Link to 2024 ACAMP Wiki

Advance CAMP Thu. Dec 12 2024

Room - I

Session Title: Managing up re: Federation (Chris); Campus buy-in for Shared IAM Governance (Kenny); EntraID Governance (~~Garrett~~)

CONVENER: Kenny Barnt (MTC/Moran), Chris Bongaarts (Univ of Minnesota)

MAIN SCRIBE(S): Dave Mak (Berklee College of Music), Julian Anderson (Oberlin College)

ADDITIONAL CONTRIBUTORS:

# of ATTENDEES: 29

DISCUSSION:

- Kenny: self-intro (currently at Moran for ~3 mos, formerly Mich State)
    - To be successful, IAM needs to be a whole-institution effort; can't be successful when HR wants to own employees, registrar wants to own students, etc. because identities don't live in a single bucket for their lifetime!
    - Questions: what works? Who was involved? What doesn't work
    - At Mich State:
        - Recently did IAM strategy review w/ Moran since university hasn't invested in IAM the way it needed to; mix of 30-y/o homegrown stuff and new off-the-shelf stuff; inefficient, batch-based (mainframe retired 2 yrs ago, takes 3 days for student to have acct after application)
        - No one wanted to change the status quo about who chooses who gets access to what data, etc. Difficult for IAM folks to make progress b/c they didn't have direction from partners besides basic tech req'mts, but when we presented anything *to* them, reaction was "why are you doing this?!"
- Kevin Carpenter (RIT): Sharing most of that

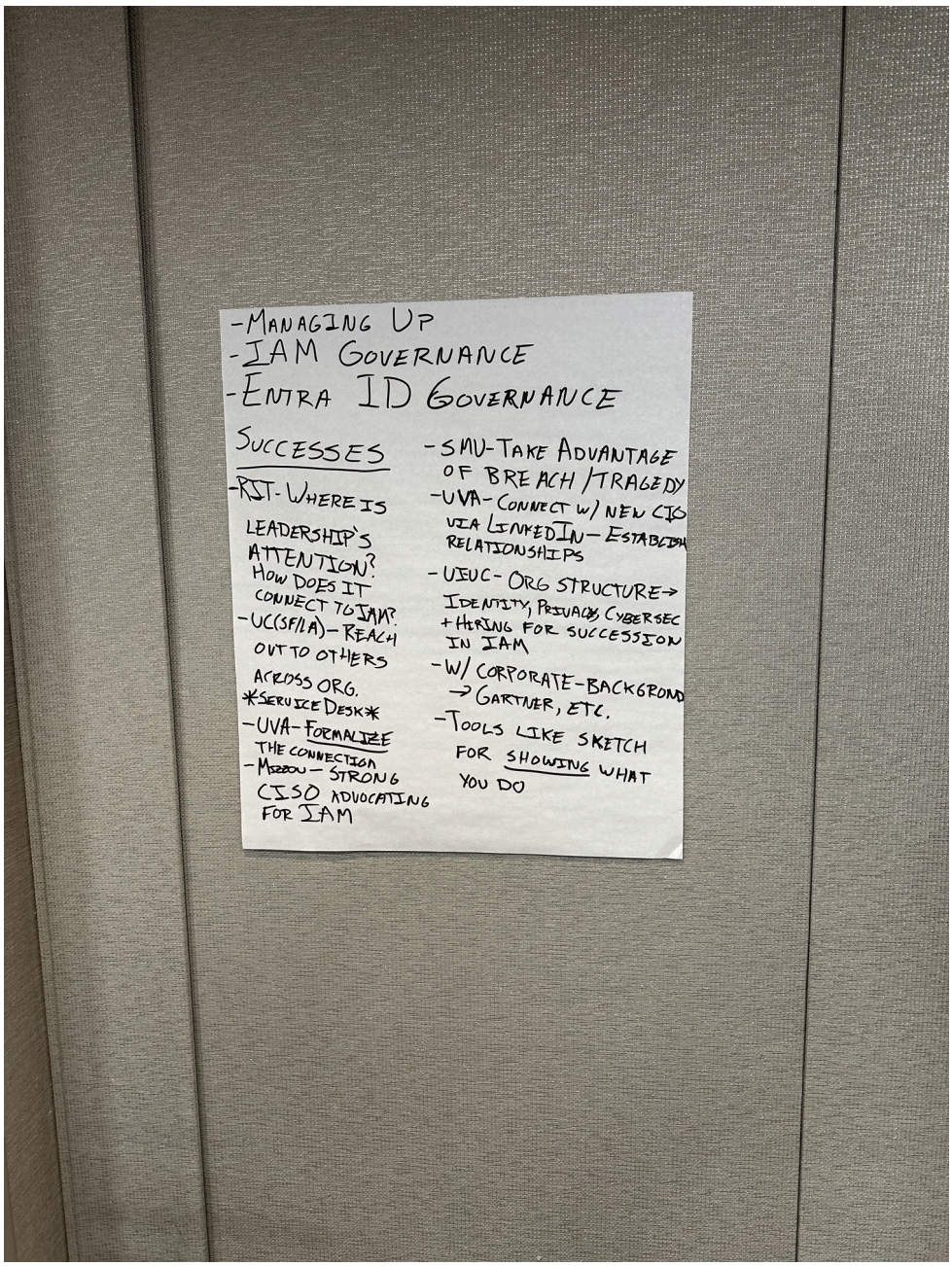
    - RIT is replacing ERP, with 2026-01-01 go-live
    - New-ish enterprise architecture group, pushing to explain w/ partners that it's not *your* (individual partner's) data, it's *institutional* data, so they don't get to make sole decisions about what happens w/ data
    - Non-SIS/HCM entities (e.g., admissions) don't want to own their own processes, so IAM ends up owning them
    - Kenny: when talking about identities, at least 3 different governance sources: *who wins? For how long? Are there exceptions?*
    - Chris Bongaarts: HIPAA/SEVIS/related contention in conflict with IAM policies. Also have colleges where people are not necessarily actively taking courses but still need accounts (e.g., College of Education students doing practicums). (BTW, HIPAA won the metaphorical cage fight)
    - Kenny: any success stories to share? A lot of shared commiseration so far, lol
- Greg Gardner (RIT): Maybe not necessarily *success*, at least *progress*:
    - Q: "are there some methods that have been successful?" A: **where is your leadership's attention?** In RIT's case, it was an ERP project, which MTC was working on; MTC wanted to talk to IAM folks, and leaders were confused. Moran response: IAM is an important component, and not involving them can be a risk! Need to connect things that are real in IAM space to things that are real in other space.
        - Doubled IAM team and got large commitment to additional funding. Can't have people who mostly do other things and moonlight as IAM folks
        - Kevin: now that IAM is a recognized program, getting asked about stuff at beginning of a project rather than just before go-live has been a benefit
            - Kenny: Are you able to parlay this into a governance program?
                - Greg: yes, we got recognition that we need a dedicated IAM program
- Jeffrey Crawford (UCSF/LA): That's great, but it required a third party coming in to intervene; when that's not available, boils down to IAM folks simply reaching out and having convos with other parts of the university.
    - Definitely not easy (especially for introverts), but helpful. Not necessarily needing to reach out to C-suite, but managers/senior mgrs
    - Reach out to service desk too!
    - Kevin: We reached out, they said go away
        - Jeffrey: we had to be persistent

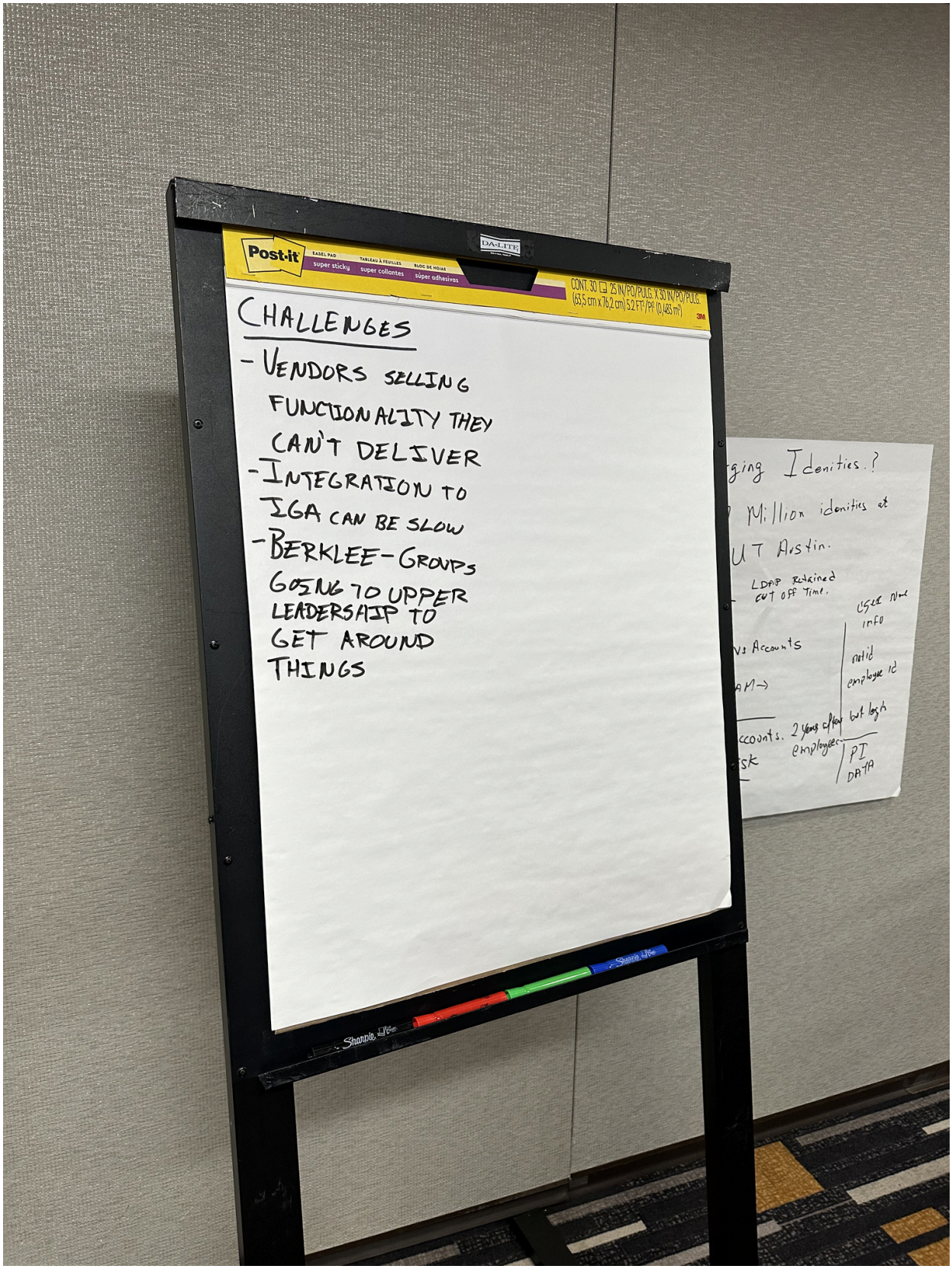
        - Greg: lack of understanding before, but MTC convinced IT organization at large to recognize need for specific IAM team and governance
    - Chris: As someone who is technically an IAM architect but is really sysadmin "under the covers", people he used to work w/ as a sysadmin have moved up organizationally. Beginning to encounter trickiness due to turnover. Even w/i IAM area, there's even diversity of viewpoints, e.g., is InCommon membership still worthwhile? (*yes*!) Has taken a lot of working over. For example, yes, Shibboleth requires a lot of futzing w/ XML, but it gives you tangible benefits that just buying Okta doesn't
    - Kellen Murphy: UVA's IAM team formed steering committee to meet quarterly to ask what is wanted, with IAM team guidance. **Formalize the connections!**
        - Kevin: impressive, but realization of responsibility often drove business partners to *avoid* being part of committee in our case at Mich State.
    - Liz (univ of Missouri): we are lucky to have an IDM team (under security team); small, but mighty: with strong leadership and advocacy from CISO. What can we do collectively for higher ed. Community?
        - Tommy Doan, SMU: it takes an account compromise/breach/etc. (tragedy) or the like to get buy-in
        - Have statistics, etc about why IAM is important, turn into graphs to give leadership
        - Graham: also need to frame as proactive vs reactive decision
    - Clara Broomfield (InCommon Academy): lots of convos this week about proving value to leadership, InCommon interested in helping
    - Heidi Berrysmith, UWash: IAM is where everything happens (invisibly). Was middleware, now part of CISO office. When it works well, is invisible; when fails, suddenly highly visible. CIO has ideas that don't necessarily align with other IT directors.
    - Kenny: these stakeholders were included with good relationships, but getting the commitment on decisions was a struggle.
    - Martin Douglas (U of Western Ontario/LARG*Net): Would another step such as enforced attendance to BaseCAMP/TechEx/etc. help with adoption?
        - Kellen: at UVA, as *soon* as new CIO was announced, I reached out to her on LinkedIn and connected to open that line of communication. Ended up coming up in handy later

        - Kellen: **don't be afraid to have these conversations!** Yes, they're hard, but the more you do it, the more others will see you as an honest operator.
        - Jeffrey (UCSF/LA): You have to have those conversations/reach out even if it's outside your responsibilities.
        - Heidi (U Wash): important to have two-way discussions with registrar, etc. about what's important, what is not going to work, etc.
    - Kenny: one reason he was successful was that we all (SIS/ERP directors, IAM) reported to same director and had priorities set by same person
    - Erica Ohman (UIUC): One thing that the IAM team did was hire a bunch of new people a few years ago to start succession planning.
        - Moved into cybersec realm, now part of Identity, Privacy, and Security aegis
        - **Make a friend in your cybersecurity team** — you might have an opportunity there
        - Also definitely helped to have a CIO who did IAM at one point in her career to help
        - Jeffrey (UCSF/LA) had Gartner access that demonstrated importance of identity governance. Helped to amplify voices within org to get leadership attention.
        - Rebekah Erins (PM with InCommon): Project: sketch project to provide tool to represent what we do. Conversation with leadership can help with use of this tool. Not ready for release yet (CommEX is target), but looking for testing volunteers.
        - Erica: also, Grouper will help you pull out visualizations that can help w/ building higher-level sketches using IAM sketch tool.
- Struggles?
    - Kellen UVA: Governing Entra ID is a challenge for us
        - We have Fischer Identity at UVA, selected in 2018; they helped UVA set up workflows.
        - "It has not worked well" - Kellen
        - Leadership is heavy on moving to Entra, but is having trouble navigating to leadership (esp. Since governance tooling is likely not ready yet, Entra is a cloud product and thus possibly vaporware)
        - Q: how do I manage that concern up, while I've got midPoint is well built for us already?

        - Dave Mak (Berklee): leadership always looking for one product/suite fits all; one of our jobs is to educate/advise/consult leadership
            - Kellen: same with Zero Trust. Our institution thought they could just “buy Zero Trust”
    - Jeffrey: going into an institution just beginning to deal with IGA, this is definitely a long process. Came from a school that had Grouper already and was able to integrate quickly / reuse code, and misses that capability. Wonders if this is possible with other systems?
        - Kellen: at the same time, what a lot of PAM products offer is not true PAM, it’s privileged *credential* mgmt. UVA bought HashiCorp Vault. It’s PCM for sure, but *not PAM*.
        - Kellen: caution about IGA deployment: Fischer built out a lot of integration, pipelines, etc. for them. In a lot of cases, same effective code/logic in a lot of different places w/ slight changes, which can make it very hard to parse when reviewing/rearchitecting. Would like to see something more modular
    - Tommy (SMU): Kellen, could you please differentiate more between PIM/PAM?
        - Managing service acct with credentials that need to be rotated, vs. policy handling
        - In other words: I am WFXYZ at given time, but I may or may not be in a position that should grant me access to a credential in near future
        - PIM is a part of PAM
    - Dave Mak (Berklee): one challenge we have is that people wear multiple, different hats. Identified that advancement office is going into ERP and changing alum status for grads to make access experience easier; although they realized it was not sustainable, meant starting a convo with other constituents (registrar, IAM, enterprise data) to correct the situation, devote resources, etc. Problems can become successes (e.g., one person doing bulk processes manually asks for help -> coordinated success)
        - Kenny: how did that happen?
            - Dave: advancement seemed to go to senior leadership to say “we can’t do this, can you bring together folks to help us with this”
            - Did require leadership to form the project/structure to solve this problem

ARTIFACTS / LINKS


-MANAGING UP
-IAM GOVERNANCE
-ENTRA ID GOVERNANCE
SUCCESSES
-RJT- WHERE IS LEADERSHIP'S ATTENTION? HOW DOES IT CONNECT TO IAM?
-UC(SF/LA)- REACH OUT TO OTHERS ACROSS ORG. *SERVICE DESK*
-UVA- FORMALIZE THE CONNECTION
-MIZZOU- STRONG CISO ADVOCATING FOR IAM
-SMU- TAKE ADVANTAGE OF BREACH/TRAGEDY
-UVA- CONNECT W/ NEW CIO VIA LINKEDIN- ESTABLISH RELATIONSHIPS
-UIUC- ORG STRUCTURE → IDENTITY, PRIVACY, CYBERSEC + HIRING FOR SUCCESSION IN IAM
-W/ CORPORATE-BACKGROUND → GARTNER, ETC.
-TOOLS LIKE SKETCH FOR SHOWING WHAT YOU DO


Post-it
DA-LITE
CHALLENGES
- VENDORS SELLING FUNCTIONALITY THEY CAN'T DELIVER
- INTEGRATION TO IGA CAN BE SLOW
- BERKLEE - GROUPS GOING TO UPPER LEADERSHIP TO GET AROUND THINGS
Million identities at
UT Austin.
LDAP Retained
CUT OFF Time.
User Name
info
retid
employee id
but login
PI
DATA