

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17

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.

18 **Notice**

19 All rights reserved. This Specification has been prepared by Participants of the Identity Assurance Working
20 Group of the Kantara Initiative. No rights are granted to Non-Participants of the Identity Assurance Working
21 Group nor any other person or entity to reproduce or otherwise prepare derivative works without the prior
22 written permission of the publisher, except in the case of brief quotations embodied in critical reviews and
23 certain other noncommercial uses permitted by copyright law. Entities seeking permission to reproduce
24 portions of this Specification for other uses must contact the Kantara Initiative to determine whether an
25 appropriate license for such use is available.

26 Implementation or use of certain elements of this Specification may require licenses under third party
27 intellectual property rights, including without limitation, patent rights. The Participants of and any other
28 contributors to the document are not and shall not be held responsible in any manner for identifying or failing
29 to identify any or all such third party intellectual property rights. This document is provided "AS IS" and no
30 Participant in the Kantara Initiative makes any warranty of any kind, expressed or implied, including any
31 implied warranties of merchantability, non-infringement of third party intellectual property rights, and fitness
32 for a particular purpose.

33 **IPR:** [Option Patent & Copyright: Reciprocal Royalty Free with Opt-Out to Reasonable And Non](#)
34 [Discriminatory terms \(RAND\)](#) | Copyright © 2018

35

36		Contents	
37	1	INTRODUCTION	4
38	1.1	Changes in this revision	4
39	2	ASSURANCE LEVELS	5
40	3	SERVICE ASSESSMENT CRITERIA - GENERAL	6
41	3.1	Context and Scope	6
42	3.2	Status and Readership	6
43	3.3	Criteria Descriptions	6
44	3.4	Terminology	8
45	4	COMMONLY-APPLICABLE SERVICE ASSESSMENT CRITERIA	9
46	4.1	Assurance Level 1	9
47	4.1.1	Enterprise and Service Maturity	9
48	4.1.2	Notices and User information	10
49	4.1.3	No stipulation	11
50	4.1.4	No stipulation	11
51	4.1.5	No stipulation	11
52	4.1.6	No stipulation	11
53	4.1.7	Secure Communications	11
54	4.2	Assurance Level 2	12
55	4.2.1	Enterprise and Service Maturity	12
56	4.2.2	Notices and User Information/Agreements	13
57	4.2.3	Information Security Management	14
58	4.2.4	Security-relevant Event (Audit) Records	16
59	4.2.5	Operational infrastructure	16
60	4.2.6	External Services and Components	17
61	4.2.7	Secure Communications	17
62	4.3	Assurance Level 3	18
63	4.3.1	Enterprise and Service Maturity	18
64	4.3.2	Notices and User Information	19
65	4.3.3	Information Security Management	21
66	4.3.4	Security-Relevant Event (Audit) Records	22
67	4.3.5	Operational Infrastructure	23
68	4.3.6	External Services and Components	24
69	4.3.7	Secure Communications	24
70	4.4	Assurance Level 4	25
71	4.4.1	Enterprise and Service Maturity	25
72	4.4.2	Notices and Subscriber Information/Agreements	26
73	4.4.3	Information Security Management	28
74	4.4.4	Security-Related (Audit) Records	29
75	4.4.5	Operational Infrastructure	30
76	4.4.6	External Services and Components	31
77	4.4.7	Secure Communications	31
78	5	OPERATIONAL SERVICE ASSESSMENT CRITERIA	32
79	6	REFERENCES / BIBLIOGRAPHY	33
80	7	REVISION HISTORY	34
81			

82 1 INTRODUCTION

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

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

95 The latest versions of each of these documents can be found on Kantara's [Identity Assurance Framework -](#)
96 [General Information web page](#).

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

100 1.1 Changes in this revision

101 The following changes are included in this revision:

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

108 2 ASSURANCE LEVELS

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

112 Commencing in 2018 Kantara Initiative put in place a new Class of Approval (see
113 <https://kantarainitiative.org/trustoperations/classes-of-approval/>) which recognized NIST Special Publication
114 800-63 revision 3 [NIST800-63r3] and developed criteria which explicitly respond to the Identity and
115 Authentication Assurance Levels 2 (IAL2 and AAL2, respectively) established by [NIST800-63r3].

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

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

123 The criteria in this document are a sub-set of the CO_SAC as presented in KIAF-1400, being reduced by a
124 small number of criteria which are not applicable to services seeking
125 to conform to [NIST800-63r3]. For services continuing to be assessed for conformance against [NIST800-
126 63r2] those criteria are transferred in to OP_SAC, defined in
127 KIAF-1420.

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

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

132 3 SERVICE ASSESSMENT CRITERIA - GENERAL

133 3.1 Context and Scope

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

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

140 3.2 Status and Readership

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

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

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

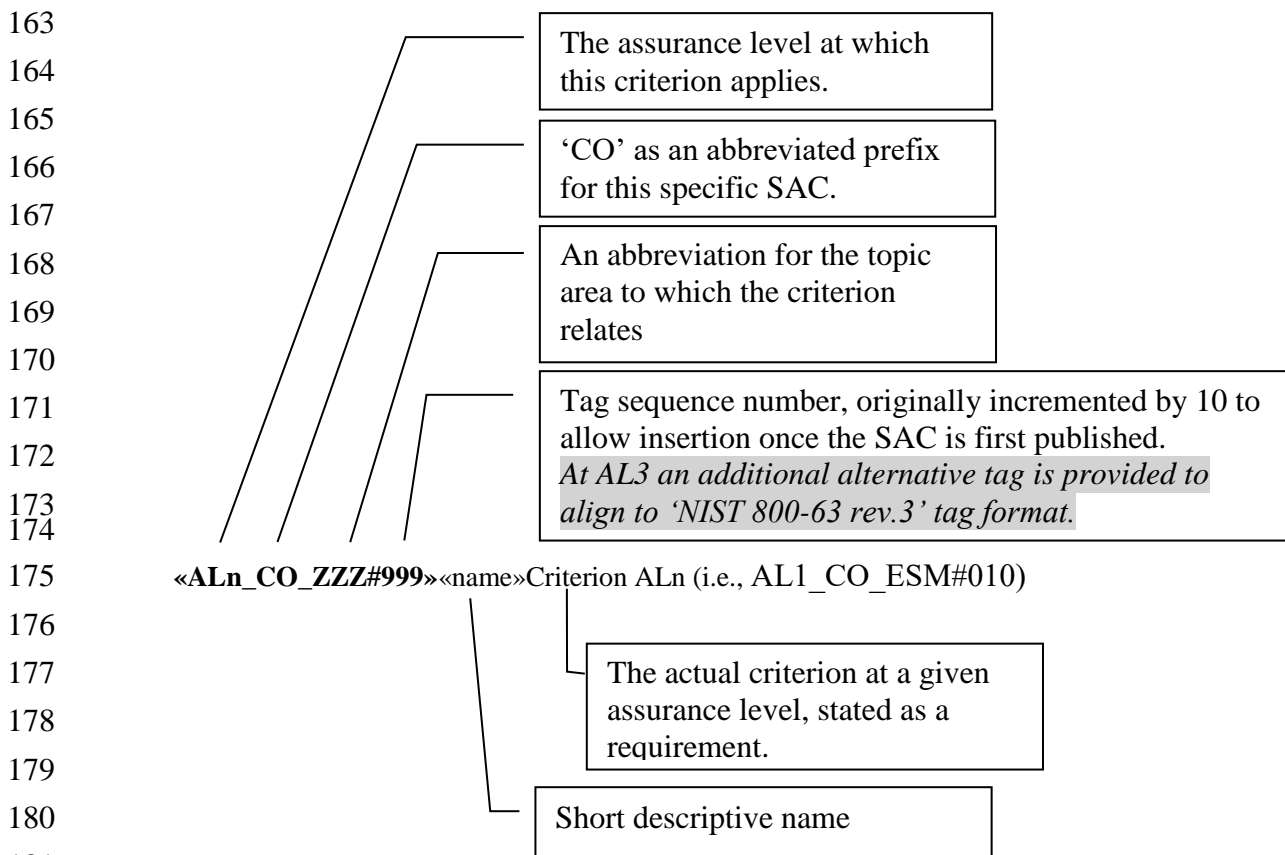
153 3.3 Criteria Descriptions

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

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

161

162 The criteria are described as follows:



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

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

188 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
189 tag which is marked 'No stipulation'. A title and appropriate criteria will be added at the higher AL which
190 occupies that position. Since in general higher ALs have a greater extent of criteria than lower ALs, where a
191 given AL extends no further through the numbering range, criteria beyond that value are by default omitted
192 rather than being included but marked 'No stipulation'.

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

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

197 **3.4 Terminology**

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

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

203 4 COMMONLY-APPLICABLE 204 SERVICE ASSESSMENT CRITERIA

205 The Service Assessment Criteria in this section establish the general business and organizational
206 requirements for conformity of services and service providers at all Assurance Levels (AL) – refer to Section
207 [2](#). These criteria are generally referred to elsewhere within IAWG documentation as CO-SAC and can be
208 identified by their tag “ALn_CO_xxxx” or by an alternative tag ‘CO#xxxx’ when applied to an assessment
209 for any non-[NIST800-63r2] Class of Approval.

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

212 4.1 Assurance Level 1

213 4.1.1 Enterprise and Service Maturity

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

216 An enterprise and its specified service must:

217 *ALI_CO_ESM#010 Established enterprise*

218 Be a valid legal entity, and a person with the legal authority to commit the organization must submit the
219 signed assessment package.

220 *ALI_CO_ESM#020 Withdrawn*

221 Withdrawn

222 *ALI_CO_ESM#030 Legal & Contractual compliance*

223 Demonstrate that it understands and complies with any legal requirements incumbent on it in connection with
224 operation and delivery of the specified service, accounting for all jurisdictions and countries within which its
225 services may be offered.

226 **Guidance:** ‘Understanding’ is implicitly the correct understanding. Both it and compliance are required
227 because it could be that understanding is incomplete, incorrect or even absent, even though compliance is
228 apparent, and similarly, correct understanding may not necessarily result in full compliance. The two are
229 therefore complementary.

230 *ALI_CO_ESM#040 No stipulation*

231 *ALI_CO_ESM#050 Data Retention and Protection*

232 Specifically set out and demonstrate that it understands and complies with those legal and regulatory
233 requirements incumbent upon it concerning the retention and destruction of private and identifiable
234 information (personal and business - i.e. its secure storage and protection against loss, accidental public
235 exposure, and/or improper destruction) and the protection of Subjects’ private information (against unlawful
236 or unauthorized access, excepting that permitted by the information owner or required by due process).

237 *ALI_CO_ESM#055 Termination provisions*

238 Define the practices in place for the protection of Subjects' private and secret information related to their use
239 of the service which must ensure the ongoing secure preservation and protection of legally required records
240 and for the secure destruction and disposal of any such information whose retention is no longer legally
241 required. Specific details of these practices must be made available.

242 **Guidance:** Termination covers the cessation of the business activities, the service provider itself ceasing
243 business operations altogether, change of ownership of the service-providing business, and other similar
244 events which change the status and/or operations of the service provider in any way which interrupts the
245 continued provision of the specific service.

246 4.1.2 Notices and User information

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

249 An enterprise and its specified service must:

250 *ALI_CO_NUI#010 General Service Definition*

251 Make available to the intended user community a Service Definition that includes all applicable Terms,
252 Conditions, and Fees, including any limitations of its usage. Specific provisions are stated in further criteria
253 in this section.

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

256 *ALI_CO_NUI#020 Service Definition inclusions*

257 Make available a Service Definition for the specified service containing clauses that provide the following
258 information:

259 a) a Privacy Policy.

260

261 *ALI_CO_NUI#030 Due notification*

262 Have in place and follow appropriate policy and procedures to ensure that it notifies Users in a timely and
263 reliable fashion of any changes to the Service Definition and any applicable Terms, Conditions, and Privacy
264 Policy for the specified service.

265 *ALI_CO_NUI#040 User Acceptance*

266 Require Subscribers and Subjects to:

267 a) indicate, prior to receiving service, that they have read and accept the terms of service as defined in
268 the Service Definition;

269 b) at periodic intervals, determined by significant service provision events (e.g. issuance, re-issuance,
270 renewal), re-affirm their understanding and observance of the terms of service;

271 c) always provide full and correct responses to requests for information.

272 *ALI_CO_NUI#050 Record of User Acceptance*

273 Obtain a record (hard-copy or electronic) of the Subscriber's and Subject's acceptance of the terms and
274 conditions of service, prior to initiating the service and thereafter at periodic intervals, determined by
275 significant service provision events (e.g. re-issuance, renewal).

276 **4.1.3 No stipulation**

277 **4.1.4 No stipulation**

278 **4.1.5 No stipulation**

279 **4.1.6 No stipulation**

280 **4.1.7 Secure Communications**

281 *ALI_CO_SCO#010 No stipulation*

282 *ALI_CO_SCO#015 No stipulation*

283 *ALI_CO_SCO#016 No stipulation*

284 *ALI_CO_SCO#020 Withdrawn*

285 Withdrawn – See KIAF-1420: AL1_CM_SCO#020.

286

287 4.2 Assurance Level 2

288 Criteria in this section address the establishment of the enterprise offering the service and its basic standing
289 as a legal and operational business entity within its respective jurisdiction or country, at AL2 per [OMB M-
290 04-04].

291 4.2.1 Enterprise and Service Maturity

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

294 An enterprise and its specified service must:

295 *AL2_CO_ESM#010 Established enterprise*

296 Be a valid legal entity, and a person with legal authority to commit the organization must submit the signed
297 assessment package.

298 *AL2_CO_ESM#020 Withdrawn*

299 Withdrawn

300 *AL2_CO_ESM#030 Legal & Contractual compliance*

301 Demonstrate that it understands and complies with any legal requirements incumbent on it in connection with
302 operation and delivery of the specified service, accounting for all jurisdictions within which its services may
303 be offered. Any specific contractual requirements shall also be identified.

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

309 *AL2_CO_ESM#040 Financial Provisions*

310 Provide documentation of financial resources that allow for the continued operation of the service and
311 demonstrate appropriate liability processes and procedures that satisfy the degree of liability exposure being
312 carried.

313 **Guidance:** The organization must show that it has a budgetary provision to operate the service for at least a
314 twelve-month period, with a clear review of the budgetary planning within that period so as to keep the
315 budgetary provisions extended. It must also show how it has determined the degree of liability protection
316 required, in view of its exposure per 'service' and the number of users it has. This criterion helps ensure that
317 Kantara Initiative, Inc. does not grant Recognition to services that are not likely to be sustainable over at least
318 this minimum period of time.

319 *AL2_CO_ESM#050 Data Retention and Protection*

320 Specifically set out and demonstrate that it understands and complies with those legal and regulatory
321 requirements incumbent upon it concerning the retention and destruction of private and identifiable
322 information (personal and business - i.e. its secure storage and protection against loss, accidental public
323 exposure, and/or improper destruction) and the protection of Subjects' private information (against unlawful
324 or unauthorized access, excepting that permitted by the information owner or required by due process).

325 **Guidance:** Note that whereas the criterion is intended to address unlawful or unauthorized access arising
326 from malicious or careless actions (or inaction) some access may be unlawful UNLESS authorized by the
327 Subscriber or Subject, or effected as a part of a specifically-executed legal process.

328 *AL2_CO_ESM#055 Termination provisions*

329 Define the practices in place for the protection of Subjects' private and secret information related to their use
330 of the service which must ensure the ongoing secure preservation and protection of legally required records
331 and for the secure destruction and disposal of any such information whose retention is no longer legally
332 required. Specific details of these practices must be made available.

333 **Guidance:** Termination covers the cessation of the business activities, the service provider itself ceasing
334 business operations altogether, change of ownership of the service-providing business, and other similar
335 events which change the status and/or operations of the service provider in any way which interrupts the
336 continued provision of the specific service.

337 4.2.2 Notices and User Information/Agreements

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

340 An enterprise and its specified service must:

341 *AL2_CO_NUI#010 General Service Definition*

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

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

347 *AL2_CO_NUI#020 Service Definition inclusions*

348 Make available a Service Definition for the specified service containing clauses that provide the following
349 information:

- 350 a) Privacy, Identity Proofing & Verification, **Authentication**, Renewal/Re-issuance, and Revocation and
351 Termination Policies;
- 352 b) the country in or legal jurisdiction under which the service is operated;
- 353 c) if different from the above, the legal jurisdiction under which Subscriber and any relying party
354 agreements are entered into;
- 355 d) applicable legislation with which the service complies;
- 356 e) obligations incumbent upon the CSP;
- 357 f) obligations incumbent upon each class of user of the service, e.g. Relying Parties, Subscribers and
358 Subjects;
- 359 g) notifications and guidance for relying parties, especially in respect of actions they are expected to
360 take should they choose to rely upon the service;
- 361 h) statement of warranties;
- 362 i) statement of liabilities toward Subscribers, Subjects and Relying Parties;
- 363 j) procedures for notification of changes to terms and conditions;
- 364 k) steps the CSP will take in the event that it chooses or is obliged to terminate the service;
- 365 l) availability of the specified service (**for the service as a whole or for each of its distinct components**)
366 and of its help desk facility.

367 **Guidance:** The term ‘Service Definition’ is used to define a notional document which has the described
368 characteristics, rather than to demand that there be a document specifically bearing such a title (though it is
369 adopted as being a particularly relevant title). The policies referred-to may be included or separate and may
370 have scope-specific titles or may adopt usage found elsewhere within this and other sets of SAC, e.g.
371 ‘Credential Policy’, ‘Identity-Proofing Policy’, according to specific criteria scope in each instance. The
372 important point is that documented and appropriately-available statements which fulfill these requirements in
373 the context of the subject service must be produced and applied by the CSP.

374 *AL2_CO_NUI#025 AL2 Configuration Specification*

375 Make available a detailed specification (accounting for the service specification and architecture) which
376 defines how a user of the service can configure it so as to be assured of receiving at least an AL2 baseline
377 service.

378 *AL2_CO_NUI#030 Due notification*

379 Have in place and follow appropriate policy and procedures to ensure that it notifies Subscribers and Subjects
380 in a timely and reliable fashion of any changes to the Service Definition and any applicable Terms,
381 Conditions, Fees, and Privacy Policy for the specified service, and provide a clear means by which
382 Subscribers and Subjects must indicate that they wish to accept the new terms or terminate their subscription.

383 *AL2_CO_NUI#040 User Acceptance*

384 Require Subscribers and Subjects to:

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

391 *AL2_CO_NUI#050 Record of User Acceptance*

392 Obtain a record (hard-copy or electronic) of the Subscriber's and Subject's acceptance of the terms and
393 conditions of service, prior to initiating the service and thereafter at periodic intervals, determined by
394 significant service provision events (e.g. re-issuance, renewal) and otherwise at least once every five years.

395 *AL2_CO_NUI#060 Withdrawn*

396 Withdrawn.

397 *AL2_CO_NUI#070 Change of Subscriber Information*

398 Require and provide the mechanisms for Subscribers and Subjects to provide in a timely manner full and
399 correct amendments should any of their recorded information change, as required under the terms of their use
400 of the service, and only after the Subscriber's and/or Subject's identity has been authenticated.

401 **4.2.3 Information Security Management**

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

406 An enterprise and its specified service must:

407 *AL2_CO_ISM#010 Documented policies and procedures*

408 Have documented all security-relevant administrative, management, and technical policies and procedures.
409 The enterprise must ensure that these are based upon recognized standards, published references or
410 organizational guidelines, are adequate for the specified service, and are implemented in the manner
411 intended.

412 *AL2_CO_ISM#020 Policy Management and Responsibility*

413 Have a clearly defined managerial role, at a senior level, in which full responsibility for the business's
414 security policies is vested and from which review, approval, and promulgation of policy and related
415 procedures is applied and managed. The latest approved versions of these policies must be applied at all
416 times.

417 *AL2_CO_ISM#030 Risk Management*

418 Demonstrate a risk management methodology that adequately identifies and mitigates risks related to the
419 specified service and its user community.

420 *AL2_CO_ISM#040 Continuity of Operations Plan*

421 Have and keep updated a Continuity of Operations Plan that covers disaster recovery and the resilience of the
422 specified service.

423 *AL2_CO_ISM#050 Configuration Management*

424 Demonstrate that there is in place a configuration management system that at least includes:

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

428 *AL2_CO_ISM#060 Quality Management*

429 Demonstrate that there is in place a quality management system that is appropriate for the specified service.

430 *AL2_CO_ISM#070 System Installation and Operation Controls*

431 Apply controls during system development, procurement installation, and operation that protect the security
432 and integrity of the system environment, hardware, software, and communications.

433 *AL2_CO_ISM#080 Internal Service Audit*

434 Be subjected to a first-party audit at least once every 12 months for the effective provision of the specified
435 service by internal audit functions of the enterprise responsible for the specified service, unless it can show
436 that by reason of its organizational size or due to other operational restrictions it is unreasonable to be so
437 audited.

438 **Guidance:** 'First-party' audits are those undertaken by an independent part of the same organization which
439 offers the service. The auditors cannot be involved in the specification, development or operation of the
440 service.

441 Using a 'third-party' (i.e. independent) auditor (i.e. one having no relationship with the Service Provider nor
442 any vested interests in the outcome of the assessment other than their professional obligations to perform the
443 assessment objectively and independently) should be considered when the organization cannot easily provide
444 truly independent internal resources but wishes to benefit from the value which audits can provide, and for
445 the purposes of fulfilling Kantara's needs, a formal Kantara Assessment performed by an Accredited Assessor
446 should be considered as such.

447 *AL2_CO_ISM#090 Withdrawn*

448 Withdrawn.

449 *AL2_CO_ISM#100 Audit Records*

450 Retain records of all audits, both internal and independent, for a period which, as a minimum, fulfills its legal
451 obligations and otherwise for greater periods either as it may have committed to in its Service Definition or
452 required by any other obligations it has with/to a Subscriber or Subject, and which in any event is not less
453 than 36 months. Such records must be held securely and be protected against unauthorized access, loss,
454 alteration, public disclosure, or unapproved destruction.

455 *AL2_CO_ISM#110 Withdrawn*

456 Withdrawn.

457 **4.2.4 Security-relevant Event (Audit) Records**

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

460 An enterprise and its specified service must:

461 *AL2_CO_SER#010 Security event logging*

462 Maintain a log of all relevant security events concerning the operation of the service, together with an
463 accurate record of the time at which the event occurred (time-stamp), and retain such records with
464 appropriate protection and controls to ensure successful retrieval, accounting for service definition, risk
465 management requirements, applicable legislation, and organizational policy.

466 **Guidance:** It is sufficient that the accuracy of the time source is based upon an internal computer/system
467 clock synchronized to an internet time source. The time source need not be authenticable.

468 *AL2_CO_SER#020 Demonstrated availability*

469 Determine actual availability achieved in comparison to the stated availability targets (refer to

470 *AL2_CO_NUI#020 1*)).

471 **4.2.5 Operational infrastructure**

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

474 An enterprise and its specified service must:

475 *AL2_CO_OPN#010 Withdrawn*

476 Withdrawn.

477 *AL2_CO_OPN#020 Defined security roles*

478 Define, by means of a job description, the roles and responsibilities for each service-related security-relevant
479 task, relating it to specific procedures, (which shall be set out in the ISMS, or other IT security management
480 methodology recognized by a government or professional body) and other service-related job descriptions
481 and applicable policies, processes and procedures. Where the role is security-critical or where special
482 privileges or shared duties exist, these must be specifically identified as such, including the applicable access
483 privileges relating to logical and physical parts of the service's operations.

484 *AL2_CO_OPN#030 Personnel recruitment*

485 Demonstrate that it has defined practices for the selection, evaluation, and contracting of all service-related
486 personnel, both direct employees and those whose services are provided by third parties.

487 *AL2_CO_OPN#040 Personnel skills*
488 Ensure that employees are sufficiently trained, qualified, experienced, and current for the roles they fulfill.
489 Such measures must be accomplished either by recruitment practices or through a specific training program.
490 Where employees are undergoing on-the-job training, they must only do so under the guidance of a mentor
491 possessing the defined service experiences for the training being provided.

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

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

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

499 **4.2.6 External Services and Components**

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

503 An enterprise and its specified service must:

504 *AL2_CO_ESC#010 Contracted policies and procedures*
505 Where the enterprise uses external suppliers for specific packaged components of the service or for resources
506 that are integrated with its own operations and under its control, ensure that those parties are engaged through
507 reliable and appropriate contractual arrangements which stipulate which critical policies, procedures, and
508 practices subcontractors are required to fulfill.

509 *AL2_CO_ESC#020 Visibility of contracted parties*
510 Where the enterprise uses external suppliers for specific packaged components of the service or for resources
511 that are integrated with its own operations and under its control, ensure that the suppliers' compliance with
512 contractually-stipulated policies and procedures, and thus with IAF Service Assessment Criteria, can be
513 independently verified, and subsequently monitored if necessary.

514 **4.2.7 Secure Communications**

515 An enterprise and its specified service must:

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

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

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

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

524

525 4.3 Assurance Level 3

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

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

531 4.3.1 Enterprise and Service Maturity

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

534 An enterprise and its specified service must:

535 *AL3_CO_ESM#010 / CO#0010 Established enterprise*

536 Be a valid legal entity and a person with legal authority to commit the organization must submit the signed
537 assessment package.

538 *AL3_CO_ESM#020 Withdrawn*

539 Withdrawn

540 *AL3_CO_ESM#030 / CO#0020 Legal & Contractual compliance*

541 Demonstrate that it understands and complies with any legal requirements incumbent on it in connection with
542 operation and delivery of the specified service, accounting for all jurisdictions within which its services may
543 be offered. Any specific contractual requirements shall also be identified.

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

549 *AL3_CO_ESM#040 / CO#0030 Financial Provisions*

550 Provide documentation of financial resources that allow for the continued operation of the service and
551 demonstrate appropriate liability processes and procedures that satisfy the degree of liability exposure being
552 carried.

553 **Guidance:** The organization must show that it has a budgetary provision to operate the service for at least a
554 twelve-month period, with a clear review of the budgetary planning within that period so as to keep the
555 budgetary provisions extended. It must also show how it has determined the degree of liability protection
556 required, in view of its exposure per 'service' and the number of users it has. This criterion helps ensure that
557 Kantara Initiative, Inc. does not grant Recognition to services that are not likely to be sustainable over at least
558 this minimum period of time.

559 *AL3_CO_ESM#050 / CO#0040 Data Retention and Protection*

560 Specifically set out and demonstrate that it understands and complies with those legal and regulatory
561 requirements incumbent upon it concerning the retention and destruction of private and identifiable
562 information (personal and business) (i.e. its secure storage and protection against loss, accidental public

563 exposure and/or improper destruction) and the protection of private information (against unlawful or
564 unauthorized access, excepting that permitted by the information owner or required by due process).

565 *AL3_CO_ESM#055 / CO#0050 Termination provisions*

566 Define the practices in place for the protection of Subjects' private and secret information related to their use
567 of the service which must ensure the ongoing secure preservation and protection of legally required records
568 and for the secure destruction and disposal of any such information whose retention is no longer legally
569 required. Specific details of these practices must be made available.

570 **Guidance:** Termination covers the cessation of the business activities, the service provider itself ceasing
571 business operations altogether, change of ownership of the service-providing business, and other similar
572 events which change the status and/or operations of the service provider in any way which interrupts the
573 continued provision of the specific service.

574 *AL3_CO_ESM#060 / CO#0060 Ownership*

575 **If the enterprise named as the CSP is a part of a larger entity, the nature of the relationship with its**
576 **parent organization shall be disclosed to the assessors and, on their request, to customers.**

577 *AL3_CO_ESM#070 / CO#0070 Independent management and operations*

578 **Demonstrate that, for the purposes of providing the specified service, its management and operational**
579 **structures are distinct, autonomous, have discrete legal accountability, and operate according to**
580 **separate policies, procedures, and controls.**

581 4.3.2 Notices and User Information

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

584 An enterprise and its specified service must:

585 *AL3_CO_NUI#010 / CO#0080 General Service Definition*

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

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

591 *AL3_CO_NUI#020 / CO#0090 Service Definition inclusions*

592 Make available a Service Definition for the specified service containing clauses that provide the following
593 information:

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

- 603 g) notifications and guidance for relying parties, especially in respect of actions they are expected to
604 take should they choose to rely upon the service's product;
605 h) statement of warranties;
606 i) statement of liabilities toward both Subjects and Relying Parties;
607 j) procedures for notification of changes to terms and conditions;
608 k) steps the CSP will take in the event that it chooses or is obliged to terminate the service;
609 l) availability of the specified service (for the service as a whole or for each of its distinct components)
610 and of its help desk facility.

611 **Guidance:** The term ‘Service Definition’ is used to define a notional document which has the described
612 characteristics, rather than to demand that there be a document specifically bearing such a title (though it is
613 adopted as being a particularly relevant title). The policies referred-to may be included or separate and may
614 have scope-specific titles or may adopt usage found elsewhere within this and other sets of SAC, e.g.
615 ‘Credential Policy’, ‘Identity-Proofing Policy’, according to specific criteria scope in each instance. The
616 important point is that documented and appropriately-available statements which fulfill these requirements in
617 the context of the subject service must be produced and applied by the CSP.

618 *AL3_CO_NUI#025 / CO#0100 AL3 Configuration Specification*

619 Make available a detailed specification (accounting for the service specification and architecture) which
620 defines how a user of the service can configure it so as to be assured of receiving at least an **AL3** baseline
621 service.

622 *AL3_CO_NUI#030 / CO#0110 Due notification*

623 Have in place and follow appropriate policy and procedures to ensure that it notifies Subscribers and Subjects
624 in a timely and reliable fashion of any changes to the Service Definition and any applicable Terms,
625 Conditions, Fees, and Privacy Policy for the specified service, and provide a clear means by which
626 Subscribers and Subjects must indicate that they wish to accept the new terms or terminate their subscription.

627 *AL3_CO_NUI#040 / CO#0120 User Acceptance*

628 Require Subscribers and Subjects to:

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

635 *AL3_CO_NUI#050 / CO#0130 Record of User Acceptance*

636 Obtain a record (hard-copy or electronic) of the Subscriber’s and Subject’s acceptance of the terms and
637 conditions of service, prior to initiating the service and thereafter reaffirm the agreement at periodic intervals,
638 determined by significant service provision events (e.g. re-issuance, renewal) and otherwise at least once
639 every five years.

640 *AL3_CO_NUI#060 Withdrawn*

641 Withdrawn.

642 *AL3_CO_NUI#070 / CO#0140 Change of Subscriber Information*

643 Require and provide the mechanisms for Subscribers and Subjects to provide in a timely manner full and
644 correct amendments should any of their recorded information change, as required under the terms of their use
645 of the service, and only after the Subscriber's and/or Subject's identity has been authenticated.

646 4.3.3 Information Security Management

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

651 An enterprise and its specified service must:

652 *AL3_CO_ISM#010 / CO#0150 Documented policies and procedures*

653 Have documented all security-relevant administrative management and technical policies and procedures.
654 The enterprise must ensure that these are based upon recognized standards, published references or
655 organizational guidelines, are adequate for the specified service, and are implemented in the manner
656 intended.

657 *AL3_CO_ISM#020 / CO#0160 Policy Management and Responsibility*

658 Have a clearly defined managerial role, at a senior level, where full responsibility for the business' security
659 policies is vested and from which review, approval, and promulgation of policy and related procedures is
660 applied and managed. The latest approved versions of these policies must be applied at all times.

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

662 Demonstrate a risk management methodology that adequately identifies and mitigates risks related to the
663 specified service and its user community **and must show that a risk assessment review is performed at**
664 **least once every six months, such as adherence to CobIT or [\[IS27001\]](#) practices.**

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

666 Have and keep updated a continuity of operations plan that covers disaster recovery and the resilience of the
667 specified service **and must show that a review of this plan is performed at least once every six months.**

668 *AL3_CO_ISM#050 / CO#0190 Configuration Management*

669 Demonstrate that there is in place a configuration management system that at least includes:

- 670 a) version control for software system components;
671 b) timely identification and installation of all organizationally-approved patches for any software used in
672 the provisioning of the specified service;
673 c) **version control and managed distribution for all documentation associated with the**
674 **specification, management, and operation of the system, covering both internal and publicly**
675 **available materials.**

676 *AL3_CO_ISM#060 / CO#0200 Quality Management*

677 Demonstrate that there is in place a quality management system that is appropriate for the specified service.

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

679 Apply controls during system development, procurement, installation, and operation that protect the security
680 and integrity of the system environment, hardware, software, and communications **having particular regard**
681 **to:**

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

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

690 *AL3_CO_ISM#080 / CO#0220 Internal Service Audit*

691 Be subjected to a first-party audit at least once every 12 months for the effective provision of the specified
692 service by internal audit functions of the enterprise responsible for the specified service, unless it can show
693 that by reason of its organizational size or due to other **justifiable** operational restrictions it is unreasonable
694 to be so audited.

695 **Guidance:** ‘First-party’ audits are those undertaken by an independent part of the same organization which
696 offers the service. The auditors cannot be involved in the specification, development or operation of the
697 service.

698 Management systems require that there be internal audit conducted as an inherent part of management review
699 processes. Any third-party (i.e. independent) audit of the management system is intended to show that the
700 internal management system controls are being appropriately applied, and for the purposes of fulfilling
701 Kantara’s needs, a formal Kantara Assessment performed by an Accredited Assessor should be considered as
702 such.

703 *AL3_CO_ISM#090 Withdrawn*

704 Withdrawn.

705 *AL3_CO_ISM#100 / CO#0230 Audit Records*

706 Retain records of all audits, both internal and independent, for a period which, as a minimum, fulfills its legal
707 obligations and otherwise for greater periods either as it may have committed to in its Service Definition or
708 required by any other obligations it has with/to a Subscriber or Subject, and which in any event is not less
709 than 36 months. Such records must be held securely and be protected against unauthorized access, loss,
710 alteration, public disclosure, or unapproved destruction.

711 *AL3_CO_ISM#110 Withdrawn*

712 Withdrawn.

713 *AL3_CO_ISM#120 / CO#0240 Best Practice Security Management*

714 **Have in place an Information Security Management System (ISMS), or other IT security management**
715 **methodology recognized by a government or professional body, that follows best practices as accepted**
716 **by the information security industry and that applies and is appropriate to the CSP in question. All**
717 **requirements expressed in preceding criteria in this section must *inter alia* fall wholly within the scope**
718 **of this ISMS or selected recognized alternative.**

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

721 **4.3.4 Security-Relevant Event (Audit) Records**

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

724 An enterprise and its specified service must:

725 *AL3_CO_SER#010 / CO#0250 Security Event Logging*

726 Maintain a log of all relevant security events concerning the operation of the service, together with an
727 accurate record of the time at which the event occurred (time-stamp), and retain such records with
728 appropriate protection and controls to ensure successful retrieval, accounting for Service Definition risk
729 management requirements, applicable legislation, and organizational policy.

730 **Guidance:** It is sufficient that the accuracy of the time source is based upon an internal computer/system
731 clock synchronized to an internet time source. The time source need not be authenticatable.

732 *AL3_CO_SER#020 / CO#0255 Demonstrated availability*

733 Determine actual availability achieved in comparison to the stated availability targets (refer to
734 *AL3_CO_NUI#020 / CO#0090 1*)).

735 4.3.5 Operational Infrastructure

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

738 An enterprise and its specified service must:

739 *AL3_CO_OPN#010 Withdrawn*

740 Withdrawn.

741 *AL3_CO_OPN#020 / CO#0260 Defined security roles*

742 Define, by means of a job description, the roles and responsibilities for each service-related security-relevant
743 task, relating it to specific procedures (which shall be set out in the ISMS, or other IT security management
744 methodology recognized by a government or professional body) and other service-related job descriptions
745 and applicable policies, processes and procedures. Where the role is security-critical or where special
746 privileges or shared duties exist, these must be specifically identified as such, including the applicable access
747 privileges relating to logical and physical parts of the service's operations.

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

749 **Require those assigned to critical security roles to acknowledge, by signature (hand-written or**
750 **electronic), that they have read and understood the system documentation applicable to their role(s)**
751 **and that they accept the associated responsibilities.**

752 *AL3_CO_OPN#030 / CO#0280 Personnel recruitment*

753 Demonstrate that it has defined practices for the selection, vetting, and contracting of all service-related
754 personnel, both direct employees and those whose services are provided by third parties. **Full records of all**
755 **searches and supporting evidence of qualifications and past employment must be kept for the duration**
756 **of the individual's employment plus the longest lifespan of any credential issued under the Service**
757 **Policy.**

758 *AL3_CO_OPN#040 / CO#0290 Personnel skills*

759 Ensure that employees are sufficiently trained, qualified, experienced, and current for the roles they fulfill.
760 Such measures must be accomplished either by recruitment practices or through a specific training program.
761 Where employees are undergoing on-the-job training, they must only do so under the guidance of a mentor
762 possessing the defined service experiences for the training being provided.

763 *AL3_CO_OPN#050 / CO#0300 Adequacy of Personnel resources*

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

766 *AL3_CO_OPN#060 Withdrawn*

767 Withdrawn – See KIAF-1420: AL3_OP_OPN#060.

768 *AL3_CO_OPN#070 Withdrawn*

769 Withdrawn – See KIAF-1420: AL3_OP_OPN#070.

770 **4.3.6 External Services and Components**

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

774 An enterprise and its specified service must:

775 *AL3_CO_ESC#010 / CO#0310 Contracted policies and procedures*

776 Where the enterprise uses external suppliers for specific packaged components of the service or for resources
777 which are integrated with its own operations and under its control, ensure that those parties are engaged
778 through reliable and appropriate contractual arrangements which stipulate which critical policies, procedures,
779 and practices sub-contractors are required to fulfill.

780 *AL3_CO_ESC#020 / CO#0320 Visibility of contracted parties*

781 Where the enterprise uses external suppliers for specific packaged components of the service or for resources
782 which are integrated with its own operations and under its controls, ensure that the suppliers' compliance
783 with contractually-stipulated policies and procedures, and thus with the IAF Service Assessment Criteria, can
784 be independently verified, and subsequently monitored if necessary. ð

785 **4.3.7 Secure Communications**

786 An enterprise and its specified service must:

787 *AL3_CO_SCO#010 Withdrawn*

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

789 *AL3_CO_SCO#015 Withdrawn*

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

791 *AL3_CO_SCO#020 Withdrawn*

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

793 *AL3_CO_SCO#030 Withdrawn*

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

795

796 **4.4 Assurance Level 4**

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

799 **4.4.1 Enterprise and Service Maturity**

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

802 An enterprise and its specified service must:

803 *AL4_CO_ESM#010 Established enterprise*

804 Be a valid legal entity and a person with legal authority to commit the organization must submit the signed
805 assessment package.

806 *AL4_CO_ESM#020 Withdrawn*

807 Withdrawn

808 *AL4_CO_ESM#030 Legal & Contractual compliance*

809 Demonstrate that it understands and complies with any legal requirements incumbent on it in connection with
810 operation and delivery of the specified service, accounting for all jurisdictions within which its services may
811 be offered. Any specific contractual requirements shall also be identified.

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

817 *AL4_CO_ESM#040 Financial Provisions*

818 Provide documentation of financial resources that allow for the continued operation of the service and
819 demonstrate appropriate liability processes and procedures that satisfy the degree of liability exposure being
820 carried.

821 **Guidance:** The organization must show that it has a budgetary provision to operate the service for at least a
822 twelve-month period, with a clear review of the budgetary planning within that period so as to keep the
823 budgetary provisions extended. It must also show how it has determined the degree of liability protection
824 required, in view of its exposure per 'service' and the number of users it has. This criterion helps ensure that
825 Kantara Initiative, Inc. does not grant Recognition to services that are not likely to be sustainable over at least
826 this minimum period of time.

827 *AL4_CO_ESM#050 Data Retention and Protection*

828 Specifically set out and demonstrate that it understands and complies with those legal and regulatory
829 requirements incumbent upon it concerning the retention and destruction of private and identifiable
830 information (personal and business) (i.e. its secure storage and protection against loss, accidental public
831 exposure, and/or improper destruction) and the protection of private information (against unlawful or
832 unauthorized access excepting that permitted by the information owner or required by due process).

833 *AL4_CO_ESM#055 Termination provisions*

834 Define the practices in place for the protection of Subjects' private and secret information related to their use
835 of the service which must ensure the ongoing secure preservation and protection of legally required records
836 and for the secure destruction and disposal of any such information whose retention is no longer legally
837 required. Specific details of these practices must be made available.

838 **Guidance:** Termination covers the cessation of the business activities, the service provider itself ceasing
839 business operations altogether, change of ownership of the service-providing business, and other similar
840 events which change the status and/or operations of the service provider in any way which interrupts the
841 continued provision of the specific service.

842 *ALA_CO_ESM#060 Ownership*

843 If the enterprise named as the CSP is a part of a larger entity, the nature of the relationship with its parent
844 organization, shall be disclosed to the assessors and, on their request, to customers.

845 *ALA_CO_ESM#070 Independent Management and Operations*

846 Demonstrate that, for the purposes of providing the specified service, its management and operational
847 structures are distinct, autonomous, have discrete legal accountability, and operate according to separate
848 policies, procedures, and controls.

849 **4.4.2 Notices and Subscriber Information/Agreements**

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

852 An enterprise and its specified service must:

853 *ALA_CO_NUI#010 General Service Definition*

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

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

859 *ALA_CO_NUI#020 Service Definition inclusions*

860 Make available a Service Definition for the specified service containing clauses that provide the following
861 information:

- 862 a) Privacy, Identity Proofing & Verification, **Authentication**, Renewal/Re-issuance, and Revocation and
863 Termination Policies;
- 864 b) the country in or legal jurisdiction under which the service is operated;
- 865 c) if different to the above, the legal jurisdiction under which Subscriber and any relying party agreements
866 are entered into;
- 867 d) applicable legislation with which the service complies;
- 868 e) obligations incumbent upon the CSP;
- 869 f) obligations incumbent upon each class of user of the service, e.g. Relying Parties, Subscribers and
870 Subjects;
- 871 g) notifications and guidance for relying parties, especially in respect of actions they are expected to take
872 should they choose to rely upon the service's product;
- 873 h) statement of warranties;
- 874 i) statement of liabilities toward both Subjects and Relying Parties;

- 875 j) procedures for notification of changes to terms and conditions;
876 k) steps the CSP will take in the event that it chooses or is obliged to terminate the service;
877 l) availability of the specified service (for the service as a whole or for each of its distinct components)
878 and of its help desk facility.

879 **Guidance:** The term ‘Service Definition’ is used to define a notional document which has the described
880 characteristics, rather than to demand that there be a document specifically bearing such a title (though it is
881 adopted as being a particularly relevant title). The policies referred-to may be included or separate and may
882 have scope-specific titles or may adopt usage found elsewhere within this and other sets of SAC, e.g.
883 ‘Credential Policy’, ‘Identity-Proofing Policy’, according to specific criteria scope in each instance. The
884 important point is that documented and appropriately-available statements which fulfill these requirements in
885 the context of the subject service must be produced and applied by the CSP.

886 *ALA_CO_NUI#025 ALA Configuration Specification*

887 Make available a detailed specification (accounting for the service specification and architecture) which
888 defines how a user of the service can configure it so as to be assured of receiving at least an **AL4** baseline
889 service.

890 *ALA_CO_NUI#030 Due Notification*

891 Have in place and follow appropriate policy and procedures to ensure that it notifies Subscribers and Subjects
892 in a timely and reliable fashion of any changes to the Service Definition and any applicable Terms,
893 Conditions, Fees, and Privacy Policy for the specified service, and provide a clear means by which
894 Subscribers and Subjects must indicate that they wish to accept the new terms or terminate their subscription.

895 *ALA_CO_NUI#040 User Acceptance*

896 Require Subscribers and Subjects to:

- 897 a) indicate, prior to receiving service, that they have read and accept the terms of service as defined in the
898 Service Definition, thereby indicating their properly-informed opt-in;
899 b) at periodic intervals, determined by significant service provision events (e.g. issuance, re-issuance,
900 renewal) and otherwise at least once every five years, re-affirm their understanding and observance of
901 the terms of service;
902 c) always provide full and correct responses to requests for information.

903 *ALA_CO_NUI#050 Record of User Acceptance*

904 Obtain a record (hard-copy or electronic) of the Subscriber’s and Subject’s acceptance of the terms and
905 conditions of service, prior to initiating the service and thereafter reaffirm the agreement at periodic intervals,
906 determined by significant service provision events (e.g. issuance, re-issuance, renewal) and otherwise at least
907 once every five years.

908 *ALA_CO_NUI#060 Withdrawn*

909 Withdrawn.

910 *ALA_CO_NUI#070 Change of Subscriber Information*

911 *Require and provide the mechanisms for Subscribers and Subjects to provide in a timely manner full and*
912 *correct amendments should any of their recorded information change, as required under the terms of their use*
913 *of the service, and only after the Subscriber’s and/or Subject’s identity has been authenticated.*

914 *ALA_CO_NUI#080 Withdrawn*

915 Withdrawn.

916 4.4.3 Information Security Management

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

921 An enterprise and its specified service must:

922 *ALA_CO_ISM#010 Documented policies and procedures*

923 Have documented all security-relevant administrative, management, and technical policies and procedures.
924 The enterprise must ensure that these are based upon recognized standards, published references, or
925 organizational guidelines, are adequate for the specified service, and are implemented in the manner
926 intended.

927 *ALA_CO_ISM#020 Policy Management and Responsibility*

928 Have a clearly defined managerial role, at a senior level, where full responsibility for the business' security
929 policies is vested and from which review, approval, and promulgation of policy and related procedures is
930 applied and managed. The latest approved versions of these policies must be applied at all times.

931 *ALA_CO_ISM#030 Risk Management*

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

935 *ALA_CO_ISM#040 Continuity of Operations Plan*

936 Have and keep updated a continuity of operations plan that covers disaster recovery and the resilience of the
937 specified service and must show that **on-going review of this plan is conducted as a part of the business'**
938 **procedures.**

939 *ALA_CO_ISM#050 Configuration Management*

940 Demonstrate that there is in place a configuration management system that at least includes:

- 941 a) version control for software system components;
942 b) timely identification and installation of all organizationally-approved patches for any software used in
943 the provisioning of the specified service;
944 c) version control and managed distribution for all documentation associated with the specification,
945 management, and operation of the system, covering both internal and publicly available materials.

946 *ALA_CO_ISM#060 Quality Management*

947 Demonstrate that there is in place a quality management system that is appropriate for the specified service.

948 *ALA_CO_ISM#070 System Installation and Operation Controls*

949 Apply controls during system development, procurement, installation, and operation that protect the security
950 and integrity of the system environment, hardware, software, and communications having particular regard
951 to:

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

- 956 e) storage of system components;
- 957 f) installation environment security;
- 958 g) system configuration;
- 959 h) transfer to operational status.

960 *ALA_CO_ISM#080 Internal Service Audit*

961 Be subjected to a first-party audit at least once every 12 months for the effective provision of the specified
962 service by internal audit functions of the enterprise responsible for the specified service, unless it can show
963 that by reason of its organizational size or due to other justifiable operational restrictions it is unreasonable to
964 be so audited.

965 **Guidance:** ‘First-party’ audits are those undertaken by an independent part of the same organization which
966 offers the service. The auditors cannot be involved in the specification, development or operation of the
967 service.

968 Management systems require that there be internal audit conducted as an inherent part of management review
969 processes. Any third-party (i.e. independent) audit of the management system is intended to show that the
970 internal management system controls are being appropriately applied, and for the purposes of fulfilling
971 Kantara’s needs, a formal Kantara Assessment performed by an Accredited Assessor should be considered as
972 such.

973 *ALA_CO_ISM#090 Withdrawn*

974 Withdrawn.

975 *ALA_CO_ISM#100 Audit Records*

976 Retain records of all audits, both internal and independent, for a period which, as a minimum, fulfills its legal
977 obligations and otherwise for greater periods either as it may have committed to in its Service Definition or
978 required by any other obligations it has with/to a Subscriber or Subject, and which in any event is not less
979 than 36 months. Such records must be held securely and be protected against unauthorized access loss,
980 alteration, public disclosure, or unapproved destruction.

981 *ALA_CO_ISM#110 Withdrawn*

982 Withdrawn.

983 *ALA_CO_ISM#120 Best Practice Security Management*

984 Have in place a **certified** Information Security Management System (ISMS), or other IT security
985 management methodology recognized by a government or professional body, that **has been assessed and**
986 **found to be in compliance with the requirements of ISO/IEC 27001 [IS27001] and which applies and is**
987 **appropriate to the CSP in question.** All requirements expressed in preceding criteria in this section must
988 *inter alia* fall wholly within the scope of this ISMS, or the selected recognized alternative.

989 **4.4.4 Security-Related (Audit) Records**

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

992 An enterprise and its specified service must:

993 *ALA_CO_SER#010 Security Event Logging*

994 Maintain a log of all relevant security events concerning the operation of the service, together with a **precise**
995 record of the time at which the event occurred (time-stamp) **provided by a trusted time-source** and retain

996 such records with appropriate protection and controls to ensure successful retrieval, accounting for service
997 definition, risk management requirements, applicable legislation, and organizational policy.

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

1000 *ALA_CO_SER#020 Demonstrated availability*

1001 Determine actual availability achieved in comparison to the stated availability targets (refer to
1002 *ALA_CO_NUI#020 1*)).

1003 **4.4.5 Operational Infrastructure**

1004 The criteria in this section address the infrastructure within which the delivery of the specified service takes
1005 place. It puts particular emphasis upon the personnel involved, and their selection, training, and duties.

1006 An enterprise and its specified service must:

1007 *ALA_CO_OPN#010 Withdrawn*

1008 Withdrawn.

1009 *ALA_CO_OPN#020 Defined Security Roles*

1010 Define, by means of a job description, the roles and responsibilities for each service-related security-relevant
1011 task, relating it to specific procedures (which shall be set out in the ISMS, or other IT security management
1012 methodology recognized by a government or professional body) and other service-related job descriptions
1013 and applicable policies, processes and procedures. Where the role is security-critical or where special
1014 privileges or shared duties exist, these must be specifically identified as such, including the applicable access
1015 privileges relating to logical and physical parts of the service's operations.

1016 *ALA_CO_OPN#025 Acknowledgement of assigned security roles and responsibilities*

1017 Require those assigned to critical security roles to acknowledge, by signature (hand-written or electronic),
1018 that they have read and understood the system documentation applicable to their role(s) and that they accept
1019 the associated responsibilities.

1020 *ALA_CO_OPN#030 Personnel Recruitment*

1021 Demonstrate that it has defined practices for the selection, vetting, and contracting of all service-related
1022 personnel, both direct employees and those whose services are provided by third parties. Full records of all
1023 searches and supporting evidence of qualifications and past employment must be kept for the duration of the
1024 individual's employment plus the longest lifespan of any credential issued under the Service Policy.

1025 *ALA_CO_OPN#040 Personnel skills*

1026 Ensure that employees are sufficiently trained, qualified, experienced, and current for the roles they fulfill.
1027 Such measures must be accomplished either by recruitment practices or through a specific training program.
1028 Where employees are undergoing on-the-job training, they must only do so under the guidance of a mentor
1029 possessing the defined service experiences for the training being provided.

1030 *ALA_CO_OPN#050 Adequacy of Personnel resources*

1031 Have sufficient staff to adequately operate and resource the specified service according to its policies and
1032 procedures.

1033 *ALA_CO_OPN#060 Withdrawn*

1034 Withdrawn – See KIAF-1420: *ALA_CM_OPN#060*.

1035 *ALA_CO_OPN#070 Withdrawn*

1036 Withdrawn – See KIAF-1420: AL4_CM_OPN#070.
1037 Employ logical access control mechanisms that ensure access to sensitive system functions and controls is
1038 restricted to authorized personnel.

1039 **4.4.6 External Services and Components**

1040 This section addresses the relationships and obligations upon contracted parties both to apply the policies and
1041 procedures of the enterprise and also to be available for assessment as critical parts of the overall service
1042 provision.

1043 An enterprise and its specified service must:

1044 *AL4_CO_ESC#010 Contracted Policies and Procedures*

1045 Where the enterprise uses external suppliers for specific packaged components of the service or for resources
1046 which are integrated with its own operations and under its control, ensure that those parties are engaged
1047 through reliable and appropriate contractual arrangements which stipulate which critical policies, procedures,
1048 and practices sub-contractors are required to fulfill.

1049 *AL4_CO_ESC#020 Visibility of Contracted Parties*

1050 Where the enterprise uses external suppliers for specific packaged components of the service or for resources
1051 which are integrated with its own operations and under its control, ensure that the suppliers' compliance with
1052 contractually-stipulated policies and procedures, and thus with the IAF Service Assessment Criteria, can be
1053 independently verified, and subsequently monitored if necessary.

1054 **4.4.7 Secure Communications**

1055 An enterprise and its specified service must:

1056 *AL4_CO_SCO#010 Withdrawn*

1057 Withdrawn – See KIAF-1420: AL4_CM_SCO#010.

1058 *AL4_CO_SCO#015 Withdrawn*

1059 Withdrawn – See KIAF-1420: AL4_CM_SCO#015.

1060 *AL4_CO_SCO#020 Withdrawn*

1061 Withdrawn – See KIAF-1420: AL4_CM_SCO#020.

1062 **5 OPERATIONAL SERVICE ASSESSMENT CRITERIA**

1063 This section is retained purely to enable the convenience of §6 and §7 ordering with those same clauses in
1064 KIAF-1400.

1065 **6 REFERENCES / BIBLIOGRAPHY**

- 1066 [CAF] Louden, Chris, Spencer, Judy; Burr, Bill; Hawkins, Kevin; Temoshok, David; Cornell, John; Wilsher,
1067 Richard G.; Timchak, Steve; Sill, Stephen; Silver, Dave; Harrison, Von; eds., "E-Authentication Credential
1068 Assessment Framework (CAF)," E-Authentication Initiative, Version 2.0.0 (March 16, 2005).
- 1069 [EAP CSAC 04011] "EAP working paper: Identity Proofing Service Assessment Criteria (ID-SAC),"
1070 Electronic Authentication Partnership, Draft 0.1.3 (July 20, 2004).
- 1071 [EAPTrustFramework] "Electronic Authentication Partnership Trust Framework" Electronic Authentication
1072 Partnership, Version 1.0. (January 6, 2005).
- 1073 [FIPS140-2] "Security Requirements for Cryptographic Modules" Federal Information Processing
1074 Standards. (May 25, 2001).
1075 <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>
- 1076 [IS27001] ISO/IEC 27001:2013 "Information technology - Security techniques - Requirements for
1077 information security management systems", International Organization for Standardization.
1078 http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103
- 1079 [IS19790] ISO/IEC 19790:2012 "Information technology - Security techniques - Security requirements for
1080 cryptographic modules", International Organization for Standardization.
1081 http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=52906
- 1082 [M-04-04] Bolton, Joshua B., ed., "E-Authentication Guidance for Federal Agencies", Office of
1083 Management and Budget, (December 16, 2003). <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>
1084
- 1085 [NIST800-63r2] Burr, William E.; Dodson, Donna F.; Polk, W. Timothy; eds., "Electronic Authentication
1086 Guideline: : Recommendations of the National Institute of Standards and Technology," Version 1.0.2,
1087 National Institute of Standards and Technology, (April, 2006).
1088 <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf>
- 1089 [NIST800-63r3] Fenton, Grassi et al., "Digital Identity Guidelines" Revision 3, National Institute of
1090 Standards and Technology, (June, 2017).
1091 <https://pages.nist.gov/800-63-3/>
- 1092 [RFC 3647] Chokhani, S.; Ford, W.; Sabett, R.; Merrill, C.; Wu, S.; eds., "Internet X.509 Public Key
1093 Infrastructure Certificate Policy and Certification Practices Framework," The Internet Engineering Task
1094 Force (November, 2003). <http://www.ietf.org/rfc/rfc3647.txt>
- 1095 [5415] Ed. Wilsher, Richard G. "SAC mapping – ISO/IEC 29115 / ITU-T X.1254 – Entity authentication
1096 assurance framework" v0.7.0.

1097 **7 REVISION HISTORY**

- 1098 1. v1.0, 2018-03-21 – first release
- 1099 2. v2.0, 2018-10-26 – revised criteria addressing service availability.