Link to 2021 ACAMP Wiki

Advance CAMP Wed. Oct 6, 2021

Title Creating Identity Standards/IAM Program for Risk Mangt

Room - Arts + Crafts

CONVENER: Mike Mays/ Joanne Boomer

MAIN SCRIBE: Eric Goodman

ADDITIONAL CONTRIBUTORS: Tom Barton

# of ATTENDEES: 31

DISCUSSION:

- Looking at starting an IAM Program around Risk Management and is looking for insight/examples etc that might be helpful.
- Deloitte did a review of IAM at UD. Lots of findings. Kicking off an IAM program, and at the end wants to have a document that addresses how risks and findings from the Audit.

Starting point:
https://docs.google.com/spreadsheets/d/14YHoQfE2ZkwWiz6zCIlgG6wQnS2P-xDmhUk4UnP985I/edit

SS linked above has questions calling out what the “rollup” decision points are, largely at a high level. Looks like for sharing the governance detail, but potentially with non-technical or non-IAM folks.

Michael H: One thing to be aware of is that just defining terms like “student” is potentially more complex than you might expect.

Tom Barton: Another consideration is that what your IAM program is accomplishing will constantly change. The questions asked in the SS are the right kinds of questions, but expect that the requirements, answers, implementations will be frequently changing. Also consider how IAM will help answer the audit and findings questions of OTHER systems; e.g., the security of

the authentication system will play into audit findings for the downstream services. Plug for Grouper - or any centralized access management/tracking system.

Related UChicago policies & procedures:
https://its.uchicago.edu/cnet-closure-process-faculty-and-other-academic-appointees/
https://its.uchicago.edu/cnetid-account-management-practices/
https://its.uchicago.edu/it-services-account-closure-procedures/
https://its.uchicago.edu/procedures-manage-user-permissions-university-email/
https://its.uchicago.edu/procedure-personal-email-deceased/
https://its.uchicago.edu/it-services-authentication-services-terms-use
https://its.uchicago.edu/it-services-trusted-agent-tag-terms-use

U Hawaii's doc for developers regarding high level roles and role transitions,
https://www.hawaii.edu/bwiki/display/UHIAM/UH+Role+Assignments+and+Transitions

Eric: Part of the "art" of this is how much access detail to track in central systems vs. within the applications because of the extra work required to duplicate the

Mona: With some provisioning happening in each COManage, Grouper, MidPoint, vendor products, it can be difficult to provide a centralized view. Can feel a little spaghetti-y if there are administrative decisions being made in too many different places.

Slavek: (quoting Tom) This works, as long as in the end you get all of the information into a single place.

How?

Eric: You can treat the "master copy" as a provisioning target of all of the other systems. But sounds like part of the concern is not just seeing the info in a consolidated view, but also understanding where someone needs to go to change or update data.

Mona: Dream is some form of MDM with the complete view of the individual where you can pull all of the relevant info. But there are limitations in each existing product (in terms of their ability to model how we want the data to look).

Tom: Biased towards Grouper because it provides a lot of flexibility.

Eric: No MDM solution is ever really going to be able to answer all of the access questions, at best they will inform them. So one of the kinds of flexibility Grouper (and other) systems can offer is to provide user information (like "current employee", etc.) but also let the downstream system owner control their own rules on top of that. E.g., use information about employment to drive access decisions/reviews, but to let the downstream system owner define those rules.

Joanne: Looking back at Michael's SS (top of scribing doc), some are policies and some are processes. Where is that line drawn?

Michael M: Hard to draw a hard line because understanding some of the policies or their implications may require looking at some of the details of the processes.

Joanne: the processes may be more likely to change over time. They do maintain documents of the processes, but they look to keep that kind of detail separate from policy (though it's still not always clear what goes in which category).

What is the goal/what are examples of an overall IAM strategy document?

(There were a couple of answers but not necessarily with answers that were directly helpful). Most didn't create IAM programs in response to Audit findings, which might be part of why.

<Copies of Erica's super secret rules document to be posted here later once declassified />

What about the more specific policies around things like Michael called out in his session proposal; password policies, definition of "active employee". Talked about calling out that the rules are in many ways more important than the tool selected.

David L: Calls out that the documents Tom linked are practices, not "capital P" Policies. Some discussion about the difference between formal policies vs. implementations/processes/practices.

Michael H: Did define a very formal Student classification that explains precisely how students are identified, status changed, etc. *Do you maintain multiple Grouper reference groups?* Different groups for different slices ("students at campus x", "students in this major"). *Do you have different definitions of students, tho? E.g., "students as of Xth week census"?* Going to have to answer "yes" to that.
UH's doc on this
https://www.hawaii.edu/bwiki/display/UHIAM/UH+Role+Assignments+and+Transitions

In one case the person is looking for an "overall program document" because there were separate documents for policy, process, etc. but audit findings called out explicitly defining a program doc.