Release and deployment: Preparation and implementation of the software release in accordance with defined quality standards; and
7. 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 service organisation:

1. 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;
2. Acceptance testing of the quality of the services provided in accordance with the agreed functional and non-functional requirements; and
3. Providing evidence that sufficient verifications have been carried out to rule out the existence of known vulnerabilities.

DEV-02.02B

Before outsourcing the development of the cloud service or components thereof, the cloud service provider conducts a risk assessment according to SSO-02 that takes into account at least the following aspects:

1. Management of source code by the service organisation;
2. Accessability of source code to the cloud service provider;
3. Human resource procedures implemented by the service organisation;
4. Required access to the development, test and preproduction environments of the cloud service provider; and
5. Management of subcontractors engaged by the service organisation.

Additional (Sharpening)

–

Additional (Complementing)

DEV-02.01AC

The cloud service provider documents and implements a procedure that enables the supervision and control of the outsourced development activity to ensure that it complies with the secure development policy of the cloud service provider, and that the security level achieved through it matches the security level achieved through internal development.

DEV-02.02AC

When a change contains work from outsourced development, the cloud service provider's personnel runs the tests needed to decide whether the change can be deployed.

Supplementary Information

About the Criteria

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

Outsourced development in the sense of the basic criterion refers to the development of system components used specifically for the cloud service, by a service organisation of the cloud service provider. The development takes place according to the processes of the service organisation.

The risks that may arise and should be taken into account can, but do not have to, include:

1. Risks that may result from the service organisation managing source code without adequate controls, including unauthorised modifications, insufficient version control, or inadequate protection against loss or theft of intellectual property;
2. Risks that may result from the service organisation granting access to source code to the cloud service provider or to third-party evaluators, including unauthorised disclosure, loss of confidentiality, or inadequate controls governing how such access is managed and restricted;
3. Risks that may result from inadequate personnel screening, insufficient background checks, lack of security awareness training, or high staff turnover within the service organisation, including insider threats or uncontrolled loss of sensitive knowledge;
4. Risks that may result from granting the service organisation access to internal development, test or preproduction environments, including excessive privileges, insufficient access controls, or inadequate logging and monitoring of such access; and
5. Risks that may result from the service organisation subcontracting parts of the service without adequate security controls in place, including insufficient contractual security requirements imposed on subcontractors or lack of transparency regarding the composition of the supply chain.

The purchase of software available on the market as well as the integration of external personnel 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 procedures with procedures and technical 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:

1. 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;
2. Requirements for the performance and documentation of tests;
3. Requirements for segregation of duties during development, testing and release of changes;

4. 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;
5. Requirements for the documentation of changes in system, operational and user documentation;
6. Requirements for the implementation and documentation of emergency changes such that - as far as reasonably possible - they comply with the same level of security as normal changes;
7. Requirements for the handling of unexpected effects of those changes, including corrective actions;
8. Requirements for the increased testing for the development of security features that implement technical mechanisms and safeguards; and
9. Requirements for managing exceptions, including emergency changes, to ensure related risks are appropriately mitigated.

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 procedures and technical 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, role-based security training and awareness for internal and external personnel on standards and methods for:

1. Secure software development and provision as well as on how to use the tools used for this purpose; and
2. 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 procedures, the assigned roles and responsibilities and the tools used.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: DEV-04.01B

This is a specialised criteria for safety training and awareness programmes for a particular target group. In HR-03, general properties of such trainings and programmes are defined.

Supplementary Information - Complementary Customer Criteria

–

DEV-05 Design Documentation for Security Features

Basic Criteria

DEV-05.01B

Design documentation for security features is based on a security analysis of the adequacy and planned effectiveness of the features. A specification of expected inputs, outputs and possible errors is included in the documentation.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: DEV-05.01B

Security features are typically features that control confidentiality (e.g. via integrating cryptography), integrity (e.g. via introducing check-sums or validating input data), availability (e.g. via redundancy or resiliency), authentication (e.g. via MFA or secure session management) and authorisation (e.g. via different roles). They usually follow from threat modelling and risk assessment. Ideally, security features are an integral part of the software development process and not additions made only after new software features have been created.

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, changes are subject to a risk assessment evaluating its potential impact on the overall cloud service in scope. In addition, when multiple changes are implemented concurrently, their mutual interactions and cumulative effects are also subject to the risk assessment in order to identify potential conflicts or dependencies. All identified risks and dependencies are categorised and prioritised accordingly.

DEV-06.02B

If the risk associated to a planned change is high, 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. This does not include changes without an effect on the service usage or security posture of the service.

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 established rules of technology. 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 security features of the cloud service are subject to tests that fully cover the security features' specification (cf. DEV-05), including all specified error conditions. The documentation of these tests covers at least the following aspects:

1. A description of the test;
2. The initial conditions;
3. The expected outcome; and
4. Procedures 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 framework (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).

Applicable to: DEV-07.01B

Test procedures for software assets can be static (SAST), dynamic (DAST) or interactive (IAST).

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 with 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 framework according to IAM-01 and authorisation mechanisms.

DEV-08.02B

The configuration of these system components ensures that all changes performed by the cloud service provider 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 cloud service provider enforces the role and rights framework by monitoring the changes made to system components of the cloud service in the production environment. Timely and appropriate remediation measures address any deviations identified during monitoring.

Supplementary Information

About the Criteria

Applicable to: DEV-08.02B

If the change has external contribution (e.g. use of third-party products, libraries), tracing back individual changes in the development is often not possible. In that case it is sufficient to record the external contribution in the software component list or Software Bill of Materials (SBOM, cf. DEV-13.01B). In addition to that, depending on the nature of the external contribution, the criterion for Outsourcing of the Development (cf. DEV-02) and the criteria for Control and Monitoring of Service Providers and Suppliers (SSO) may apply.

Supplementary Information - Complementary Customer Criteria

–

DEV-09 Version Control

Basic Criteria

DEV-09.01B

The cloud service provider uses a version control system that adequately ensures the confidentiality, integrity and authenticity of the source code during all development stages.

DEV-09.02B

Version control procedures track dependencies of individual changes and attribute each change to individual contributors. The version control procedures are capable of restoring affected system components back to a previous state.

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 keeps a record of all deployed software versions and system configurations. This record enables the recreation of a previously implemented environment in a test environment.

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 process is monitored. Timely and appropriate remediation measures address any deviations identified during monitoring.

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 fulfil 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 with 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 (cf. OIS-07) and are protected with appropriate security measures against identified risks. This also includes extending the backup plan (cf. OPS-06) to the necessary parts of those environments.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: DEV-11.01B

Note that the backup policies and procedures (cf. OPS-06) are preceded by a risk assessment and

does not need to include all elements of those environments, but only the ones considered necessary based on the risk assessment. Some parts can be build from scatch more easily than backing them up.

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. Cloud service customer data contained in the production environments is not used in test or development environments, unless explicitly approved 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 list of software components is created, maintained, and kept up-to-date for every developed or integrated software component.

DEV-13.02B

The cloud service provider maintains a list of software components for integrated software components as well, except where such information is not available and cannot be produced with reasonable effort. The risk from these exceptions is treated according to SP-03.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: DEV-13.01B

This criteria can be fulfilled via a sufficiently detailed list of software components. Sufficient detail means that the list allows the cloud service provider to identify all cloud services affected by any given known vulnerability. This criteria can also be fulfilled via a Software Bill of Materials (SBOM). The established rules of technology 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 software component lists or SBOMs are recommended to ensure accuracy and integration into security and vulnerability management processes. Please note that it may not be necessary to store every version of the SBOM - just like in the other development processes for components - as long as the cloud service provider is able to keep track of the changes.

Applicable to: DEV-13.02B

This subcriterion only applies to integrated software components. If integrated software components are e.g. open-source and if this criterion is fulfilled via SBOMs, there may be cases where a SBOM is not available and cannot be produced with reasonable effort. Reasonable implies that changing this component to one that has a SBOM is economically not feasible. However, the risks from these exceptions are treated within the exception process (cf. SP-03).

Supplementary Information - Complementary Customer Criteria

–

DEV-14 Secure Use of Third Party Hardware and Software

Basic Criteria

DEV-14.01B

Policies and procedures for the use of third party and open source software are documented, communicated and provided in accordance with SP-01.

DEV-14.02B

For the hardware and software products (cf. DEV-13) used in the development of the cloud service, a list of dependencies to those products is maintained.

DEV-14.03B

Only trusted sources are used to retrieve third party software. Whenever possible, the authenticity of the software is verified.

Additional (Sharpening)

–

Additional (Complementing)

DEV-14.01AC

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

Applicable to: DEV-14.01B

The policy should consider, where applicable, the same aspects as the policy for the proper and secure use of assets (cf. AM-05).

Supplementary Information - Complementary Customer Criteria

–

DEV-15 Exceptions to the Change Management Process

Basic Criteria

DEV-15.01B

The cloud service provider's change management process implements procedures for managing exceptions, including emergency changes, to ensure related risks are appropriately mitigated.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: DEV-15.01B

This criteria refers mainly to the exception process demanded in SP-03, although all exceptions from the standard procedure for changes are meant here.

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 (service organisation) can access and monitor the agreed services and security requirements.

SSO-01 Policies and Procedures for Controlling and Monitoring Service Organisations

Basic Criteria

SSO-01.01B

Policies and procedures for controlling and monitoring service organisations 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:

1. Requirements for the assessment of risks resulting from the procurement of third-party services;
2. 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;
3. Information security requirements for the processing, storage or transmission of information by service organisations based on the established rules of technology, and under consideration of the criteria in this catalogue;
4. Information security awareness and training requirements for personnel;
5. Applicable legal and regulatory requirements;
6. Requirements for dealing with vulnerabilities, security incidents and incidents;
7. Specifications for the contractual agreement of these requirements;
8. Specifications for the monitoring of these requirements; and
9. 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 procedures 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:

1. 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 service organisation;
2. Impact of a protection breach on the provision of the cloud service;
3. 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;
4. Complementary subservice organisation controls (CSOCs) assumed in the design of cloud service provider's controls to meet the applicable C5 criteria;
5. 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;
6. The ability of the cloud service provider to diversify sources of supply and limit vendor lock-in;
7. Whether service organisations used by the cloud service provider themselves use subcontracted service organisations (subcontractors) that contribute to the development and operation of the cloud service; and
8. If service organisations used by the cloud service provider themselves use subcontractors, the types of data processed by the subcontractors.

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)

–

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 this subcriterion, such a risk assessment should take into account technical and, where relevant, non-technical risk factors.

Information on CSOC has to be obtained for subservice organisations only. Not every service organisation is a subservice organisation, cf. section 'Consideration of Subservice Organisations').

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 for the operation of the cloud service, it does not allow those suppliers or service organisations to access any cloud service customer data, cloud service derived data or account data. Exceptions are made only if the cloud service provider has performed a risk assessment according to OIS-07 on the possibility of cloud service customer data, cloud service derived data or account data being exposed.

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 pre-authorisation between the cloud service provider and the customer.

Additional (Sharpening)

SSO-03.01AS, sharpening SSO-03.01B

If the cloud service provider relies on assets from a supplier or on services from subservice organisations for the operation of the cloud service, it does not allow those suppliers or service organisations to access any cloud service customer data, cloud service derived data or account data. Exceptions are made only if the cloud service provider has performed a risk assessment according to OIS-07 on the possibility of cloud service customer data, cloud service derived data or account data being exposed, and it is ensured that all operations requiring access to those data types are performed or supervised by authorised personnel (cf. HR-01).

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: SSO-03.02B

This subcriterion does not apply to cloud service derived data that does not contain any customer-owned data. Examples for such cloud service derived data include operational metrics or technical telemetry data.

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 that contribute services to the delivery of the cloud service. The following information is maintained in the directory:

1. Company name;
2. Address of the head office;
3. Applicable legal jurisdiction;
4. Locations where cloud service customer data, cloud service derived data, cloud service provider data and account data is processed and stored;
5. Responsible contact group/person at the service organisation;
6. Responsible contact group/person at the cloud service provider;
7. Description of the service;
8. Classification based on the risk assessment;
9. Beginning of service usage; and
10. 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 procedures 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:

1. Reports on the quality of the service provided;
2. Certificates of the management systems' compliance with international standards;
3. Records of the service organisations on the handling of vulnerabilities, security incidents and incidents;
4. Independent third party reports on the design and operation of their service-related system of internal control; and
5. If service organisations used by the cloud service provider themselves use subcontractors, the compliance of their subcontractors with relevant contractual, legal and regulatory requirements.

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 cloud service provider assesses this relationship and carries out appropriate procedures to ensure that the applicable C5 criteria are met. Appropriate procedures provide reasonable assurance:

1. That the subservice organisation has designed and operated relevant controls; and
2. That the subservice organisation's controls correspond to the expected complementary subservice organisation controls (CSOCs) assumed in the design of the cloud service providers controls.

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

If a service organisation contributing to the provision of the cloud service undergoes a change that has a significant adverse effect on the cloud service provider's level of security, the cloud service provider communicates this to 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 service organisations 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:

1. Configuration of system components;
2. Performance and availability of system components;
3. Response time to incidents and security incidents; and
4. 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 service organisations. The nature and scope of these security assessments correspond to the risk associated with each service organisation. These risk-based security assessments ensure that service organisations 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, ANSSI SecNumCloud or CSA CCM. Second party audits based on such frameworks may be useful here. For analysing BSI C5 reports in a structured manner, BSI has published an Excel-based evaluation guideline.

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:

1. The scope and the validity respectively the period covered by the report;
2. Modifications of the opinion, deviations/exceptions noted and management's response thereon;
3. Complementary User Entity Controls (CUEC) to be designed and operated by the cloud service provider;
4. Disclosed subservice organisations incl. any changes among those (e.g. additional subservice organisations); and
5. Stated security incidents.

Information on CSOC has to be obtained for subservice organisations only. Not every service organisation is a subservice organisation, cf. 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.

Applicable to: SSO-05.02B

When reviewing the information provided by the service organisation, the cloud service provider should distinguish between flawed information that was produced in good faith (such as reports about perceived security concerns that eventually turned out to be ill-founded), and deliberately false or malicious information.

Monitoring of subcontractors can occur via audits, certifications and third party reports (cf. SSO-05) and may be performed by the service organisations of the cloud service provider. The cloud service provider remains responsible for reviewing the results of compliance monitoring and assessing the risk.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure with 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 protection need 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:

1. Analysis of the potential costs, impacts, resources and timing of the transition of a purchased service to an alternative service organisation;
2. Definition and allocation of roles, responsibilities and sufficient resources to perform the activities for a transition;
3. Definition of success criteria for the transition; and
4. 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:

1. Provides the cloud service from data centres operated by service organisations; or
2. 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:

1. It is unique on the market and no other service organisation can deliver it;
2. It is strongly individualised by the service organisation and/or the cloud service provider;
3. It cannot be supplied by any other service organisation in the required quality of service; or
4. It requires specific knowledge that is only/mainly available to the current service organisation and not to the cloud service provider.

Exit strategies may vary in complexity based on the nature and degree of dependency of the cloud service on third party services and service organisations. Using a cloud service broker is an example of a complex scenario. Aspects listed in SSO-06.02B should be considered based on the results of the cloud service provider's risk assessment. Where a lower degree of dependency has been identified, exit strategies or individual aspects thereof are not mandatory in the sense of this criterion.

Supplementary Information - Complementary Customer Criteria

–

SSO-07 Ensuring Transparency within Service Organisations

Basic Criteria

SSO-07.01B

The cloud service provider designs, implements and maintains controls to ensure transparency within its service organisations with respect to the following aspects:

1. Data flow and interfaces between the cloud service provider and service organisations used by the cloud service provider are documented, including measures regarding the secure transmission and access control for data shared with service organisations; and
2. Cloud service customers are informed of service organisations used by the cloud service provider for development and operation of the cloud service and what type of data these service organisations and their subcontractors are processing.

Cloud service customers are informed which of the service organisations themselves use subcontractors to process cloud service customer data.

SSO-07.02B

The cloud service provider documents this information and reviews its completeness, accuracy and validity at least annually.

Additional (Sharpening)

SSO-07.01AS, sharpening SSO-07.01B

The cloud service provider designs, implements and maintains controls to ensure transparency within its service organisations with respect to the following aspects:

1. Data flow and interfaces between the cloud service provider and service organisations used by the cloud service provider are documented, including measures regarding the secure transmission and access control for data shared with service organisations; and
2. Cloud service customers are informed of service organisations and their subcontractors used by the cloud service provider for development and operation of the cloud service and what type of data these service organisations and their subcontractors are processing.

Cloud service customers are informed which of the service organisations themselves use subcontractors to process cloud service customer data.

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: SSO-07.01B

This criterion addresses the need for managing supply chain risks (e.g. service organisation vulnerabilities, data handling practices, compliance gaps or operational disruptions) and for those risks to be communicated to cloud service customers, enabling them to monitor and manage their own supply chain risks effectively.

Supplementary Information - Complementary Customer Criteria

–

SSO-08 Controlling Exchanges with Suppliers of Functional Components

Basic Criteria

SSO-08.01B

When functional components used for the provision of the cloud service may directly or indirectly access cloud service customer data, the cloud service provider defines and implements a policy according to SP-01 that does not allow a direct exchange between such components and their suppliers.

SSO-08.02B

In addition, procedures are defined and implemented according to SP-01 that require the cloud service provider to authorise any content provided by a supplier for its functional components or to be sent from a functional component to its supplier. The authorisation takes place before the content is transferred and for each transfer.

SSO-08.03B

When a procedure for authorising content before its transfer is automated, the cloud service provider implements it using a solution that maintains traces of:

1. The operations that are proposed by the functional component's supplier;
2. The verification that is performed to authorise the content before its transfer; and
3. The transfers, both incoming and outgoing, that are effectively performed.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

Applicable to: SSO-08.01B, SSO-08.02B, SSO-08.03B

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, procedures and technical 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 Security Incident Response Team' (CSIRT), 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.

SIM-01.04B

There are procedures as to how the data of a suspicious system can be collected in a conclusive manner in the event of a security incident.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure with 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

Applicable to: SIM-02.01B

Relevant stakeholders in the sense of this criterion are those that need to know the incident response plan, for example due to their involvement in its execution or due to contractual or regulatory agreements.

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

The results of these root-cause analyses are documented, shared with relevant stakeholders, and used as part of evaluation and learning processes.

SIM-03.03B

If the cloud service provider determines that it requires external assistance for processing a security incident, it selects an incident response service based on their competence and trustworthiness or by following the recommendations of a national cybersecurity authority.

SIM-03.04B

A catalogue providing clear identification of information security incidents affecting cloud service customer data is maintained and used for the classification of information security incidents.

SIM-03.05B

The cloud service provider also uses the incident classification mechanism for the correlation of information security events, and assesses as well as classifies the correlated information security events according to their criticality.

SIM-03.06B

All documents and evidence that provide details on security incidents related to the cloud service are archived in a secure and tamper-proof manner, in line with criticality and regulatory requirements.

SIM-03.07B

The analysis process provides sufficient traceability to understand root causes and attack progression, appropriate to the risk and impact of the 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

An integrated team of forensic/incident responder personnel, specifically qualified to preserve evidence and manage a chain of custody, is established or contracted for their services.

SIM-03.03AC

The cloud service provider verifies the application of incident management policies and procedures by monitoring the information security incident handling processes. Timely and appropriate remediation measures address any deviations identified during monitoring.

Supplementary Information

About the Criteria

Applicable to: SIM-03.06B

Regulatory requirements may necessitate maintaining a chain of custody to ensure that documents can be relied upon in legal proceedings.

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 documentation is sent to the affected customers for final acknowledgement or, if applicable, as confirmation.

SIM-04.02B

Information on security incidents or confirmed security breaches is made available to all affected customers.

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

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

Applicable to: SIM-04.02B

Security breaches in the sense of this criterion are security incidents caused by unauthorised access and compromise of cloud service customer data or service delivery as a result of violations of policies and procedures or applicable legal and regulatory requirements (cf. HR-04.02B)

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure with 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 timely forwarded to the entity responsible for handling them so that an appropriate response can be made.

SIM-05 Duty of the Personnel to Report Security Incidents to a Central Body

Basic Criteria

SIM-05.01B

The cloud service provider informs personnel and external business partners of their obligations. If necessary, they agree to or are contractually obliged to timely 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.

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 information security incident reporting mechanisms are communicated to personnel, cloud service customers and service organisations of the cloud service provider.

Additional (Sharpening)

–

Additional (Complementing)

–

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure with suitable controls that identified security events, which the cloud service provider is required to process, are communicated timely 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 supporting bodies.

SIM-06.02B

The cloud service provider defines, implements and maintains a knowledge repository containing:

- Security incidents;
- Measures taken for the solution of these security incidents; and
- Information about the assets affected by these security incidents.

This information is used to supplement the classification catalogue of incidents (cf. SIM-03).

SIM-06.03B

The information obtained from the security incident monitoring and the intelligence gathered in the knowledge repository is used to identify recurring security events or security incidents, or potential significant security incidents, to determine the need for advanced safeguards, and for implementing them.

SIM-06.04B

The evaluation and learning process includes the results of root-cause analyses conducted in accordance with SIM-03.

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 with 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 procedures for the cloud service's business continuity management, including strategy and guidelines, business impact analyses, and business continuity plans, are documented, communicated, and made available in accordance with SP-01 regarding the following aspects:

1. Goals of the BCM;
2. Roles and responsibilities, management commitment;
3. Scoping of the BCM, identifying relevant business processes;
4. Interfaces, in particular to Incident Management;
5. Communication with relevant entities and competent authorities;
6. Methodology;
7. Consideration of Risk;
8. Business Impact Analysis (BIA);
9. Business Continuity Plan (BCP);
10. Resource Planning (usually part of the BCP);
11. Testing of Business Continuity Plans and regular updates to BCM documentation; and
12. Continuous improvement of the Business Continuity Management.

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 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 personnel to actively contribute to the effectiveness of continuity and emergency management.

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.

Applicable to: BCM-01.02B

Please note: BCM can be integrated into enterprise risk management (ERM) to gain more efficiency and overcome management silos.

Applicable to: BCM-01.03B

The top management responsibility can be delegated from top management to another individual as long this individual has the scope, responsibilities and capabilities to influence the cloud-service-wide business continuity strategy and activities just as the top management could do.

Supplementary Information - Complementary Customer Criteria

–

BCM-02 Business Impact Analysis

Basic Criteria

BCM-02.01B

The cloud service provider performs a Business Impact Analysis (BIA). In this BIA, 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 procedures with at least the following aspects:

1. Possible scenarios based on a risk assessment that includes cybersecurity risks;
2. Identification of critical products and services;
3. Identification of dependencies, including processes (including resources required), applications, business partners and third parties;

4. Capturing threats to critical products and services;
5. Identification of effects resulting from planned and unplanned outages, service degradations and changes over time;
6. Determination of the maximum tolerable period of downtime and service degregation;
7. Identification of restoration priorities;
8. Determination of time targets for the resumption of critical products and services within the maximum acceptable time period (i.e. RTO);
9. 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
10. Estimation of the resources needed for resumption.

BCM-02.02B

The business impact analysis adheres to the applicable policies and procedures and 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 with 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 procedures.

Business continuity plans take the following aspects into account:

1. Defined purpose and scope with consideration of the relevant dependencies;
2. Accessibility and comprehensibility of the plans for persons who are to act accordingly;
3. Ownership by at least one designated person responsible for review, updating and approval;
4. Defined communication channels, roles and responsibilities including notification of the customer;
5. Recovery procedures, manual interim solutions and reference information (taking into account prioritisation in the recovery of cloud hardware objects and services and alignment with customers);
6. Methods for putting the plans into effect;
7. Continuous process improvement;
8. Consistency over all locations, zones, regions and partitions; and
9. 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 with 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 with 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 time frame for the operations as well as a description of the work to be carried out.

BCM-04.03AC

The cloud service provider provides cloud service customers an assessment of the potential impacts of those tests and excercises 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 and notification 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.:

1. Test of technical precautionary safeguards;
2. Functional tests; and
3. Plan review.

Exercises also take place on a tactical and strategic level. These include e.g.:

1. Plan meeting;
2. Personnel exercise;
3. Command post exercise;
4. Communication and alerting exercise;
5. Simulation of scenarios; and
6. 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). A cloud service customer is affected (in the sense of this criterion) if the test or excercise leads to a service downgrade outside of the level defined in the SLA or if the effectiveness of the plans can only be tested if the cloud service customer has to take action.

Applicable to: BCM-04.04AC

The term 'alarm and notification plan' refers to the documented procedure for alerting responsible personnel and stakeholders in case of incidents or disruptions.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure with 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 with 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.

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 of the procedures described in the basic criterion upon request by the 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:

1. Requirements for the protection of personal data (e.g. EU General Data Protection Regulation);
2. Requirements regarding the information security posture of the cloud service provider (e.g. NIS 2 Directive, BSIG as applicable to KRITIS);
3. Compliance requirements based on contractual obligations with cloud service customers (e.g. ISO/IEC 27001, SOC 2, PCI-DSS); and
4. Requirements regarding exchange and use of data (e.g. EU Data Act).

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 multiple years that defines the scope and the frequency of the audits. The audit programme takes into consideration the management of change, policies, and the results of the risk assessment (cf. OIS-07).

COM-02.02B

Risk-based policies and procedures for planning and conducting audits are documented, communicated and made available in accordance with SP-01 and address the following aspects in order to prevent adversal effects on the operation of the cloud service from the audit:

1. Restriction to read-only access to system components in accordance with the agreed audit plan and as necessary to perform the activities;
2. Activities that may result in outages, degradations of the cloud service or breaches of contractual requirements are performed during scheduled maintenance windows or outside peak periods;
3. Logging and monitoring of activities;
4. Review of server and network equipment configurations under the responsibility of the cloud service provider;
5. Intrusion testing for external access points; and
6. Source code reviews of internally developed security features.

Additional (Sharpening)

COM-02.01AS, sharpening 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. The audit programme takes into consideration the management of change, policies, and the results of the risk assessment (cf. OIS-07).

Additional (Complementing)

COM-02.01AC

The cloud service provider grants its cloud service customers contractually agreed 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, COM-02.01AS

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. The audit programme may, for example, comprise a time frame of three years, and 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.

Applicable to: COM-02.02B

See DEV-05 for further explanation on security features.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure with suitable controls that appropriate responses are made to outages or degradations of the cloud service through such audits.

To the extent that contractually agreed information and audit rights exist, the cloud service customers ensure with 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:

1. Compliance with the policies and procedures (cf. SP-01) within their scope of responsibility (cf. OIS-01); and
2. 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 as well as non-conformities from the applicable legal, regulatory, self-imposed and contractual requirements relevant to the information security of the cloud service, are subjected to a risk assessment in accordance with the risk management procedure (cf. OIS-07). Follow-up measures are defined and tracked (cf. OPS-18).

Additional (Sharpening)

–

Additional (Complementing)

COM-03.01AC

Based on a risk assessment (cf. OIS-07) and technical feasibility, the cloud service provider decides to which extent internal audits are supplemented by procedures to automatically monitor applicable requirements of policies and procedures with regard to the following aspects:

1. Configuration of system components to provide the cloud service within the cloud service provider's area of responsibility;
2. Performance and availability of these system components;
3. Response time to incidents and security incidents; and
4. 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, cf. 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 programme. When establishing the internal audit programme(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 procedures (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 is 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.

COM-04.02AC

The responsible business units of the cloud service provider report at least annually to the top management on the the status and effectiveness of the policies and procedures that are relevant to the top management review of the information security management system. This reporting includes at least:

1. Implemented changes to address cybersecurity risks for the topic addressed in the policy or procedure;
2. Information security incidents for the topic addressed in the policy or procedure and the follow-up;
3. Performance of the internal controls regarding information security for the topic addressed in the policy or procedure; and
4. Planned changes for the topic addressed in the policy or procedure to address cybersecurity risks and information security and cybersecurity.

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 Investigation 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.

INQ-01.02B

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-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.

Applicable to: INQ-01.02B

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-03, 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

Cloud service customers ensure with suitable controls that the type and scope of government agen-

cies' 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, unless the applicable legal basis, on which the government agency's request is based, prohibits this or there are clear indications of illegal actions 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 with suitable controls that such notifications are received and assessed from a legal perspective according to their own specifications and possibilities.

INQ-03 Limiting Access to or Disclosure of Data in Investigation Requests

Basic Criteria

INQ-03.01B

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-03.02B

If no clear limitation of the cloud service customer data and cloud service derived data is possible, the cloud service provider anonymises or pseudonymises this 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-03.01AC

The access and activities performed by or on behalf of investigators are monitored by the cloud service provider as determined by the process described in INQ-01.

INQ-03.02AC

Timely and appropriate remediation measures address any deviations identified during the monitoring of the activities performed by or on behalf of investigators.

Supplementary Information

About the Criteria

–

Supplementary Information - Complementary Customer Criteria

–

INQ-04 Communication of Technical Procedures for Data Disclosure in Investigation Requests

Basic Criteria

INQ-04.01B

The cloud service provider documents the technical procedures per service and other technical information regarding the provision or disclosure of cloud service customer data in response to valid investigation requests and provides it to cloud service customers.

INQ-04.02B

The type and scope of the information provided to the cloud service customers is based on the needs of their expert personnel to assess risks to the cloud service customer's data confidentiality. At a minimum, the following aspects are addressed:

1. The process for the provision and disclosure of cloud service customer data in response to legitimate investigation requests;
2. The technical capabilities and limitations of the cloud service provider regarding disclosure of cloud service customer data;
3. Logging mechanisms implemented to records access for disclosure of cloud service customer data;
4. Access possibilities for cloud service customers to review such logs;

5. Methods and technical procedures per service for accessing and disclosing cloud service customer data; and
6. 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-04.03B

The aforementioned 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-04.01B, INQ-04.02B, INQ-04.03B

The criterion is limited to cloud service customer data. The cloud service provider typically has 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:

1. If the cloud service customers store their cloud service customer data in unencrypted form;
2. If the cloud service provider encrypts cloud service customer data in storage and transit;
3. 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;
4. Retention periods for cloud service derived data relating to the cloud service customer and whether such data is stored in encrypted form;
5. Possibilities for decrypting cloud service customer data or for extracting cloud service customer data during the decryption process;
6. Disclosure of user identities and credentials; and
7. 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 with suitable controls that they minimise potential disclosure of their customer data. According to the protection need of the cloud service customer data, the cloud

service customers take the decision if the particular cloud service can be used or if the risk of disclosure is too 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 publishes guidelines and recommendations for cloud service customers regarding the secure use of the cloud service provided. The information contained therein is intended to assist the cloud service customer in the secure configuration 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 service customer.

PSS-01.02B

The type and scope of the information in the guidelines and recommendations for the secure use of the cloud service 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:

1. Procedures for secure configuration;
2. Information sources on known vulnerabilities and update mechanisms;
3. Malware protection for containers or virtual machines;
4. Error handling and logging mechanisms;
5. Authentication mechanisms;
6. Roles and rights framework including combinations that result in an elevated risk;
7. Services and functions for administration of the cloud service by privileged users;
8. Complementary user entity controls;
9. Encryption mechanisms and services;
10. Data leakage prevention;
11. Secure application development and operation on the cloud service;
12. Instructions for using and configuring defensive mechanisms;
13. Instructions for using and configuring wide-area distributed architecture mechanisms;
14. Methods used for client data separation (cf. OPS-30 and OPS-31);
15. How information security risks related to the use of the cloud service can be addressed through proper logging and monitoring mechanisms; and
16. Inbound and outbound interfaces through which the cloud service can be accessed by other cloud services or IT systems of cloud service customers (cf. PI-01).

PSS-01.03B

The cloud service provider describes in the user documentation all necessary complementary user entity controls (CUECs) and corresponding explanations of them, so that the cloud service customer has sufficient information for appropriate risk management on its side.

PSS-01.04B

The above-mentioned 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 notifies cloud service customers in a timely manner about any planned modifications to the cloud service so that the affected cloud service customers can react appropriately with organisational and technical measures before the changes take effect.

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 fault tolerance through replication, avoidance of localised outages and disasters through the use of multiple cloud regions, as well as the reduction of user-facing latency through the geo-dispersion of service endpoints.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure with suitable controls that the cloud service provider's information is used to derive policies, frameworks and measures for the secure configuration and use (according to their own risk assessment) of the cloud service. Compliance with these policies, frameworks and measures is checked. Changes to the information are timely 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:

1. Static Application Security Testing;
2. Dynamic Application Security Testing;
3. Code reviews by the cloud service provider's subject matter experts;
4. Conducting security checks based on a list of software components or Software Bill of Materials (SBOM); and
5. 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, Incidents 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 through a coordinated process that cloud service customers have access to regularly updated information about known vulnerabilities associated with the cloud service that may impact the information security of the customer. This includes:

1. Known-exploited vulnerabilities;
2. 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
3. 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 information provided to the cloud service customers includes, where available, a description of applicable and planned remediation or mitigation measures for the identified vulnerabilities.

PSS-03.03B

These vulnerabilities are also identified based on data from a list of software components or 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:

1. The Common Vulnerability Scoring System (CVSS); and
2. The Exploit Prediction Scoring System (EPSS), the Stakeholder-Specific Vulnerability Categorization (SSVC) or other similar scoring metrics

in the latest version valid at the time of the assessment.

This information is accessible to all cloud customers and supports their risk assessment and follow-up actions, with references to vulnerability-specific measures where applicable.

PSS-03.05B

The cloud service provider consults the vulnerability information of its suppliers and service organisations at least daily. The published vulnerabilities are analysed in regards to their potential impact on the cloud service, and handled in accordance with the vulnerability handling process (cf. OPS-18). If the supplier or service organisation does not provide daily information, the related risk is managed according to OIS-07.

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-03.01B

This criterion supports transparency in vulnerability management. It requires the cloud service provider to proactively inform customers about vulnerabilities that may pose a residual risk due to the absence of remediation options. Such disclosures help customers assess their exposure and implement compensating controls where necessary.

Information about known-exploited vulnerabilities and known vulnerabilities can include, for example, the information about vulnerabilities in authorisation mechanisms obtained from the validation process carried out as part of PSS-09.

Applicable to: PSS-03.03B

Although the cloud service provider has to identify the vulnerabilities based on SBOM data to fulfil this criterion, this SBOM data need not be handed over to the customer to fulfil the criterion.

Applicable to: PSS-03.04B

Vulnerability-specific measures can for instance be found in the 'Vulnerability, Exploitability eXchange' (VEX) or the 'Common Security Advisory Frameworks' (CSAF).

The Common Vulnerability Scoring System (CVSS) assesses the severity of identified vulnerabilities (cf. OPS-18). The Exploit Prediction Scoring System (EPSS), the Stakeholder-Specific Vulnerability Categorization (SSVC) and other similar scoring metrics prioritise measures to be implemented for

remediating or mitigating identified vulnerabilities. Both kinds of systems should be used in tandem.

Applicable to: PSS-03.05B

There can be various ways to obtain information about vulnerabilities from suppliers and service organisations. The criteria does not demand a particular way for obtaining this information but that the information is obtained at least daily.

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 with suitable controls that the obtained vulnerability information is incorporated timely 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 service customers 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 service customers to check the following aspects, insofar as they are applicable to the cloud service:

1. Which cloud service customer data and cloud service derived data, services or functions available to the cloud service customer within the cloud service, have been accessed by whom, when and from where (Audit Logs);
2. Malfunctions during processing of automatic or manual actions; and

3. 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

Where applicable, the cloud service customer can activate or de-activate the logging and can control the scope and verbosity of the logging the cloud service provides.

PSS-04.06B

The logging of management plane actions by the cloud service customers covers all relevant systems and system components.

Additional (Sharpening)

–

Additional (Complementing)

PSS-04.01AC

Cloud service customers 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-04.06B, 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 strictly to system components under the responsibility of the cloud service customer only. The extent of the logging depends on the cloud service. There may therefore be cloud services, such as SaaS services for which the amount of system components under the responsibility of the cloud service customer is very limited, to which this criterion is not applicable.

Applicable to: PSS-04.04B

The deletion of the logged information by the cloud service customer can, for example, be implemented by providing the cloud service customer with a process to request this deletion.

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 provided is equipped with authentication mechanisms that can force multi-factor authentication for users, IT components or applications within the cloud service customers' 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 under the responsibility of the cloud service customer, these authentication mechanisms can be enforced by the cloud service customer.

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 should be enforced and can e.g. be performed with cryptographic certificates, smart cards or tokens.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure with suitable controls that the authentication mechanisms offered by the cloud service are used in accordance with the customer's identity and authorisation management requirements. If cloud service customers operate virtual machines or containers with

the cloud service, they ensure with suitable controls that the authentication mechanisms cover container-specific scenarios, such as multi-factor authentication for container hosts and registry access.

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 established rules of technology 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, the cloud service provider provides the cloud service customers with the following procedures to protect the confidentiality of the passwords:

1. 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;
2. When creating passwords, compliance with the length and complexity requirements of the cloud service provider (cf. IAM-08) or the cloud service customer is technically enforced;
3. The user is informed about changing or resetting the password. Password reset procedures are valid for at most 48 hours. After the reset procedure has been used, the password is to be changed by the user; and
4. The server-side storage uses hash functions in combination with salt values, both corresponding to the state of the art.

PSS-07.02B

Rules and recommendations are shared with the cloud service customers as applicable to the users under their responsibility. The cloud service provider offers the cloud service customers tools for the management and enforcement of these rules.

PSS-07.03B

When distributing credentials, the cloud service provider verifies the recipient's identity, validates the request and protects the credentials by using additional security mechanisms such as multi-factor authentication.

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 with suitable controls that they use sufficiently secure passwords (cf. IAM-08) and employ the procedures provided by the cloud service provider to protect the confidentiality of the passwords according to their own assessment, and that the risks of unauthorised access associated with their own choice are borne. If cloud service customers operate virtual machines or containers with the cloud service, they ensure with suitable controls that the confidentiality of the information is also ensured for the allocation of authentication information of the virtual machines or containers.

PSS-08 Roles and Rights Framework

Basic Criteria

PSS-08.01B

The cloud service provided comprises a roles and rights framework for users of the cloud service customer. This framework allows users to manage their own access rights. It describes access rights and roles for the functions provided by the cloud service. Cloud service customers can configure relevant access control parameters themselves.

PSS-08.02B

The access rights and roles are suitable for enabling users of the cloud service customer 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 ('segregation of duties').

PSS-08.03B

The cloud service provided is equipped with a functionality to help cloud service customers review user access rights under their responsibility.

PSS-08.04B

In case the cloud service includes the management of customer identities, for a given customer identity, the cloud service provided is equipped with a functionality 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 framework would describe, among other things, the access rights and roles for the following functions of the cloud service:

1. Administration of the states of virtual machines (start, pause, stop) as well as for their migration or monitoring;
2. Management of available images that can be used to create virtual machines; and
3. Management of virtual networks (e.g. configuration of virtual routers and switches).

Applicable to: PSS-08.03B

This functionality can e.g. include gaining a list of all roles and accesses the cloud service customer has activated and when they were changed the last time.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure with suitable controls that:

1. They actively utilise the roles and rights framework and accompanying functionalities offered by the cloud service provider;
2. The granting of permissions to users in their area of responsibility is subject to authorisation; and
3. 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. personnel 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 service customers and in the event of changes to the authorisation mechanisms of existing functions (cf. DEV-07).

PSS-09.03B

If validation activities reveal vulnerabilities, the procedures for identifying vulnerabilities (cf. PSS-02) are applied and measures for timely remediation or mitigation are initiated.

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 with 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 service customers 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 with 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 provided is equipped with functionalities that ensure the following aspects:

1. 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;
2. 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;
3. Images provided by the cloud service provider are labelled with information regarding their origin; and
4. Images provided by the cloud service provider are hardened according to generally accepted industry standards.

Additional (Sharpening)

–

Additional (Complementing)

PSS-11.01AC

The cloud service provider checks the integrity and authenticity of virtual machines or container images at startup and informs the cloud service customer accordingly about the results of those checks.

PSS-11.02AC

During runtime, the cloud service provider protects the virtual machines or container images against tampering and informs the cloud service customer accordingly about the status during runtime.

Supplementary Information

About the Criteria

Applicable to: PSS-11.01B

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.

Applicable to: PSS-11.01AC

Typical measures for checking virtual machines or container images against integrity and authenticity include cryptographical signing.

Supplementary Information - Complementary Customer Criteria

Cloud service customers ensure with 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 regions.

PSS-12.02B

Processing and storage of cloud service customer 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 in which the aforementioned data is processed or stored. 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 architecture of the cloud service, including the technical design of its infrastructure, ensures that the cloud service customer data, cloud service derived 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 regions.

PSS-12.02AS, sharpening PSS-12.02B

Processing and storage of cloud service customer data and cloud service derived data within the service organisations of the cloud service provider also adheres to the regions selected by the cloud service customer.

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:

1. Privileged access to the production environment by the cloud service provider, including potential access to cloud service customer data and cloud service derived data;
2. 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; and
3. 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.

Supplementary Information

About the Criteria

Applicable to: PSS-12.03B

This criterion refers to the architecture of the cloud service and does not put any constraints on the architecture the cloud service customer designs.

If a cloud service provider has several regions that provide the same service, the cloud service customer is free to use the service in different regions (e.g. for more resilience).

This subcriterion refers to contractual agreements which include the pledge for cloud service customer data, cloud service derived data, cloud service provider data and account data to reside in the chosen region. It also covers how contractual agreements are updated, ensuring transparent communication and continued residency for all four types of data in the agreed region(s).

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 General Condition GC-01. It does not require the cloud service provider to offer multiple regions or 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 as-

surance 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.

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 - Complementary Customer Criteria

Cloud service customers ensure with 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:
Federal Office for Information Security (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:
2026

Content and editing:
Federal Office for Information Security (BSI)

This brochure is part of the Federal Office for Information Security's public relations work.
It is provided free of charge and is not intended for sale.