InCommon Assurance Community Call

Refocusing Community Guidance of InCommon's Trust Programs:
Baseline & Bronze
October 4th, 2017

Brett Bieber
InCommon Assurance Advisory Chair

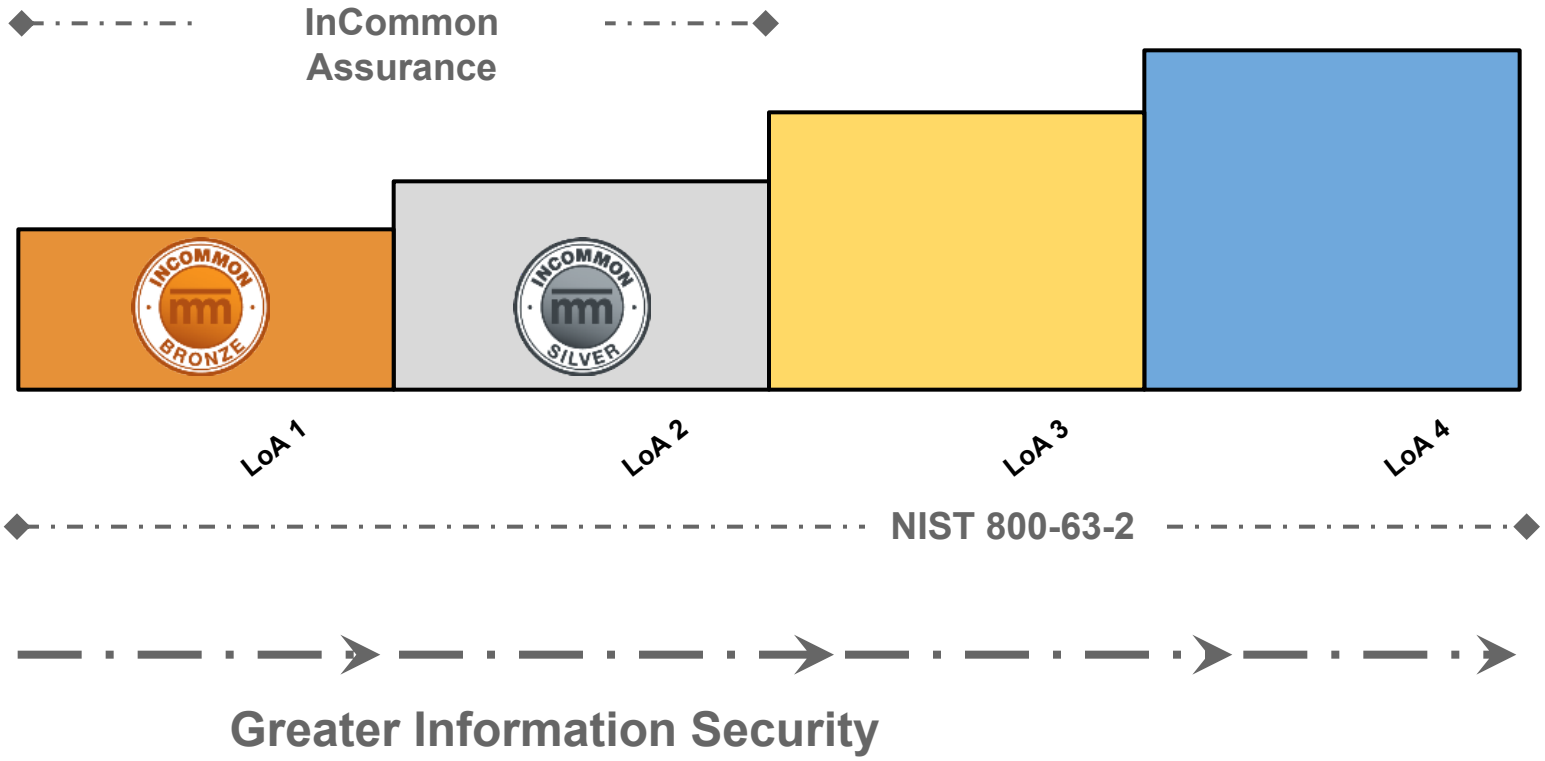
Topics

- Background on the AAC
- How Assurance is Changing
- Bronze Survey: What Do LoA Users Think?
- Next Steps & Recommendations

What is the InCommon Assurance Advisory Committee?

What is the AAC?

The Assurance Advisory Committee (AAC) is the oversight body of the InCommon Assurance Program and an advisory body to the InCommon Steering Committee.


InCommon
Assurance
INCOMMON
BRONZE
INCOMMON
SILVER
LoA 1
LoA 2
LoA 3
LoA 4
NIST 800-63-2
Greater Information Security

InCommon
Bronze & Silver

NIST
800-63-2

FICAM Trust Framework Providers

Federal Identity, Credential, and Access Management Architecture

CertiPath	Aerospace
SAFE BioPharma	Healthcare
STRAC	State & Local
TSCP Inc.	Aerospace
InCommon	Higher Education
Kantara	General
NIEF	Law Enforcement

5 schools

1 school
(did not renew)

InCommon
Bronze & Silver

≠

NIST
800-63-3

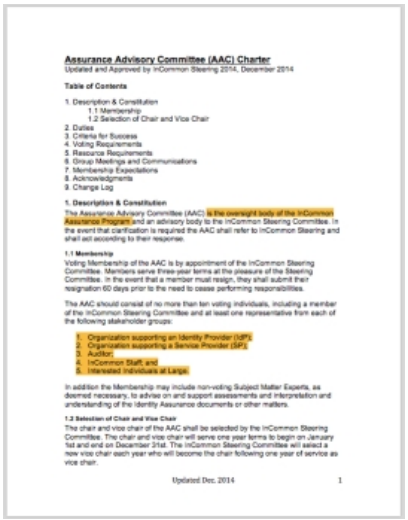
Assurance Progress

Assurance is growing, but not through Bronze & Silver:

- MFA Interoperability Profile
- SIRTFI
- REFEDS Assurance WG
- Baseline Expectations

Where do we go from here?

AAC Charter Changes Needed



Assurance Advisory Committee (AAC) Charter
Updated and Approved by InCommon Steering 2014, December 2014

Table of Contents

1. Description & Constitution

The Assurance Advisory Committee (AAC) is the oversight body of the InCommon Assurance Program and an advisory body to the InCommon Steering Committee. In the event that clarification is required the AAC shall refer to InCommon Steering and shall act according to their response.

1.1 Membership

Voting Membership of the AAC is by appointment of the InCommon Steering Committee. Members serve three-year terms at the pleasure of the Steering Committee. In the event that a member must resign, they shall submit their resignation 60 days prior to the need to cease performing responsibilities.

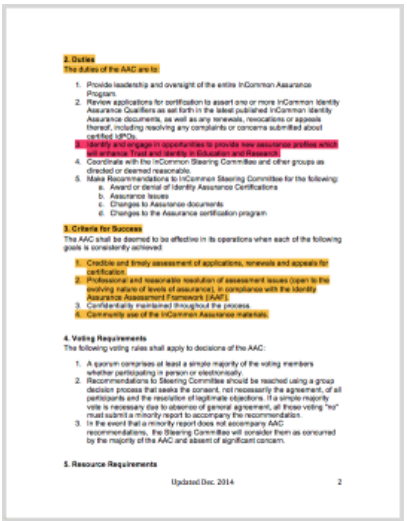
The AAC should consist of no more than ten voting individuals, including a member of the InCommon Steering Committee and at least one representative from each of the following stakeholder groups:

1. Organization supporting an Identity Provider (IdP)
2. Organization supporting a Service Provider (SP)
3. Auditor
4. InCommon Staff, and
5. Interested Individuals at Large.

In addition the Membership may include non-voting Subject Matter Experts, as deemed necessary, to advise on and support assessments and interpretation and understanding of the Identity Assurance documents or other matters.

1.2 Selection of Chair and Vice Chair

The chair and vice chair of the AAC shall be selected by the InCommon Steering Committee. The chair and vice chair will serve one year terms to begin on January 1st and end on December 31st. The InCommon Steering Committee will select a new vice chair each year who will become the chair following one year of service as vice chair.



2. Duties

The duties of the AAC are to:

1. Provide leadership and oversight of the entire InCommon Assurance Program.
2. Review applications for certification to assert one or more InCommon Identity Assurance Qualifiers as set forth in the latest published InCommon Identity Assurance documents, as well as any renewals, revocations or appeals thereof, including resolving any complaints or concerns submitted about certified IdPOs.
3. Identify and engage in opportunities to provide new assurance profiles which will enhance Trust and Identity in Education and Research.
4. Coordinate with the InCommon Steering Committee and other groups as directed or deemed reasonable.
5. Make Recommendations to InCommon Steering Committee for the following:
   a. Award or denial of Identity Assurance Certifications
   b. Assurance Issues
   c. Changes to Assurance documents
   d. Changes to the Assurance certification program

3. Criteria for Success

The AAC shall be deemed to be effective in its operations when each of the following goals is consistently achieved:

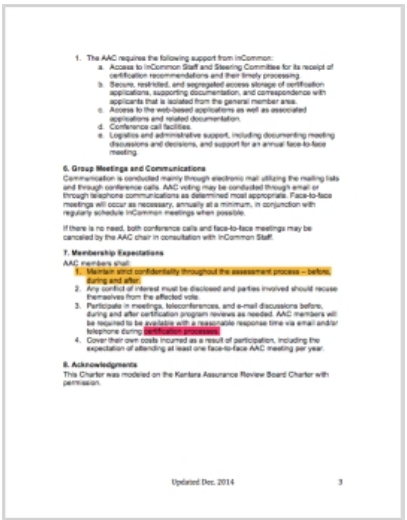
1. Credible and timely assessment of applications, renewals and appeals for certification.
2. Professional and reasonable resolution of assessment issues (open to the evolving nature of levels of assurance) in compliance with the Identity Assurance Assessment Framework (IAAF).
3. Confidentiality maintained throughout the process.
4. Community use of the InCommon Assurance materials.

4. Voting Requirements

The following voting rules shall apply to decisions of the AAC:

1. A quorum comprises at least a simple majority of the voting members whether participating in person or electronically.
2. Recommendations to Steering Committee should be reached using a group decision process that seeks the consent, not necessarily the agreement, of all participants and the resolution of legitimate objections. If a simple majority vote is necessary due to absence of general agreement, all those voting "no" must submit a minority report to accompany the recommendation.
3. In the event that a minority report does not accompany AAC recommendations, the Steering Committee will consider them as concurred by the majority of the AAC and absent of significant concern.

5. Resource Requirements



1. The AAC requires the following support from InCommon:
   a. Access to InCommon Staff and Steering Committee for its receipt of certification recommendations and their timely processing.
   b. Secure, restricted, and segregated access storage of certification applications, supporting documentation, and correspondence with applicants that is isolated from the general member area.
   c. Access to the web-based applications as well as associated applications and related documentation.
   d. Conference call facilities.
   e. Logistics and administrative support, including documenting meeting discussions and decisions, and support for an annual face-to-face meeting.

6. Group Meetings and Communications

Communication is conducted mainly through electronic mail utilizing the mailing lists and through conference calls. AAC voting may be conducted through email or through telephone communications as determined most appropriate. Face-to-face meetings will occur as necessary, annually at a minimum, in conjunction with regularly schedule InCommon meetings when possible.

If there is no need, both conference calls and face-to-face meetings may be canceled by the AAC chair in consultation with InCommon Staff.

7. Membership Expectations

AAC members shall:

1. Maintain strict confidentiality throughout the assessment process – before, during and after;
2. Any conflict of interest must be disclosed and parties involved should recuse themselves from the affected vote.
3. Participate in meetings, teleconferences, and e-mail discussions before, during and after certification program reviews as needed. AAC members will be required to be available with a reasonable response time via email and/or telephone during certification processes.
4. Cover their own costs incurred as a result of participation, including the expectation of attending at least one face-to-face AAC meeting per year.

8. Acknowledgments

This Charter was modeled on the Kantara Assurance Review Board Charter with permission.

AAC Membership

The AAC should consist of no more than ten voting individuals, including a member of the InCommon Steering Committee and at least one representative from each of the following stakeholder groups:

1. Organization supporting an Identity Provider (IdP);
2. Organization supporting a Service Provider (SP);
3. Auditor;
4. InCommon Staff; and
5. Interested Individuals at Large.

Proposed AAC Membership?

- Security representative
- Membership should represent all of InCommon (large & small)
- Research Organizations
- Experts in mediation and consensus building
- Others?

AAC Duties

1. Provide leadership and oversight of the entire InCommon Assurance Program.
2. Review applications for certification to assert one or more InCommon Identity Assurance Qualifiers as set forth in the latest published InCommon Identity Assurance documents, as well as any renewals, revocations or appeals thereof, including resolving any complaints or concerns submitted about certified IdPOs.
3. Identify and engage in opportunities to provide new assurance profiles which will enhance Trust and Identity in Education and Research.
4. Coordinate with the InCommon Steering Committee and other groups as directed or deemed reasonable.
5. Make Recommendations to InCommon Steering Committee for the following:
    a. Award or denial of Identity Assurance Certifications
    b. Assurance Issues
    c. Changes to Assurance documents
    d. Changes to the Assurance certification program

Proposed AAC Duties

- Maintain and support the Baseline Expectations of InCommon Participants.
  - Shepherd community consensus
  - Review disputes between parties
  - Recommend action to InCommon Steering
- Support the InCommon Assurance Program.
- Identify and engage in opportunities to provide new assurance profiles which will enhance Trust and Identity in Education and Research.
- Coordinate with the InCommon Steering Committee and other groups as directed or deemed reasonable.
- Others?

Bronze Institution Survey

The Five Bronze holders were surveyed to gather their perspectives on the current and potential future of this form of Level of Assurance certification, and more broadly on where InCommon should focus related effort.

Summary of Survey Questions

- Is there value in Bronze?
- Is Kantara an option?
- Are you looking for NIST 800-63-3?
- Suggestions for the Future?

Link to Survey Questions

Summary of Survey Responses

- Is there value in Bronze?
  - Yes! Best practices are of value
- Is Kantara an option?
  - Kantara who?
- Are you looking for NIST 800-63-3?
  - No expectation of actual LoA use online
- Suggestions for the Future?
  - NIST 800-171 (FISMA) would be more useful than 800-63-3
  - Baseline & SIRTFI are great, where’s identity-proofing?

Questions for the Community

Questions

- Is there any value in continuing to offer InCommon Bronze?
- Is there any value in continuing to offer InCommon Silver?
- Should InCommon seek to move from 800-63-2 to 800-63-3
- Should InCommon continue as a FICAM certified trust framework provider?

Summary & Recommendations

Next Steps

- Develop recommendations on the future of the Assurance Program
- Change AAC Charter, including new duties and success factors
- Recruit new AAC members
- Boot-up Baseline Expectations & Maintenance Processes
  - Communicate changes in support of Baseline Expectations
  - Seed community consensus process
  - Support community dispute resolution process

If the idea of helping InCommon to mature and increase its value appeals to you, please consider serving on the AAC, or on a Review Board when asked.