Title:	Identity Assurance Framework: NIST SP 800-63A Service Assessment Criteria
Document id:	KIAF-1430
Version:	3.1.7
Document type:	Draft Recommendation
Publication Date:	2020-06-16
Effective Date:	tbd
Status:	Editor's Draft
Approval Authority:	IAWG
Editor:	R.G. Wilsher, Zygma Inc.
Sponsor:	ID.me Inc.
IAWG Sub-group Participants / Non-participants	Ken DAGG (Individual contributor) Nathan FAUT (KPMG) Mark HAPNER (Resilient Networks) Andrew HUGHES (IDEMIA) James JUNG (Slandala) Ruth PUENTE (Kantara Initiative) Martin SMITH (Individual contributor) Colin WALLIS (Kantara Initiative) Richard WILSHER (Zygma Inc.)
IPR:	Patent and Copyright Option: Reciprocal Royalty Free with Opt-Out to Reasonable and Non-Discriminatory terms (RAND) | © 2019
Abstract:	This Specification sets forth KI's Service Assessment Criteria for assessments against the requirements of NIST's SP 800-63A as published 2017-12-01 (with errata) at IAL2, to be generally referred-to as the '63A_SAC'. It is anticipated that these criteria will be reviewed 12 months after publication, for any required re-expression,
Notice:	All rights reserved. This Specification has been prepared by Participants of the Identity Assurance Working Group of the Kantara Initiative. No rights are granted to Non-Participants of the Identity Assurance Working Group nor any other person or entity to reproduce or otherwise prepare derivative works without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. Entities seeking permission to reproduce portions of this Specification for other uses must contact the Kantara Initiative to determine whether an appropriate license for Implementation or use of certain elements of this Specification may require licenses under third party intellectual property rights, including without limitation, patent rights. The Participants of and any other contributors to the document are not and shall not be held responsible in any manner for identifying or failing to identify any or all such third party intellectual property rights. This document is provided "AS IS" and no Participant in the Kantara Initiative makes any warranty of any kind, expressed or implied, including any implied warranties of merchantability, non-infringement of third party intellectual property rights, and fitness for a particular purpose.
Revision history:	See Revision History

Users' Guide

Structure of these criteria:

The criteria in this document relate to the requirements of NIST SP 800-63A at IAL2 and IAL3. Principal criteria are in the worksheet '63A_SAC' and three tables from SP 800-63A are interpreted in Kantara terms in the other three worksheets, which have the Table 5-x reference built into their labels.

The original NIST criteria headings and text FOR NORMATIVE SECTIONS ONLY are available in columns A to H, giving the heading components of the applicable levels and then the actual text of the NIST clause. However, as downloaded from Kantara, columns B to H are hidden, so as to focus attention on the Kantara criteria. There is no prohibition on Users un-hiding these columns, should they so choose.

Columns I to L inclusive identify four different types of entity to which the criteria may apply and assign applicability accordingly.

Kantara's criteria (i.e. the 63A_SAC) are set out in columns N to T, commencing with a unique tag in the form '63A#9999', possible sub-indexes following, and then the actual criteria in col. R. Columns S & T denote the applicable Assuramce Level(s).

Col. U provides Guidance which is presently minimal but will be added-to as the Kantara IAWG sees a need for it.

Because there is not a Kantara criterion derived from each and every clause in the original NIST SP some rows in the criteria columns may not bear a criterion - in this case they are shaded and marked 'n/a', in an attempt to avoid any error of omission. Some may refer to already-defined criteria which achieve the required goal and therefore evidence of conformity is not required twice.

The three worksheets which address Tables 5-1, 5-2 and 5-3 in SP 800-63A have a similar, but not precisely the same, layout with which Users will be readily familiar after working-through the 63A_SAC worksheet.

Use as a Statement of Conformity (SoC)

Users (principally Assessors and CSPs) are at liberty to adopt this document for their own use as an SoC, for use in applications to Kantara's ARB (ref KIAF-1340 'SAH') for initial Registration, to record findings etc. during an assessment, and for a grant of Approval.

Title:	Kantara Identity Assurance Framework: Common Organizational Service Assessment Criteria (SAC) & Statement of Criteria Applicability (SoCA)
Document id:	KIAF-1410
Version:	3.0
Document type:	Recommendation
Publication Date:	2020-10-15
Effective Date:	2021-02-01
Status:	Final
Approval Authority:	IAWG
IAWG Participants / Non-participants	https://kantarainitiative.org/confluence/display/IAWG/Participant+Roster
IPR:	Patent and Copyright Option: Reciprocal Royalty Free with Opt-Out to Reasonable and Non-Discriminatory terms (RAND) | © 2019

Abstract: This Specification sets forth KI's Service Assessment Criteria for assessments whose scope includes the good standing of the organization which provides the service which is subject to assessment, be generally referred-to as the 'CO_SAC'. It is anticipated that these criteria will be reviewed 12 months after publication, for any required re-expression, revision, etc.

Though this document is structured with headers, footers etc. for document management purposes, the CO_SAC worksheet itself is not intended to be published in a printed page format, and hence 'Normal' View is recommended at all times.

Revision history: See Revision History

KIAF-1410 Commonly-Applicable Service Assessment Criteria (CO_SAC)

Version	*Date*	*Status*	*Summary of changes*
Note re. version numbers:			*Changes which the IAWG considers to be Non-Material shall be incremented by '0.1', whereas changes considered to be MATERIAL shall be raised to the next whole number.*
v3.0	10/15/20	Final - Material changes - released for application	Re-expression in Spreadsheet format with addition of explicit SoCA and SoC columns.

For versions v1.0 and v2.0, refer to the Word versions of KIAF-1410.

This Worksheet realization includes changes to eliminate historical artefacts, such as use of 'omitted' where changes have lead to the removal of text, and 'normalization' of criteria tags to have greater commonality with those used an all other SACs. Essentially, a 'clean start' for these criteria.

CO_SAC SAC / SoCA v3.0			Applies to				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'			LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used		Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index	KI_criterion	1	2	3	4	read this comment	
Enterprise and Service Maturity			read this comment												
		Established enterprise	as applicable				CO#0010		Be a valid legal entity and a person with legal authority to commit the organization must submit the signed assessment package.	✓	✓	✓	✓		
		Legal & Contractual compliance	as applicable				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.	✓					'Understanding' is implicitly the correct understanding. Both it and compliance are required because it could be that understanding is incomplete, incorrect or even absent, even though compliance is apparent, and similarly, correct understanding may not necessarily result in full compliance. The two are therefore complementary.
		Legal & Contractual compliance	as applicable				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.**		✓	✓	✓		See LoA1 guidance.
		Financial Provisions	as applicable				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.**		✓	✓	✓		The organization must show that it has a budgetary provision to operate the service for at least a twelve-month period, with a clear review of the budgetary planning within that period so as to keep the budgetary provisions extended. It must also show how it has determined the degree of liability protection required, in view of its exposure per 'service' and the number of users it has. This criterion helps ensure that Kantara Initiative, Inc. does not grant Recognition to
		Data Retention and Protection	as applicable				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)	✓	✓	✓	✓		Note that whereas the criterion is intended to address unlawful or unauthorized access arising from malicious or careless actions (or inaction) some access may be unlawful UNLESS authorized by the Subscriber or Subject, or effected as a part of a specifically-executed legal process.
		Termination provisions	as applicable				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.	✓	✓	✓	✓		Termination covers the cessation of the business activities, the service provider itself ceasing business operations altogether, change of ownership of the service-providing business, and other similar events which change the status and/or operations of the service provider in any way which interrupts the continued provision of the specific
		Ownership	as applicable				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.**			✓	✓		
		Independent management and operations	as applicable				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.**			✓	✓		
Notices and Subscriber Information/Agreements															
		General Service Definition	as applicable				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	✓	✓	✓	✓		The intended user community encompasses potential and actual Subscribers, Subjects, and Relying Parties.
		Service Definition inclusions	as applicable				CO#0090		Make available a Service Definition for the specified service containing clauses that provide the following information:	✓					The term 'Service Definition' is used to define a notional document which has the described characteristics, rather than to demand that there be a document specifically bearing such a title (though it is adopted as being a particularly relevant title). The policies referred-to may be included or separate and may have scope-specific titles or may adopt usage found elsewhere within this and other sets of SAC, e.g. 'Credential Policy', 'Identity-Proofing Policy', according to specific criteria scope in each instance. The important point is that

CO_SAC SAC / SoCA v3.0				Applies to				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'			LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used			Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index	KI_criterion	1	2	3	4	read this comment	
			Service Definition inclusions	as applicable				CO#0090	a)	a Privacy Policy.	✓					
			Service Definition inclusions	as applicable				CO#0090		Make available a Service Definition for the specified service containing clauses that provide the following information:		✓	✓	✓		See LoA1 guidance.
			Service Definition inclusions	as applicable				CO#0090	a)	Privacy, **Identity Proofing & Verification, Authentication, Renewal/Re-issuance, and Revocation and Termination Policies;**		✓	✓	✓		
			Service Definition inclusions	as applicable				CO#0090	b)	**the country in or legal jurisdiction under which the service is operated;**		✓	✓	✓		
			Service Definition inclusions	as applicable				CO#0090	c)	**different from the above, the legal jurisdiction under which Subscriber and any relying party agreements are entered into;**		✓	✓	✓		
			Service Definition inclusions	as applicable				CO#0090	d)	**applicable legislation with which the service complies;**		✓	✓	✓		
			Service Definition inclusions	as applicable				CO#0090	e)	**obligations incumbent upon the CSP;**		✓	✓	✓		
			Service Definition inclusions	as applicable				CO#0090	f)	**obligations incumbent upon each class of user of the service, e.g. Relying Parties, Subscribers and Subjects;**		✓	✓	✓		
			Service Definition inclusions	as applicable				CO#0090	g)	**notifications and guidance for relying parties, especially in respect of actions they are expected to take should they choose**		✓	✓	✓		
			Service Definition inclusions	as applicable				CO#0090	h)	**statement of warranties;**		✓	✓	✓		
			Service Definition inclusions	as applicable				CO#0090	i)	**statement of liabilities toward Subscribers, Subjects and Relying Parties;**		✓	✓	✓		
			Service Definition inclusions	as applicable				CO#0090	j)	**procedures for notification of changes to terms and conditions;**		✓	✓	✓		
			Service Definition inclusions	as applicable				CO#0090	k)	**steps the CSP will take in the event that it chooses or is obliged to terminate the service;**		✓	✓	✓		
			Service Definition inclusions	as applicable				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.**		✓	✓	✓		
			ALx Configuration Specification	as applicable				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**		✓	✓	✓		
			Due notification	as applicable				CO#0110		Have in place and follow appropriate policy and procedures to ensure that it notifies Users in a timely and reliable fashion of any changes to the Service Definition and any applicable Terms.	✓					
			Due notification	as applicable				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**		✓	✓	✓		
			User Acceptance	as applicable				CO#0120		Require Subscribers and Subjects to:	✓					
			User Acceptance	as applicable				CO#0120	a)	indicate, prior to receiving service, that they have read and accept the terms of service as defined in the Service Definition;	✓					
			User Acceptance	as applicable				CO#0120	b)	at periodic intervals, determined by significant service provision events (e.g. issuance, re-issuance, renewal), re-affirm their	✓					
			User Acceptance	as applicable				CO#0120	c)	always provide full and correct responses to requests for information.	✓					
			User Acceptance	as applicable				CO#0120		Require Subscribers and Subjects to:		✓	✓	✓		

CO_SAC SAC / SoCA v3.0			Applies to				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'			LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used		Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index	KI_criterion	1	2	3	4	read this comment	
		User Acceptance	as applicable				CO#0120	a)	indicate, prior to receiving service, that they have read and accept the terms of service as defined in the Service Definition;		✓	✓	✓		
		User Acceptance	as applicable				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		✓	✓	✓		
		User Acceptance	as applicable				CO#0120	c)	always provide full and correct responses to requests for information.		✓	✓	✓		
		Record of User Acceptance	as applicable				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 at periodic intervals, determined	✓					
		Record of User Acceptance	as applicable				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-		✓	✓	✓		
		Change of Subscriber Information	as applicable				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.**		✓	✓	✓		
Information Security Management															
		Documented policies and procedures	as applicable				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**		✓	✓	✓		
		Policy Management and Responsibility	as applicable				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.**		✓	✓	✓		
		Risk Management	as applicable				CO#0170		**Demonstrate a risk management methodology that adequately identifies and mitigates risks related to the specified service and**		✓				
		Risk Management	as applicable				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**			✓	✓		
		Continuity of Operations Plan	as applicable				CO#0180		**Have and keep updated a Continuity of Operations Plan that covers disaster recovery and the resilience of the specified**		✓				
		Continuity of Operations Plan	as applicable				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**			✓			
		Continuity of Operations Plan	as applicable				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 on-going review of this plan is conducted as a part of**				✓		
		Configuration Management	as applicable				CO#0190		**Demonstrate that there is in place a configuration management system that at least includes:**		✓				
		Configuration Management	as applicable				CO#0190	a)	**version control for software system components;**		✓				
		Configuration Management	as applicable				CO#0190	b)	**timely identification and installation of all organizationally-approved patches for any software used in the provisioning of the**		✓				
		Configuration Management	as applicable				CO#0190		Demonstrate that there is in place a configuration management system that at least includes:			✓	✓		

CO_SAC SAC / SoCA v3.0				Applies to				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used			Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index		KI_criterion	1	2	3	4	read this comment	
			Configuration Management	as applicable				CO#0190	a)		version control for software system components;			✓	✓		
			Configuration Management	as applicable				CO#0190	b)		timely identification and installation of all organizationally-approved patches for any software used in the provisioning of the specified			✓	✓		
			Configuration Management	as applicable				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**			✓	✓		
			Quality Management	as applicable				CO#0200			**Demonstrate that there is in place a quality management system that is appropriate for the specified service.**		✓	✓	✓		
			System Installation and Operation Controls	as applicable				CO#0210			**Apply controls during system development, procurement installation, and operation that protect the security and integrity of the system environment, hardware, software, and**		✓				
			System Installation and Operation Controls	as applicable				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**			✓	✓		
			System Installation and Operation Controls	as applicable				CO#0210	**a)**		**the software and hardware development environments, for customized components;**			✓	✓		
			System Installation and Operation Controls	as applicable				CO#0210	**b)**		**the procurement process for commercial off-the-shelf (COTS) components;**			✓	✓		
			System Installation and Operation Controls	as applicable				CO#0210	**c)**		**contracted consultancy/support services;**			✓	✓		
			System Installation and Operation Controls	as applicable				CO#0210	**d)**		**shipment of system components;**			✓	✓		
			System Installation and Operation Controls	as applicable				CO#0210	**e)**		**storage of system components;**			✓	✓		
			System Installation and Operation Controls	as applicable				CO#0210	**f)**		**installation environment security;**			✓	✓		
			System Installation and Operation Controls	as applicable				CO#0210	**g)**		**system configuration;**			✓	✓		
			System Installation and Operation Controls	as applicable				CO#0210	**h)**		**transfer to operational status.**			✓	✓		
			Internal Service Audit	as applicable				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.**		✓				'First-party' audits are those undertaken by an independent part of the same organization which offers the service. The auditors cannot be involved in the specification, development or operation of the service. Using a 'third-party' (i.e. independent) auditor (i.e. one having no relationship with the Service Provider nor any vested interests in the outcome of the assessment other than their professional obligations to perform the assessment objectively and independently) should be considered when the organization cannot easily provide truly
			Internal Service Audit	as applicable				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.			✓	✓		'First-party' audits are those undertaken by an independent part of the same organization which offers the service. The auditors cannot be involved in the specification, development or operation of the service. Management systems require that there be internal audit conducted as an inherent part of management review processes. Any third-party (i.e. independent) audit of the management system is intended to

CO_SAC SAC / SoCA v3.0			Applies to				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'			LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used	Criterion title		CSP	RP	FA	US Fed Agcy	new tag	index	KI_criterion	1	2	3	4	read this comment	
	Audit Records		as applicable				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.		✓	✓	✓		
	Best Practice Security Management		as applicable				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.			✓			Third party auditors determining that this ISMS meets the above requirement must be appropriately qualified in assessing the specific management system or methodology applied.
	Best Practice Security Management		as applicable				CO#0240		Have in place a **certified** Information Security Management System (ISMS), or other IT security management methodology recognized by a government or professional body, that **has been assessed and found to be in compliance with the requirements of ISO/IEC 27001 [IS27001] and which applies and is appropriate to the CSP in question**. All requirements expressed in preceding criteria in this				✓		See LoA3 guidance.
Security-Related (Audit) Records															
	Security event logging		as applicable				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**		✓	✓			It is sufficient that the accuracy of the time source is based upon an internal computer/system clock synchronized to an internet time source. The time source need not be authenticable.
	Security event logging		as applicable				CO#0250		Maintain a log of all relevant security events concerning the operation of the service, together with **a precise** record of the time at which the event occurred (time-stamp) **provided by a trusted time-source** 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.				✓		See LoA2 guidance.
	Demonstrated availability		as applicable				CO#0260		**Determine actual availability achieved in comparison to the stated availability targets (refer to CO#0090 I)).**		✓	✓	✓		
Operational Infrastructure															
	Defined security roles		as applicable				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,**		✓	✓	✓		

CO_SAC SAC / SoCA v3.0			Applies to				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'			LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used		Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index	KI_criterion	1	2	3	4	read this comment	
		Acknowledgement of assigned security roles and responsibilities	as applicable				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.			✓	✓		
		Personnel recruitment	as applicable				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		✓				
		Personnel recruitment	as applicable						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			✓	✓		
		Personnel skills	as applicable				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		✓	✓	✓		
		Adequacy of Personnel resources	as applicable				CO#0310		Have sufficient staff to adequately operate and resource the specified service according to its policies and procedures.		✓	✓	✓		
External Services and Components															
		Contracted policies and procedures	as applicable				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.		✓	✓	✓		
		Visibility of Contracted Parties	as applicable				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		✓	✓	✓		
End of CO_SAC criteria															

Tag cross-references

==>

Criterion title	*old tag*	*new tag*
Contracted policies and procedures	*ALx_CO_ESC#010*	*CO#0320*
Visibility of Contracted Parties	*ALx_CO_ESC#020*	*CO#0330*
Established enterprise	*ALx_CO_ESM#001*	*CO#0010*
Legal & Contractual compliance	*ALx_CO_ESM#030*	*CO#0020*
Financial Provisions	*ALx_CO_ESM#040*	*CO#0030*
Data Retention and Protection	*ALx_CO_ESM#050*	*CO#0040*
Termination provisions	*ALx_CO_ESM#055*	*CO#0050*
Ownership	*ALx_CO_ESM#060*	*CO#0060*
Independent management and operations	*ALx_CO_ESM#070*	*CO#0070*
Documented policies and procedures	*ALx_CO_ISM#010*	*CO#0150*
Policy Management and Responsibility	*ALx_CO_ISM#020*	*CO#0160*
Risk Management	*ALx_CO_ISM#030*	*CO#0170*
Continuity of Operations Plan	*ALx_CO_ISM#040*	*CO#0180*
Configuration Management	*ALx_CO_ISM#050*	*CO#0190*
Quality Management	*ALx_CO_ISM#060*	*CO#0200*
System Installation and Operation Controls	*ALx_CO_ISM#070*	*CO#0210*
Internal Service Audit	*ALx_CO_ISM#080*	*CO#0220*
Audit Records	*ALx_CO_ISM#100*	*CO#0230*
Best Practice Security Management	*ALx_CO_ISM#120*	*CO#0240*
General Service Definition	*ALx_CO_NUI#010*	*CO#0080*
Service Definition inclusions	*ALx_CO_NUI#020*	*CO#0090*
ALx Configuration Specification	*ALx_CO_NUI#025*	*CO#0100*
Due notification	*ALx_CO_NUI#030*	*CO#0110*
User Acceptance	*ALx_CO_NUI#040*	*CO#0120*
Record of User Acceptance	*ALx_CO_NUI#050*	*CO#0130*
Change of Subscriber Information	*ALx_CO_NUI#070*	*CO#0140*
Defined security roles	*ALx_CO_OPN#020*	*CO#0270*
Acknowledgement of assigned security roles and responsibilities	*ALx_CO_OPN#025*	*CO#0280*

Personnel recruitment	*ALx_CO_OPN#030*	*CO#0290*
Personnel skills	*ALx_CO_OPN#040*	*CO#0300*
Adequacy of Personnel resources	*ALx_CO_OPN#050*	*CO#0310*
Security event logging	*ALx_CO_SER#010*	*CO#0250*
Demonstrated availability	*ALx_CO_SER#020*	*CO#0260*
	End of ALx_CO_SAC criteria	

==>

Criterion title	*new tag*	*old tag*
Established enterprise	*CO#0010*	*ALx_CO_ESM#001*
Legal & Contractual compliance	*CO#0020*	*ALx_CO_ESM#030*
Financial Provisions	*CO#0030*	*ALx_CO_ESM#040*
Data Retention and Protection	*CO#0040*	*ALx_CO_ESM#050*
Termination provisions	*CO#0050*	*ALx_CO_ESM#055*
Ownership	*CO#0060*	*ALx_CO_ESM#060*
Independent management and operations	*CO#0070*	*ALx_CO_ESM#070*
General Service Definition	*CO#0080*	*ALx_CO_NUI#010*
Service Definition inclusions	*CO#0090*	*ALx_CO_NUI#020*
ALx Configuration Specification	*CO#0100*	*ALx_CO_NUI#025*
Due notification	*CO#0110*	*ALx_CO_NUI#030*
User Acceptance	*CO#0120*	*ALx_CO_NUI#040*
Record of User Acceptance	*CO#0130*	*ALx_CO_NUI#050*
Change of Subscriber Information	*CO#0140*	*ALx_CO_NUI#070*
Documented policies and procedures	*CO#0150*	*ALx_CO_ISM#010*
Policy Management and Responsibility	*CO#0160*	*ALx_CO_ISM#020*
Risk Management	*CO#0170*	*ALx_CO_ISM#030*
Continuity of Operations Plan	*CO#0180*	*ALx_CO_ISM#040*
Configuration Management	*CO#0190*	*ALx_CO_ISM#050*
Quality Management	*CO#0200*	*ALx_CO_ISM#060*
System Installation and Operation Controls	*CO#0210*	*ALx_CO_ISM#070*
Internal Service Audit	*CO#0220*	*ALx_CO_ISM#080*
Audit Records	*CO#0230*	*ALx_CO_ISM#100*
Best Practice Security Management	*CO#0240*	*ALx_CO_ISM#120*
Security event logging	*CO#0250*	*ALx_CO_SER#010*
Demonstrated availability	*CO#0260*	*ALx_CO_SER#020*
Defined security roles	*CO#0270*	*ALx_CO_OPN#020*
Acknowledgement of assigned security roles and responsibilities	*CO#0280*	*ALx_CO_OPN#025*

Personnel recruitment	*CO#0290*	*ALx_CO_OPN#030*
Personnel skills	*CO#0300*	*ALx_CO_OPN#040*
Adequacy of Personnel resources	*CO#0310*	*ALx_CO_OPN#050*
Contracted policies and procedures	*CO#0320*	*ALx_CO_ESC#010*
Visibility of Contracted Parties	*CO#0330*	*ALx_CO_ESC#020*
		End of ALx_CO_SAC criteria