Minutes of Assurance Call of 9-Jan-2013

Draft Minutes: Assurance Implementers Call of 9-Jan-2013

Attending

Ann West, InCommon/Internet2
Mary Dunker, Virginia Tech
Karen Harrington Virginia Tech
Jim Green, Michigan State University
Mark Jones, UT Houston
Susan Neitsch, Texas A&M
David Walker, Independent
David Bantz, University of Alaska
Benn Oshrin, Internet2
Michael Brogan, U. Washington
Steven Carmody, Brown
Chris Spadanuda, U-W Milwaukee
Mark Rank, U-W Milwaukee
Thomas Callaci, U-W Madison
Shreya Kumar, Michigan Tech University
David Langenberg, University of Chicago
Ron Thielen, University of Chicago
Mary Murphy, University of Chicago
Eric Goodman, UCSC
Emily Eisbruch, Internet2, scribe

DISCUSSION

FICAM Process

There was a call with FICAM in late December to discuss version 1.2 and another call will take place this afternoon. Important topics are criteria for Alternative Means and a process for publishing approved Alternative Means for the community. The goal is that once an Alternative Means is approved, it in effect becomes part of the spec, so another campus could also use the approved alternative approach.

Most likely we will be on track for FICAM approval in January. There will then be an opportunity for public review of the spec. Then it will be reviewed by Assurance Advisory Committee (AAC) and recommended to InCommon Steering for approval.

Review of Virginia Tech Implementation Example Draft

https://spaces.at.internet2.edu/x/MwAlAg

Mary Dunker has been developing a Virginia Tech Implementation example, based on a template available on the wiki. The goal is to share the Virginia Tech experience getting bronze and silver certification so that other campuses can benefit from this information during their own process.

As indicated in the top section of the implementation example, Virginia Tech was certified under Version 1.1. Since other sites will be seeking certificaiton under a higher version, this will likely create some differences. This implementation example will reflect the VA Tech experience. Subsequent campuses will have a different experience.

The implementation example uses the gap analysis template available on the assurance wiki:https://spaces.at.internet2.edu/display/InCAssurance/Wiki+page+template+for+gap+analysis%2C+IAP+1.2+%28pending+approval%29

The management assertions are close to verbatim from what Virginia Tech gave to the auditors. However, the "Evidence of Compliance" sections are summaries, since there was so much detail in that area.

Comments on the VA Tech Implementation Example

Q: Did VA Tech use the Silver Assessment Report Template, that is linked from the Assurance wiki Toolkits page:https://spaces.at.internet2.edu/display/InCAssurance/Assurance+Implementation+Toolkits

A: No. The VA Tech internal audit dept had their own format. They were encouraged to look at the template

Comment: It would be good to call out the fact that VA Tech used their own internal audit and that was acceptable,.

Comment: Under the lessons learned heading, the last bullet that says "Obtain a clear understanding of the information InCommon expects to see in the audit summary, particularly if an alternative means is being used to satisfy one or more criteria in the IAP." Possibly we should elaborate on that and mention that it could be helpful to use the Silver Assessment Report Template.

Documentation is now being developed on what needs to be in the audit for a site using alternative means. At the time VA Tech was applying for certification, the requirements/procedures around alternative means area were not yet well defined.

Q: As a campus working towards assurance, how do we know if our efforts are good enough?
A: If your auditor and you as IdP have questions on whether a practice addresses a requirement in the profile, then send that question to the Assurance list.

Q: Now that VA Tech has been certified, have you issued a token to all staff and faculty?

A: Mary: we were already issuing the tokens prior to be certified. The people who already had them have qualified under bronze. After achieving silver, we started issuing new silver-level tokens to those who met the strict requirements. The tokens expire every 2 years.

Q: Could more detail be included on how registration and identity proofing is handled?
A: This detail exists, but wanted to keep the implementation example at a reasonable size.

Comment: Would be helpful to define more of the terms that the reader won't immediately be familiar with.

Comment: in the gap analysis table, would be helpful to give more info on what was done to address each gap.

Password Entropy Calculators

There have been requests for an InCommon Assurance Password Entropy Calculators tool. A couple of existing 800-63 calculators can be found at https://spaces.at.internet2.edu/x/RQAlAg

Do we want to develop a tool specifically for Bronze and Silver?

Thomas Callaci from UW- Madison spoke about the tool he's developed:

https://spaces.at.internet2.edu/download/attachments/35979333/entropenator_expanded-draft2.xlsx?version=1&modificationDate=1357673939643

Tom stated that his first goal in developing the tool was to see if he could do the calculations according to NIST 863 for LOA1 or LOA2. His tool succeeded in that. Once more people started using the tool, Tom improved the user interface. The UI could probably use additional improvement.

Others on the call said they had used this tool and found it worked pretty well. There was agreement that perhaps the UI could be improved.

It might be helpful if the user could specify the variables around how many password guesses are allowed per second / per hour or per other timeframe, before a password reset is required.

Should InCommon Assurance identify recommendations around password safety that have broad buy-in and list those on the wiki?

We may need to continue the discussion on the list in order to decide if developing a bronze/silver Password Entropy Tool is a worthwhile project.

Next Call: Wed. 6-Feb-2013 at noon ET