Identity Assurance Framework: - KIAF-1410
Commonly-Applicable
Service Assessment Criteria

Version	2.0
Publication Date	2018-11-09
Effective Date	Immediate
Status	Final Recommendation
Approval Authority	IAWG

Editor	Richard G. Wilsher Zygma Inc.
Contributors	IAWG Participants / Non-participants, current as of the date of publication.

Abstract

This Specification describes the Service Assessment Criteria which are to be applied to all assessed credential services, irrespective of their standards basis or applicable assurance levels.

Notice

Contents

1 INTRODUCTION

Kantara Initiative, Inc. formed the Identity Assurance Work Group (IAWG) to foster adoption of consistently managed identity trust services. The IAWG's objective is to create a Framework of baseline policy requirements (criteria) and rules against which identity trust services can be assessed. The goal is to facilitate trusted identity federation and to promote uniformity and interoperability amongst identity service providers, with a specific focus on the level of trust, or assurance, associated with identity assertions. The primary deliverable of IAWG is the Identity Assurance Framework (IAF).

The IAF specifies criteria for a harmonized, best-of-breed, industry-recognized identity assurance standard. The IAF is a Framework supporting mutual acceptance, validation, and life cycle maintenance across identity federations. It is composed of a set of documents that includes an *Overview* publication, the IAF *Glossary*, a summary document on *Assurance Levels*, a Service Assessment Handbook and an Assessor Accreditation Handbook, as well as several subordinate documents. The present document, describes the Commonly-Applicable Service Assessment Criteria component of the IAF.

The latest versions of each of these documents can be found on Kantara's Identity Assurance Framework - General Information web page.

The Commonly-Applicable Service Assessment Criteria part of the IAF establishes baseline criteria for general organizational conformity, identity proofing services, credential strength, and credential management services against which all CSPs will be assessed.

1.1 Changes in this revision

The following changes are included in this revision:

1) '*AL*[*2/3/4*]*_CO_NUI#020 Service Definition inclusions*' has been modified to specifically mention 'Authentication' and to accommodate separate availability specification for different components of an overall service, with '*AL*[*2/3/4*]*_CO_SER#020 Demonstrated availability*' being introduced to require that availability be determined and therefore assessable;
2) Additional explanatory material added to §3.3;
3) Insubstantial editorial revisions.

2 ASSURANCE LEVELS

From its inception (2005), the Kantara Initiative has adopted Assurance Levels (ALs), based on the four levels of assurance posited by the U.S. Federal Government and described in OMB M-04-04 [M-04-04] and NIST Special Publication 800-63 revisions 1 and 2 [NIST800-63r2].

Commencing in 2018 Kantara Initiative put in place a new Class of Approval (see https://kantarainitiative.org/trustoperations/classes-of-approval/) which recognized NIST Special Publication 800-63 revision 3 [NIST800-63r3] and developed criteria which explicitly respond to the Identity and Authentication Assurance Levels 2 (IAL2 and AAL2, respectively) established by [NIST800-63r3].

The criteria in this document are those previously published in KIAF-1400 under the collective grouping referred-to as the 'CO_SAC', which applied to commonly-applicable criteria which had to be met by all service providers, but which were written from a general [NIST800-63r2] perspective.

This present document, KIAF-1410, presents a modified form of the CO_SAC originally published as part of KIAF-1400, which is intended to be applicable to CSPs irrespective of the technical basis for their services' functions. The intended applicability based on the target assurance level of the service in question should be based on the ALs identified in §4.1 through §4.4, as applicable.

The criteria in this document are a sub-set of the CO_SAC as presented in KIAF-1400, being reduced by a small number of criteria which are not applicable to services seeking to conform to [NIST800-63r3]. For services continuing to be assessed for conformance against [NIST800-63r2] those criteria are transferred in to OP_SAC, defined in KIAF-1420.

An overall description of Kantara's operations can be found on the Trust Framework Operations Program (TFOP) web page - https://kantarainitiative.org/trustoperations/.

The latest versions of each of the above-referenced documents can be found on Kantara's Identity Assurance Framework web page - https://kantarainitiative.org/confluence/display/LC/Identity+Assurance+Framework.

3 SERVICE ASSESSMENT CRITERIA - GENERAL

3.1 Context and Scope

These Service Assessment Criteria (SAC) are prepared and maintained by the Identity Assurance Work Group (IAWG) as part of its Identity Assurance Framework. These criteria set out commonly-applicable requirements for credential services and their providers at assurance levels AL2 and AL3/(IAL/AAL/FAL)2.

These criteria are intended to be complemented by other criteria sets which address particular standards-based operational functionality, as defined for specific Classes of Approval. The Classes of Approval and their parameters (AL, etc.) are described at https://kantarainitiative.org/trustoperations/classes-of-approval/ .

3.2 Status and Readership

This document sets out **normative** Kantara requirements and is required reading for Kantara-Accredited Assessors and applicant Service Providers. It will also be of interest to those wishing to gain a detailed knowledge of the workings of the Kantara Initiative Inc.'s Identity Assurance Framework. It sets out the Service Assessment Criteria to which credential services must conform in order to be granted Kantara Approval.

The description of criteria in this document is required reading for all organizations wishing to become Kantara-Approved credential services, and also for those wishing to become Kantara-Accredited Assessors. It is also recommended reading for those involved in the governance and day-to-day administration of the Identity Assurance Framework.

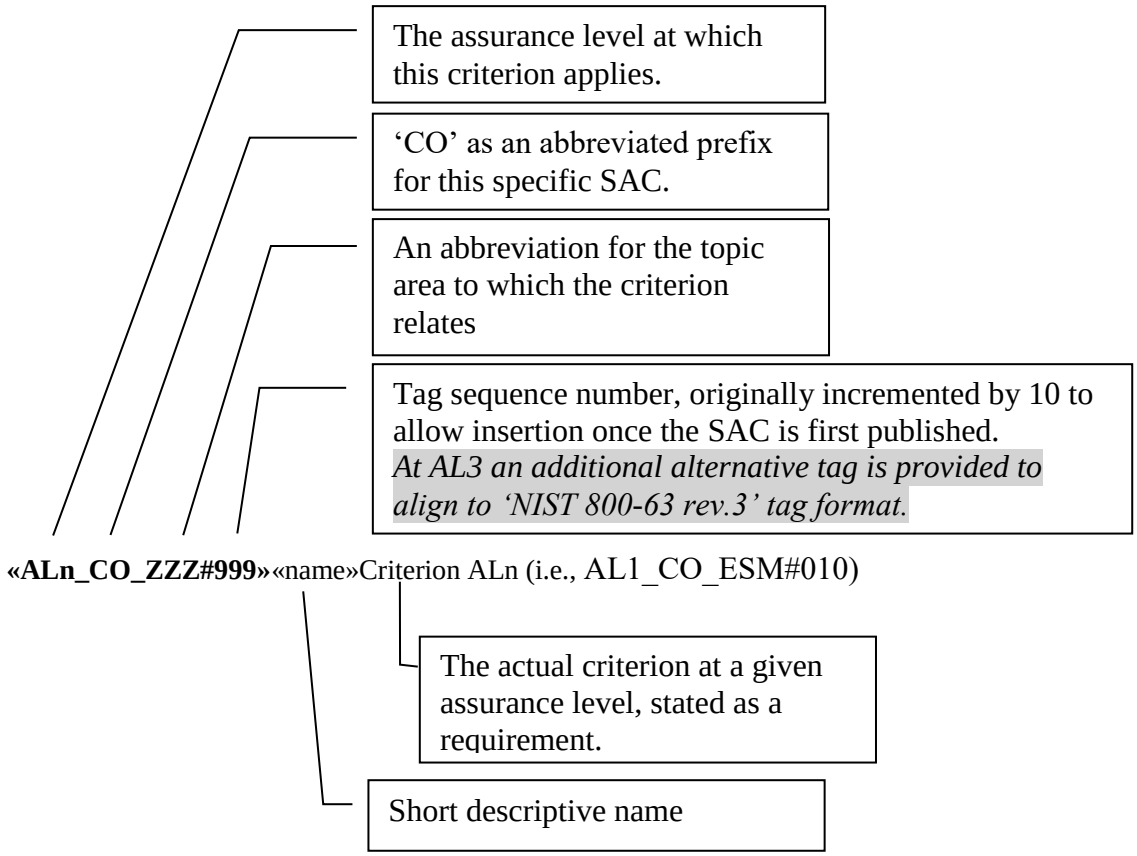
This document will also be of interest to those seeking a detailed understanding of the operation of the Identity Assurance Framework but who are not actively involved in its operations or in services that may fall within the scope of the Framework.

3.3 Criteria Descriptions

The Service Assessment Criteria are organized by AL. Subsections within each level describe the criteria that apply to specific functions. The subsections are parallel. Subsections describing the requirements for the same function at different levels of assurance have the same title.

Each criterion consists of three components: a unique alphanumeric tag, a short name, and the criterion (or criteria) associated with the tag. The tag provides a unique reference for each criterion that assessors and service providers can use to refer to that criterion. The name identifies the intended scope or purpose of the criterion.

The criteria are described as follows:



When a given criterion changes (i.e. becomes more rigorous) at higher Assurance Levels the new or revised text is **shown in bold** or '**[Omitted]**' is indicated where text has been removed. With the obvious exception of AL1, when a criterion is first introduced it is also shown in bold.

As noted in the above schematic, when originally prepared, the tags had numbers incrementing in multiples of ten to permit the later insertion of additional criteria. Since then there has been addition and withdrawal of criteria.

Where a criterion is not used in a given AL but is used at a higher AL its place is held by the inclusion of a tag which is marked 'No stipulation'. A title and appropriate criteria will be added at the higher AL which occupies that position. Since in general higher ALs have a greater extent of criteria than lower ALs, where a given AL extends no further through the numbering range, criteria beyond that value are by default omitted rather than being included but marked 'No stipulation'.

Further, over time, some criteria have been removed, or withdrawn. In order to avoid the re-use of that tag such tags are retained but marked 'Withdrawn'.

Not only do these editorial practices preserve continuity they also guard against possible omission of a required criterion through an editing error.

3.4 Terminology

All special terms used in this document are defined in the *IAF Glossary*, which can be found on Kantara's Identity Assurance Framework - General Information page.

Note that when, in these criteria, the term 'Subscriber' is used it applies equally to 'Subscriber' and 'Subject' as defined in the *IAF Glossary*, according to the context in which used. The term 'Subject' is used when the reference is explicitly toward that party.

4 COMMONLY-APPLICABLE SERVICE ASSESSMENT CRITERIA

The Service Assessment Criteria in this section establish the general business and organizational requirements for conformity of services and service providers at all Assurance Levels (AL) – refer to Section 2. These criteria are generally referred to elsewhere within IAWG documentation as CO-SAC and can be identified by their tag "ALn_CO_ xxxx" or by an alternative tag 'CO#xxxx' when applied to an assessment for any non-[NIST800-63r2] Class of Approval.

These criteria must be conformed-to by all applicants for Approval, whether for Service Components or Full Service Provision.

4.1 Assurance Level 1

4.1.1 Enterprise and Service Maturity

These criteria apply to the establishment of the organization offering the service and its basic standing as a legal and operational business entity within its respective jurisdiction or country.

An enterprise and its specified service must:

AL1_CO_ESM#010 Established enterprise
Be a valid legal entity, and a person with the legal authority to commit the organization must submit the signed assessment package.

AL1_CO_ESM#020 Withdrawn
Withdrawn

AL1_CO_ESM#030 Legal & Contractual compliance
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 and countries within which its services may be offered.

Guidance: '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.

AL1_CO_ESM#040 No stipulation

AL1_CO_ESM#050 Data Retention and Protection
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).

AL1_CO_ESM#055 Termination provisions

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.

Guidance: 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 service.

4.1.2 Notices and User information

These criteria address the publication of information describing the service and the manner of and any limitations upon its provision.

An enterprise and its specified service must:

AL1_CO_NUI#010 General Service Definition
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.

Guidance: The intended user community encompasses potential and actual Subscribers, Subjects, and Relying Parties.

AL1_CO_NUI#020 Service Definition inclusions
Make available a Service Definition for the specified service containing clauses that provide the following information:

a) a Privacy Policy.

AL1_CO_NUI#030 Due notification
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, Conditions, and Privacy Policy for the specified service.

AL1_CO_NUI#040 User Acceptance
Require Subscribers and Subjects to:

a) indicate, prior to receiving service, that they have read and accept the terms of service as defined in the Service Definition;
b) at periodic intervals, determined by significant service provision events (e.g. issuance, re-issuance, renewal), re-affirm their understanding and observance of the terms of service;
c) always provide full and correct responses to requests for information.

AL1_CO_NUI#050 Record of User Acceptance
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 by significant service provision events (e.g. re-issuance, renewal).

4.1.3 No stipulation

4.1.4 No stipulation

4.1.5 No stipulation

4.1.6 No stipulation

4.1.7 Secure Communications

AL1_CO_SCO#010 No stipulation
AL1_CO_SCO#015 No stipulation
AL1_CO_SCO#016 No stipulation
AL1_CO_SCO#020 Withdrawn
Withdrawn – See KIAF-1420: AL1_CM_SCO#020.

4.2 Assurance Level 2

Criteria in this section address the establishment of the enterprise offering the service and its basic standing as a legal and operational business entity within its respective jurisdiction or country, at AL2 per [OMB M-04-04].

4.2.1 Enterprise and Service Maturity

These criteria apply to the establishment of the enterprise offering the service and its basic standing as a legal and operational business entity.

An enterprise and its specified service must:

AL2_CO_ESM#010 Established enterprise
Be a valid legal entity, and a person with legal authority to commit the organization must submit the signed assessment package.

AL2_CO_ESM#020 Withdrawn
Withdrawn

AL2_CO_ESM#030 Legal & Contractual compliance
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.

Guidance: Kantara Initiative Inc. will not recognize a service which is not fully released for the provision of services to its intended user/client community. Systems, or parts thereof, which are not fully proven and released shall not be considered in an assessment and therefore should not be included within the scope of the assessment package. Parts of systems still under development, or even still being planned, are therefore ineligible for inclusion within the scope of assessment.

AL2_CO_ESM#040 Financial Provisions
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.

Guidance: 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 services that are not likely to be sustainable over at least this minimum period of time.

AL2_CO_ESM#050 Data Retention and Protection
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).

Guidance: 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.

AL2_CO_ESM#055 Termination provisions
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.

Guidance: 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 service.

4.2.2 Notices and User Information/Agreements

These criteria apply to the publication of information describing the service and the manner of and any limitations upon its provision, and how users are required to accept those terms.

An enterprise and its specified service must:

AL2_CO_NUI#010 General Service Definition
Make available to the intended user community a Service Definition that includes all applicable Terms, Conditions, and Fees, including any limitations of its usage, and definitions of any terms having specific intention or interpretation. Specific provisions are stated in further criteria in this section.

Guidance: The intended user community encompasses potential and actual Subscribers, Subjects, and Relying Parties.

AL2_CO_NUI#020 Service Definition inclusions
Make available a Service Definition for the specified service containing clauses that provide the following information:

a) Privacy, Identity Proofing & Verification, Authentication, Renewal/Re-issuance, and Revocation and Termination Policies;
b) the country in or legal jurisdiction under which the service is operated;
c) if different from the above, the legal jurisdiction under which Subscriber and any relying party agreements are entered into;
d) applicable legislation with which the service complies;
e) obligations incumbent upon the CSP;
f) obligations incumbent upon each class of user of the service, e.g. Relying Parties, Subscribers and Subjects;
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;
h) statement of warranties;
i) statement of liabilities toward Subscribers, Subjects and Relying Parties;
j) procedures for notification of changes to terms and conditions;
k) steps the CSP will take in the event that it chooses or is obliged to terminate the service;
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.

Guidance: 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 documented and appropriately-available statements which fulfill these requirements in the context of the subject service must be produced and applied by the CSP.

AL2_CO_NUI#025 AL2 Configuration Specification
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 at least an AL2 baseline service.

AL2_CO_NUI#030 Due notification
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.

AL2_CO_NUI#040 User Acceptance
Require Subscribers and Subjects to:

a) indicate, prior to receiving service, that they have read and accept the terms of service as defined in the Service Definition;
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;
c) always provide full and correct responses to requests for information.

AL2_CO_NUI#050 Record of User Acceptance
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 by significant service provision events (e.g. re-issuance, renewal) and otherwise at least once every five years.

AL2_CO_NUI#060 Withdrawn
Withdrawn.

AL2_CO_NUI#070 Change of Subscriber Information
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.

4.2.3 Information Security Management

These criteria address the way in which the enterprise manages the security of its business, the specified service, and information it holds relating to its user community. This section focuses on the key components that comprise a well-established and effective Information Security Management System (ISMS), or other IT security management methodology recognized by a government or professional body.

An enterprise and its specified service must:

AL2_CO_ISM#010 Documented policies and procedures
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.

AL2_CO_ISM#020 Policy Management and Responsibility
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.

AL2_CO_ISM#030 Risk Management
Demonstrate a risk management methodology that adequately identifies and mitigates risks related to the specified service and its user community.

AL2_CO_ISM#040 Continuity of Operations Plan
Have and keep updated a Continuity of Operations Plan that covers disaster recovery and the resilience of the specified service.

AL2_CO_ISM#050 Configuration Management
Demonstrate that there is in place a configuration management system that at least includes:

a) version control for software system components;
b) timely identification and installation of all organizationally-approved patches for any software used in the provisioning of the specified service.

AL2_CO_ISM#060 Quality Management
Demonstrate that there is in place a quality management system that is appropriate for the specified service.

AL2_CO_ISM#070 System Installation and Operation Controls
Apply controls during system development, procurement installation, and operation that protect the security and integrity of the system environment, hardware, software, and communications.

AL2_CO_ISM#080 Internal Service Audit
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.

Guidance: '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 independent internal resources but wishes to benefit from the value which audits can provide, and for the purposes of fulfilling Kantara's needs, a formal Kantara Assessment performed by an Accredited Assessor should be considered as such.

AL2_CO_ISM#090 Withdrawn
Withdrawn.

AL2_CO_ISM#100 Audit Records
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.

AL2_CO_ISM#110 Withdrawn
Withdrawn.

4.2.4 Security-relevant Event (Audit) Records

These criteria apply to the need to provide an auditable log of all events that are pertinent to the correct and secure operation of the service.

An enterprise and its specified service must:

AL2_CO_SER#010 Security event logging
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.

Guidance: 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.

AL2_CO_SER#020 Demonstrated availability
Determine actual availability achieved in comparison to the stated availability targets (refer to *AL2_CO_NUI#020 l)).*

4.2.5 Operational infrastructure

These criteria apply to the infrastructure within which the delivery of the specified service takes place. These criteria emphasize the personnel involved and their selection, training, and duties.

An enterprise and its specified service must:

AL2_CO_OPN#010 Withdrawn
Withdrawn.

AL2_CO_OPN#020 Defined security roles
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.

AL2_CO_OPN#030 Personnel recruitment
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.

AL2_CO_OPN#040 Personnel skills
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.

AL2_CO_OPN#050 Adequacy of Personnel resources
Have sufficient staff to adequately operate and resource the specified service according to its policies and procedures.

AL2_CO_OPN#060 Withdrawn
Withdrawn – See KIAF-1420: AL2_CM_OPN#060.

AL2_CO_OPN#070 Withdrawn
Withdrawn – See KIAF-1420: AL2_CM_OPN#070.

4.2.6 External Services and Components

These criteria apply to the relationships and obligations upon contracted parties both to apply the policies and procedures of the enterprise and also to be available for assessment as critical parts of the overall service provision.

An enterprise and its specified service must:

AL2_CO_ESC#010 Contracted policies and procedures
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.

AL2_CO_ESC#020 Visibility of contracted parties
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 the suppliers' compliance with contractually-stipulated policies and procedures, and thus with IAF Service Assessment Criteria, can be independently verified, and subsequently monitored if necessary.

4.2.7 Secure Communications

An enterprise and its specified service must:

AL2_CO_SCO#010 Withdrawn
Withdrawn – See KIAF-1420: AL2_CM_SCO#010.

AL2_CO_SCO#015 Withdrawn
Withdrawn – See KIAF-1420: AL2_CM_SCO#015.

AL2_CO_SCO#020 Withdrawn
Withdrawn – See KIAF-1420: AL2_CM_SCO#020.

AL2_CO_SCO#030 Withdrawn
Withdrawn – See KIAF-1420: AL2_CM_SCO#030.

4.3 Assurance Level 3

Achieving AL3 per [OMB M-04-04] or xAL2 per at [NIST800-63r3] requires meeting more stringent criteria in addition to all criteria required to achieve AL2 per [OMB M-04-04]. The criteria at this level of rigour are stated in full.

Criteria in this section carry a second tag reference which may be preferentially used when related to assessments against Kantara's [NIST800-63r3] criteria, which have a similar tag form (see KIAF-1430).

4.3.1 Enterprise and Service Maturity

Criteria in this section address the establishment of the enterprise offering the service and its basic standing as a legal and operational business entity.

An enterprise and its specified service must:

AL3_CO_ESM#010 / CO#0010 Established enterprise
Be a valid legal entity and a person with legal authority to commit the organization must submit the signed assessment package.

AL3_CO_ESM#020 Withdrawn
Withdrawn

AL3_CO_ESM#030 / CO#0020 Legal & Contractual compliance
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.

Guidance: Kantara Initiative, Inc. will not recognize a service which is not fully released for the provision of services to its intended user/client community. Systems, or parts thereof, which are not fully proven and released shall not be considered in an assessment and therefore should not be included within the scope of the assessment package. Parts of systems still under development, or even still being planned, are therefore ineligible for inclusion within the scope of assessment.

AL3_CO_ESM#040 / CO#0030 Financial Provisions
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.

Guidance: 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 services that are not likely to be sustainable over at least this minimum period of time.

AL3_CO_ESM#050 / CO#0040 Data Retention and Protection
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 private information (against unlawful or unauthorized access, excepting that permitted by the information owner or required by due process).

AL3_CO_ESM#055 / CO#0050 Termination provisions
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.

Guidance: 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 service.

AL3_CO_ESM#060 / CO#0060 Ownership
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.

AL3_CO_ESM#070 / CO#0070 Independent management and operations
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.

4.3.2 Notices and User Information

Criteria in this section address the publication of information describing the service and the manner of and any limitations upon its provision, and how users are required to accept those terms.

An enterprise and its specified service must:

AL3_CO_NUI#010 / CO#0080 General Service Definition
Make available to the intended user community a Service Definition that includes all applicable Terms, Conditions, and Fees, including any limitations of its usage, and definitions of any terms having specific intention or interpretation. Specific provisions are stated in further criteria in this section.

Guidance: The intended user community encompasses potential and actual Subscribers, Subjects and Relying Parties.

AL3_CO_NUI#020 / CO#0090 Service Definition inclusions
Make available a Service Definition for the specified service containing clauses that provide the following information:

a) Privacy, Identity Proofing & Verification, Authentication, Renewal/Re-issuance, and Revocation and Termination Policies;)
b) the country in or the legal jurisdiction under which the service is operated;
c) if different to the above, the legal jurisdiction under which Subscriber and any relying party agreements are entered into;
d) applicable legislation with which the service complies;
e) obligations incumbent upon the CSP;
f) obligations incumbent upon each class of user of the service, e.g. Relying Parties, Subscribers and Subjects, ...;

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's product;
h) statement of warranties;
i) statement of liabilities toward both Subjects and Relying Parties;
j) procedures for notification of changes to terms and conditions;
k) steps the CSP will take in the event that it chooses or is obliged to terminate the service;
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.

Guidance: 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 documented and appropriately-available statements which fulfill these requirements in the context of the subject service must be produced and applied by the CSP.

AL3_CO_NUI#025 / CO#0100 AL3 Configuration Specification
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 at least an **AL3** baseline service.

AL3_CO_NUI#030 / CO#0110 Due notification
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.

AL3_CO_NUI#040 / CO#0120 User Acceptance
Require Subscribers and Subjects to:

a) indicate, prior to receiving service, that they have read and accept the terms of service as defined in the Service Definition;
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;
c) always provide full and correct responses to requests for information.

AL3_CO_NUI#050 / CO#0130 Record of User Acceptance
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.

AL3_CO_NUI#060 Withdrawn
Withdrawn.

AL3_CO_NUI#070 / CO#0140 Change of Subscriber Information

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.

4.3.3 Information Security Management

These criteria address the way in which the enterprise manages the security of its business, the specified service, and information it holds relating to its user community. This section focuses on the key components that make up a well-established and effective Information Security Management System (ISMS), or other IT security management methodology recognized by a government or professional body.

An enterprise and its specified service must:

AL3_CO_ISM#010 / CO#0150 Documented policies and procedures
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.

AL3_CO_ISM#020 / CO#0160 Policy Management and Responsibility
Have a clearly defined managerial role, at a senior level, where full responsibility for the business' 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.

AL3_CO_ISM#030 / CO#0170 Risk Management
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**.

AL3_CO_ISM#040 / CO#0180 Continuity of Operations Plan
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**.

AL3_CO_ISM#050 / CO#0190 Configuration Management
Demonstrate that there is in place a configuration management system that at least includes:

a) version control for software system components;
b) timely identification and installation of all organizationally-approved patches for any software used in the provisioning of the specified service**;**
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.

AL3_CO_ISM#060 / CO#0200 Quality Management
Demonstrate that there is in place a quality management system that is appropriate for the specified service.

AL3_CO_ISM#070 / CO#0210 System Installation and Operation Controls
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:**

a) the software and hardware development environments, for customized components;

b) the procurement process for commercial off-the-shelf (COTS) components;
c) contracted consultancy/support services;
d) shipment of system components;
e) storage of system components;
f) installation environment security;
g) system configuration;
h) transfer to operational status.

AL3_CO_ISM#080 / CO#0220 Internal Service Audit
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.

Guidance: '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 show that the internal management system controls are being appropriately applied, and for the purposes of fulfilling Kantara's needs, a formal Kantara Assessment performed by an Accredited Assessor should be considered as such.

AL3_CO_ISM#090 Withdrawn
Withdrawn.

AL3_CO_ISM#100 / CO#0230 Audit Records
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.

AL3_CO_ISM#110 Withdrawn
Withdrawn.

AL3_CO_ISM#120 / CO#0240 Best Practice Security Management
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.

Guidance: The auditors determining that this ISMS meets the above requirement must be appropriately qualified in assessing the specific management system or methodology applied.

4.3.4 Security-Relevant Event (Audit) Records

The criteria in this section are concerned with the need to provide an auditable log of all events that are pertinent to the correct and secure operation of the service.

An enterprise and its specified service must:

AL3_CO_SER#010 / CO#0250 Security Event Logging
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.

Guidance: 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 authenticatable.

AL3_CO_SER#020 / CO#0255 Demonstrated availability
Determine actual availability achieved in comparison to the stated availability targets (refer to *AL3_CO_NUI#020 / CO#0090 l)).*

4.3.5 Operational Infrastructure

The criteria in this section address the infrastructure within which the delivery of the specified service takes place. It puts particular emphasis upon the personnel involved, and their selection, training, and duties.

An enterprise and its specified service must:

AL3_CO_OPN#010 Withdrawn
Withdrawn.

AL3_CO_OPN#020 / CO#0260 Defined security roles
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.

AL3_CO_OPN#025 / CO#0270 Acknowledgement of assigned security roles and responsibilities
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.

AL3_CO_OPN#030 / CO#0280 Personnel recruitment
Demonstrate that it has defined practices for the selection, vetting, 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.**

AL3_CO_OPN#040 / CO#0290 Personnel skills
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.

AL3_CO_OPN#050 / CO#0300 Adequacy of Personnel resources

Have sufficient staff to adequately operate and resource the specified service according to its policies and procedures.

AL3_CO_OPN#060 Withdrawn
Withdrawn – See KIAF-1420: AL3_OP_OPN#060.
AL3_CO_OPN#070 Withdrawn
Withdrawn – See KIAF-1420: AL3_OP_OPN#070.

4.3.6 External Services and Components

This section addresses the relationships and obligations upon contracted parties both to apply the policies and procedures of the enterprise and also to be available for assessment as critical parts of the overall service provision.

An enterprise and its specified service must:

AL3_CO_ESC#010 / CO#0310 Contracted policies and procedures
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 those parties are engaged through reliable and appropriate contractual arrangements which stipulate which critical policies, procedures, and practices sub-contractors are required to fulfill.

AL3_CO_ESC#020 / CO#0320 Visibility of contracted parties
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 controls, 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. å

4.3.7 Secure Communications

An enterprise and its specified service must:

AL3_CO_SCO#010 Withdrawn
Withdrawn – See KIAF-1420: AL3_OP_SCO#010.

AL3_CO_SCO#015 Withdrawn
Withdrawn – See KIAF-1420: AL3_OP_SCO#015.

AL3_CO_SCO#020 Withdrawn
Withdrawn – See KIAF-1420: AL3_OP_SCO#020.

AL3_CO_SCO#030 Withdrawn
Withdrawn – See KIAF-1420: AL3_OP_SCO#030.

4.4 Assurance Level 4

Achieving AL4 requires meeting even more stringent criteria in addition to the criteria required to achieve AL3.

4.4.1 Enterprise and Service Maturity

Criteria in this section address the establishment of the enterprise offering the service and its basic standing as a legal and operational business entity.

An enterprise and its specified service must:

AL4_CO_ESM#010 Established enterprise
Be a valid legal entity and a person with legal authority to commit the organization must submit the signed assessment package.

AL4_CO_ESM#020 Withdrawn
Withdrawn

AL4_CO_ESM#030 Legal & Contractual compliance
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.

Guidance: Kantara Initiative, Inc. will not recognize a service which is not fully released for the provision of services to its intended user/client community. Systems, or parts thereof, which are not fully proven and released shall not be considered in an assessment and therefore should not be included within the scope of the assessment package. Parts of systems still under development, or even still being planned, are therefore ineligible for inclusion within the scope of assessment.

AL4_CO_ESM#040 Financial Provisions
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.

Guidance: 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 services that are not likely to be sustainable over at least this minimum period of time.

AL4_CO_ESM#050 Data Retention and Protection
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 private information (against unlawful or unauthorized access excepting that permitted by the information owner or required by due process).

AL4_CO_ESM#055 Termination provisions

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.

Guidance: 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 service.

AL4_CO_ESM#060 Ownership
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.

AL4_CO_ESM#070 Independent Management and Operations
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.

4.4.2 Notices and Subscriber Information/Agreements

Criteria in this section address the publication of information describing the service and the manner of and any limitations upon its provision, and how users are required to accept those terms.

An enterprise and its specified service must:

AL4_CO_NUI#010 General Service Definition
Make available to the intended user community a Service Definition that includes all applicable Terms, Conditions, and Fees, including any limitations of its usage, and definitions of any terms having specific intention or interpretation. Specific provisions are stated in further criteria in this section.

Guidance: The intended user community encompasses potential and actual Subscribers, Subjects, and Relying Parties.

AL4_CO_NUI#020 Service Definition inclusions
Make available a Service Definition for the specified service containing clauses that provide the following information:

a) Privacy, Identity Proofing & Verification, Authentication, Renewal/Re-issuance, and Revocation and Termination Policies;
b) the country in or legal jurisdiction under which the service is operated;
c) if different to the above, the legal jurisdiction under which Subscriber and any relying party agreements are entered into;
d) applicable legislation with which the service complies;
e) obligations incumbent upon the CSP;
f) obligations incumbent upon each class of user of the service, e.g. Relying Parties, Subscribers and Subjects;
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's product;
h) statement of warranties;
i) statement of liabilities toward both Subjects and Relying Parties;

j) procedures for notification of changes to terms and conditions;
k) steps the CSP will take in the event that it chooses or is obliged to terminate the service;
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.

Guidance: 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 documented and appropriately-available statements which fulfill these requirements in the context of the subject service must be produced and applied by the CSP.

AL4_CO_NUI#025 AL4 Configuration Specification
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 at least an **AL4** baseline service.

AL4_CO_NUI#030 Due Notification
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.

AL4_CO_NUI#040 User Acceptance
Require Subscribers and Subjects to:

a) indicate, prior to receiving service, that they have read and accept the terms of service as defined in the Service Definition, thereby indicating their properly-informed opt-in;
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;
c) always provide full and correct responses to requests for information.

AL4_CO_NUI#050 Record of User Acceptance
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. issuance, re-issuance, renewal) and otherwise at least once every five years.

AL4_CO_NUI#060 Withdrawn
Withdrawn.

AL4_CO_NUI#070 Change of Subscriber Information
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.

AL4_CO_NUI#080 Withdrawn
Withdrawn.

4.4.3 Information Security Management

These criteria address the way in which the enterprise manages the security of its business, the specified service, and information it holds relating to its user community. This section focuses on the key components that comprise a well-established and effective Information Security Management System (ISMS), or other IT security management methodology recognized by a government or professional body.

An enterprise and its specified service must:

AL4_CO_ISM#010 Documented policies and procedures
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.

AL4_CO_ISM#020 Policy Management and Responsibility
Have a clearly defined managerial role, at a senior level, where full responsibility for the business' 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.

AL4_CO_ISM#030 Risk Management
Demonstrate a risk management methodology that adequately identifies and mitigates risks related to the specified service and its user community and must show that on-going risk assessment review is conducted as a part of the business' procedures, such as adherence to CobIT or [IS27001] methods.

AL4_CO_ISM#040 Continuity of Operations Plan
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 the business' procedures**.

AL4_CO_ISM#050 Configuration Management
Demonstrate that there is in place a configuration management system that at least includes:

a) version control for software system components;
b) timely identification and installation of all organizationally-approved patches for any software used in the provisioning of the specified service;
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.

AL4_CO_ISM#060 Quality Management
Demonstrate that there is in place a quality management system that is appropriate for the specified service.

AL4_CO_ISM#070 System Installation and Operation Controls
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:

a) the software and hardware development environments, for customized components;
b) the procurement process for commercial off-the-shelf (COTS) components;
c) contracted consultancy/support services;
d) shipment of system components;

e) storage of system components;
f) installation environment security;
g) system configuration;
h) transfer to operational status.

AL4_CO_ISM#080 Internal Service Audit
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.

Guidance: '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 show that the internal management system controls are being appropriately applied, and for the purposes of fulfilling Kantara's needs, a formal Kantara Assessment performed by an Accredited Assessor should be considered as such.

AL4_CO_ISM#090 Withdrawn
Withdrawn.

AL4_CO_ISM#100 Audit Records
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.

AL4_CO_ISM#110 Withdrawn
Withdrawn.

AL4_CO_ISM#120 Best Practice Security Management
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 section must *inter alia* fall wholly within the scope of this ISMS, or the selected recognized alternative.

4.4.4 Security-Related (Audit) Records

The criteria in this section are concerned with the need to provide an auditable log of all events that are pertinent to the correct and secure operation of the service.

An enterprise and its specified service must:

AL4_CO_SER#010 Security Event Logging
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.

Guidance: The trusted time source could be an external trusted service or a network time server or other hardware timing device. The time source must be not only precise but authenticatable as well.

AL4_CO_SER#020 Demonstrated availability
Determine actual availability achieved in comparison to the stated availability targets (refer to *AL4_CO_NUI#020 l)).*

4.4.5 Operational Infrastructure

The criteria in this section address the infrastructure within which the delivery of the specified service takes place. It puts particular emphasis upon the personnel involved, and their selection, training, and duties.

An enterprise and its specified service must:

AL4_CO_OPN#010 Withdrawn
Withdrawn.

AL4_CO_OPN#020 Defined Security Roles
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.

AL4_CO_OPN#025 Acknowledgement of assigned security roles and responsibilities
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.

AL4_CO_OPN#030 Personnel Recruitment
Demonstrate that it has defined practices for the selection, vetting, 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.

AL4_CO_OPN#040 Personnel skills
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.

AL4_CO_OPN#050 Adequacy of Personnel resources
Have sufficient staff to adequately operate and resource the specified service according to its policies and procedures**.**

AL4_CO_OPN#060 Withdrawn
Withdrawn – See KIAF-1420: AL4_CM_OPN#060.

AL4_CO_OPN#070 Withdrawn

Withdrawn – See KIAF-1420: AL4_CM_OPN#070.
Employ logical access control mechanisms that ensure access to sensitive system functions and controls is restricted to authorized personnel.

4.4.6 External Services and Components

This section addresses the relationships and obligations upon contracted parties both to apply the policies and procedures of the enterprise and also to be available for assessment as critical parts of the overall service provision.

An enterprise and its specified service must:

AL4_CO_ESC#010 Contracted Policies and Procedures
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 those parties are engaged through reliable and appropriate contractual arrangements which stipulate which critical policies, procedures, and practices sub-contractors are required to fulfill.

AL4_CO_ESC#020 Visibility of Contracted Parties
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.

4.4.7 Secure Communications

An enterprise and its specified service must:

AL4_CO_SCO#010 Withdrawn
Withdrawn – See KIAF-1420: AL4_CM_SCO#010.

AL4_CO_SCO#015 Withdrawn
Withdrawn – See KIAF-1420: AL4_CM_SCO#015.

AL4_CO_SCO#020 Withdrawn
Withdrawn – See KIAF-1420: AL4_CM_SCO#020.

5 OPERATIONAL SERVICE ASSESSMENT CRITERIA

This section is retained purely to enable the convenience of §6 and §7 ordering with those same clauses in KIAF-1400.

6 REFERENCES / BIBLIOGRAPHY

[CAF] Louden, Chris, Spencer, Judy; Burr, Bill; Hawkins, Kevin; Temoshok, David; Cornell, John; Wilsher, Richard G.; Timchak, Steve; Sill, Stephen; Silver, Dave; Harrison, Von; eds., "E-Authentication Credential Assessment Framework (CAF)," E-Authentication Initiative, Version 2.0.0 (March 16, 2005).

[EAP CSAC 04011] "EAP working paper: Identity Proofing Service Assessment Criteria (ID-SAC)," Electronic Authentication Partnership, Draft 0.1.3 (July 20, 2004).

[EAPTrustFramework] "Electronic Authentication Partnership Trust Framework" Electronic Authentication Partnership, Version 1.0. (January 6, 2005).

[FIPS140-2] "Security Requirements for Cryptographic Modules" Federal Information Processing Standards. (May 25, 2001).
http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[IS27001] ISO/IEC 27001:2013 "Information technology - Security techniques - Requirements for information security management systems", International Organization for Standardization.
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

[IS19790] ISO/IEC 19790:2012 “Information technology - Security techniques - Security requirements for cryptographic modules”, International Organization for Standardization.
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=52906

[M-04-04] Bolton, Joshua B., ed., "E-Authentication Guidance for Federal Agencies", Office of Management and Budget, (December 16, 2003). http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

[NIST800-63r2] Burr, William E.; Dodson, Donna F.; Polk, W. Timothy; eds., "Electronic Authentication Guideline: : Recommendations of the National Institute of Standards and Technology," Version 1.0.2, National Institute of Standards and Technology, (April, 2006).
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

[NIST800-63r3] Fenton, Grassi et al., "Digital Identity Guidelines" Revision 3, National Institute of Standards and Technology, (June, 2017).
https://pages.nist.gov/800-63-3/

[RFC 3647] Chokhani, S.; Ford, W.; Sabett, R.; Merrill, C.; Wu, S.; eds., "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework," The Internet Engineering Task Force (November, 2003). http://www.ietf.org/rfc/rfc3647.txt

[5415] Ed. Wilsher, Richard G. “SAC mapping – ISO/IEC 29115 / ITU-T X.1254 – Entity authentication assurance framework” v0.7.0.

7 REVISION HISTORY

1. v1.0, 2018-03-21 – first release
2. v2.0, 2018-10-26 – revised criteria addressing service availability.