Federal Office
for Information Security

Criteria enabling Cloud Computing Autonomy (C3A)

Federal Office for Information Security (BSI)

Document history

Version	*Date*	*Editor*	*Description*
v1.0	27.04.2026		

Table 1 Document history

Federal Office for Information Security
P.O. Box 20 03 63
53133 Bonn
E-Mail: cloudsecurity@bsi.bund.de
Internet: https://www.bsi.bund.de

Table of Contents

1 Introduction

1.1 Cloud Computing and digital sovereignty

Digital sovereignty describes the abilities and opportunities of individuals and institutions to perform their role(s) in the digital world independently, self-determinedly (autonomous) and securely.

The decision to use cloud services is based on the shared responsibility model, which means that responsibility is shared between the cloud service provider and the cloud service customer. This model inherently limits the scope of decisions that the cloud service customer is able to take, including those that impact the customer's digital sovereignty. Cloud service providers can enable their cloud service customers to maintain the desired degree of self-determination in various ways — or not. To ensure transparency and enable cloud service customers to make risk-based decisions in this context, there is a need for generally recognized, objective, and verifiable criteria for self-determination i.e. autonomy.

C3A - Criteria enabling Cloud Computing Autonomy provide a set of criteria for assessing whether a given set of cloud services allows for self-determined use within its respective risk context. C3A are a guiding framework and are intended to increase transparency. The C3A Framework is not binding in itself.

1.2 EU Cloud Sovereignty Framework and BSI C5:2026 as the C3A foundation

C3A adopt the structure (categorization) and objectives of the European Union's Cloud Sovereignty Framework (EU CSF). In addition, the contributing factors of the EU CSF are reflected in the verifiable criteria of the C3A, but are expanded to include further aspects.

Two areas of the EU CSF are intentionally not covered by the C3A: SOV-7 Security & Compliance Sovereignty is already covered by established BSI publications like C5:2026, IT-Grundschutz or the HA Benchmark compact. The aspects of SOV-8 Environmental Sustainability are not part of the area of BSI's responsibility.

C3A presupposes that the cloud service provider meets the C5 criteria, as they reflect the security aspect of the sovereignty definition. The C5:2026 also includes criteria covering aspects in the overlap of autonomy and security.

1.3 Structure

C3A criteria are divided into criteria and additional criteria. Supplementary information is provided for some of the criteria. Depending on the use-case and the requirements of the cloud service customer, it can be determined which criteria and which additional criteria apply.

Criterion: These criteria help to define concrete requirements for an autonomous use of cloud services. The set of criteria help to improve transparency and measure self-determination of cloud services.

Additional Criterion**:** Additional criteria raise the bar on existing requirements or expand the scope of autonomy. It is up to the cloud service customers to request an additional criterion according to their digital sovereignty needs.

Supplementary Information: Additional information on the criteria e.g. the scope, exceptions or external references.

1.4 Terms of Use

C3A can be used by cloud service providers as well as cloud service customers:

- A cloud service provider can demonstrate compliance with criteria by providing evidence. To do so, the cloud service provider should select which criteria apply to the respective set of cloud services and then provide the relevant evidence through an audit.
- A cloud service customer can use the framework to identify criteria within the various domains that he considers relevant. By using the framework, cloud customers can define their baseline level of sovereignty in the context of cloud computing and, for the audited services, assess the fulfilment of the criteria identified as important.

1.5 Definitions

In the following, definitions are provided for key terms used in this document. The definitions are derived from the BSI's IT-Grundschutz-Kompendium and the international standard ISO/IEC 22123:2023 (Information Technology - Cloud Computing - Part 1: Vocabulary):

Account data

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

Authenticity

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

Availability

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

Cloud computing

Paradigm for enabling network access to a scalable and elastic pool of shared physical or virtual resources with self-service provisioning and administration on-demand. Examples of resources include servers, operating systems, networks, software, applications, and storage equipment. Self-service provisioning refers to the provisioning of resources provided to cloud services performed by cloud service customers through automated means. The acronym cloud is synonymous with cloud computing and will also be used in the C3A.

Cloud service

Information technology service offered via cloud computing. This includes infrastructure (e.g. computing power, storage space), platforms and software.

Cloud service provider

Natural or legal person providing a cloud service.

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 authorized users and their identities. It can also include any configuration or customization data, where the cloud service has such configuration and customization functionalities.

Cloud service provider data

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

Confidentiality

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

Integrity

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

2 Criteria, Additional Criteria and Supplementary Information

2.1 SOV-1 Strategic Sovereignty

2.1.1 SOV-1 Jurisdiction

SOV-1-01-C1 Criterion

The cloud service provider MUST operate under EU jurisdiction, with contract governance and dispute resolution.

SOV-1-01-C2 Criterion

The cloud service provider MUST operate under German jurisdiction, with contract governance and dispute resolution.

SOV-1-01-SI Supplementary information

If restrictions are imposed by cloud service customers for Germany, they should be justified, and it should be ensured that their implementation, for example, in procurement procedures, is legally permissible on the basis of reasons such as public safety.

2.1.2 SOV-1 Registered Office

SOV-1-02-C1 Criterion

The cloud service provider MUST have a registered head office in the EU.

SOV-1-02-C2 Criterion

The cloud service provider MUST have a registered head office in Germany.

SOV-1-02-SI Supplementary information

If the cloud service provider uses a subcontractor for the provision of services, such as operations, that subcontractor MUST also meet the criteria.

If restrictions are imposed by cloud service customers for EU or Germany, they should be justified, and it should be ensured that their implementation, for example, in procurement procedures, is legally permissible on the basis of reasons such as public safety.

2.1.3 SOV-1 CSP Effective Control

SOV-1-03-C1 Criterion

The cloud service provider MUST be effectively controlled by one or more EU corporations. The cloud service provider MUST ensure that effective controls are transparent to cloud service customers.

SOV-1-03-C2 Criterion

The cloud service provider MUST be under the effective control of one or more German undertakings. The cloud service provider MUST ensure that effective controls are transparent to cloud service customers.

SOV-1-03-SI Supplementary information

Effective control in this context means the possibility to exert direct or indirect influence, or determine the key strategic, financial, or operational decisions from non-EU undertakings.

If restrictions are imposed by cloud service customers for EU or Germany, they should be justified, and it should be ensured that their implementation, for example, in procurement procedures, is legally permissible on the basis of reasons such as public safety.

2.1.4 SOV-1 CSP Control Change

SOV-1-04-C Criterion

The cloud service provider MUST inform cloud service customers 90 days in advance of any actual changes affecting the cloud service provider's control that could undermine or affect the C3A controls associated with the cloud service, including significant changes to ownership, shareholding, or governance relationships of the cloud service provider.

2.2 SOV-2 Legal & Jurisdictional Sovereignty

2.2.1 SOV-2 Extraterritorial Exposure

SOV-2-01-C Criterion

The cloud service provider MUST identify, at least once a year, any non-EU law relating directly to the provided cloud services that have cross-border implications for the availability of cloud services and the confidentiality and integrity of customer created data. They MUST also carry out a structured risk assessment to evaluate the risks arising from these laws.

2.2.2 SOV-2 Audit Rights

SOV-2-02-C1 Criterion

The cloud service provider MUST document procedures that allow the relevant federal or national cybersecurity authority to verify compliance with the C3A criteria by an audit. The responsible authority is the one in the country where the data center is located.

SOV-2-02-C2 Criterion

The cloud service provider MUST document procedures that allow the German federal administration to verify compliance with the C3A criteria by an audit.

SOV-2-02-SI Supplementary information

The audit rights may be derived from a contract or law that explicitly reserves the right for the federal or national authority to conduct audits. If possible, the authority tries to make use of existing audits (e.g., BSI C5, SOC 2 Type 2) before carrying out an audit.

Any audit shall be conducted in accordance with the cloud service provider's strict security and confidentiality protocols, including defined notice periods, to protect the data of other tenants and the integrity of the data centre. While costs are a commercial matter, the right to audit is a regulatory mandate. Fees shall not be so high as to effectively deny this right.

2.2.3 SOV-2 State of Defense Takeover

SOV-2-03-C1 Criterion

If an EU member state declares a state of defense, the cloud service provider MUST enable the EU member state to take over the capabilities required to operate the cloud, including the necessary physical assets and personnel, within the framework of legal possibilities.

SOV-2-03-C2 Criterion

If Germany declares a state of defense, the cloud service provider MUST enable the German federal administration to take over the capabilities required to operate the cloud, including the necessary material assets and personnel, within the framework of legal possibilities.

SOV-2-03-SI Supplementary information

This usually means that the cloud service provider has the documentation, source code and administration tools in a portable format so that a federal administration can use them.

2.3 SOV-3 Data Sovereignty

2.3.1 SOV-3 Data Residence

SOV-3-01-C1 Criterion

A cloud service customer MUST be able to check where their cloud service derived data, cloud service customer data, and account data are stored and processed.

SOV-3-01-C2 Criterion

The cloud service provider MUST provide a service option where cloud service derived data and account data are exclusively stored and processed in the EU.

SOV-3-01-C3 Criterion

The cloud service provider MUST provide a service option where cloud service customer data is exclusively stored and processed in the EU.

SOV-3-01-C4 Criterion

The cloud service provider MUST provide a service option where cloud service customer data is exclusively stored and processed in Germany.

SOV-3-01-C5 Criterion

The cloud service provider MUST provide a service option where cloud service provider data is exclusively stored and processed in the EU.

SOV-3-01-SI Supplementary information

If a cloud service provider operates in other locations/regions in addition to the EU or Germany, the location/region of processing and storing MUST be clearly identifiable for the cloud service customer.

2.3.2 SOV-3 External Key Management

SOV-3-02-C Criterion

The cloud service provider MUST allow the integration of external encryption key management system for creating, managing, and storing encryption keys outside of the cloud service provider environment for the use of IaaS and PaaS, or provide functionally equivalent mechanisms that ensure the customer can only create, manage and store the encryption keys only outside of the cloud service provider environment.

SOV-3-02-AC Additional criterion

The cloud service provider MUST allow the integration of external key management systems for creating, managing and storing keys outside of the cloud environment also for SaaS, or provide functionally equivalent mechanisms that ensure the customer can only create, manage and store the encryption keys outside of the cloud service provider environment.

SOV-3-02-SI Supplementary information

The integration of external key management systems for IaaS and PaaS is widely implemented and commonly standardized. For SaaS solutions, external encryption key management systems are less common; therefore, cloud service providers should support external encryption key management capabilities for SaaS where technically feasible and appropriate to the service architecture. If this criterion is only fulfilled for some SaaS, the cloud service provider MUST provide a list of these services to the cloud services customer.

2.3.3 SOV-3 External Identity Provider

SOV-3-03-C Criterion

The cloud service provider MUST support standards-based integration of external identity providers for authentication and access management for the cloud service.

SOV-3-03-AC1 Additional criterion

The integration of an external Identity Provider MUST be implemented via open, non-proprietary standards.

SOV-3-03-AC2 Additional criterion

The provider MUST support a stateless authentication model that does not mandate the creation and copies of accounts within the provider’s directory.

SOV-3-03-AC3 Additional criterion

Authorization MUST be controllable via dynamic claims and attributes issued directly by the customer's external identity provider.

2.3.4 SOV-3 Logging and Monitoring

SOV-3-04-C Criterion

The cloud service provider MUST provide customers with the capability to record, retain, and review logs of management and data access activities related to cloud service customer data. These logs MUST enable customers to identify when access occurred, the identity associated with the request, and the relevant operational context available through the service’s logging capabilities.

SOV-3-04-AC1 Additional criterion

The logging service MUST ensure full data flow transparency by providing real-time access via standardized open-source APIs.

SOV-3-04-AC2 Additional criterion

The service MUST support granular filtering.

2.3.5 SOV-3 Client-Side Encryption

SOV-3-05-C Criterion

The cloud service provider MUST enable client-side encryption of cloud service customer data. Whenever the cloud service customer data is transmitted, processed or stored inside the cloud environment, it MUST be encrypted with a private key that is only available to the cloud service customer outside of the cloud service provider environment.

SOV-3-05-SI Supplementary information

If this criterion is only fulfilled for some cloud services, the cloud service provider MUST provide a list of these services to the cloud services customer.

2.4 SOV-4 Operational Sovereignty

2.4.1 SOV-4 Operating Personnel

SOV-4-01-C1 Criterion

All personnel who have logical or physical access to infrastructure used to operate the cloud service, as well as those who are responsible for customer support, and all persons who have management control of the cloud service provider MUST be EU citizens with EU as main residency.

SOV-4-01-C2 Criterion

All personnel who have logical or physical access to infrastructure used to operate the cloud service, as well as those who are responsible for customer support, and all persons who have management control of the cloud service provider MUST be EU citizens with Germany as main residency.

SOV-4-01-C3 Additional criterion

The operating personnel is part of an organization that MUST be a standalone European organization.

2.4.2 SOV-4 Remote Work

SOV-4-02-C1 Criterion

The cloud service provider MUST implement organizational and technical measures ensuring that administrative access to systems used to operate the cloud service is performed through access paths located within the EU. Administrative access originating from locations outside the EU MUST be technically restricted, except in narrowly defined and controlled exceptional scenarios that are subject to additional authorization and monitoring controls.

SOV-4-02-C2 Criterion

The cloud service provider MUST implement organizational and technical measures ensuring that administrative access to systems used to operate the cloud service is performed through access paths located within the EU. Administrative access originating from locations outside Germany MUST be technically restricted, except in narrowly defined and controlled exceptional scenarios that are subject to additional authorization and monitoring controls.

2.4.3 SOV-4 Redundant connectivity providers

SOV-4-03-C Criterion

The cloud service provider MUST ensure redundant and independent connectivity for the delivery of the sovereign cloud service. In the event of a disruption of one connectivity provider, alternative connectivity providers MUST be able to maintain connectivity in accordance with the contractual service level agreements.

At least one of the connectivity providers MUST be an EU based company.

SOV-4-03-AC Additional criterion

At least one of the connectivity providers is not part of the corporate structure of the cloud service provider.

2.4.4 SOV-4 SOC

SOV-4-04-C1 Criterion

The cloud service provider MUST ensure that Security Operations Center (SOC) capabilities for the offered cloud services are established and operated within the EU. In the case of a disconnect (SOV-4-10), a stand-alone and equivalent SOC MUST be provided in the EU.

SOV-4-04-C2 Criterion

The cloud service provider MUST ensure that Security Operations Center (SOC) capabilities for the offered cloud services are established and operated within Germany. In the case of a disconnect (SOV-4-10), a stand-alone and equivalent SOC MUST be provided in Germany.

2.4.5 SOV-4 Ingress Data Control

SOV-4-05-C Criterion

All software updates and operational data affecting the cloud service MUST be received, authorized and validated in a secured network area managed and controlled by the cloud service provider.

The cloud service provider MUST verify and check updates for known vulnerabilities.

Updates MUST include documentation satisfying the needs of the cloud service provider.

The update process MUST be based on a controlled change management processes.

SOV-4-05-AC1 Additional criterion

The cloud service provider MUST implement the secure network area (e. g. DMZ) on dedicated physical devices.

SOV-4-05-AC2 Additional criterion

The cloud service provider MUST provide technical documentation how the criterion SOV-4-05-C is implemented to the responsible cybersecurity authority if requested, in accordance with applicable law and established supervisory, cooperation agreements or audit mechanisms. The responsible authority is the one in the country where the data center is located. Such information may be provided through appropriate confidentiality protections and secure disclosure procedures.

SOV-4-05-SI Supplementary information

A vulnerability is regarded as known, when it is listed in the European Union Vulnerability Database (EUVD) or in the Common Vulnerabilities and Exposures (CVE) Program from the National Institute of Standards and Technology (NIST).

2.4.6 SOV-4 Update threat analysis

SOV-4-06-C Criterion

When using third-party software under the cloud service provider’s responsibility, the cloud service provider MUST implement risk-based security analysis prior to deployment, including measures to detect and mitigate malicious code, viruses, spyware, and ransomware.

2.4.7 SOV-4 Data exchange monitoring

SOV-4-07-C Criterion

Any cloud service derived data, cloud service customer data and account data exchanged between the cloud service provider and third parties MUST always be monitored, controlled and logged. In order to do so, the

cloud service provider MUST establish a documented process. The documentation MUST be reviewed and updated regularly, at least once a year.

The cloud service provider MUST document what kind of data is exchanged with third parties. This documentation MUST ensure that it is clear which data is flowing to which party and this can also be meaningfully aggregated. The cloud service provider MUST make this documentation available to the cloud service customer. It is acceptable that this is only made available to the customer if they have agreed to keep the information confidential and not publicly disclose it.

The cloud service provider MUST clearly define the exchange format and document it as part of the data exchange documentation.

SOV-4-07-SI Supplementary information

In the context of this requirement, a cloud service customer is not considered a third party. An associated company within the same group of companies is classified as a third party.

2.4.8 SOV-4 Data exchange gateways

SOV-4-08-C Criterion

The cloud service provider MUST document, define, and visualize (via a Data Flow Diagram) all data exchanges between the cloud service provider and third parties of cloud service derived data, cloud service customer data, and account data. The data exchanges MUST occur only via known gateways. The documentation MUST clearly identify data origins, destinations, transport protocols, data type and security mechanisms protecting these exchanges. The documentation MUST be reviewed and updated regularly, at least once a year. This documentation does not need to be published publicly.

SOV-4-08-AC Additional criterion

The cloud service provider MUST provide the Data Flow Diagram to the responsible cybersecurity authority if requested, in accordance with applicable law and established supervisory, cooperation agreements or audit mechanisms.

The responsible authority is the one in the country where the data center is located. Such information may be provided through appropriate confidentiality protections and secure disclosure procedures.

SOV-4-08-SI Supplementary information

In the context of this requirement, a cloud service customer is not considered a third party. An associated company within the same group of companies is classified as a third party.

2.4.9 SOV-4 Disconnect

SOV-4-09-C Criterion

The cloud service provider MUST be able to disconnect all non-EU network-connections to the cloud without an impairment of the availability, integrity, authenticity and confidentiality of the cloud service. This includes all incoming updates and data exchanges with non-EU entities (including but not limited to: external heartbeat signals and global license validation servers) that are in the responsibility of the cloud service provider.

The cloud service provider MUST establish and document a process, when and how a disconnect is executed. This process MUST be independent from non-EU entities. The cloud service provider MUST update this documentation regularly, at least once a year.

The cloud service provider MUST conduct disconnection tests for ensuring the availability of all cloud services in case of a disconnection from the non-EU network-connections at least once a year. The cloud

service provider MUST document these tests as part of the aforementioned documentations. The documentation MUST include, but is not limited to, the results of the performed test.

SOV-4-09-AC Additional criterion

The cloud service provider MUST provide the documentation of the disconnect process and disconnection tests to the responsible cybersecurity authority if requested, in accordance with applicable law and established supervisory, cooperation agreements or audit mechanisms. Where relevant, the cloud service provider may provide supporting documentation. The responsible authority is the one in the country where the data center is located. Such information may be provided through appropriate confidentiality protections and secure disclosure procedures.

SOV-4-09-SI Supplementary information

In the context of the disconnect requirement, network connections between the cloud service provider and cloud service customers are excluded from the scope of the disconnection capability.

2.4.10 SOV-4 Reconnect

SOV-4-10-C Criterion

The cloud service provider MUST be able to reestablish all non-EU-connections after a disconnect in accordance of criterion SOV-4-9-C ("Disconnect") has been performed and has a process to install updates if the cloud environment was disconnected for a maximum of 90 days.

The process to install updates if the cloud environment was disconnected for at most 90 days MUST also be tested.

2.5 SOV-5 Supply Chain Sovereignty

2.5.1 SOV-5 Software Dependencies

SOV-5-01-C Criterion

The cloud service provider MUST identify, for each cloud service, the software components used and their respective countries of origin. A list of the relevant software suppliers and their country or countries for each service, MUST be compiled and available on demand to cloud service customers.

The identification of the software components should be based on a Software Bill of Materials (SBOM) (e.g. TR-03183-2) or achieve a comparable level of quality.

SOV-5-01-AC Additional criterion

The cloud service provider MUST maintain a risk-based process for identifying and mitigating dependencies on external software suppliers relevant to the operation of the cloud service. Where critical dependencies are identified, the cloud service provider MUST implement appropriate mitigation strategies and maintain architectural flexibility that enables substitution of software components. If it is not technically and reasonably feasible, this information MUST be adequately provided to the cloud service customer.

SOV-5-01-SI Supplementary information

The terms software components and software suppliers refer exclusively to software used by the cloud service provider to deliver the cloud service. Software deployed by customers or marketplace providers is excluded. Software components under widely used open-source licenses may be excluded from origin reporting where license terms restrict redistribution of such information.

TR-03183 current version: https://www.bsi.bund.de/dok/TR-03183 . The quality of the SBOM should meet the requirements of the TR-03183 or use comparable alternatives.

It is acceptable that this is only made available to the customer if he has agreed to keep the information confidential and not publicly disclose it.

2.5.2 SOV-5 Hardware Dependencies

SOV-5-02-C Criterion

The cloud service provider MUST maintain a documented inventory of the hardware components used to provide cloud services. A list of the relevant hardware suppliers and their country or countries MUST be compiled and available on demand to cloud service customers.

SOV-5-02-AC Additional criterion

The cloud service provider MUST maintain a risk-based process for identifying and mitigating dependencies on hardware suppliers relevant to the operation of the cloud service. Where critical dependencies are identified, the cloud service provider MUST implement mitigation strategies and maintain architectural flexibility enabling substitution of hardware components. If it is not technically and operationally feasible, this information MUST be adequately provided to the cloud service customer.

SOV-5-02-SI Supplementary information

It is acceptable that this is only made available to the customer if he has agreed to keep the information confidential and not publicly disclose it.

2.5.3 SOV-5 External Service Dependencies

SOV-5-03-C Criterion

The cloud service provider MUST maintain a documented inventory of used external cloud services that are necessary for the delivery of the cloud service. The list of information regarding the relevant external service providers and the country or countries of service provision or development MUST be made available to cloud service customers.

SOV-5-03-AC Additional criterion

The cloud service provider MUST maintain a documented process for identifying and managing external service dependencies relevant to the delivery of the cloud service. Where critical dependencies are identified, the cloud service provider MUST implement mitigation strategies and maintain architectural flexibility enabling substitution of service dependencies. If it is not technically and operationally feasible, this information MUST be adequately provided to the cloud service customer.

SOV-5-03-SI Supplementary information

External services refer exclusively to services that are functionally required for the provision of the cloud service itself. In this context, external cloud services refer to services provided by third-party cloud providers that are integrated into the delivery of the primary cloud service but are operated and maintained by separate providers.

It is acceptable that this is only made available to the customer if he has agreed to keep the information confidential and not publicly disclose it.

2.5.4 SOV-5 Export Restriction

SOV-5-04-C Criterion

The cloud service provider MUST maintain documented processes for identifying and mitigating risks related to export restrictions or supply chain disruptions affecting software, external services, and hardware used in the delivery of the cloud service. Where such restrictions may materially affect the operation of the cloud service, the cloud service provider MUST inform affected customers.

2.5.5 SOV-5 Capacity Management

SOV-5-05-C1 Criterion

Capacity management MUST be performed in the EU in accordance with C5.

SOV-5-05-C2 Criterion

Capacity management MUST be performed in Germany in accordance with C5.

2.6 SOV-6 Technology Sovereignty

2.6.1 SOV-6 Source Code Availability

SOV-6-01-C Criterion

The cloud service provider MUST have a backup of the source code in the EU that is not older than 24 hours and contains at minimum 5 versions of the cloud services so that the operation of the cloud service is possible at any time without external dependencies. This includes all infrastructure-as-code build-scripts and deployment toolchains.

The local source code backup MUST include a documentation that enables the cloud service provider to independently work with the source code and develop it further at any time without external dependencies.

2.6.2 SOV-6 Continuous Service Delivery

SOV-6-02-C Criterion

In the event of disconnection of third parties, the cloud service provider MUST maintain documented contingency strategies ensuring continued secure delivery of the cloud services. These strategies may include alternative software suppliers, internal remediation capabilities, or compensating security controls.

SOV-6-02-AC Additional criterion

In the event of disruption or loss of an external software vendor, the cloud service provider MUST maintain the capability to remediate software vulnerabilities and implement necessary changes.

The cloud provider MUST maintain specialized engineering talent and local build-environments necessary to compile, test, and deploy emergency security patches to the cloud services independently of third parties.

2.6.3 SOV-6 Software Development

SOV-6-03-C Criterion

The cloud service provider MUST ensure that authorised personnel have access to the software development tools and environments necessary to maintain and update the cloud services.

The cloud service provider MUST also maintain documented contingency procedures for scenarios in which access to critical software development tools or development environment dependencies is disrupted, ensuring the continued ability to maintain and update the cloud services.