| KIAF-1410 CO_SAC & SoCA v3.0 | | THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview' | | | CRITERION APPLICABILITY (SoCA) |
|---|---|---|---|---|---|
| Not Used | Criterion title | tag | index | KI_criterion | read this comment |
| Enterprise and Service Maturity | | | | | |
| | **Established enterprise** | *CO#0010* | | Be a valid legal entity and a person with legal authority to commit the organization must submit the signed assessment package. | **In scope - Applicable** |
| | **Legal & Contractual compliance** | *CO#0020* | | | |
| | **Legal & Contractual compliance** | *CO#0020* | | Demonstrate that it understands and complies with any legal requirements incumbent on it in connection with operation and delivery of the specified service, accounting for all jurisdictions within which its services may be offered. Any specific contractual requirements shall also be identified. | **In scope - Applicable** |
| | **Financial Provisions** | *CO#0030* | | **Provide documentation of financial resources that allow for the continued operation of the service and demonstrate appropriate liability processes and procedures that satisfy the degree of liability exposure being carried.** | **In scope - Applicable** |
| | **Data Retention and Protection** | *CO#0040* | | Specifically set out and demonstrate that it understands and complies with those legal and regulatory requirements incumbent upon it concerning the retention and destruction of private and identifiable information (personal and business - i.e. its secure storage and protection against loss, accidental public exposure, and/or improper destruction) and the protection of Subjects' private information (against unlawful or unauthorized access, excepting that permitted by the information owner or required by due process). | **In scope - Applicable** |

| | | | | | | |
|---|---|---|---|---|---|---|
| | **Termination provisions** | *CO#0050* | | | Define the practices in place for the protection of Subjects' private and secret information related to their use of the service which must ensure the ongoing secure preservation and protection of legally required records and for the secure destruction and disposal of any such information whose retention is no longer legally required. Specific details of these practices must be made available. | **In scope - Applicable** |
| | **Ownership** | *CO#0060* | | | **If the enterprise named as the CSP is a part of a larger entity, the nature of the relationship with its parent organization shall be disclosed to the assessors and, on their request, to customers.** | **In scope - Applicable** |
| | **Independent management and operations** | *CO#0070* | | | **Demonstrate that, for the purposes of providing the specified service, its management and operational structures are distinct, autonomous, have discrete legal accountability, and operate according to separate policies, procedures, and controls.** | **In scope - Applicable** |
| **Notices and Subscriber Information/Agreements** | | | | | | |
| | **General Service Definition** | *CO#0080* | | | Make available to the intended user community a Service Definition that includes all applicable Terms, Conditions, and Fees, including any limitations of its usage. Specific provisions are stated in further criteria in this section. | **In scope - Applicable** |
| | **Service Definition inclusions** | *CO#0090* | | | Make available a Service Definition for the specified service containing clauses that provide the following information: | **In scope - Applicable** |
| | **Service Definition inclusions** | *CO#0090* | *a)* | | Privacy, Identity Proofing & Verification, Authentication, Renewal/Re-issuance, and Revocation and Termination Policies; | **In scope - Applicable** |
| | **Service Definition inclusions** | *CO#0090* | *b)* | | **the country in or legal jurisdiction under which the service is operated;** | **In scope - Applicable** |

| | | | | | | |
|---|---|---|---|---|---|---|
| | **Service Definition inclusions** | *CO#0090* | *c)* | | **different from the above, the legal jurisdiction under which Subscriber and any relying party agreements are entered into;** | **In scope - Applicable** |
| | **Service Definition inclusions** | *CO#0090* | *d)* | | **applicable legislation with which the service complies;** | **In scope - Applicable** |
| | **Service Definition inclusions** | *CO#0090* | *e)* | | **obligations incumbent upon the CSP;** | **In scope - Applicable** |
| | **Service Definition inclusions** | *CO#0090* | *f)* | | **obligations incumbent upon each class of user of the service, e.g. Relying Parties, Subscribers and Subjects;** | **In scope - Applicable** |
| | **Service Definition inclusions** | *CO#0090* | *g)* | | **notifications and guidance for relying parties, especially in respect of actions they are expected to take should they choose to rely upon the service;** | **In scope - Applicable** |
| | **Service Definition inclusions** | *CO#0090* | *h)* | | **statement of warranties;** | **In scope - Applicable** |
| | **Service Definition inclusions** | *CO#0090* | *i)* | | **statement of liabilities toward Subscribers, Subjects and Relying Parties;** | **In scope - Applicable** |
| | **Service Definition inclusions** | *CO#0090* | *j)* | | **procedures for notification of changes to terms and conditions;** | **In scope - Applicable** |
| | **Service Definition inclusions** | *CO#0090* | *k)* | | **steps the CSP will take in the event that it chooses or is obliged to terminate the service;** | **In scope - Applicable** |
| | **Service Definition inclusions** | *CO#0090* | *l)* | | **availability of the specified service (for the service as a whole or for each of its distinct components) and of its help desk facility.** | **In scope - Applicable** |
| | **ALx Configuration Specification** | *CO#0100* | | | **Make available a detailed specification (accounting for the service specification and architecture) which defines how a user of the service can configure it so as to be assured of receiving a service which at least meets the applicable Assurance Level baseline** | **In scope - Applicable** |

| | | | | | | |
|---|---|---|---|---|---|---|
| | **Due notification** | *CO#0110* | | | **Have in place and follow appropriate policy and procedures to ensure that it notifies Subscribers and Subjects in a timely and reliable fashion of any changes to the Service Definition and any applicable Terms, Conditions, Fees, and Privacy Policy for the specified service, and provide a clear means by which Subscribers and Subjects must indicate that they wish to accept the new terms or terminate their subscription.** | **In scope - Applicable** |
| | **User Acceptance** | *CO#0120* | | | Require Subscribers and Subjects to: | **In scope - Applicable** |
| | **User Acceptance** | *CO#0120* | *a)* | | indicate, prior to receiving service, that they have read and accept the terms of service as defined in the Service Definition; | **In scope - Applicable** |
| | **User Acceptance** | *CO#0120* | *b)* | | at periodic intervals, determined by significant service provision events (e.g. issuance, re-issuance, renewal) and otherwise at least once every five years, re-affirm their understanding and observance of the terms of service; | **In scope - Applicable** |
| | **User Acceptance** | *CO#0120* | *c)* | | always provide full and correct responses to requests for information. | **In scope - Applicable** |
| | **Record of User Acceptance** | *CO#0130* | | | Obtain a record (hard-copy or electronic) of the Subscriber's and Subject's acceptance of the terms and conditions of service, prior to initiating the service and thereafter reaffirm the agreement at periodic intervals, determined by significant service provision events (e.g. re-issuance, renewal) and otherwise at least once every five years. | **In scope - Applicable** |
| | **Change of Subscriber Information** | *CO#0140* | | | **Require and provide the mechanisms for Subscribers and Subjects to provide in a timely manner full and correct amendments should any of their recorded information change, as required under the terms of their use of the service, and only after the Subscriber's and/or Subject's identity has been authenticated.** | **In scope - Applicable** |
| **Information Security Management** | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | **Documented policies and procedures** | *CO#0150* | | | **Have documented all security-relevant administrative, management, and technical policies and procedures. The enterprise must ensure that these are based upon recognized standards, published references or organizational guidelines, are adequate for the specified service, and are implemented in the manner intended.** | **In scope - Applicable** |
| | **Policy Management and Responsibility** | *CO#0160* | | | **Have a clearly defined managerial role, at a senior level, in which full responsibility for the business's security policies is vested and from which review, approval, and promulgation of policy and related procedures is applied and managed. The latest approved versions of these policies must be applied at all times.** | **In scope - Applicable** |
| | **Risk Management** | *CO#0170* | | | Demonstrate a risk management methodology that adequately identifies and mitigates risks related to the specified service and its user community and must show that a risk assessment review is performed at least once every six months, such as adherence to CobIT or [IS27001] practices. | **In scope - Applicable** |
| | **Continuity of Operations Plan** | *CO#0180* | | | Have and keep updated a continuity of operations plan that covers disaster recovery and the resilience of the specified service and must show that a review of this plan is performed at least once every six months. | **In scope - Applicable** |
| | **Configuration Management** | *CO#0190* | | | Demonstrate that there is in place a configuration management system that at least includes: | **In scope - Applicable** |
| | **Configuration Management** | *CO#0190* | *a)* | | version control for software system components; | **In scope - Applicable** |
| | **Configuration Management** | *CO#0190* | *b)* | | timely identification and installation of all organizationally-approved patches for any software used in the provisioning of the specified service. | **In scope - Applicable** |
| | **Configuration Management** | *CO#0190* | ***c)*** | | **version control and managed distribution for all documentation associated with the specification, management, and operation of the system, covering both internal and publicly available materials.** | **In scope - Applicable** |

| | | | | | | |
|---|---|---|---|---|---|---|
| | **Quality Management** | *CO#0200* | | | **Demonstrate that there is in place a quality management system that is appropriate for the specified service.** | **In scope - Applicable** |
| | **System Installation and Operation Controls** | *CO#0210* | | | **Apply controls during system development, procurement installation, and operation that protect the security and integrity of the system environment, hardware, software, and communications.** | **In scope - Applicable** |
| | **System Installation and Operation Controls** | *CO#0210* | | | Apply controls during system development, procurement, installation, and operation that protect the security and integrity of the system environment, hardware, software, and communications having particular regard to: | **In scope - Applicable** |
| | **System Installation and Operation Controls** | *CO#0210* | ***a)*** | | **the software and hardware development environments, for customized components;** | **In scope - Applicable** |
| | **System Installation and Operation Controls** | *CO#0210* | ***b)*** | | **the procurement process for commercial off-the-shelf (COTS) components;** | **In scope - Applicable** |
| | **System Installation and Operation Controls** | *CO#0210* | ***c)*** | | **contracted consultancy/support services;** | **In scope - Applicable** |
| | **System Installation and Operation Controls** | *CO#0210* | ***d)*** | | **shipment of system components;** | **In scope - Applicable** |
| | **System Installation and Operation Controls** | *CO#0210* | ***e)*** | | **storage of system components;** | **In scope - Applicable** |
| | **System Installation and Operation Controls** | *CO#0210* | ***f)*** | | **installation environment security;** | **In scope - Applicable** |
| | **System Installation and Operation Controls** | *CO#0210* | ***g)*** | | **system configuration;** | **In scope - Applicable** |
| | **System Installation and Operation Controls** | *CO#0210* | ***h)*** | | **transfer to operational status.** | **In scope - Applicable** |

| | | | | | | |
|---|---|---|---|---|---|---|
| | **Internal Service Audit** | *CO#0220* | | | **Be subjected to a first-party audit at least once every 12 months for the effective provision of the specified service by internal audit functions of the enterprise responsible for the specified service, unless it can show that by reason of its organizational size or due to other operational restrictions it is unreasonable to be so audited.** | **In scope - Applicable** |
| | **Internal Service Audit** | *CO#0220* | | | Be subjected to a first-party audit at least once every 12 months for the effective provision of the specified service by internal audit functions of the enterprise responsible for the specified service, unless it can show that by reason of its organizational size or due to other justifiable operational restrictions it is unreasonable to be so audited. | **In scope - Applicable** |
| | **Audit Records** | *CO#0230* | | | **Retain records of all audits, both internal and independent, for a period which, as a minimum, fulfills its legal obligations and otherwise for greater periods either as it may have committed to in its Service Definition or required by any other obligations it has with/to a Subscriber or Subject, and which in any event is not less than 36 months. Such records must be held securely and be protected against unauthorized access loss, alteration, public disclosure, or unapproved destruction.** | **In scope - Applicable** |
| | **Best Practice Security Management** | *CO#0240* | | | **Have in place an Information Security Management System (ISMS), or other IT security management methodology recognized by a government or professional body, that follows best practices as accepted by the information security industry and that applies and is appropriate to the CSP in question. All requirements expressed in preceding criteria in this section must inter alia fall wholly within the scope of this ISMS or selected recognized alternative.** | **In scope - Applicable** |
| **Security-Related (Audit) Records** | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | **Security event logging** | *CO#0250* | | | **Maintain a log of all relevant security events concerning the operation of the service, together with an accurate record of the time at which the event occurred (time-stamp), and retain such records with appropriate protection and controls to ensure successful retrieval, accounting for Service Definition, risk management requirements, applicable legislation, and organizational policy.** | **In scope - Applicable** |
| | **Demonstrated availability** | *CO#0260* | | | **Determine actual availability achieved in comparison to the stated availability targets (refer to CO#0090 l) ).** | **In scope - Applicable** |
| **Operational Infrastructure** | | | | | | |
| | **Defined security roles** | *CO#0270* | | | **Define, by means of a job description, the roles and responsibilities for each service-related security-relevant task, relating it to specific procedures, (which shall be set out in the ISMS, or other IT security management methodology recognized by a government or professional body) and other service-related job descriptions and applicable policies, processes and procedures. Where the role is security-critical or where special privileges or shared duties exist, these must be specifically identified as such, including the applicable access privileges relating to logical and physical parts of the service's operations.** | **In scope - Applicable** |
| | **Acknowledgement of assigned security roles and responsibilities** | *CO#0280* | | | **Require those assigned to critical security roles to acknowledge, by signature (hand-written or electronic), that they have read and understood the system documentation applicable to their role(s) and that they accept the associated responsibilities.** | **In scope - Applicable** |

| | | | | | | |
|---|---|---|---|---|---|---|
| | **Personnel recruitment** | *CO#0290* | | | Demonstrate that it has defined practices for the selection, evaluation, and contracting of all service-related personnel, both direct employees and those whose services are provided by third parties. Full records of all searches and supporting evidence of qualifications and past employment must be kept for the duration of the individual's employment plus the longest lifespan of any credential issued under the Service Policy. | **In scope - Applicable** |
| | **Personnel skills** | *CO#0300* | | | **Ensure that employees are sufficiently trained, qualified, experienced, and current for the roles they fulfill. Such measures must be accomplished either by recruitment practices or through a specific training program. Where employees are undergoing on-the-job training, they must only do so under the guidance of a mentor possessing the defined service experiences for the training being provided.** | **In scope - Applicable** |
| | **Adequacy of Personnel resources** | *CO#0310* | | | **Have sufficient staff to adequately operate and resource the specified service according to its policies and procedures.** | **In scope - Applicable** |
| **External Services and Components** | | | | | | |
| | **Contracted policies and procedures** | *CO#0320* | | | **Where the enterprise uses external suppliers for specific packaged components of the service or for resources that are integrated with its own operations and under its control, ensure that those parties are engaged through reliable and appropriate contractual arrangements which stipulate which critical policies, procedures, and practices subcontractors are required to fulfill.** | **In scope - Applicable** |

| | | | | | | |
|---|---|---|---|---|---|---|
| | **Visibility of Contracted Parties** | *CO#0330* | | | **Where the enterprise uses external suppliers for specific packaged components of the service or for resources which are integrated with its own operations and under its control, ensure that the suppliers' compliance with contractually-stipulated policies and procedures, and thus with the IAF Service Assessment Criteria, can be independently verified, and subsequently monitored if necessary.** | **In scope - Applicable** |
| ***End of CO_SAC criteria*** | | | | | | |

***In scope - Applicable***
***In scope - Not applicable***

***In scope - Applicable - fulfilled by ...***