

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29



# Identity Assurance Framework: Assessor Qualifications & Requirements

**Version:** 2.0

**Date:** 2010-04-24

**Editor:** Richard G. Wilsher  
Zygma LLC

## Contributors

The full list of contributors can be referenced here:  
<http://kantarainitiative.org/confluence/display/idassurance/IAF+2.0+Contributors>

## Abstract

The Kantara Initiative Identity Assurance Work Group (IAWG) was formed to foster adoption of identity trust services. The primary deliverable of the IAWG is the Identity Assurance Framework (IAF), which is comprised of many different documents that detail the levels of assurance and the assurance and certification program that bring the Framework to the marketplace, among them the [Assurance Assessment Scheme \(AAS\)](#), which encompasses the associated assessment and certification program, as well as the [Service Assessment Criteria \(SAC\)](#), which establishes baseline criteria for general organizational conformity, identity proofing services, credential strength, and credential management services against which all CSPs will be evaluated. The present document provides an overview of the requirements which applicant assessors must fulfill in order to become Kantara-Accredited Assessors.

**Filename:** Kantara IAF-1600-Assessor Qualifications and Requirements.doc

30

### Notice

31 This document has been prepared by Participants of Kantara Initiative. Permission is  
32 hereby granted to use the document solely for the purpose of implementing the  
33 Specification. No rights are granted to prepare derivative works of this Specification.  
34 Entities seeking permission to reproduce portions of this document for other uses must  
35 contact Kantara Initiative to determine whether an appropriate license for such use is  
36 available.

37

38 Implementation or use of certain elements of this document may require licenses under  
39 third party intellectual property rights, including without limitation, patent rights. The  
40 Participants of and any other contributors to the Specification are not and shall not be  
41 held responsible in any manner for identifying or failing to identify any or all such third  
42 party intellectual property rights. This Specification is provided "AS IS," and no  
43 Participant in the Kantara Initiative makes any warranty of any kind, expressed or  
44 implied, including any implied warranties of merchantability, non-infringement of third  
45 party intellectual property rights, and fitness for a particular purpose. Implementers of  
46 this Specification are advised to review the Kantara Initiative's website  
47 (<http://www.kantarainitiative.org/>) for information concerning any Necessary Claims  
48 Disclosure Notices that have been received by the Kantara Initiative Board of Trustees.

49

50 Copyright: The content of this document is copyright of Kantara Initiative. © 2010  
51 Kantara Initiative.

52

53

54

55 **1 INTRODUCTION .....4**

56 **2 GLOSSARY .....5**

57 **3 ASSESSOR QUALIFICATIONS & REQUIREMENTS (AQR).....6**

58 3.1 General Introduction .....6

59 3.2 Baseline Assessor Qualifications & Experience .....6

60 3.2.1 Audit Organization (AO) Requirements .....8

61 3.2.2 Auditor Qualification (AQ) Requirements .....12

62 3.2.3 Audit Team (AT) Requirements.....15

63 3.2.4 Audit Domain (AD) Requirements (i.e. «*specific domain & technology*») 16

64 3.3 Recognition of prior qualification.....18

65 3.3.1 Assessor Qualifications & Experience matrix .....19

66 3.3.2 Minimum Criteria .....19

67 3.3.3 Validity.....20

68 3.3.4 Waivers .....20

69 3.3.5 Revisions to baseline AQE .....20

70 3.4 Compliance Table.....22

71

**Contents**

## 72 1 INTRODUCTION

---

73 In order to have conformity to the Kantara Initiative IAF Service Assessment Criteria assessed  
74 and determined by qualified and independent assessors, Kantara Initiative operates an  
75 [Assurance Assessment Scheme \(AAS\)](#) which describes the process by which Assessors,  
76 Service Approval Authorities (future work item), Service Providers, and Federation Operators  
77 can show themselves to be fit to be granted use of the Kantara Initiative Mark, for their  
78 specific services, all of which are orientated toward the provision and use of identity  
79 credentials at recognized Assurance Levels and across a wide spectrum of public, private, and  
80 individual sectors.

81 This document sets out the requirements which applicant assessors must fulfill in order to  
82 become Kantara-Accredited Assessors. These requirements will be used to validate  
83 applicants' suitability by the Assessment Review Board (ARB), according to the processes  
84 described in the [Assurance Assessment Scheme](#).

## 85 2 GLOSSARY

---

86 The following terms are used specifically in this document, in addition to other terms from the  
87 [IAF Glossary](#):

88 **Audit Organization** - an organization which undertakes audits or assessments of  
89 entities and their services to establish their conformity to or compliance with specific  
90 standards or other widely-recognized criteria. Specifically, in the context of the AAS,  
91 entities providing credentialing or identity management services which are claiming  
92 conformance to the IAF;

93 **(Accreditation) Applicant** - an **Audit Organization** applying to Kantara Initiative for  
94 accreditation under the ACS;

95 **(Kantara-Accredited) Assessor** – an **Applicant** which has satisfied the requirements  
96 of the AAS and to which accreditation has been granted;

97 **(Audit) Subject** - the organization submitting its nominated services to a **Kantara-**  
98 **accredited Assessor** for audit and certification. *(Note – this usage of ‘Subject’ is*  
99 *exclusive strictly to this document – readers should note that it has a different and very*  
100 *specific meaning in other contexts, including within Kantara Initiative, e.g. in the PKI*  
101 *and Identity Management domains, and is consequently defined otherwise in the IAF*  
102 *Glossary, for wider use).*

## 103 **3 Assessor Qualifications & Requirements (AQR)**

---

### 104 **3.1 General Introduction**

105 Baseline Assessor Qualifications and Requirements (AQR) are those characteristics  
106 which the [IAF Assurance Assessment Scheme](#) document requires of its assessors,  
107 irrespective of whether they have prior recognition and qualification under any other  
108 scheme, framework, or process acknowledged by the ARB, or are seeking *ab initio*  
109 demonstration against the baseline characteristics.

### 110 **3.2 Baseline Assessor Qualifications & Experience**

111 The baseline characteristics selected for the Kantara Initiative Assurance Assessment  
112 Scheme (AAS) are derived from the following sources:

113	[AICPA_ATT]	AICPA
114		“ <i>Attestation Standards</i> ”, yyyy-mm-dd
115	[AICPA_AUD]	AICPA
116		“ <i>Auditing Standards</i> ”, yyyy-mm-dd
117	[AICPA_CPC]	AICPA
118		“ <i>Code of Professional Conduct</i> ”, 1997-10-28
119	[AICPA_CPE]	AICPA
120		“ <i>Continuing Professional Education</i> ”, Revised 2001-12-31
121	[AICPA_QCS]	AICPA
122		“ <i>Quality Control Standards</i> ”, 2009-01-01
123	[FPKI FSC PAG]	Federal PKI Policy Authority, SAFE-BioPharma Policy
124		Authority and CertiPath Policy Management Authority
125		“ <i>PKI Audit Guidelines</i> ”, Draft v0-7
126	[IAF]	Kantara Initiative Identity Assurance Framework
127	[IRCA802]	IRCA/802/08/1
128		“ <i>Criteria for Certification as an Information Security Auditor</i> ”,
129		2008-02
130	[IS 17021]	ISO/IEC 17021:2006
131		“ <i>Conformity assessment - Requirements for bodies providing</i>
132		<i>audit and certification of management systems</i> ”

133	[IS 19011]	ISO/IEC 19011:2002
134		“Guidelines on Quality and/or Environmental Management
135		Systems Auditing”
136	[IS 27006]	ISO/IEC 27006:2007
137		“ <i>Information technology – Security - Requirements for bodies</i>
138		<i>providing audit and certification of information security</i>
139		<i>management systems”</i>
140		(NB – IS 27006 mirrors IS 17021 but, where deemed necessary,
141		provides supplemental requirements explicitly for <i>information</i>
142		<i>security</i> management systems)
143	[ISACA_SGP]	“ <i>ISACA IS Standards, Guidelines and Procedures for Auditing</i>
144		<i>and Control Professionals”</i> , 2008-10-15
145	[ISACA_CISA]	“ <i>ISACA Candidate’s Guide to the CISA Exam and Certification”</i> ,
146		2007 (no more-specific date)
147	[PCIQSA]	Payment Card Industry Security Standards Council
148		“ <i>Validation Requirements for Qualified Security Assessors”</i>
149		Version 1.1, 2006-09

150 The AAS has drawn on these sources to identify useful attributes which represent the  
151 positive characteristics which Kantara Initiative requires of its accredited assessors,  
152 whether by virtue of their prior qualifications or by the provision of explicit evidence  
153 relating to specific requirements.

154 In order to be accredited by Kantara Initiative, Applicants must demonstrate that they  
155 possess all of these characteristics by fulfilling the following requirements. The  
156 following headings preface requirements which address:

- 157 1. The Audit Organization itself;
- 158 2. Individual Auditors;
- 159 3. The collective Audit Team;
- 160 4. Audit Domain-specific requirements.

161 Use of the above sources requires some qualification:

- 162 1. AICPA publications are generally directed at the accounting profession,  
163 rather than information security, and hence specific qualification of any  
164 clause having apparent relevance is required for the infosec domain. As a  
165 clear example of this, refer to [AICPA\_QCS] §10.45 as a very specific  
166 case where it identifies the possible need for an IT professional to be  
167 brought into the audit team to extend its capabilities, which in the case of  
168 the ACS requirements is their fundamental scope, and moreover  
169 specifically in the infosec domain. Because of this concern over  
170 applicability any AICPA member organization will have to show how  
171 their qualification relates to information security management.

- 172 2. IS 17021 is general in its requirements for bodies auditing and certifying  
173 management systems in general. For application to the specific interests  
174 of the AAS it must be supplemented by specific IT / information security  
175 management systems capabilities – these are, at the ISO level, provided in  
176 IS 27006 as requirements supplemental to those of IS 17021;
- 177 3. Whilst IS 19011 focuses on quality and/or environmental systems  
178 auditing, its provisions are largely general in their expression and  
179 therefore widely applicable, (see, e.g., IS 17021 §7,2.11), and even where  
180 its clauses are explicitly in a quality and/or environmental context, it is the  
181 intention that the standard can, in most instances, be readily interpreted in  
182 (e.g.) an information (security) management system context. The  
183 requirements of IS 19011 are therefore seen to be significantly relevant to  
184 the AAS goals;
- 185 4. ISACA\_SGP has been assessed only against the Standards, not the  
186 Guidelines and Procedures, which underpin adherence to the Standards.  
187 This is justified on the basis that the Standards are the prevailing authority,  
188 in addition to which ISACA\_CISA ensures that knowledge in reasonable  
189 depth is determined.

190 It should be noted that the AAS neither strives nor claims to embody a rigorous  
191 inclusion of all parts of the above references nor to be a proven mapping or  
192 comparison between their respective requirements.

193 The following baseline requirements are to be considered as an holistic set, rather than  
194 being individual and separate. Each requirement should therefore be considered to  
195 apply in principal to all other requirement topics, e.g., where requirement AO.8  
196 expresses expectations for competencies, such competencies must be shown to  
197 address the implied needs of any other requirement area.

198 Note that the tags used for these requirements are deliberately distinct from the format  
199 used to define SACs, to avoid any possibility of confusion between them.

200 References to the IAF are included so as to demonstrate that the provisions of that  
201 version of the IAF have been taken into consideration when formulating the present  
202 requirements (the AAS document of the IAF applies here).

### 203 **3.2.1 Audit Organization (AO) Requirements**

204 Applicant organizations must:

#### 205 **AO.1 Established business status**

- 206 1) have a recognized legal status as a business entity operating in compliance with all  
207 applicable requirements of the jurisdiction in which the business is principally  
208 established and also in those jurisdictions in which it has a base(s) of operations.



209 **Guidance:** For reasons of confidence in the existence and durability of the Applicant, the  
210 business has to be formally registered in some way as to there being no doubt that it is  
211 entitled to purvey its services and that it has an operational background which gives  
212 confidence that it has established practices and relevant experience, and all reasonable  
213 expectation that it will continue to operate for the medium-term future (at least three years).

214 Also of significance is that where the Applicant offers services in more than one  
215 jurisdiction (Country, State, Province, etc.) and has an established office in that jurisdiction  
216 (rather than providing a trans-border service) which it requires the Accreditation to cover,  
217 the same requirements apply to such additional jurisdiction.

218 Representative evidence would typically be verifiable copies of, or links to, licenses and/or  
219 business registrations, etc.

220 2) be in good standing with a level of liability protection set according to a risk-based  
221 determination, accounting for the scale of the business and the jurisdictions in which  
222 operations are conducted.

223 **Guidance:** To provide protection for the Subject organizations which it will assess,  
224 liability protection is necessary. Potential liabilities may be covered by business insurance  
225 or other instruments, e.g. reserves. Representative evidence would be such policies or  
226 proof of secured (i.e. fire-walled from application for any other purposes) reserves.

227 3) have effective documented management and approval structures.

228 **Guidance:** Possession and demonstrated application of a documented management  
229 structure with clear ownership and approval responsibilities is the most effective way to  
230 assess whether the organization is set up to manage and perform assessments in the way  
231 required (e.g. with integrity and independence) by other criteria in this set. Representative  
232 evidence would therefore be the defined processes and records of their implementation.

## 233 **AO.2 Independence & impartiality**

234 1) produce a documented commitment to maintaining its impartiality and independence  
235 from any of the potential providers of services within the Kantara Initiative community,  
236 and with other CSPs in other Federations with which Kantara Initiative may established  
237 agreements of any kind.

238 **Guidance:** The primary requirement is to show the senior management's commitment to  
239 allowing no ownership, shareholding, or conflicting contractual or like bindings between the  
240 Applicant and those whom it may assess, or with those parties which may have an interest  
241 in the outcome of any assessment, e.g. competitors of the Subject. A formal declaration is  
242 at the least a basis for addressing any lack of independence should it arise, although the  
243 ARB may seek further assurances where any potential conflicts of interest are known to  
244 them, in fact or as possibilities. Note that this requirement focuses on specific parties with  
245 which the Kantara Initiative community has relationships and because of this specific focus

246 would generally be provided as a specific statement in support of the application.  
247 Representative evidence would be a published statement.

248 2) acts at all times so as to preserve its impartiality.

249 **Guidance:** Whilst a declaration of impartiality is an important public statement, the  
250 practices to effect that impartiality must exist and be implemented. This requirement is that  
251 such practices be in place and continuously exercised. Potential threats to impartiality relate  
252 to organizational conflicts as well as those arising from other services which may have been  
253 offered to the Subject or personal interests or participation of individuals. Representative  
254 evidence would be records of instances where the Applicant has had to exhibit its  
255 impartiality (potentially in addressing a complaint or appeal, e.g.).

256 3) produce documented practices to review threats to impartiality in any assignment, at all  
257 stages of its conduct.

258 **Guidance:** Ensure that the Applicant undertakes an assessment of the risks, with regard to  
259 its impartiality undertakings, involved with each assessment it is engaged to perform, and  
260 that there is a review of that risk over the duration of the assignment. As a minimum, an  
261 initial assessment and one immediately prior to issuing a report would be expected, although  
262 others may be included where the assignment is extended or there are other obvious reasons  
263 to do so, such as a change of ownership or significant re-organization (of either party).  
264 'Practices' include documented record of the application of such practice, and the ARB may  
265 require evidence to be provided, as it may for any criterion. This requirement essentially  
266 underpins sub-requirement (3) of this clause. Representative evidence would be the  
267 required documentation.

### 268 **AO.3 Management responsibility & liability**

269 1) show management commitment to adherence to best governance practices supported by  
270 having documented policies and procedures which ensure adherence to professional  
271 standards and practices and in particular to the auditing standards and processes under  
272 which it operates.

273 **Guidance:** Notwithstanding the clear need for the practitioners actually undertaking the  
274 assessments to have requisite skills (addressed in subsequent requirements) it is important  
275 that the Applicant organization actually demonstrates that it is set up for and capable of  
276 employing best management practices as required. Representative evidence would therefore  
277 be identification as to how the Applicant's practices fulfill this requirement and identify the  
278 audit and technical standards and/or other references on which its operations are based.

### 279 **AO.4 Openness / Defined audit process**

280 1) faithfully document and publish the audit process(es) it applies, describing the technical  
281 procedures, accounting for principles such as impartiality, objectivity and

282 confidentiality, any applicable reference standards, and its contractual arrangements  
283 with its clients.

284 **Guidance:** Kantara Initiative seeks a consistency in the application of assessments leading  
285 to certification of Kantara-recognized Service Providers and therefore requires that Kantara-  
286 Accredited Assessors have in place a documented and well-defined process for engaging  
287 with clients and performing their assessments which can be repeated and in an ideal world  
288 would yield consistent results for the same Subject service. Representative evidence would  
289 be the documentation defining the process and records of its implementation.

#### 290 **AO.5 Confidentiality**

291 1) have in place procedures which ensure that proprietary information relating to clients is  
292 securely stored and controlled in all aspects of its use.

293 **Guidance:** Many Subjects will be vying for business from Kantara Initiative members and  
294 other participants in the wider community, and as a result assessors will potentially be  
295 exposed to proprietary information relating to one or more of another service provider's  
296 competitors. As representative evidence, Applicants must show that they have in place  
297 procedures which will safeguard their clients' confidentiality in all respects.

#### 298 **AO.6 Responsiveness to complaints**

299 1) have a means by which clients may lodge appeals or complaints concerning their  
300 practices and determinations and have a documented process for objectively addressing  
301 those complaints.

302 **Guidance:** The Applicant should have the means to receive, process, and respond fairly to  
303 any complaints or appeals arising from the conduct of its assessment services, since an  
304 objective audit process may be a cause for contention where findings are concerned.  
305 Having in place the means to address and resolve any such issues contributes to the overall  
306 assurance from the accreditation process. Representative evidence would be the  
307 documented process and samples of its implementation where there are any.

#### 308 **AO.7 Resources**

309 1) have qualified and competent personnel to manage the organization and to perform the  
310 audits.

311 **Guidance:** Provision of documentary evidence of the organization's conformity to  
312 preceding criteria is not, of itself, sufficient – the AAS also requires that the Applicant  
313 shows that it has personnel with the requisite competencies and qualifications necessary to  
314 effectively apply the organization's policies, procedures, etc. A register of roles, related job  
315 descriptions, and current employee names for the positions having specific relevance would  
316 fulfill this requirement.

- 317 2) have documented processes to ensure that audit and support personnel have and  
318 maintain the competencies necessary to fulfill their duties according to the systems  
319 being assessed, their complexity and their geographic location(s).

320 **Guidance:** Provision of documentary evidence of the organization's conformity to  
321 preceding criteria is not, of itself, sufficient – Kantara Initiative also requires that the  
322 Applicant shows that it has personnel with the requisite competencies and qualifications  
323 necessary to effectively apply the organization's policies, procedures, etc. A register of  
324 roles, related job descriptions, and current employee names for the positions having specific  
325 relevance would fulfill this requirement.

## 326 **AO.8 Technical competence**

- 327 1) have an operating record of a minimum accumulation of three person months of  
328 provision of audit services over an elapsed period of 12 months OR, if unable to fulfill  
329 either requirement, having staff who can demonstrate these minima in their professional  
330 experience immediately prior to establishing/joining the Applicant organization.

331 **Guidance:** Apart from having appropriate competencies, actual experience in their  
332 application is required to be shown. This is intended to ensure that the Applicant,  
333 organizationally, is active in the auditing arena. Provision is made to 'grandfather'  
334 experience from specific staff members when they are able to demonstrate their currency  
335 and are assuming an active role within an organization which might otherwise not meet the  
336 AAS requirement. Representative evidence would be illustration of past assignments, in  
337 terms of scope, date, and resources applied, including which specific personnel participated.

## 338 **3.2.2 Auditor Qualification (AQ) Requirements**

339 Although the AAS does not accredit individuals, the organization must commit to ensuring that  
340 the assessors it uses fulfill the following requirements and that it has in place the means to  
341 ensure that these requirements are fulfilled. Applicant organizations must ensure that their  
342 individual Auditors:

### 343 **AQ.1 Personal attributes**

- 344 1) exhibit ethical standards by performing audits in an honest, fair, objective, and discreet  
345 manner and with due diligence and professional care, with neither record of  
346 professional mal-practice nor of criminal conviction such as to bring into doubt their  
347 ability to so perform the audit.

348 **Guidance:** Ethical standing is required of all personnel involved in the oversight,  
349 management, performance, review, and granting of certification relating to any audit  
350 process. Ethics require the auditor to be fair, truthful, and honest in their dealings with the  
351 audit client, in their assessment of only factual matters, and in their overall performance of  
352 the audit. This requires strict adherence to professional and technical standards as well as  
353 having a balanced personal nature. Whilst some infractions of the law might be identified

354 they may equally be considered to be inconsequential in the context of the performance of  
355 the required assessments. On the other hand, convictions such as fraud, embezzlement,  
356 other acts of moral turpitude, bankruptcy, would be serious concerns, in the event of which  
357 judgment would have to be made as to the risk that may be presented to the good standing  
358 of the AAS as a whole should the Applicant be granted Accreditation. On-going  
359 investigations or existing allegations may also require careful consideration by the ARB.  
360 Factors in such determinations might be the role of any affected individuals within the  
361 Applicant organization. The greater the authority and influence of anyone having any  
362 unfavorable record should be balanced against the severity and nature of their (possibly  
363 alleged) offense when deciding whether to recognize them or not. Required evidence could  
364 be an employee-screening process operated by the organization, records of application of  
365 that process including background checks, questionnaires, etc.

366 Note that this requirement does not assess experience and knowledge in the specific auditing  
367 field – see AQ.3.

## 368 **AQ.2 Technical competence**

369 1) have and maintain the requisite knowledge, training, and experience of applicable  
370 generic audit standards and those specifically addressing information security  
371 governance and management, risk assessment, information technology, and related  
372 security controls.

373 **Guidance:** In addition to overall technical competence across the organization, individual  
374 technical competence must be shown for individual auditors. Required evidence would be  
375 identification of the specific training undertaken, of standards and other references about  
376 which the individuals have knowledge, and of particular techniques applied.

377 2) have the requisite knowledge, training and experience of applicable laws, regulations  
378 and other such requirements.

379 **Guidance:** A comprehensive assessment must investigate the regulatory aspects of the  
380 subject and hence, in addition to technical skills, assessors must have knowledge of  
381 applicable legislation, etc. Required evidence would be identification of such laws, etc., and  
382 where the assessor purveys their work in more than one jurisdiction, indication of the  
383 differing requirements across jurisdictions.

## 384 **AQ.3 Subject Matter-specific competence**

385 1) be knowledgeable about, trained, and current in the specific management, operational,  
386 and technical aspects of the «*specific domain & technology*» in which the audit is  
387 performed (see note below), including accepted practices, and applicable standards and  
388 specifications.

389 **Note:** For the purposes of being deemed qualified to perform assessments of CSPs claiming  
390 conformity to the Kantara Initiative IAF Service Assessment Criteria, the requirements for

391 «*specific domain & technology*» shall be fulfilled by conformity to the requirements set  
392 forth herein under group ‘AD’.

393 Where other organizations and federations wish to use Kantara-accredited assessor  
394 organizations for assessments performed in their own «*specific domain & technology*» (e.g.  
395 PCI DSS, Federal PKI, ...) they should state their own criteria to be used in lieu of (or in  
396 addition to, according to their chosen scoping) those in group ‘AD’ herein when fulfilling  
397 this AAS requirement and take their own measures to determine the Applicant’s conformity  
398 to those specific needs.

399 **Guidance:** Subject-specific knowledge and experience is required to enable the effective  
400 application of the generic audit competencies to the specific subject area. Since the Kantara  
401 Initiative Assurance Assessment Scheme is, but for this particular requirement, generic and  
402 agnostic in its choice of baseline characteristics such that it can be adopted for other uses or  
403 assessors accredited against it can be used in other domains where the only additional  
404 requirement is the domain-specific knowledge, this present requirement can be either  
405 substituted for by an alternative domain’s set of specific requirements or extended with  
406 other such requirements where the two specific areas are both necessary.

#### 407 **AQ.4 Education / Professional qualification/certification**

408 1) have received at least a secondary education (and would preferably hold a bachelor’s  
409 degree in any subject) plus any one (at least) of the following professional technical  
410 IT/information security management qualifications, which must be current: CGEIT,  
411 CISA, CISSP, CISM, CITP, IRCA for ISMS/ITSM, PCI QSA, or proven equivalent  
412 qualification or experience.

413 **Guidance:** Current professional qualifications are the more important part of this  
414 requirement, underpinning the basic training qualifications – although a secondary  
415 education is the minimum acceptable, a bachelor’s degree is the preferred baseline  
416 educational experience and those without it may have to show stronger work experience to  
417 be acceptable. Holding one of these professional qualifications gives confidence in the  
418 underlying knowledge of the assessor, which may be broader than some specific experience  
419 has allowed. Required evidence would typically be certified copies of award of  
420 qualification or a URL to a professional body’s registry, which can be authenticated.

#### 421 **AQ.5 Impartiality & Professional Competence**

422 1) have no connection to the client, the material subject to the audit, or any relevant parties  
423 other than in their professional auditing capacity, nor be of a disposition vulnerable to  
424 coercion.

425 **Guidance:** Although preceding requirements require independence and impartiality on the  
426 part of the organization, its audit staff must also exhibit these qualities and be qualified to  
427 perform the audit. Past professional experience and assignments will be one way to make  
428 an assessment of their impartiality, e.g. ensuring that the auditee organization was not a



429 previous employer of the auditor, or the auditor a previous employer of any of the auditee's  
430 staff, or that the auditor had not previously given consultancy to the auditee organization,  
431 preferably in any form whatsoever, or otherwise demonstrably in a manner which could not  
432 have any relationship to the material which the audit will address. Inter-personal  
433 relationships might also color judgment but will be harder to identify without the  
434 cooperation of the auditor. Even harder to assess, unless there is a pattern of auditee's  
435 complaints about the fairness of an auditor, is the intellectual objectivity, truthfulness, and  
436 impartiality which are the scope of professional competence in this context.

437 Forms of evidence could be the individual auditor's assertions or the applicant  
438 organization's processes and records for reviewing previous employment or customer  
439 complaints.

#### 440 **AQ.6 Experience**

441 1) have participated for a minimum of 20 days of audit services, of which 10 days must  
442 have been on-site, over an elapsed period of 36 months.

443 **Guidance:** This requirement accommodates 'desk auditing', i.e. review of documents from  
444 the auditor's own offices, but also requires on-site auditing experience, since this is the most  
445 demanding, challenging, and also effective experience. Verifiable personal or  
446 organizational records of assignments undertaken would generally satisfy this need.

### 447 **3.2.3 Audit Team (AT) Requirements**

448 Auditor Teams must:

#### 449 **AT.1 Collective skills**

450 1) consist of professionals who collectively have the necessary skills and experience to  
451 assess the policies, procedures, and practices of the subject in all general and specific  
452 respects; a single auditor is acceptable but must meet the requirements for Lead Auditor  
453 (below).

454 **Guidance:** Although an audit team may actually be a single person, the nature of the audit  
455 subject may require a range of differing expertise which can only be effectively fulfilled by  
456 a team of complementary individuals. A process for determining the skill requirements for  
457 any particular audit and selecting suitably skilled audit staff, supported where required by  
458 evidence of past assignments and the selected team's skills would typically be the form of  
459 required evidence.

#### 460 **AT.2 Leader Auditor's skills**

461 1) be led by an individual who has participated as a Team Leader (including supervised in  
462 that capacity) for a minimum of 15 days of audit services, of which 10 days must have  
463 been on-site, over an elapsed period of 24 months.

464 **Guidance:** This simply requires that the Lead Auditor has either received training in this  
465 role or has performed it as a qualified Leader within a reasonable period of time and at a  
466 reasonable level of effort. Staff records should be the most practical form of evidence to  
467 support conformity to this requirement.

468 2) be led by an individual who has a knowledge of all areas which are addressed by the  
469 audit, although other team members may have specialist roles.

470 **Guidance:** The selected Lead Auditor's curriculum vitae, or similar evidence of past  
471 experience and training, should demonstrate that they have the requisite skills, at least at a  
472 level where, supported by specialist advice, they can make informed and balanced decisions.

473 3) be capable of planning an audit with such a scope.

474 **Guidance:** The Applicant is expected to demonstrate by past performance, available  
475 resource, and tactical capability that they are able to plan and execute an audit of the form  
476 required to satisfy Kantara Initiative expectations. Record of past performance would be an  
477 obvious way to evidence conformity to this requirement.

### 478 **AT.3 Use of SMEs**

479 1) where necessary, only use Subject Matter Experts which exhibit the same degree of  
480 impartiality and competence in their specific field as do the auditors in theirs. SMEs  
481 may advise the Lead Auditor but may not dictate findings, recommendations, or  
482 remedial actions.

483 **Guidance:** SMEs may be either internal or external, although in the latter case the ARB  
484 would expect to see that the organization had in place the means to ensure that the SME,  
485 organizationally and individually, would not impinge upon the applicant organization's  
486 ability (once accredited) to fulfill the AAS requirements. Evidence of a process for  
487 validating and selecting SMEs, possibly supported by records of the application of that  
488 process, would be appropriate evidence.

### 489 **3.2.4 Audit Domain (AD) Requirements (i.e. «specific domain & 490 technology»)**

491 Auditors assessing Subjects which are Credential Service Providers must be highly  
492 knowledgeable about:



493 **AD.1 Applicable credential and identity management standards**

- 494 1) current and evolving international standards  
495 DIS 27046,  
496 DIS 29115 (a.k.a. ITU-T x.eaa<sup>1</sup>).

497 **Guidance:** Whether it is the above-cited standards or others which over time may be added  
498 or used to replace those here-cited, applicants should show as evidence against this  
499 requirement any or a combination of: a training program for its auditors which imparts  
500 knowledge and understanding of these standards; previous performance of audits where  
501 knowledge and understanding of the standards was applied, or; direct participation as an  
502 author / editor / expert contributor to development of the standard(s).

- 503 2) current and evolving sector-specific standards  
504 Draft ITU-T x.eaa.

505 **Guidance:** Evidential requirements and principles are as stated for AD.1(1) above.

- 506 3) national/regional standards:  
507 - Federal Credential Assessment Framework Credential Assessment Profiles,  
508 - NIST Federal Information Processing Standard 201, NIST Special Publication  
509 800-63,  
510 - Federal Identity Credentialing Committee “*Criteria for Assessing FIPS 201*  
511 *Compliance of PIV Applicant Registration and Card Issuance Services*”, v2.Z .

512 **Guidance:** Evidential requirements and principles are as stated for AD.1(1) above.

- 513 4) IAF Service Assessment Criteria (Common Organizational, Identity Proofing,  
514 Credential Management).

515 **Guidance:** Evidential requirements and principles are as stated for AD.1(1) above.

516 **AD.2 Technical knowledge**

- 517 1) the credential management subject area, across the entire life-cycle and encompassing  
518 management and technical matters, the definition and implications of the specified  
519 Assurance Levels, and knowledge of the various technologies employed.

520 **Guidance:** Evidential requirements and principles are as stated for AD.1(1) above.

---

<sup>1</sup> A standard published by ITU-T would be a sector-specific standard. Although this document may evolve through the same channel as Draft International Standard 29115, and have no material differences, this clause is retained to accommodate potential future sector-specific criteria, and if ITU-T x.eaa and DIS 29115 do evolve as a common standard then conformity to this requirement (at least in the context of this specific standard) will suffice to show conformity to the following requirement

### 521 3.3 Recognition of prior qualification

522 The AAS is based upon the principle that it shall impose the minimum additional effort upon  
523 Applicants, and Kantara Initiative itself, commensurate with sufficient confidence being  
524 established in the Applicants' conformity to all of the requirements know collectively as the  
525 'baseline characteristics'. Through the 'grandfathering' principle maximum recognition is  
526 given to Applicants who can demonstrate their qualification against certain recognized industry  
527 references, these being:

528	[AICPA_ATT]	AICPA
529		" <i>Attestation Standards</i> ", yyyy-mm-dd
530	[AICPA_AUD]	AICPA
531		" <i>Auditing Standards</i> ", yyyy-mm-dd
532	[AICPA_CPC]	AICPA
533		" <i>Code of Professional Conduct</i> ", 1997-10-28
534	[AICPA_CPE]	AICPA
535		" <i>Continuing Professional Education</i> ", Revised 2001-12-31
536	[AICPA_QCS]	AICPA
537		" <i>Quality Control Standards</i> ", 2009-01-01
538	[FPKI FSC PAG]	Federal PKI Policy Authority, SAFE-BioPharma Policy
539		Authority and CertiPath Policy Management Authority
540		" <i>PKI Audit Guidelines</i> ", Draft v0-7
541	[IAF]	Kantara Initiative Identity Assurance Framework, v2.0
542		(specifically the Assurance Assessment Scheme)
543	[IRCA802]	IRCA/802/08/1
544		" <i>Criteria for Certification as an Information Security Auditor</i> ",
545		2008-02
546	[IS 17021]	ISO/IEC 17021:2006
547		" <i>Conformity assessment - Requirements for bodies providing</i>
548		<i>audit and certification of management systems</i> "
549	[IS 19011]	ISO/IEC 19011:2002
550		" <i>Guidelines on Quality and/or Environmental Management</i>
551		<i>Systems Auditing</i> "
552	[IS 27006]	ISO/IEC 27006:2007
553		" <i>Information technology – Security - Requirements for bodies</i>
554		<i>providing audit and certification of information security</i>
555		<i>management systems</i> "
556		(NB – IS 27006 mirrors IS 17021 but, where deemed necessary,

557		provides supplemental requirements explicitly for <i>information</i>
558		<i>security</i> management systems)
559	[ISACA_SGP]	“ISACA IS Standards, Guidelines and Procedures for Auditing
560		and Control Professionals”, 2008-10-15
561	[ISACA_CISA]	“ISACA Candidate’s Guide to the CISA Exam and Certification”,
562		2007 (no more-specific date)
563	[PCIQSA]	Payment Card Industry Security Standards Council
564		“Validation Requirements for Qualified Security Assessors”
565		Version 1.1, 2006-09

566 By their very nature, these references provide ‘credit’ against different groups of the AAS  
567 requirements, and Applicants may use collective credits from multiple prior qualifications.

568 The ARB will, where the published credit allowed is ‘qualified’ or ‘none’, allow credit where  
569 the Applicant can demonstrate that specific AAS requirements were in fact addressed by the  
570 particular prior qualification they are presenting. This recognizes that the determination made  
571 in this document is based upon a generic interpretation of the applicable reference, rather than  
572 a specific instance of it.

573 The continued validity of the credit granted to Applicants with certified (or otherwise proven)  
574 conformity to the requirements of each reference shall be reviewed and revised accordingly  
575 whenever the relevant reference source is revised.

### 576 3.3.1 Assessor Qualifications & Experience (AQE) matrix

577 The AQE matrix in Table 1 provides a color-coded quick-look reference for each of the  
578 recognized sources of pre-qualification which will allow Applicants with multiple forms of  
579 pre-qualification, and the ARB, to determine the AAS requirements where the Applicant must  
580 provide specific evidential inputs rather than have their conformity ‘grandfathered’ on account  
581 of credit given for their pre-qualification status.

582 Where there may be two or more clauses from the same reference source applicable for any  
583 given AAS requirement which do not have the same ‘credit’ determination the least favorable  
584 determination is given (things can only get better from thereon). Such instances are marked ‘†’  
585 in the matrix (e.g. ‘Qualified †’).

### 586 3.3.2 Minimum Criteria

587 These criteria establish minima: Applicants who seek credit on the basis of prior qualification  
588 under other schemes acceptable to Kantara Initiative shall be expected to be in full compliance  
589 with the most demanding of the combined criteria, at all times during which they seek the  
590 benefit of any prior qualification(s).

591 **3.3.3 Validity**

592 Where an Applicant's accreditation is based on prior qualification the accreditation will lapse  
593 six months after the first-occurring expiration date of any claimed prior qualifications, at any  
594 given point during the first two-and-a-half years of the three year accreditation validity.  
595 Kantara Initiative considers that a six-month window offers the Applicant sufficient latitude in  
596 renewing the applicable qualification(s) or offering supplemental evidence of conformity  
597 should they choose to no longer rely upon that prior qualification for the applicable AAS  
598 requirements.

599 **3.3.4 Waivers**

600 Applicants with reasonable grounds for doing so may request that a waiver be granted where  
601 the AAS requirements are not strictly met but the Applicant requests a 'conformity exception –  
602 CE' and offers sufficient evidence to convince the ARB that their specific qualifications or  
603 evidence are equally acceptable. For example, special experience may have been acquired and  
604 used to gain a professional qualification in lieu of conventional requirements, in which case,  
605 assuming that the qualification was one recognized by the ARB, the same argument would  
606 most likely be accepted as fulfillment of the AAS' requirement for relevant experience.

607 Kantara Initiative reserves the right, at the sole determination of the ARB, to decline requests  
608 for waivers, grant waivers on a one-off basis and for whatever time period it deems fit, or to  
609 undertake revision of the AAS requirements to include the circumstances of the request as a  
610 permanent part of the AAS (see below).

611 **3.3.5 Revisions to baseline AQE**

612 Kantara Initiative reserves the right, subject to due notice and consultation, to revise these  
613 criteria as it sees fit, including the addition of requirements in response to any CE requests  
614 which suggest that such evidence is justifiable and likely to be sufficiently commonplace or  
615 valuable to the overall accreditation process to deserve recognition through revision to  
616 requirement.

617 **Table 3-1** Assessor Qualifications & Experience ‘credit’ reference matrix

ACS Rqt		AICPA	IRCA	ISO 19011	ISO 17021	ISO 27006	ISACA	PCI SSC
AO.1	1)	Qualified	None	None	Qualified	Qualified	None	Qualified
	2)	None	None	None	Unqualified	Unqualified	None	None †
	3)	None	None	None	Unqualified	Unqualified	None	None †
AO.2	1)	None	None	None	Qualified	Qualified	Qualified	Qualified
	2)	Qualified	None	None	Qualified	Qualified	Unqualified	Qualified
	3)	None	None	None	Unqualified	Unqualified	Qualified	Qualified
AO.3	1)	Qualified	None	None	Unqualified	Unqualified	None	None
AO.4	1)	Qualified	None	Qualified	Unqualified	Unqualified	Qualified	None
AO.5	1)	Qualified	None	None	Unqualified	Unqualified	None	Unqualified
AO.6	1)	Qualified	None	None	Unqualified	Unqualified	None	None
AO.7	1)	Qualified	None	Qualified	Unqualified	Unqualified	Qualified	Qualified
	2)	Qualified	None	Qualified	Unqualified	Unqualified	None †	None
AO.8	1)	None	None	Qualified	None	Qualified	None	Qualified
AQ.1	1)	Qualified	None	Qualified	None	None	Qualified	Qualified
AQ.2	1)	Qualified	Unqualified	Unqualified	Unqualified	Unqualified	Unqualified	Qualified
	2)	Qualified	None	Unqualified	None	Unqualified	None	None
AQ.3	1)	None (defers to AD group)						
AQ.4	1)	None	Unqualified	Qualified	None	Unqualified	None	None
AQ.5	1)	Qualified	None	Qualified	Unqualified	Unqualified	Unqualified	None
AQ.6	1)	None	Unqualified	None	None	Unqualified	None	None
AT.1	1)	Qualified	None	Unqualified	Unqualified	Unqualified	None	None
AT.2	1)	None	Unqualified	Unqualified	Unqualified	Unqualified	None	None
	2)	Qualified	Unqualified	Unqualified	Unqualified	Unqualified	None	None
	3)	Qualified	Unqualified	Unqualified	Unqualified	Unqualified	Qualified †	None
AT.3	1)	Qualified	None	Unqualified	Unqualified	Unqualified	Unqualified	None
AD.1	1) - 4)	None (Non-IAF frameworks may specify their own domain-specific requirements for which different credit may be determined in recognition of prior qualification)						
AD.2	1)							

618

619

### 3.4 Compliance Table

Use the following table to correlate criteria and the evidence offered to support compliance.

Assessors preparing an application can use the table to correlate evidence with criteria or to justify non-applicability based upon their prior qualification or other factors they believe to be valid.

The ARB may use the table to record the steps in its assessment and its determination of compliance or of any non-compliances.

**Table 3-2** AQR Compliance

Clause	Description	Compliance
<u><a href="#">Audit Organization (AO) Requirements</a></u>		
AO.1	<u><a href="#">Established business status</a></u>	
AO.2	<u><a href="#">Independence &amp; impartiality</a></u>	
AO.3	<u><a href="#">Management responsibility &amp; liability</a></u>	
AO.4	<u><a href="#">Openness / Defined audit process</a></u>	
AO.5	<u><a href="#">Confidentiality</a></u>	
AO.6	<u><a href="#">Responsiveness to complaints</a></u>	
AO.7	<u><a href="#">Resources</a></u>	
AO.8	<u><a href="#">Technical competence</a></u>	
<u><a href="#">Auditor Qualification (AQ) Requirements</a></u>		
AQ.1	<u><a href="#">Personal attributes</a></u>	
AQ.2	<u><a href="#">Technical competence</a></u>	
AQ.3	<u><a href="#">Subject Matter-specific competence</a></u>	
AQ.4	<u><a href="#">Education / Professional qualification/certification</a></u>	
AQ.5	<u><a href="#">Impartiality &amp; Professional Competence</a></u>	
AQ.6	<u><a href="#">Experience</a></u>	

<u>Audit Team (AT) Requirements</u>		
AT.1	<u>Collective skills</u>	
AT.2	<u>Leader Auditor's skills</u>	
AT.3	<u>Use of SMEs</u>	
<u>Audit Domain (AD) Requirements</u>		
AD.1	<u>Applicable credential and identity management standards</u>	
AD.2	<u>Technical knowledge</u>	

626

627

## Revision History

1. 8May2008 – Identity Assurance Framework Version 1.0 Initial Draft
  - a. Released by Liberty Alliance
  - b. Revision and scoping of Initial Draft release
2. 23JUNE 2008 – Identity Assurance Framework Version 1.1 Final Draft
  - a. Released by Liberty Alliance
  - b. Inclusion of comments to Final Draft
3. 1OCTOBER2009 – Identity Assurance Framework Version 1.1 Final Draft
  - a. Documents contributed to Kantara Initiative by Liberty Alliance
4. XAPRIL2010 – Identity Assurance Framework Version 2.0
  - a. Released by Kantara Initiative
  - b. Significant scope build
  - c. Original Identity Assurance Framework all inclusive document broken in to a set of documents with specific focus:
    - i. Kantara IAF-1000-Overview
    - ii. Kantara IAF-1100-Glossary
    - iii. Kantara IAF-1200-Levels of Assurance
    - iv. Kantara IAF-1300-Assurance Assessment Scheme
    - v. Kantara IAF-1400-Service Assessment Criteria
    - vi. Kantara IAF-1600-Assessor Qualifications and Requirements