Identity Assurance Framework:
Assessor Qualifications & Requirements

Version: draft 0.6

Date: 2009-10-13

Editor: Richard G. Wilsher
Zygma LLC

Contributors

This document is a draft and not in final release form. The full list of contributors will be added prior to the final release of this document.

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

Notice

Contents

1 INTRODUCTION **4**
2 GLOSSARY **5**
3 ASSESSOR QUALIFICATIONS & REQUIREMENTS (AQR) **6**
3.1 General Introduction 6
3.2 Baseline Assessor Qualifications & Experience 6
3.2.1 Audit Organization (AO) Requirements 8
3.2.2 Auditor Qualification (AQ) Requirements 12
3.2.3 Audit Team (AT) Requirements 15
3.2.4 Audit Domain (AD) Requirements (i.e. «*specific domain & technology*») 16
3.3 Recognition of prior qualification 17
3.3.1 Assessor Qualifications & Experience matrix 19
3.3.2 Minimum Criteria 19
3.3.3 Validity 19
3.3.4 Waivers 19
3.3.5 Revisions to baseline AQE 20
3.4 Compliance Table 22

Deleted: 4
Formatted: Font: Times New
Deleted: 5
Formatted: Font: Times New
Formatted: Font: Times New
Deleted: 6

1 INTRODUCTION

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

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

2 GLOSSARY

The following terms are used specifically in this document, in addition to other terms from the IAF Glossary:

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

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

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

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

3 Assessor Qualifications & Requirements (AQR)

3.1 General Introduction

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

3.2 Baseline Assessor Qualifications & Experience

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

[AICPA_ATT]	AICPA "*Attestation Standards*", yyyy-mm-dd
[AICPA_AUD]	AICPA "*Auditing Standards*", yyyy-mm-dd
[AICPA_CPC]	AICPA "*Code of Professional Conduct*", 1997-10-28
[AICPA_CPE]	AICPA "*Continuing Professional Education*", Revised 2001-12-31
[AICPA_QCS]	AICPA "*Quality Control Standards*", 2009-01-01
[FPKI FSC PAG]	Federal PKI Policy Authority, SAFE-BioPharma Policy Authority and CertiPath Policy Management Authority "*PKI Audit Guidelines*", Draft v0-7
[IAF]	Kantara Initiative Identity Assurance Framework
[IRCA802]	IRCA/802/08/1 "*Criteria for Certification as an Information Security Auditor*", 2008-02
[IS 17021]	ISO/IEC 17021:2006 "*Conformity assessment - –Requirements for bodies providing audit and certification of management systems*"
[IS 19011]	ISO/IEC 19011:2002 "Guidelines on Quality and/or Environmental Management Systems Auditing"

[IS 27006] ISO/IEC 27006:2007 "*Information technology – Security - Requirements for bodies providing audit and certification of information security management systems*" (NB – IS 27006 mirrors IS 17021 but, where deemed necessary, provides supplemental requirements explicitly for *information security* management systems)

[ISACA_SGP] "*ISACA IS Standards, Guidelines and Procedures for Auditing and Control Professionals*", 2008-10-15

[ISACA_CISA] "*ISACA Candidate's Guide to the CISA Exam and Certification*", 2007 (no more-specific date)

[PCIQSA] Payment Card Industry Security Standards Council "*Validation Requirements for Qualified Security Assessors*" Version 1.1, 2006-09

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

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

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

Use of the above sources requires some qualification:

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

2. IS 17021 is general in its requirements for bodies auditing and certifying management systems in general. For application to the specific interests of the AAS it must be supplemented by specific IT / information security

management systems capabilities – these are, at the ISO level, provided in IS 27006 as requirements supplemental to those of IS 17021;

3. Whilst IS 19011 focuses on quality and/or environmental systems auditing, its provisions are largely general in their expression and therefore widely applicable, (see, e.g., IS 17021 §7,2.11), and even where its clauses are explicitly in a quality and/or environmental context, it is the intention that the standard can, in most instances, be readily interpreted in (e.g.) an information (security) management system context. The requirements of IS 19011 are therefore seen to be significantly relevant to the AAS goals;

4. ISACA_SGP has been assessed only against the Standards, not the Guidelines and Procedures, which underpin adherence to the Standards. This is justified on the basis that the Standards are the prevailing authority, in addition to which ISACA_CISA ensures that knowledge in reasonable depth is determined.

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

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

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

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

3.2.1 Audit Organization (AO) Requirements

Applicant organizations must:

AO.1 Established business status

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

Guidance: For reasons of confidence in the existence and durability of the Applicant, the business has to be formally registered in some way as to there being no doubt that it is entitled to purvey its services and that it has an operational background which gives

confidence that it has established practices and relevant experience, and all reasonable expectation that it will continue to operate for the medium-term future (at least three years).

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

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

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

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

3) have effective documented management and approval structures.

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

AO.2 Independence & impartiality

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

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

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

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

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

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

AO.3 Management responsibility & liability

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

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

AO.4 Openness / Defined audit process

1) faithfully document and publish the audit process(es) it applies, describing the technical procedures, accounting for principles such as impartiality, objectivity and confidentiality, any applicable reference standards, and its contractual arrangements with its clients.

Guidance: Kantara Initiative seeks a consistency in the application of assessments leading to certification of Kantara-recognized Service Providers and therefore requires that Kantara-Accredited Assessors have in place a documented and well-defined process for engaging

with clients and performing their assessments which can be repeated and in an ideal world would yield consistent results for the same Subject service. Representative evidence would be the documentation defining the process and records of its implementation.

AO.5 Confidentiality

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

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

AO.6 Responsiveness to complaints

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

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

AO.7 Resources

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

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

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

Guidance: Provision of documentary evidence of the organization's conformity to preceding criteria is not, of itself, sufficient – Kantara Initiative also requires that the

Applicant shows that it has personnel with the requisite competencies and qualifications necessary to effectively apply the organization's policies, procedures, etc. A register of roles, related job descriptions, and current employee names for the positions having specific relevance would fulfill this requirement.

AO.8 Technical competence

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

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

3.2.2 Auditor Qualification (AQ) Requirements

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

AQ.1 Personal attributes

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

Guidance: Ethical standing is required of all personnel involved in the oversight, management, performance, review, and granting of certification relating to any audit process. Ethics require the auditor to be fair, truthful, and honest in their dealings with the audit client, in their assessment of only factual matters, and in their overall performance of the audit. This requires strict adherence to professional and technical standards as well as having a balanced personal nature. Whilst some infractions of the law might be identified they may equally be considered to be inconsequential in the context of the performance of the required assessments. On the other hand, convictions such as fraud, embezzlement, other acts of moral turpitude, bankruptcy, would be serious concerns, in the event of which judgment would have to be made as to the risk that may be presented to the good standing of the AAS as a whole should the Applicant be granted Accreditation. On-going investigations or existing allegations may also require careful consideration by the ARB.

Factors in such determinations might be the role of any affected individuals within the Applicant organization. The greater the authority and influence of anyone having any unfavorable record should be balanced against the severity and nature of their (possibly alleged) offense when deciding whether to recognize them or not. Required evidence could be an employee-screening process operated by the organization, records of application of that process including background checks, questionnaires, etc.

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

AQ.2 Technical competence

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

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

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

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

AQ.3 Subject Matter-specific competence

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

Note: For the purposes of being deemed qualified to perform assessments of CSPs claiming conformity to the Kantara Initiative IAF Service Assessment Criteria, the requirements for «*specific domain & technology*» shall be fulfilled by conformity to the requirements set forth herein under group 'AD'.

Where other organizations and federations wish to use Kantara-accredited assessor organizations for assessments performed in their own «*specific domain & technology*» (e.g. PCI DSS, Federal PKI, …) they should state their own criteria to be used in lieu of (or in addition to, according to their chosen scoping) those in group 'AD' herein when fulfilling

this AAS requirement and take their own measures to determine the Applicant's conformity to those specific needs.

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

AQ.4 Education / Professional qualification/certification

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

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

AQ.5 Impartiality & Professional Competence

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

Guidance: Although preceding requirements require independence and impartiality on the part of the organization, its audit staff must also exhibit these qualities and be qualified to perform the audit. Past professional experience and assignments will be one way to make an assessment of their impartiality, e.g. ensuring that the auditee organization was not a previous employer of the auditor, or the auditor a previous employer of any of the auditee's staff, or that the auditor had not previously given consultancy to the auditee organization, preferably in any form whatsoever, or otherwise demonstrably in a manner which could not have any relationship to the material which the audit will address. Inter-personal relationships might also color judgment but will be harder to identify without the cooperation of the auditor. Even harder to assess, unless there is a pattern of auditee's complaints about the fairness of an auditor, is the intellectual objectivity, truthfulness, and impartiality which are the scope of professional competence in this context.

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

AQ.6 Experience

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

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

3.2.3 Audit Team (AT) Requirements

Auditor Teams must:

AT.1 Collective skills

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

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

AT.2 Leader Auditor's skills

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

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

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

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

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

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

AT.3 Use of SMEs

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

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

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

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

AD.1 Applicable credential and identity management standards

1) current and evolving international standards
   DIS 27046,
   DIS 29115 (a.k.a. ITU-T x.eaa[1]).

Guidance: Whether it is the above-cited standards or others which over time may be added or used to replace those here-cited, applicants should show as evidence against this requirement any or a combination of: a training program for its auditors which imparts knowledge and understanding of these standards; previous performance of audits where

[1] 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

knowledge and understanding of the standards was applied, or; direct participation as an author / editor / expert contributor to development of the standard(s).

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

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

3) national/regional standards:
- Federal Credential Assessment Framework Credential Assessment Profiles,
- NIST Federal Information Processing Standard 201, NIST Special Publication 800-63,
- Federal Identity Credentialling Committee "*Criteria for Assessing FIPS 201 Compliance of PIV Applicant Registration and Card Issuance Services*", v2.Z .

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

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

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

AD.2 Technical knowledge

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

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

3.3 Recognition of prior qualification

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

[AICPA_ATT] AICPA
"*Attestation Standards*", yyyy-mm-dd

[AICPA_AUD] AICPA
"*Auditing Standards*", yyyy-mm-dd

[AICPA_CPC] AICPA
"*Code of Professional Conduct*", 1997-10-28

[AICPA_CPE] AICPA
"*Continuing Professional Education*", Revised 2001-12-31

[AICPA_QCS] AICPA
"*Quality Control Standards*", 2009-01-01

[FPKI FSC PAG] Federal PKI Policy Authority, SAFE-BioPharma Policy Authority and CertiPath Policy Management Authority
"*PKI Audit Guidelines*", Draft v0-7

[IAF] Kantara Initiative Identity Assurance Framework, v2.0 (specifically the Assurance Assessment Scheme)

[IRCA802] IRCA/802/08/1
"*Criteria for Certification as an Information Security Auditor*", 2008-02

[IS 17021] ISO/IEC 17021:2006
"*Conformity assessment - –Requirements for bodies providing audit and certification of management systems*"

[IS 19011] ISO/IEC 19011:2002
"Guidelines on Quality and/or Environmental Management Systems Auditing"

[IS 27006] ISO/IEC 27006:2007
"*Information technology – Security - Requirements for bodies providing audit and certification of information security management systems*"
(NB – IS 27006 mirrors IS 17021 but, where deemed necessary, provides supplemental requirements explicitly for *information security* management systems)

[ISACA_SGP] "*ISACA IS Standards, Guidelines and Procedures for Auditing and Control Professionals*", 2008-10-15

[ISACA_CISA] "*ISACA Candidate's Guide to the CISA Exam and Certification*", 2007 (no more-specific date)

[PCIQSA] Payment Card Industry Security Standards Council
"*Validation Requirements for Qualified Security Assessors*"
Version 1.1, 2006-09

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

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

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

3.3.1 Assessor Qualifications & Experience (AQE) matrix

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

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

3.3.2 Minimum Criteria

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

3.3.3 Validity

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

3.3.4 Waivers

Applicants with reasonable grounds for doing so may request that a waiver be granted where the AAS requirements are not strictly met but the Applicant requests a 'conformity exception – CE' and offers sufficient evidence to convince the ARB that their specific qualifications or evidence are equally acceptable. For example, special experience may have been acquired and used to gain a professional qualification in lieu of conventional requirements, in which case,

assuming that the qualification was one recognized by the ARB, the same argument would most likely be accepted as fulfillment of the AAS' requirement for relevant experience.

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

3.3.5 Revisions to baseline AQE

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

616 **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)							

617

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-compliancies.

Table 3-2 AQR Compliance

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

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

624