



2023 INTERNET2
TECHNOLOGY
exchange

IAM Archaeology

Christopher Bongaarts, IAM Architect – University of Minnesota

Kellen Murphy, Identity Architecture and Solutions Engineer – University of Virginia

September 19, 2023



**DIGGING UP LESSONS
FROM OUR LATEST
ATTEMPT AT LEGACY
SYSTEM ABATEMENT AT
THE UNIVERSITY OF
MINNESOTA**

Disclaimer

- Advice, conclusions, representations are my own and should not be construed as “official” positions of our IAM team or the University of Minnesota
 - One of the benefits of having a larger team is a diversity of views on how IAM should work
 - Both from philosophical as well as role viewpoints
 - BA – why, developer – how, project manager – when/who

About the University of Minnesota

- Large public R1 institution
- ~68K students, 27K faculty/staff
- ~4.2M identities in IAM system
- IAM team ~30 full time staff

The history lesson

- Once upon a time (1992 or so), we built an IAM system
 - Central (academic) Computing needed staff and student data for first campus-wide email service
 - Anticipated similar data need for new ID card project
 - Got data from mainframe-based student and HR systems (later, Alumni Assoc.)
 - Provisioned to central email (UNIX) and enterprise directory (X.500, later LDAP)
 - Later, provisioned Active Directory “people” tree
 - This system was internally referred to as “The Database” or “Kevin’s Stuff” (later as “X.500”)
 - **LESSON: It’s better to actually create something that works and build off it than to try to design the One True System right from the beginning.**

History lesson continued

- Around 2007, reorg splits team of 8 leaving just 2 “identity” team members
- Management shift away from custom-built software
 - Still OK with open source as long as we don’t have to write it
 - Deployed Shibboleth IdP (replaced locally written SSO), Grouper
- Purchased Oracle Identity Manager in 2009, but postponed implementation due to Enterprise Systems Upgrade Project (Peoplesoft split)
- Eventually implemented OIM 2016-present
 - Data sources: PS CS (students) and HR (fac/staff), Foundation/Alum Assoc
 - Provisioning targets: LDAP, AD, Foundation, PS, Duo
- Team grows, split off into independent directorate
- Original IAM system author retired in 2018
- Soon (spring 2024?): Okta to replace OIM (and probably other stuff)

Know thyself

- Know **WHY** you do what you do.
 - You can always figure out WHAT a system does and HOW based on the code, but it doesn't tell you **WHY** it does what it does, **who** asked for it, or who is currently **depending on it** to work that way.
 - Comments in code/commit messages can be good for this
- **Requirements drift** over time
 - Periodically **review** them to ensure you're delivering the right services in the best way
 - Need to keep contacts current at a minimum

Know thyself

- Understand the **business value** of your stuff.
 - A system that is “good enough” but not ideal may be worth keeping around
 - This is the flip-side of agile's “minimum viable product” – maximizing delivered value
 - One simple standalone system that does one or a few things very well or is well adapted to business needs, and is easily understood by a newcomer because it is small/simple/self-contained - do you really want to trade this for a One-Sprint Wonder in that big app suite that no one understands?

Know thy customers

- **IAM is not an end in itself**, but a means to securely enable applications
 - Meet applications halfway - support the protocols they support (but indicate your preferences)
- **Build relationships** with both the business *and* technical people who manage the systems you need to interact with
- **Learn how the other side works**, at least a little bit
 - Helps build compassion for the app owners
 - Makes you less likely to accidentally break them
- **Don't ignore the little guys**
 - Enterprise apps affect a lot of people in your institution, but smaller apps (think LIGO) may have a bigger impact on humanity as a whole
 - You can't always predict which will be which

Know thy customers

- Untangling decades-old IAM solutions requires **effort**
 - Original requester is often no longer around (retired, promoted, demoted, won the lottery, etc.)
 - Current business owners may have no idea how access was originally structured
 - Current technical administrators may not know current requirements
 - This will likely impact your schedule – this **takes a lot of time** to work through
 - Don't underestimate the ignorance of your customers
 - If you need to push, be sure you have cover from higher-ups (CIO or CISO)
 - Security can be a stick (wish I had more carrots though)

Know thy customers

- Pay attention to **new business processes or teams** that are now central players
 - Integrations and Data Management teams became very central to our work
 - Built processes fundamental to our retirement projects that were not necessarily on our radar at the start
 - Respect, collaboration, making room for other stakeholders is vital to getting the work done

Know thy customer

- **Helpdesk is a customer** of yours if they need to use identity tooling to support users (password resets!)
 - **Listen** to them!
 - **Lurk** on their chat channels
 - **Meet** with their management regularly
 - Understand their pain points and **prioritize making life better for them**
 - Making them happy will pay off when you want to “shift left”

Know thy data

- Centralize data governance
 - IAM does not own most of its data*
 - Ensure it's easy for apps to get data owner approval to make use of IAM data
- Simple **provenance is not enough** to understand your data
 - Also need to understand the **selection** and **transformation** of data
 - Both on the way **in** AND the way **out**
- IAM **may need more data** than the source systems keep around
 - Example: ESUP did not convert older staff data
 - No way to identify “campus” for retirees for determining library privileges

Know thy data

- **Build relationships** with the data owners and experts
- Helps understand what their data means and how it fits into the Big Picture
- Facilitates getting help when the data gets weird
- Also helpful for getting buy-in for **moving logic out of IAM** and into source systems

Know thy peers

- Talk to other institutions at Internet2 TechEx and other meetings/fora
 - Be amazed at how far ahead *and* behind you are simultaneously
 - Great source of ideas for improving IAM services
 - Recycle, reuse, reinvent (mostly the first two)
 - Anticipate challenges that aren't at your campus yet, but may be soon
 - Higher Ed often faces common challenges – lots of approaches to solutions

Architect for resiliency

- Create/implement well-defined **interfaces** for interactions
 - Then swap out parts of your architecture as needed
 - Helps with disaster recovery - what happens if various parts of your IAM setup were to be vaporized by an asteroid, or encrypted by Bad People?
- **Testing** can be tricky
 - Old X.500 could generate LDAP directory at will
 - Easy to validate changes to LDAP generation code - run with old, run with new, diff
 - OIM can't do that – much harder to check (and hard to make changes effective across population)
 - **Cross-product of test** instances across systems (sorry, can't help here)

Architect for resiliency

- Let other people do the work when possible
 - Move **logic into source systems** where appropriate
 - Build/leverage **self-service** systems
 - Be transparent/share documentation widely; the more people know about how the system works, the more effectively they can use it and understand how to resolve problems
- Higher Ed IAM has high-touch/high-volume change events multiple times a year
 - Semester start/end, professional/admin staff annual contract renewal
 - Easy to accidentally build a system that takes way too long to converge after those events

Architect for resiliency

- Try to be **state-driven** rather than exclusively event-driven (credit Mary McKee)
 - OIM strategy – get updates from PS IB (events), but ignores contents - pulls data in fresh
 - Avoids event ordering requirements
 - Easy reconciliation of sources if updates missed
- Know how the parts of your system **impact uptime**
 - SSO probably needs 7x24x365.25
 - Password changes can probably tolerate longer downtime
 - Batch processing can probably tolerate even more (if done right)
 - Minimize dependencies between systems to optimize this

Keep it clean, but not *too* clean

- Periodically (or continuously – automate it!) **tidy up**
 - If no one is using X any more, get rid of it
 - Less stuff to deal with at the next migration
- **Avoid short-sighted shortcuts** when migrating IAM systems
 - Example: not importing all accounts from legacy system to new system
 - Still dealing with the fallout from that choice 7 years later...
- Good **logging** is essential
 - Good log analysis tools/SIEMs are a big win
 - Storage is cheap these days -- keep copies of transaction data, batch feed files, etc. for a reasonable time (automate deletion)
 - Facilitates debugging
 - Fix-by-replay possible

The moral of the story

- Know why you do what you do, and who you're doing it for, and keep in touch with them.



REPLACING A LEGACY GROUP MANAGEMENT TOOL

**Lessons Learned from
Deploying Grouper at The
University of Virginia**



27
VARSITY ATHLETIC TEAMS
13 MEN'S & 14 WOMEN'S

#1

Best Value Public
College For
Financial Aid,
Princeton Review,
2022

17k

Total Faculty and
Staff

3k

Full-Time Faculty

6.5k

Full-Time Staff

\$14,878

2022-23 1st Year
Students, In-State,
College of Arts &
Sciences

#3

Best Public
National
University, U.S.
News & World
Report, 2023

17k

Undergraduate
Students (On
Grounds)

8.7k

Graduate &
Professional
Students (On
Grounds)

#1

Hospital in Virginia,
Newsweek, 2022

#1

Best Public Law School, U.S.
News & World Report, 2023

#1

EDUCATION EXPERIENCE,
DARDEN SCHOOL OF BUSINESS
THE ECONOMIST



Identity & Access Management at UVA



Operations & Product Team



Technical & Architecture Team



@ TechEx

- What do we do?
 - Manage approximately 1.25M identities using Fischer Identity for IGA
 - Password Management
 - Role Management
 - Policy Management
 - Policy Enforcement
 - Duo Management
- What do we *not* do?
 - “Infrastructure”
 - Active Directory / Azure AD
 - LDAP
 - Email List Management
 - Authentication
 - Shibboleth SSO **
 - *Group Management* *
 - Email Alias Management *
 - Non-person Identities **
 - Social Identities **

So how did this all start?

- Project was conceived (draft) in 2020. Plan was to find something that would allow for “secure groups” (primary use: VPN access).
 - Tighter controls, etc. would be needed for these vs. MyGroups.
- COVID hit and everything basically stagnated for *years*.
 - Hybrid learning shifts lead to realizations of many use-cases for Groups for which MyGroups was not suited.
- Project “resumed” in May 2022.

Current Group Solution

- UVA MyGroups
 - Originally launched ca. 2006
 - Developed internally.
 - Maintained / managed by Enterprise Infrastructure team.
 - Group memberships go only to Active Directory & LDAP
- “Facelift” in mid-2022 to current user interface.
 - Positively received, didn’t deliver the “upgrade” that people wanted.
 - People still getting used to the “new” UI.
 - Cleaned up the codebase but quickly realized we would have too much work to deliver the product that people really wanted.

The screenshot shows the 'MyGroups Management' interface for the University of Virginia. At the top, there are navigation links for 'CREATE GROUP', 'MANAGE GROUPS', and 'LOG OUT'. The main heading is 'MANAGE GROUPS'. Below this is a search filter for '(21 groups)' with a 'Clear' button. The main content is a table listing various groups and their associated roles.

Name *	Roles %
eatcam	Member
iam_core	Member
iam_etc	Member
iam-automation	Admin, Member, Moderator
iam-dev-admins	Admin, Member
iam-harbor-developer	Admin
iam-harbor-maintainer	Admin
iam-harbor-projadmin	Admin, Member
iam-refactor-test	Admin, Member
identity	Member
its-all-access	Member
isp_program	Member
in_its-12-helpdeskusers	Member
splunkcloudiamusers	Member
stacs_iam_dingo_group	Member
stacs-jira-iam-agents	Admin, Member
stacs-jira-iam-padmins	Member
stacs-jira-itsm	Member

Grouper Project Goals – Top 10 List



Grouper Does Everything

- Automation ✓
- Attestation ✓
- Folder structure ✓
- Metadata ✓
- API ✓
- Auditing ✓
- Containerized ✓
- Permissions ✓
- Nice UI ✓
- Pluggable Architecture? ✓

+ Request new group

Quick links

- My groups
- My folders
- My favorites
- My services
- My activity
- Miscellaneous

Browse folders

- UVA
 - Applications
 - Basis Groups
 - Grouper Configuration
 - Intake
 - MyGroups Attestation
 - Organizational Groups
 - Personal Groups
 - Reference Groups
 - Testing

Home

Grouper

University of Virginia

This website allows you to manage groups associated with your organization and the members of those groups. For a list of answers to frequently asked questions, refer to the [support documentation](#).

Recent activity

Recent activity	Activity Date
Added Cox, Brennan (bncB) as a member of the ad-hoc additions (app) group.	2023/07/17 3:41 PM
Added group foo (app).	2023/07/03 11:22 AM
Added attribute value to attribute attestation/CalculatedDaysLeft.	2023/05/26 1:39 PM
Added attribute attestation/CalculatedDaysLeft to an attribute assignment.	2023/05/26 1:39 PM
Added attestation on group AT_stacs-jra-iam-agents.	2023/05/26 1:39 PM
Added attribute value to attribute attestation/HasAttestation.	2023/05/26 1:39 PM

My memberships

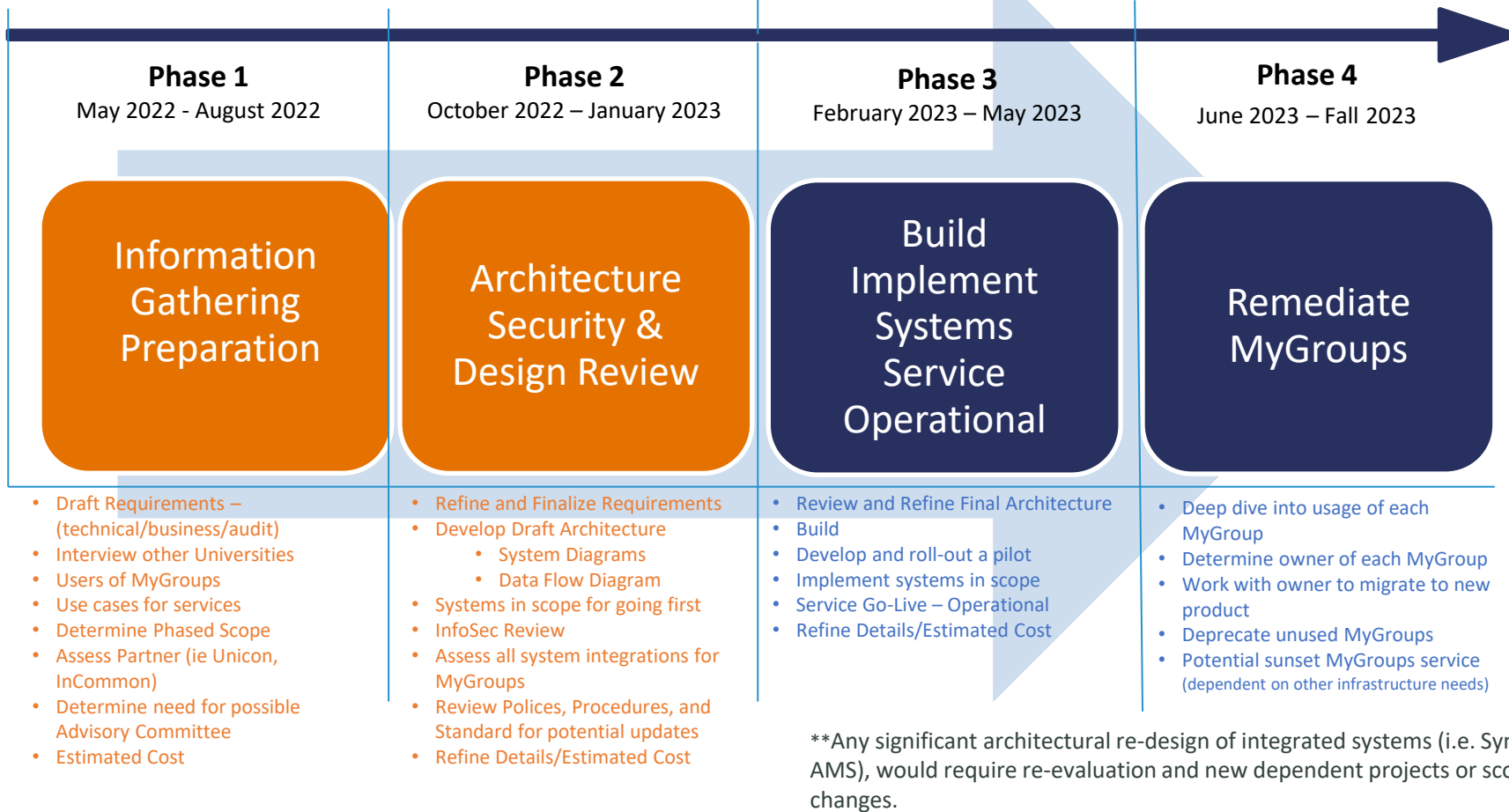
- authorized
Applications : ITS : IAM : Grouper (app)
- eligible
Applications : ITS : IAM : Grouper : rules (app)
- staff
Basis Group (basis)
- grouper/ldUserData
Grouper Configuration : grouper-ui (etc)
- sysadminsgroup
Grouper Configuration (etc)
- uivPrivilegedViewers
Grouper Configuration : uiv/ViewContg (etc)
- AT_stacs-jra-iam-agents
MyGroups Attestation

Groups I manage

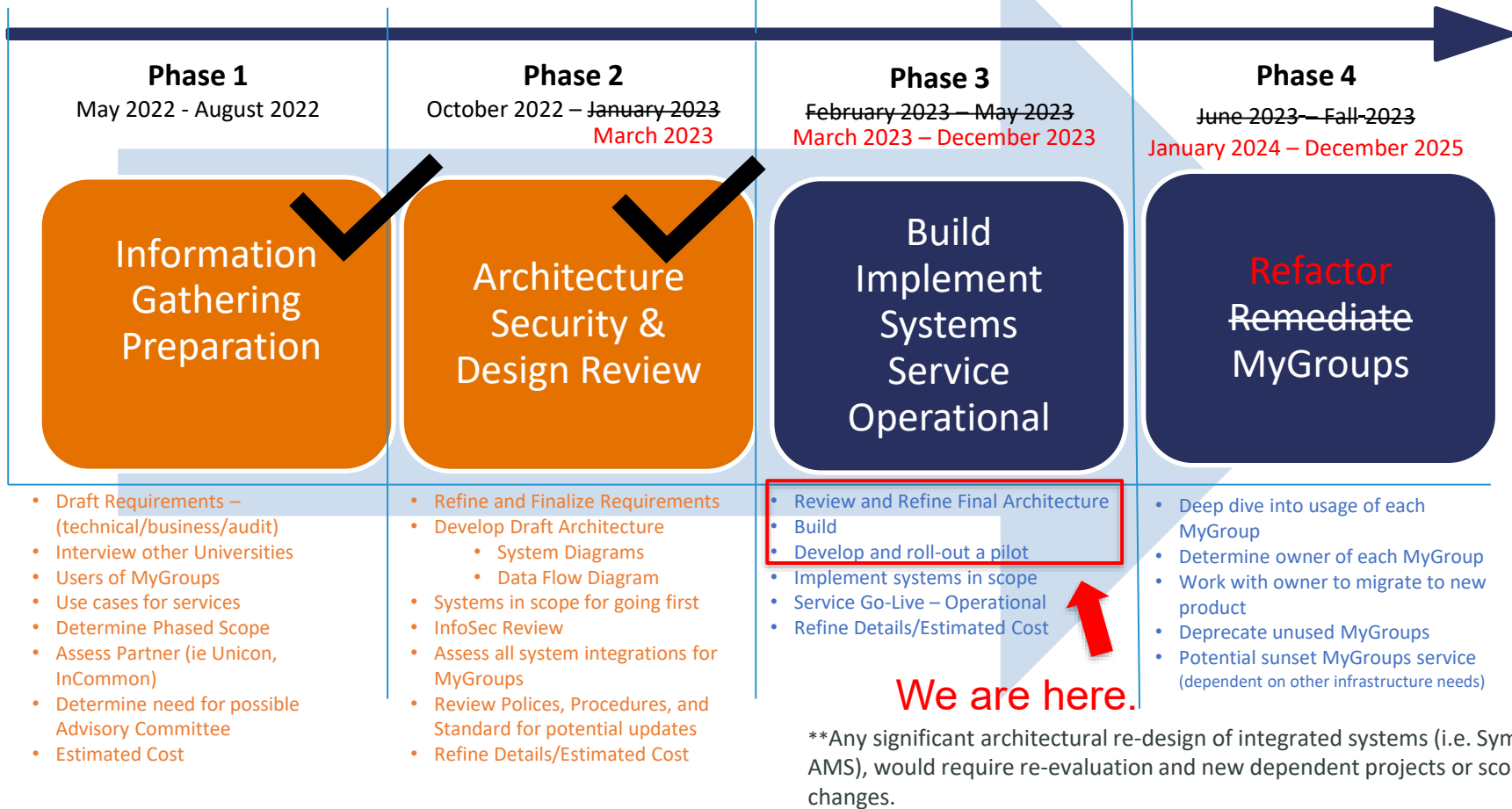
- foo
Applications (app)
- authorized
Applications : ITS : IAM : Grouper (app)
- ad-hoc additions
Applications : ITS : IAM : Grouper : rules additions (app)
- eligible
Applications : ITS : IAM : Grouper : rules (app)
- ad-hoc removals
Applications : ITS : IAM : Grouper : rules : removals (app)
- all removals
Applications : ITS : IAM : Grouper : rules : removals (app)

Recently used

- ad-hoc additions
Applications : ITS : IAM : Grouper : rules : additions (app)
- foo
Applications (app)
- AT_stacs-jra-iam-agents
MyGroups Attestation
- stacs-jra-iam-agents
MyGroups Attestation
- Chris Group
Personal Groups
- MyGroups Attestation
UVA
- ops_testing_template_demo
Testing (test)
- OTMAY111016



**Any significant architectural re-design of integrated systems (i.e. Sympa or AMS), would require re-evaluation and new dependent projects or scope changes.



We are here.

**Any significant architectural re-design of integrated systems (i.e. Sympa or AMS), would require re-evaluation and new dependent projects or scope changes.

Things that should've happened during Phase 1 and didn't.

- We should have paid much closer attention to gathering SMART requirements.
 - Specific: there should be no ambiguity, and it should be clear to all stakeholders.
 - Measurable: it's possible to define a “success” criteria.
 - Attainable: can the requirement actually be achieved during the course of the project?
 - Realistic: are the requirements coherent in the context of the project?
 - Traceable: Can be tracked easily with clear dependencies.

Things that happened during Phase 1 and shouldn't have.

- We engaged with contractor(s) way too early.
 - Brought in outside contractor to gather information about existing MyGroups.
 - How are these groups used?
 - How can they be automated?
 - Who needs help with integrations?

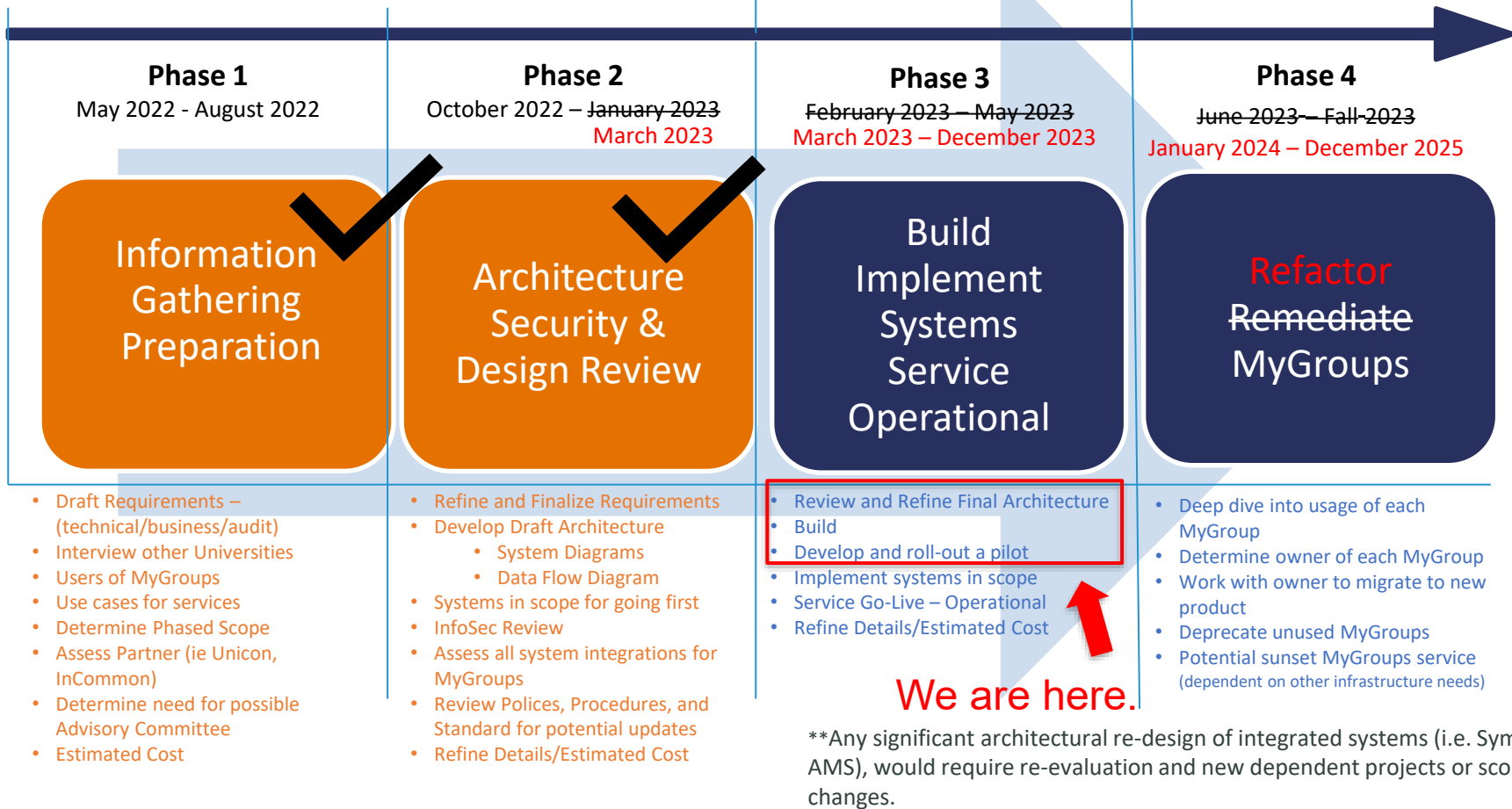
} Problem

The questions that we wanted answered were vague, but more importantly, we weren't prepared for WHY we wanted this information?

Why hire someone to “gather” info if you don't have a plan for how to use the data?!

Takeaways:

- Focus early on requirements. They drive the project.
- Requirements aren't JUST for this project...
 - Don't underestimate the impact on other teams and their priorities.
 - This is really just communication.
- Clarity and conciseness is key.
 - If you have to spend hours arguing about / interpreting a requirement... it's not a good requirement.



We are here.

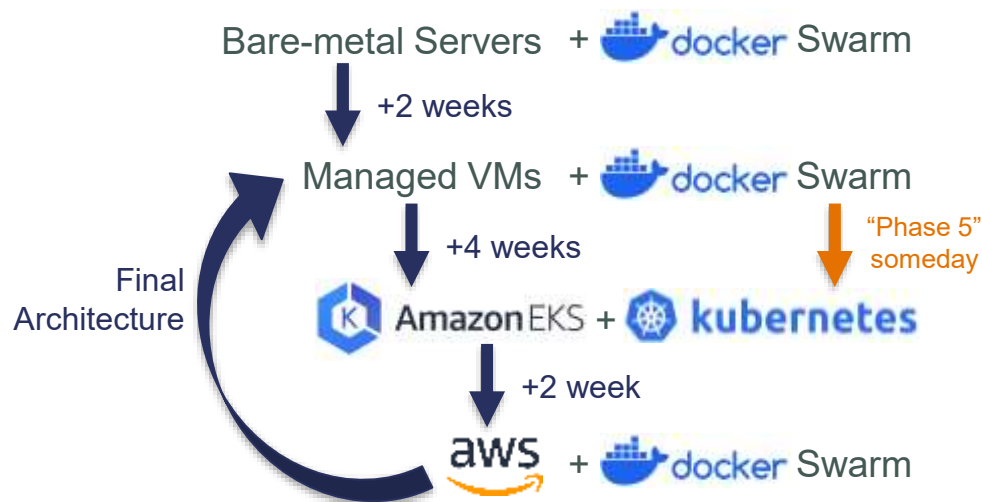
**Any significant architectural re-design of integrated systems (i.e. Sympa or AMS), would require re-evaluation and new dependent projects or scope changes.

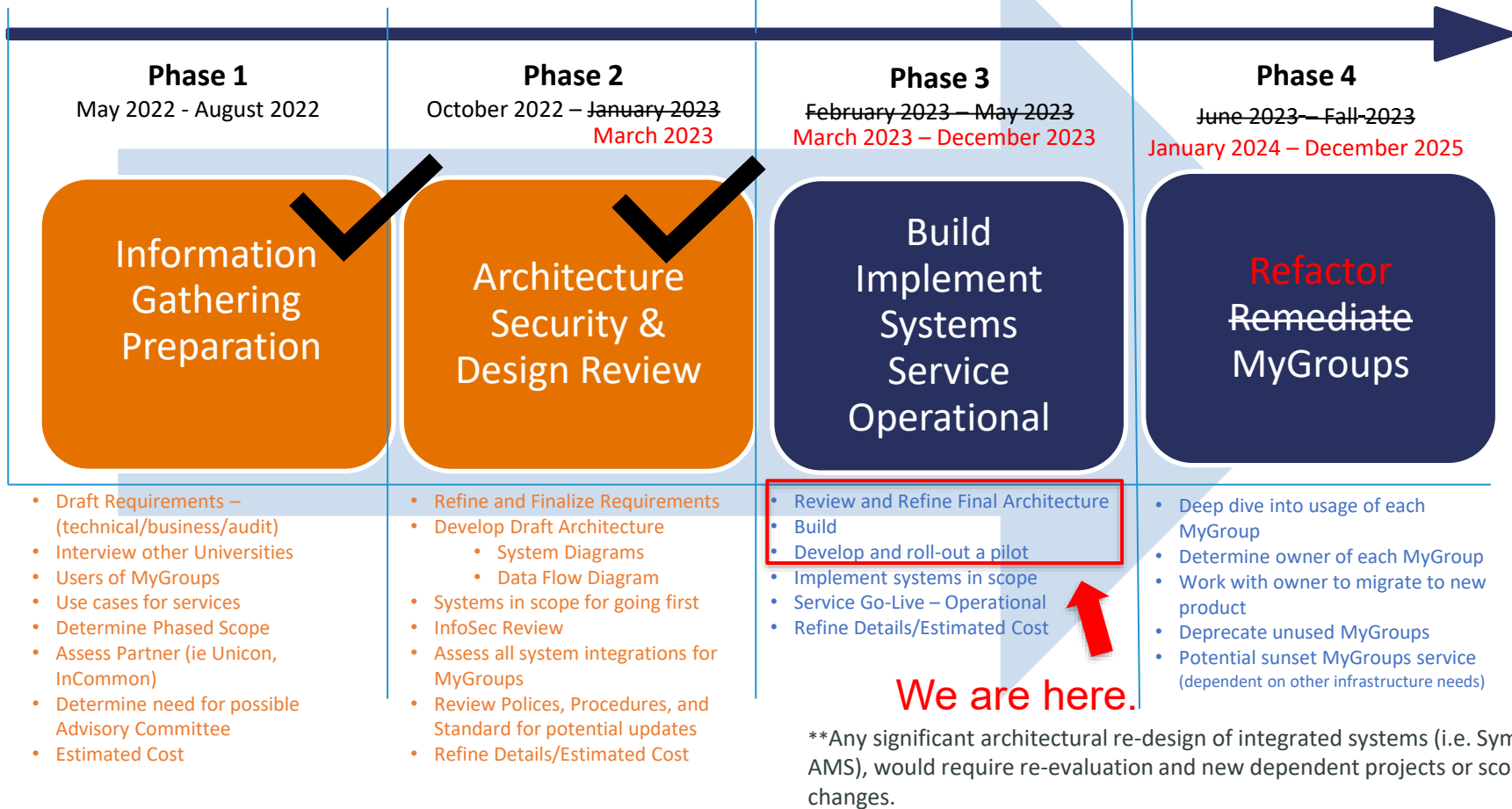
Phase 2 – Architecture

Major architectural changes occurred several times because of the requests / demands from other teams.

Takeaway:

We could have worked more closely and communicated better with our partners on other teams to validate some of our earliest architectural decisions (like bare metal) and probably landed on the ultimate solution much, much faster.





Phase #3 – If you build it, they will come.

But don't have a major cybersecurity incident. Just my suggestion. 🤖



Our team was responsible for facilitating reset of ~80k creds, scrambling another ~200k, ensuring remaining ~1M accounts couldn't reactivate with compromised credentials.

- our time was lost
- hard to work with others
- change freezes
- still feeling an impact

Phase 3: Build Phase Problems

- Nearly universally what slows us down *now* is stuff we “forgot” in some way.
- Problems we should have architected around much, much sooner:
 - Sympa Decoupling
 - Grouper Authentication
 - Refactoring MyGroups groups into Grouper Groups
- Delays were completely reasonable, but the reasoning behind these delays weren't always communicated to leadership clearly.

Final Thoughts

- Retiring a legacy system means addressing years (or decades) of technical and organizational debt.
- Communication – did you notice how it was always underlined? That’s because every issue we ever faced could be traced back to poor communication somewhere within our project team.
- Also... innovation comes with challenges:
 - First major IAM application running in a containerized fashion.
 - Fully implementing a CI/CD workflow for deployments.
 - No dev environment – each developer has an entire dev environment on their workstation with Vagrant VM; deploy to dev VM using same scripts as higher environments.



QUESTIONS - DISCUSSION

Contact:

Christopher Bongaarts – cab@umn.edu

Kellen Murphy - wfx6yz@virginia.edu

Thanks for listening!

Drive the Bus!

Leadership and Advisory Groups

Leadership opportunities for
community members who contribute
their insights, expertise, and talents
within Identity & Access Management

Taking nominations now through
October 1!

InCommon Steering Committee

InCommon Technical Advisory Committee (TAC)

InCommon Community Trust and Assurance Board (CTAB)

Community Architecture Committee for Trust and Identity (CACTI)

eduroam-US Advisory Committee

Please visit the Advisory Committee poster in TechEX foyer for more information and submit a nomination. Otherwise, you may click this [link](#) to submit a nomination.