



# Accelerating Secure Medical Research in the Cloud

Jamie Lam, Data Security Compliance Manager  
Pavan Gupta, Cloud Architect  
Victor Vargas Reyes, Software Engineering Manager

# Agenda

1. Background and Compliance Approach
2. Architecture, Tools
3. Operations
4. Looking Ahead

## Who is UCSF SOM Tech?



**We are technology advocates.** Our broad technology expertise, deep knowledge of the UCSF ecosystem, and human-centered approach help you take innovative digital projects further, faster.



# Background and Compliance Approach

# How did this all start?

## Demand

- Rising demand for cloud computing **with PHI** (multiple inquiries / month and increasing)

## Cost

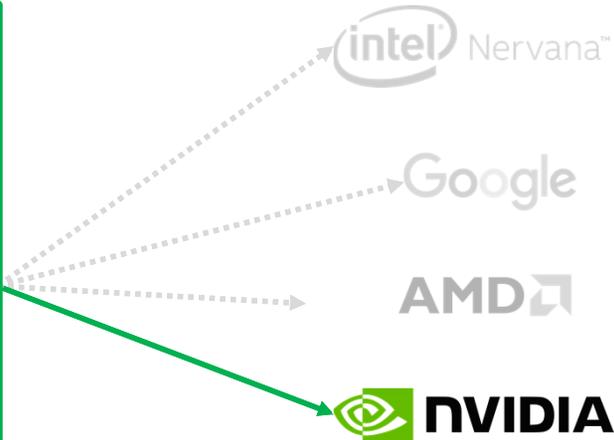
- >\$500k spend at UCSF / year on AWS

## Security

- No visibility into existing accounts
- No controls vetting researchers using cloud infrastructure

# Governance Accelerated Path Forward

Enterprise Hybrid Cloud	Departmentally Managed Public Cloud
<p>Hybrid cloud hosting is a model that allows UCSF to provision dedicated servers and storage and shared cloud servers and storage <u>on the same network</u>. UCSF IT will offer a cloud service catalog.</p>	<p>In <b>public clouds</b>, cloud resources are owned and operated by a third-party cloud service provider and <b>delivered over the Internet</b>. Departments are responsible for managing their own public clouds.</p>
<ul style="list-style-type: none"> <li>Business requirement to connect to UCSF network / systems, and/or</li> <li>Department wants to leverage enterprise security tools that will be integrated to the enterprise hybrid cloud infrastructure</li> </ul>	<ul style="list-style-type: none"> <li><b>No business requirement to have persistent connectivity to UCSF network / systems</b>, and Department has resources and expertise to configure and operationally manage a secure public cloud infrastructure</li> </ul>
<ul style="list-style-type: none"> <li>Identify and commit to timeline, resource need, and tools (such as DirectConnect) required</li> <li>Funding for resources and tools</li> <li>Define service lines available</li> <li>Define roles and responsibilities for UCSF IT vs. Department IT under this model</li> <li>Other requirements may be defined as we learn</li> </ul>	<ul style="list-style-type: none"> <li>Department must document architecture design and correlate how cloud tools and configurations are used to meet HIPAA/CSA security controls</li> <li>Department must draft IT Security Plan with policies and procedures to operationally manage the public cloud</li> <li>Other requirements may be defined as we learn</li> </ul>
<p>UCSF can better leverage existing enterprise security tools and will have more visibility into our cloud infrastructure. Enterprise cloud service line allows departments and PIs without cloud security expertise to consume cloud services securely.</p>	<p>Can get started now and provides department an option to roll their own. Multiple deployments of public clouds will result in inefficiency and added resource requirements with each department deploying their own SIEM/ host based detection/ VPN services, etc.</p>



## Cloud Computing Provides:

- **Hardware Access**
- **Hardware Optionality**
- **Compute Flexibility**

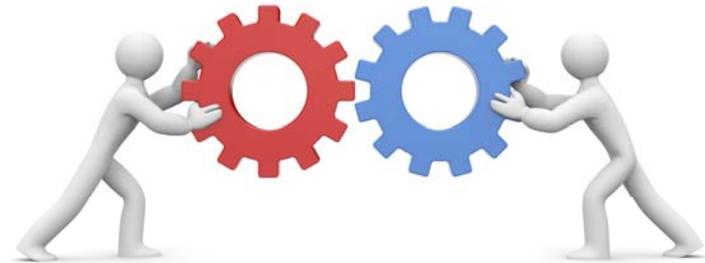
# Compelling Research Use Cases

## Four Early Use Cases:

1. Linux Research Computing (FAST and Pregnancy Ultrasound Research)
2. Containerized Computing (UCSB's BisQue Platform, HPC Analog)
3. De-identified clinical data warehouse (Information Commons)
4. Specialized Clinical Applications (CDHI's Fax-2-Referral)

# Initial Team

- SOM Tech Data Security Compliance Manager
- SOM Tech Project Manager
- CDHI AWS Architect
- ClearScale Architect
- ClearScale DevOps Engineers
- UCSF Enterprise:
  - IT Security
  - Privacy



# Compliance

- **Cloud Security Alliance Cloud Controls Matrix**
  - ~130 cloud specific security controls mapped to industry security standards / regulations such as ISO 27001/27002, NIST, and HIPAA
  - Mapped each control to an operational procedure
  - Incorporated as technical design requirements
- **UCOP IS-3 Electronic Information Security**
  - Drafted IT Security Plan for environment
- **UCSF Policy 650-16 (Minimum Security Standards)**
  - Standards pushed into technical design
- **UCOP-AWS Business Associate Agreement (BAA)**

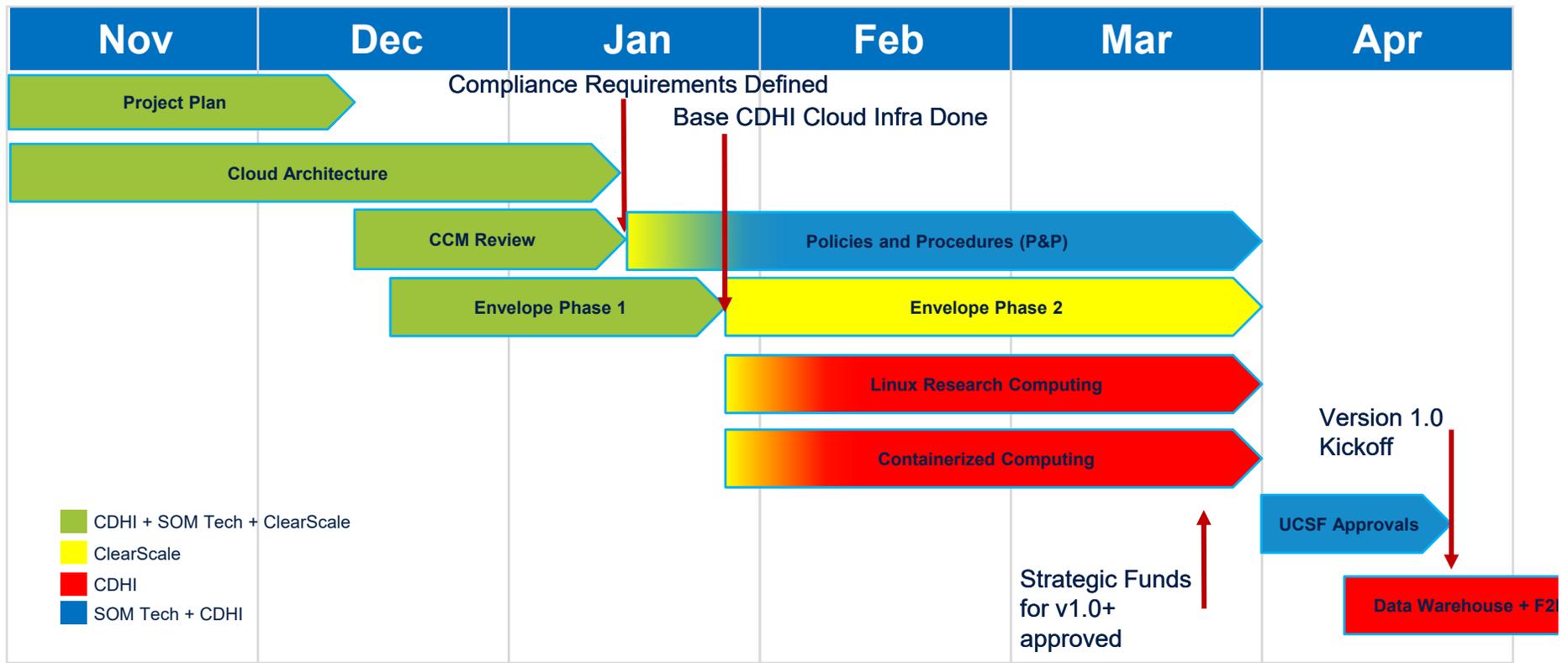


# Compliance Documentation

- IT Security Plan
- 12 procedures
  1. Risk Management
  2. Information Access Management
  3. Systems Inventory, Data Management & Retention
  4. Configuration Management
  5. Encryption & Key Management
  6. Vulnerability Scanning & Management
  7. Change Management
  8. Logging and Monitoring
  9. Business Continuity & Disaster Recovery
  10. Incident Response
  11. Security Awareness and Training
  12. Physical Security



# Sprinting Toward Actual Operations

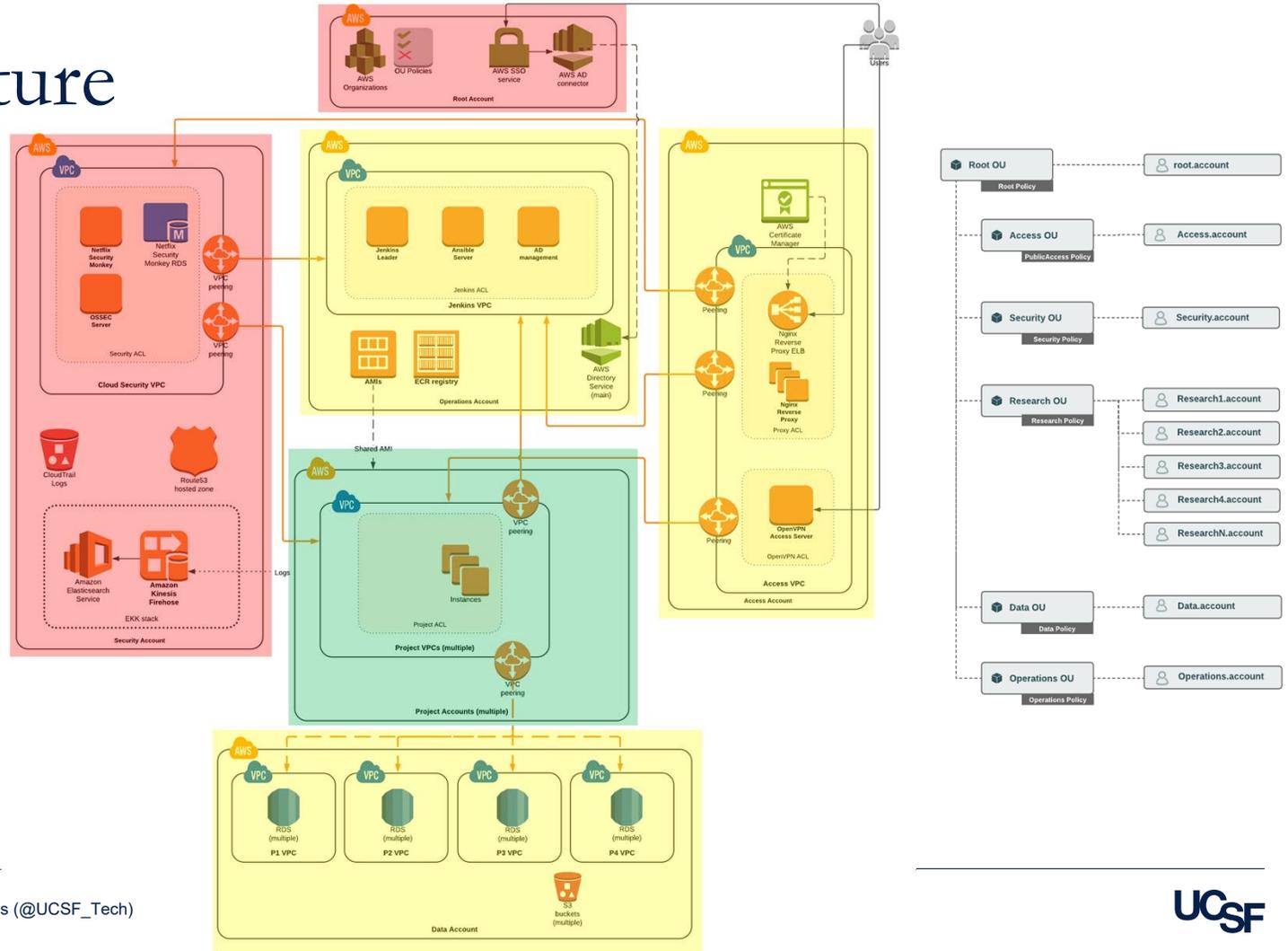




Architecture

# Architecture

- Security
- Operations
- Projects



# VPN and Web Connectivity

## Goal:

Single point of entry, RBAC, auditable and extremely secure, layers of additional web-related security

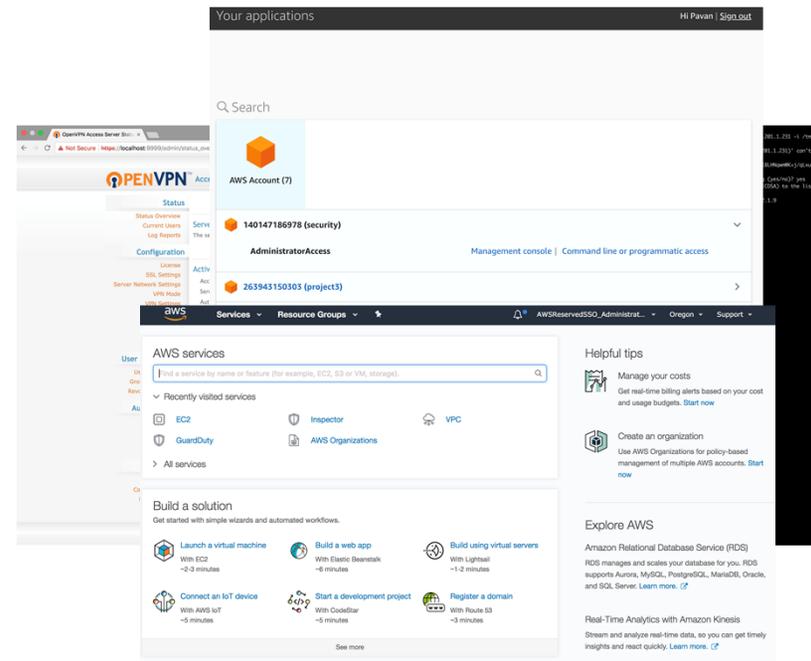
## Current Challenges:

OpenVPN is not the enterprise choice

Security (host posture checking, dlp) not used

Route53 used with cdhi.cloud right now

Ngix Reverse Proxy != MyAccess SSO



# Compliance/Security Tooling

## Goal:

Sophisticated tools to ensure auditability and active monitoring of cloud deployment

## Current Challenges:

Tools lack enterprise bells and whistles

Alerting is not effectively enabled

Better tools may exist within UCSF

Dome9 is still experimental within our platform

The screenshot displays three overlapping web dashboards. The top dashboard is Security Monkey, showing 'Accounts' and 'Current findings' for AWS. The middle dashboard is Dome9, showing a 'Compliance Engine' with three circular progress indicators for 'Project 3 Account' (97.14%), 'InfoCommons1' (91.43%), and 'Operations Account' (91.43%). The bottom dashboard is another Security Monkey view showing a list of 'Recent Runs (Last 10)' with columns for Date Run and Status.

Date Run	Status
-2018-04- Today at 4:30 AM (GMT-7)	Analysis complete
-2018-04- Last Friday at 4:18 PM (GMT-7)	Analysis complete
-2018-02- 02/12/2018 (GMT-7)	Analysis complete
-2018-02- 02/12/2018 (GMT-7)	Analysis complete
-2018-02- 02/12/2018 (GMT-7)	Canceled

# Data Management

## Goals:

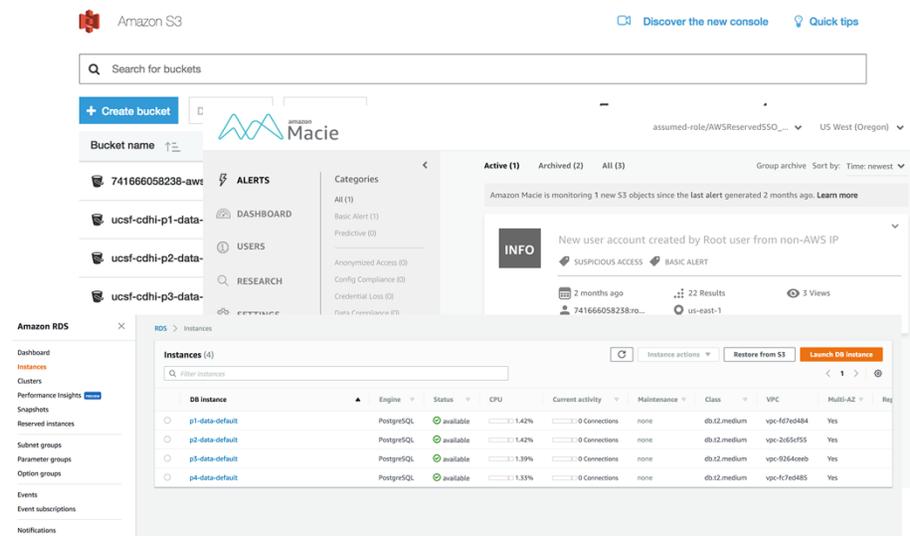
Extremely segmented, manual distribution of secure data

## Current Challenges:

Integration with enterprise data stores not used

Data availability not guaranteed

Vanilla data stores being used



# Account, User, & Billing Management

## Goal:

Centrally managed, centrally organized account and billing structure requiring minimal direct maintenance

## Current Challenges:

- IAM + Organizations Policies can be improved
- No multi-factor authentication available
- Another set of credentials required for users
- Manual validation of all active users required

The screenshot displays the AWS Organizations console. The top section is titled 'Bills' and includes an important notice: 'Important: Starting in May, linked account bills will reflect that account's unblended costs. Learn more'. Below this, there's a date selector set to 'April 2018' and buttons for 'Download CSV' and 'Print'. The 'Estimated Total' is shown as '\$9.62'. A 'Credits' section follows, with a note: 'Your invoiced total will be displayed once an invoice is issued.' Below this, there are tabs for 'Bill details by service' and 'Bill details by account'. The main area is titled 'Users' and shows a table of users. The table has columns for 'Email', 'Confirmed At', 'Login Count', 'Last Login At', 'Current Login At', 'Last Login IP', 'Current Login IP', 'Daily Email', 'Change Reports', 'Active', and 'Role'. One user is listed: 'pavan@cdhi.cloud' with a confirmed date of '2018-04-16 09:28:05.076', a login count of '5', and a last login of '2018-04-17 04:44:30.736'. The user is active and has the role 'Admin'. Below the table, there are navigation buttons: 'First', 'Previous', '1', 'Next', 'Last'. On the left side, there is a navigation tree showing the organizational structure: 'Root' -> 'Operations OU' -> 'Access OU' -> 'Data OU' -> 'Security OU' -> 'Project OU'. Under 'Security OU', there is a folder 'Active Directory Users and Groups' which contains 'ad' -> 'Computers' -> 'Users'. The right side of the console shows a list of users and their roles: 'Data Admin' (Security Group - Global), 'join domain' (User), 'LDAP Bind' (User), 'Operations Admin' (Security Group - Global), 'Pavan Gupta' (User), 'Project1 Admin' (Security Group - Global), 'Project2 Admin' (Security Group - Global), 'Project3 Admin' (Security Group - Global), 'Security Admin' (Security Group - Global), 'Tikhon Kolomytsin' (User), and 'Vitaliy Krasovskiy' (User).

# Operations/Change/Config Management

## Goals:

Centrally managed, integrated change and config management strategy

## Current Challenges:

ServiceNow integration not available

JIRA + Confluence not the best CM option

Only one baseline image available

Match enterprise configuration management tools

Terraform/Packer/Docker/Ansible are not simple

The image shows two overlapping screenshots. The top one is a Kanban board titled 'CDHI\_Kanban' with columns for 'To Do', 'In Progress', 'Ready for review', and 'Done'. It contains several task cards with IDs like UCSFCDHI-163, UCSFCDHI-165, UCSFCDHI-176, UCSFCDHI-190, UCSFCDHI-166, UCSFCDHI-172, and UCSFCDHI-323. The bottom screenshot is a GitHub repository page for 'UCSFCDHI / cdhi-infra'. It shows repository statistics (235 commits, 3 branches, 0 releases, 4 contributors) and a list of recent commits by users like pavgup, ansible, docker, packer, terraform, .gitignore, and readme.md.

# Real User Experience

```
1. pavan@ip-10-201-8-139: ~ (ssh)
→ ~ ssh pavan@10.201.8.139
pavan@10.201.8.139's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-1047-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Get cloud support with Ubuntu Advantage Cloud Guest:
http://www.ubuntu.com/business/services/cloud

11 packages can be updated.
0 updates are security updates.

*** System restart required ***
Last login: Fri Apr 27 18:49:05 2018 from 10.201.1.231
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

pavan@ip-10-201-8-139:~$
```

Your applications Hi Pavan | [Sign out](#)

---

Q Search

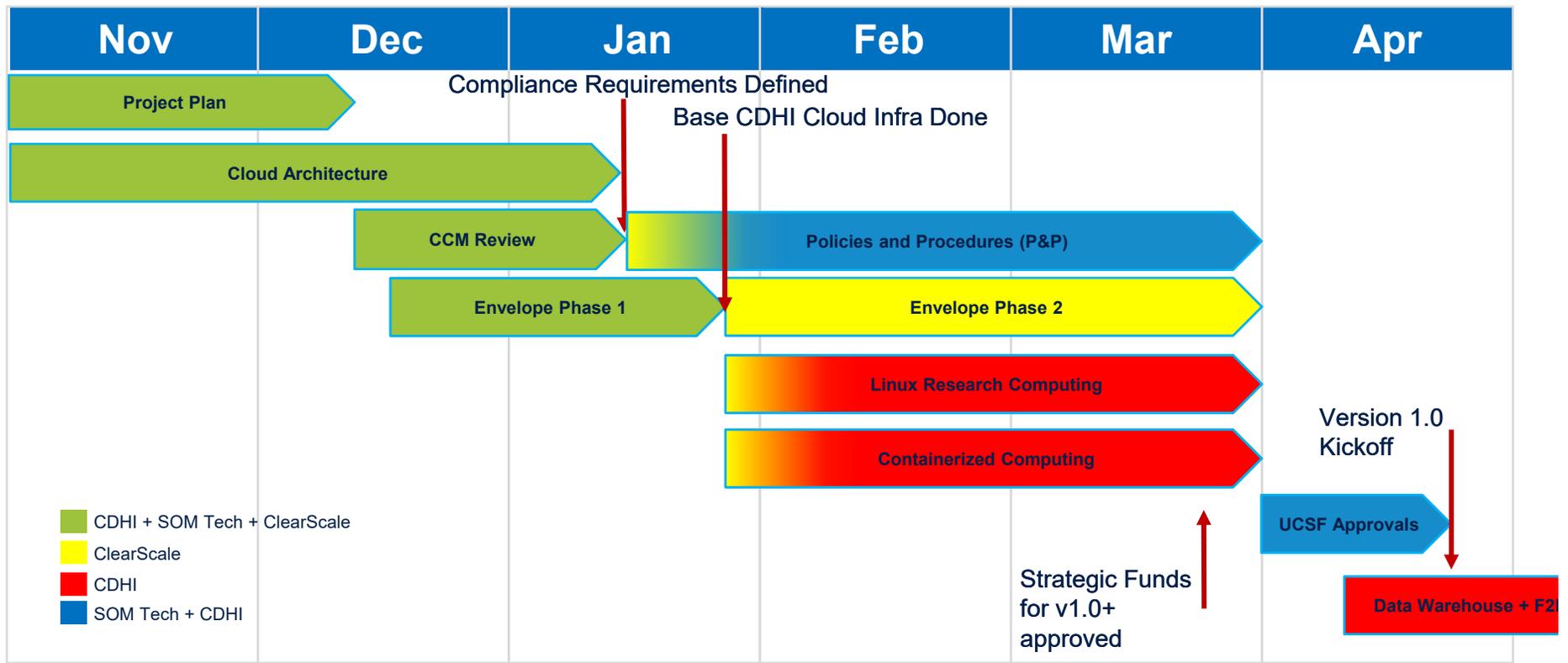


**AWS Account (7)**

 <b>140147186978 (security)</b>	▼
<b>AdministratorAccess</b>	<a href="#">Management console</a>   <a href="#">Command line or programmatic access</a>
 <b>263943150303 (project3)</b>	>
 <b>384144303322 (access)</b>	▼
<b>AdministratorAccess</b>	<a href="#">Management console</a>   <a href="#">Command line or programmatic access</a>
 <b>735810906445 (project1)</b>	▼
<b>AdministratorAccess</b>	<a href="#">Management console</a>   <a href="#">Command line or programmatic access</a>
 <b>741666058238 (data)</b>	▼
<b>AdministratorAccess</b>	<a href="#">Management console</a>   <a href="#">Command line or programmatic access</a>
 <b>755560526803 (project2)</b>	>
 <b>879064210775 (operations)</b>	▼
<b>AdministratorAccess</b>	<a href="#">Management console</a>   <a href="#">Command line or programmatic access</a>

Terms of Use Powered by 

# Sprinting Toward Actual Operations





# Operations

# Ops, Ops, Ops and More Ops



# Operations – Technology

- Terraform
- Packer
- Ansible
- GitHub
- Jenkins Pipelines
- ServiceNow
- Jira



 Jira Software



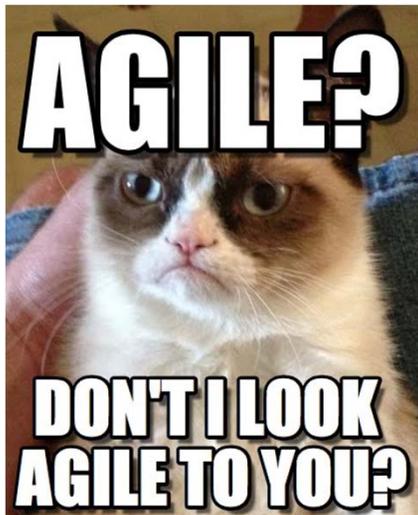
now™



# Operations – Procedures and Support

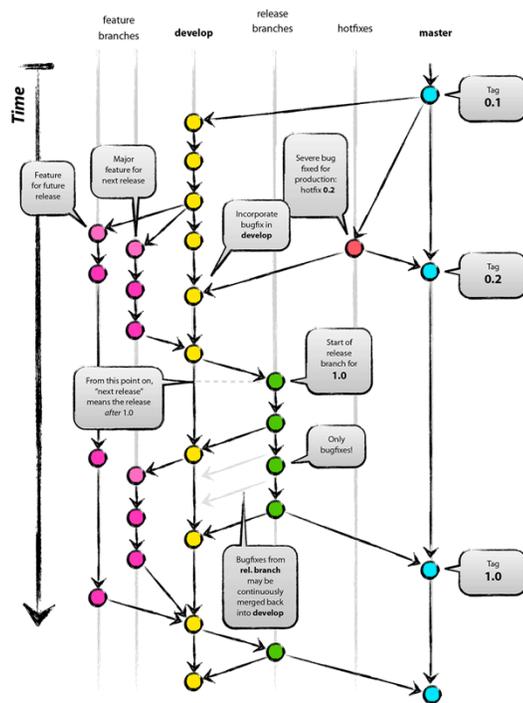
- Compliance Tasks
  - Dome9 Review
  - AD Review
  - Network Review
  - Privileged account use
  - Inspector Reviews
  - Encryption
  - And more...
- Operations Tasks
  - AMI Builds
  - Resource Tagging
  - Remediation
  - Provisioning
  - IaC Tech Debt
  - Billing
  - And more...

# Operations – Tech Debt Management



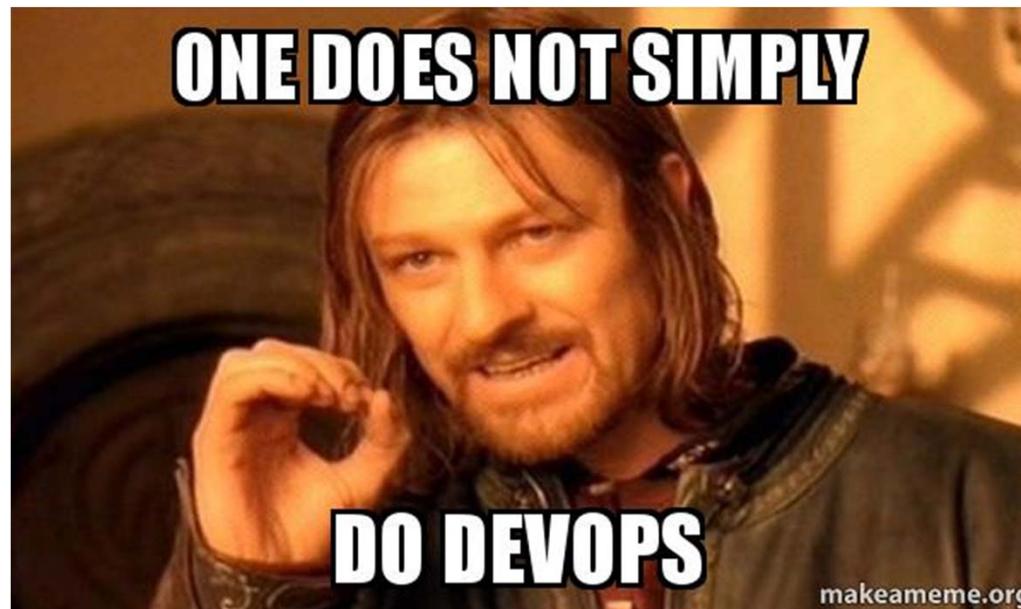
- Agile Project
  - Migrate infrastructure
  - New features
  - New automation pieces
- DevOps Team
  - .5 FTE for Operations
  - 1.5 FTE for Tech Debt and Remediation

# Operations – Procedures and Team



- Change Management
  - Testing
  - Code Review
  - Peer Review
- SCM
  - Pull Requests
  - Protected Branches
  - Git flow

# Operations – Challenges for SOM Tech



# Operations – Challenges for SOM Tech

- New technologies with steep learning curve
- New development life cycle
- Automation
- IaC vs direct configuration
- Scalability and Enterprise IT
- Handoff



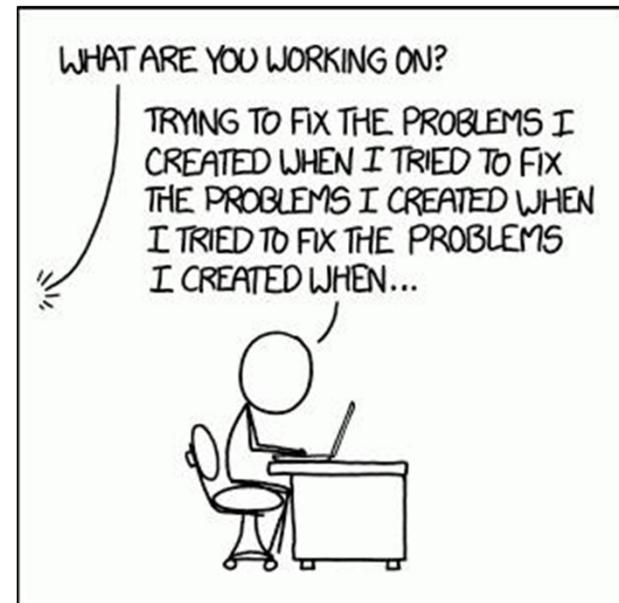


# Looking Forward

# Strategically Looking Forward

- **Scalability**

1. Operations and Security efficiency
2. Enterprise integrations
3. Billing
4. Training



# Strategically Looking Forward

- **Enabling Research**

1. 30+ projects waiting for access, 90% research related
2. Containerized computing with
3. Serverless computing
4. Advice and consulting



# Acknowledgements

- **UCSF Enterprise:**
  - Pat Phelan, Chief Information Security Officer
  - Tom Poon, Interim Chief Privacy Officer
  - Toby Barber, Information Security Architect
  - Bianca Paraguya, Privacy Office
- **SOM Tech:**
  - Kristin Chu, Director SOM Tech
  - Kymberly Ainsworth, Business Process Manager
  - Sean Thomas, Project Manager
- **CDHI:**
  - Rachael Callcut, Associate Professor of Surgery, Director of Data Science
  - Ed Martin, Director of Technology
  - Joe Hesse, Director of Innovation

