PLEASE NOTE

Original Publication by BSI: BSI C3A Publication

This transcription has been created and published for research and facilitation purposes only.

The transcript has been created by using automated means; no guarantee is provided on the accuracy of such transcript.

If you recongise any errors – be it material or formatting – that do not origin in the officla C3A publication by BSI, please, reach out to

https://ingenrieth-online.de/en/contact

v.1.0 – April 2026

C3A Criteria – Full List

Sovereignty Dimension	Sub-Dimension	Type	Identifier	Criterion	Additional Criterion	Supplementary Information
Strategic	Jurisdiction	Criterion	SOV-1-01-C1	The cloud service provider MUST operate under EU jurisdiction, with contract governance and dispute resolution.		
Strategic	Jurisdiction	Criterion	SOV-1-01-C2	The cloud service provider MUST operate under German jurisdiction, with contract governance and dispute resolution.		
Strategic	Jurisdiction	Supp. Info	SOV-1-01-SI			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.
Strategic	Registered Office	Criterion	SOV-1-02-C1	The cloud service provider MUST have a registered head office in the EU.		
Strategic	Registered Office	Criterion	SOV-1-02-C2	The cloud service provider MUST have a registered head office in Germany.		
Strategic	Registered Office	Supp. Info	SOV-1-02-SI			If the cloud service provider uses a subcontractor for the provision of services, such as operations, that subcontractor MUST also meet the criteria.
Strategic	CSP Effective Control	Criterion	SOV-1-03-C1	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.		

	Strategic	CSP Effective Control	Criterion	SOV-1-03-C2	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.
	Strategic	CSP Control Change	Criterion	SOV-1-04-C	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.
	Legal & Jurisdictional	Extraterritorial Exposure	Criterion	SOV-2-01-C	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.
	Legal & Jurisdictional	Audit Rights	Criterion	SOV-2-02-C1	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.

	Legal & Jurisdictional	Audit Rights	Criterion	SOV-2-02-C2	The cloud service provider MUST document procedures that allow the German federal administration to verify compliance with the C3A criteria by an audit.	
	State of Defense Takeover		Criterion	SOV-2-03-C1	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.	
	State of Defense Takeover		Criterion	SOV-2-03-C2	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.	
	Data	Data Residence	Criterion	SOV-3-01-C1	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.	
	Data	Data Residence	Criterion	SOV-3-01-C2	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.	
	Data	Data Residence	Criterion	SOV-3-01-C3	The cloud service provider MUST provide a service option where cloud service customer data is exclusively stored and processed in the EU.	
	Data	Data Residence	Criterion	SOV-3-01-C4	The cloud service provider MUST provide a service option where cloud service customer data is exclusively stored and processed in Germany.	

	Data	Data Residence	Criterion	SOV-3-01-C5	The cloud service provider MUST provide a service option where cloud service provider data is exclusively stored and processed in the EU.	
	Data	External Key Management	Criterion	SOV-3-02-C	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.	
	Data	External Key Management	Add. Crit.	SOV-3-02-AC		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.
	Data	External Identity Provider	Criterion	SOV-3-03-C	The cloud service provider MUST support standards-based integration of external identity providers for authentication and access management for the cloud service.	
	Data	External Identity Provider	Add. Crit.	SOV-3-03-AC1		The integration of an external Identity Provider MUST be implemented via open, non-proprietary standards.

	Data	External Identity Provider	Add. Crit.	SOV-3-03-AC2		The provider MUST support a stateless authentication model that does not mandate the creation and copies of accounts within the provider's directory.
	Data	External Identity Provider	Add. Crit.	SOV-3-03-AC3		Authorization MUST be controllable via dynamic claims and attributes issued directly by the customer's external identity provider.
	Data	Logging and Monitoring	Criterion	SOV-3-04-C	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.	
	Data	Logging and Monitoring	Add. Crit.	SOV-3-04-AC1		The logging service MUST ensure full data flow transparency by providing real-time access via standardized open-source APIs.
	Data	Logging and Monitoring	Add. Crit.	SOV-3-04-AC2		The service MUST support granular filtering.
	Data	Client-Side Encryption	Criterion	SOV-3-05-C	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.	

	Operational	Operating Personnel	Criterion	SOV-4-01-C1	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.	
	Operational	Operating Personnel	Criterion	SOV-4-01-C2	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.	
	Operational	Operating Personnel	Add. Crit.	SOV-4-01-C3		The operating personnel is part of an organization that MUST be a standalone European organization.
	Operational	Remote Work	Criterion	SOV-4-02-C1	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.	

	Operational	Remote Work	Criterion	SOV-4-02-C2	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.	
	Operational	Redundant Connectivity	Criterion	SOV-4-03-C	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.	
	Operational	Redundant Connectivity	Add. Crit.	SOV-4-03-AC		At least one of the connectivity providers is not part of the corporate structure of the cloud service provider.
	Operational	SOC	Criterion	SOV-4-04-C1	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.	

	Operational	SOC	Criterion	SOV-4-04-C2	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.	
	Operational	Ingress Data Control	Criterion	SOV-4-05-C	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.	
	Operational	Ingress Data Control	Add. Crit.	SOV-4-05-AC1		The cloud service provider MUST implement the secure network area (e. g. DMZ) on dedicated physical devices.
	Operational	Ingress Data Control	Add. Crit.	SOV-4-05-AC2		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.

	Operational	Update Threat Analysis	Criterion	SOV-4-06-C	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.
	Operational	Data Exchange Monitoring	Criterion	SOV-4-07-C	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.

	Operational	Data Exchange Gateways	Criterion	SOV-4-08-C	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.	
	Operational	Data Exchange Gateways	Add. Crit.	SOV-4-08-AC		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.
	Operational	Disconnect	Criterion	SOV-4-09-C	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 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.	

	Operational	Disconnect	Add. Crit.	SOV-4-09-AC		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.
	Operational	Reconnect	Criterion	SOV-4-10-C	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.	
	Supply Chain	Software Dependencies	Criterion	SOV-5-01-C	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.	

	Supply Chain	Software Dependencies	Add. Crit.	SOV-5-01-AC		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.
	Supply Chain	Hardware Dependencies	Criterion	SOV-5-02-C	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.	
	Supply Chain	Hardware Dependencies	Add. Crit.	SOV-5-02-AC		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.

Supply Chain	External Services	Criterion	SOV-5-03-C	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.	
Supply Chain	External Services	Add. Crit.	SOV-5-03-AC		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.
Supply Chain	Export Restriction	Criterion	SOV-5-04-C	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.	
Supply Chain	Capacity Mgmt	Criterion	SOV-5-05-C1	Capacity management MUST be performed in the EU in accordance with C5.	
Supply Chain	Capacity Mgmt	Criterion	SOV-5-05-C2	Capacity management MUST be performed in Germany in accordance with C5.	

	Technology	Source Code Availability	Criterion	SOV-6-01-C	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.	
	Technology	Continuous Service Delivery	Criterion	SOV-6-02-C	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.	
	Technology	Continuous Service Delivery	Add. Crit.	SOV-6-02-AC		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.
	Technology	Software Development	Criterion	SOV-6-03-C	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.	

C3A Criteria – Full List w/o German specific Criteria

Sovereignty Dimension	Sub-Dimension	Type	Identifier	Criterion	Additional Criterion	Supplementary Information
Strategic	Jurisdiction	Criterion	SOV-1-01-C1	The cloud service provider MUST operate under EU jurisdiction, with contract governance and dispute resolution.		
Strategic	Registered Office	Criterion	SOV-1-02-C1	The cloud service provider MUST have a registered head office in the EU.		
Strategic	Registered Office	Supp. Info	SOV-1-02-SI			If the cloud service provider uses a subcontractor for the provision of services, such as operations, that subcontractor MUST also meet the criteria.
Strategic	CSP Effective Control	Criterion	SOV-1-03-C1	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.		
Strategic	CSP Control Change	Criterion	SOV-1-04-C	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.		

	Legal & Jurisdictional	Extraterritorial Exposure	Criterion	SOV-2-01-C	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.	
	Legal & Jurisdictional	Audit Rights	Criterion	SOV-2-02-C1	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.	
	State of Defense Takeover		Criterion	SOV-2-03-C1	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.	
	Data	Data Residence	Criterion	SOV-3-01-C1	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.	
	Data	Data Residence	Criterion	SOV-3-01-C2	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.	

	Data	Data Residence	Criterion	SOV-3-01-C3	The cloud service provider MUST provide a service option where cloud service customer data is exclusively stored and processed in the EU.	
	Data	Data Residence	Criterion	SOV-3-01-C5	The cloud service provider MUST provide a service option where cloud service provider data is exclusively stored and processed in the EU.	
	Data	External Key Management	Criterion	SOV-3-02-C	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.	
	Data	External Key Management	Add. Crit.	SOV-3-02-AC		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.
	Data	External Identity Provider	Criterion	SOV-3-03-C	The cloud service provider MUST support standards-based integration of external identity providers for authentication and access management for the cloud service.	

	Data	External Identity Provider	Add. Crit.	SOV-3-03-AC1		The integration of an external Identity Provider MUST be implemented via open, non-proprietary standards.
	Data	External Identity Provider	Add. Crit.	SOV-3-03-AC2		The provider MUST support a stateless authentication model that does not mandate the creation and copies of accounts within the provider's directory.
	Data	External Identity Provider	Add. Crit.	SOV-3-03-AC3		Authorization MUST be controllable via dynamic claims and attributes issued directly by the customer's external identity provider.
	Data	Logging and Monitoring	Criterion	SOV-3-04-C	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.	
	Data	Logging and Monitoring	Add. Crit.	SOV-3-04-AC1		The logging service MUST ensure full data flow transparency by providing real-time access via standardized open-source APIs.
	Data	Logging and Monitoring	Add. Crit.	SOV-3-04-AC2		The service MUST support granular filtering.

	Data	Client-Side Encryption	Criterion	SOV-3-05-C	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.	
	Operational	Operating Personnel	Criterion	SOV-4-01-C1	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.	
	Operational	Operating Personnel	Add. Crit.	SOV-4-01-C3		The operating personnel is part of an organization that MUST be a standalone European organization.
	Operational	Remote Work	Criterion	SOV-4-02-C1	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.	

	Operational	Redundant Connectivity	Criterion	SOV-4-03-C	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.	
	Operational	Redundant Connectivity	Add. Crit.	SOV-4-03-AC		At least one of the connectivity providers is not part of the corporate structure of the cloud service provider.
	Operational	SOC	Criterion	SOV-4-04-C1	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.	
	Operational	Ingress Data Control	Criterion	SOV-4-05-C	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.	

	Operational	Ingress Data Control	Add. Crit.	SOV-4-05-AC1		The cloud service provider MUST implement the secure network area (e. g. DMZ) on dedicated physical devices.
	Operational	Ingress Data Control	Add. Crit.	SOV-4-05-AC2		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.
	Operational	Update Threat Analysis	Criterion	SOV-4-06-C	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.	

	Operational	Data Exchange Monitoring	Criterion	SOV-4-07-C	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.
	Operational	Data Exchange Gateways	Criterion	SOV-4-08-C	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.

	Operational	Data Exchange Gateways	Add. Crit.	SOV-4-08-AC		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.
	Operational	Disconnect	Criterion	SOV-4-09-C	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 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.	
	Operational	Disconnect	Add. Crit.	SOV-4-09-AC		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.

	Operational	Reconnect	Criterion	SOV-4-10-C	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.	
	Supply Chain	Software Dependencies	Criterion	SOV-5-01-C	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.	
	Supply Chain	Software Dependencies	Add. Crit.	SOV-5-01-AC		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.

	Supply Chain	Hardware Dependencies	Criterion	SOV-5-02-C	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.	
	Supply Chain	Hardware Dependencies	Add. Crit.	SOV-5-02-AC		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.
	Supply Chain	External Services	Criterion	SOV-5-03-C	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.	

Supply Chain	External Services	Add. Crit.	SOV-5-03-AC		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.
Supply Chain	Export Restriction	Criterion	SOV-5-04-C	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.	
Supply Chain	Capacity Mgmt	Criterion	SOV-5-05-C1	Capacity management MUST be performed in the EU in accordance with C5.	
Technology	Source Code Availability	Criterion	SOV-6-01-C	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.	
Technology	Continuous Service Delivery	Criterion	SOV-6-02-C	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.	

	Technology	Continuous Service Delivery	Add. Crit.	SOV-6-02-AC		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.
	Technology	Software Development	Criterion	SOV-6-03-C	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.	

C3A Criteria – German specific Criteria (only)

Sovereignty Dimension	Sub-Dimension	Type	Identifier	Criterion	Additional Criterion	Supplementary Information
Strategic	Jurisdiction	Criterion	SOV-1-01-C2	The cloud service provider MUST operate under German jurisdiction, with contract governance and dispute resolution.		
Strategic	Jurisdiction	Supp. Info	SOV-1-01-SI			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.
Strategic	Registered Office	Criterion	SOV-1-02-C2	The cloud service provider MUST have a registered head office in Germany.		
Strategic	CSP Effective Control	Criterion	SOV-1-03-C2	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.		
Legal & Jurisdictional	Audit Rights	Criterion	SOV-2-02-C2	The cloud service provider MUST document procedures that allow the German federal administration to verify compliance with the C3A criteria by an audit.		
State of Defense Takeover		Criterion	SOV-2-03-C2	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.		

	Data	Data Residence	Criterion	SOV-3-01-C4	The cloud service provider MUST provide a service option where cloud service customer data is exclusively stored and processed in Germany.
	Operational	Operating Personnel	Criterion	SOV-4-01-C2	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.
	Operational	Remote Work	Criterion	SOV-4-02-C2	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.
	Operational	SOC	Criterion	SOV-4-04-C2	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.
	Supply Chain	Capacity Mgmt	Criterion	SOV-5-05-C2	Capacity management MUST be performed in Germany in accordance with C5.