Audit Issues-Questions

I'd love to get their thoughts about the remote proofing approaches on the I2 wikispaces - I talked a bit with Chad Sharp from Iowa and Steve Kurncz from MSU about this, but they had mentioned the possibility of getting some more detailed feedback at their upcoming meeting.

1. Remote identity proofing -- from Nick Roy of Iowa -- as far as I can tell institutions are not able to do remote identity proofing as described in the IAP (checking a combination of government ID numbers and financial account numbers obtained through credit bureaus or similar databases). Two alternate methods have been proposed: a) the person to be verified can appear in person with the appropriate documents and a form and have the verification confirmed by a notary public near where they live; the notarized form would serve as proof of the verification event; b) The identity documents could be verified remotely using some kind of videoconferencing technology. See Remote-Proofing Approaches.

Do the auditors think either or both of these methods can be asserted as equivalent to the approach the IAP describes? What are the issues?

2. Strong password authentication -- a question came up on one of the documentation group's calls as to whether an institution can legitimately claim to be in compliance via strong password authentication (described in 4.2.3.3 of v. 1.2 of the IAP) when we cannot technically force non-IdP applications always to use protected channels as required in 4.2.3.6. With regard to 4.2.3.6, the discussion has always centered around the idea of presenting institutional policy requirements for non-IdP applications as mitigating controls. But many of us are uncomfortable with that concept as we do not have much in the way of enforcement authority for our policies. I am wondering what the auditors think about this -- what would policies and enforcement mechanisms that legitimately constitute equivalent controls look like? How would we document this for the audit, and how would the auditor go about evaluating it?

3. Multi-factor authentication -- a number of institutions plan to pursue certification based on multi-factor authentication technology, as did Virginia Tech. Since compliance via multi-factor is not described in the IAP, how do we go about documenting that our particular flavor of multi-factor is equivalently strong, and how will the auditor evaluate our management assertions?

4. Do the auditors have guidelines or suggestions as to how we should prepare our submission to facilitate the auditor's job, and to include the right amount of information? From time to time we've had auditors or people with audit experience on our conference calls talk about including just enough information to meet the scope of whatever factor we're writing our assertion for. It reminds me of things our general counsel's office has said from time to time -- if you include too much information you have a risk of inadvertently expanding the scope.