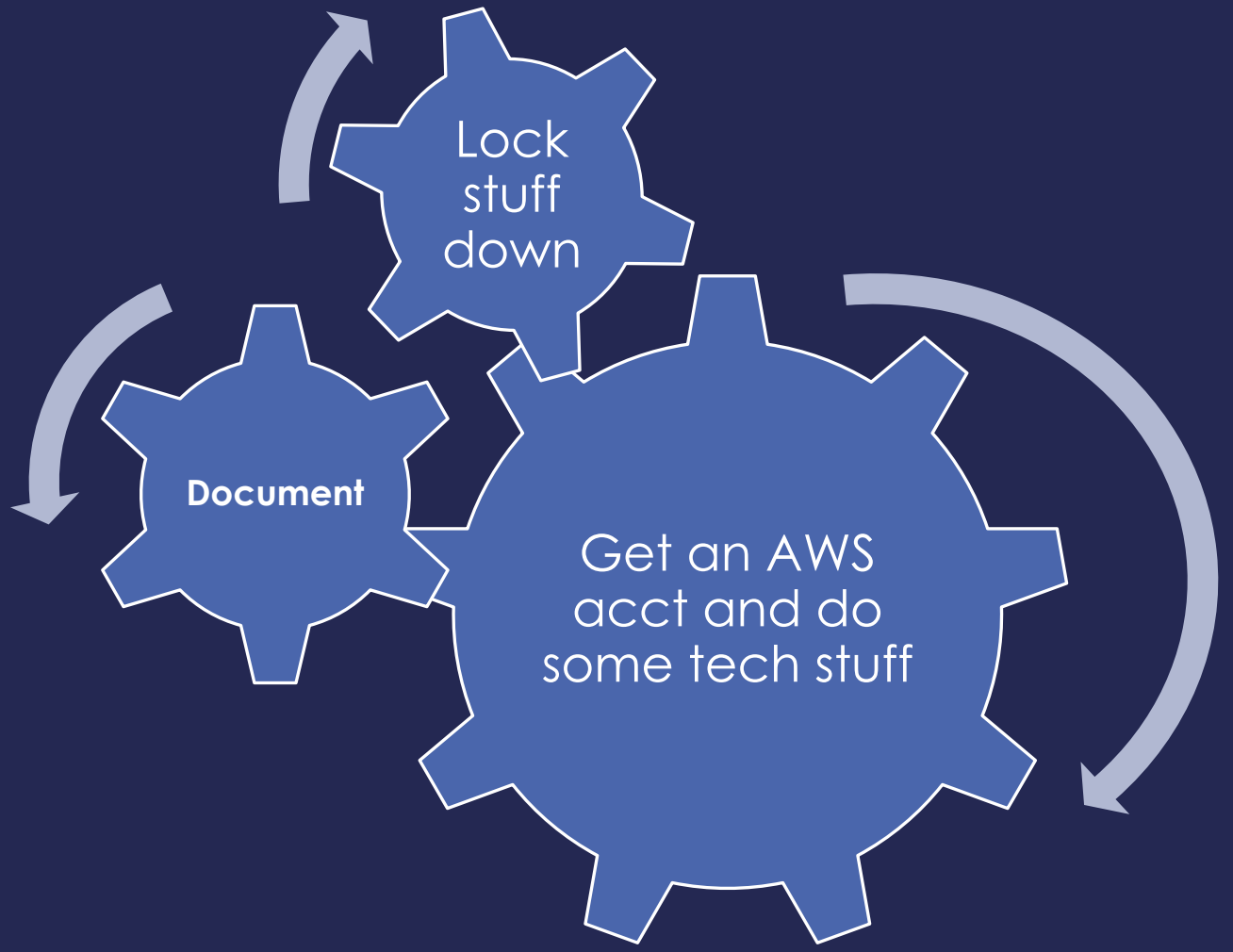
Securing the Cloud for Research: A Collaborative Effort

Claire Mizumoto

UCCSC 2018

Originally this is what we thought

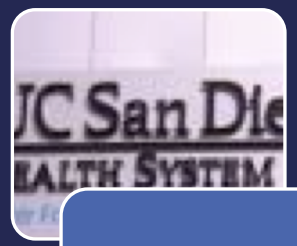


Instead this is what it really looks like

Technical engagement

Compliance Docs

Technical Engagement, take 2



Enter UC San Diego Health

Technical Process

What's Next

December 2016
Assumed it was mostly a technical problem that we needed to solve

March 2017
First pilot participants with ***de-identified, open data***

April 2017
We began to dig deep on the HIPAA certification docs

Wait…this was mostly a compliance issue

So we rebooted…..

We stepped up the pace to create:

- Systems Design Document
- System Security Plan
- Backup and Recovery Policy
- Configuration Management Document
- Contingency Plan
- IAM Policy
- IDS Document
- Incident Reporting Plan
- Production Support Document

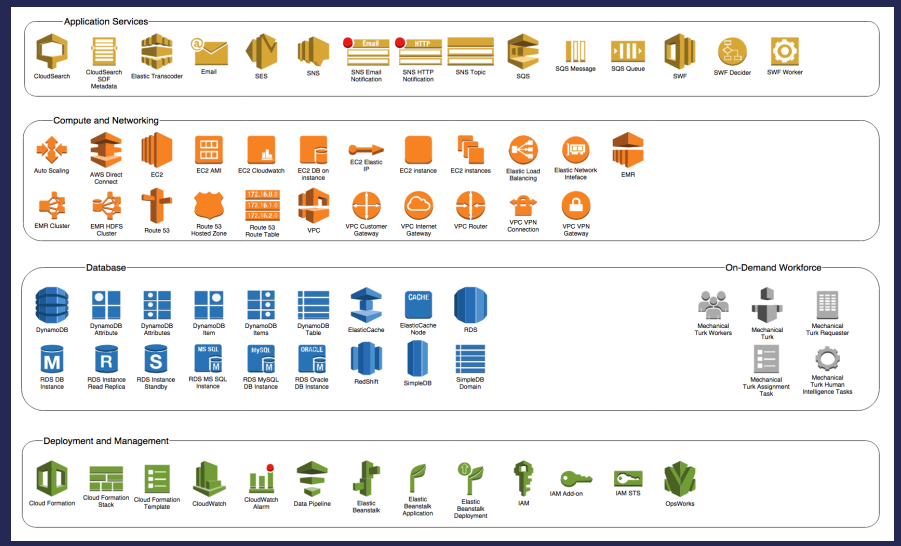
May 2017

First official meetings with:
Campus IT Security
UC San Diego Health

Already engaged a specialist – HIPAA/FISMA with the technical knowledge to put them together

And the glue that binds Health and Campus together: Health engaged the same consultant

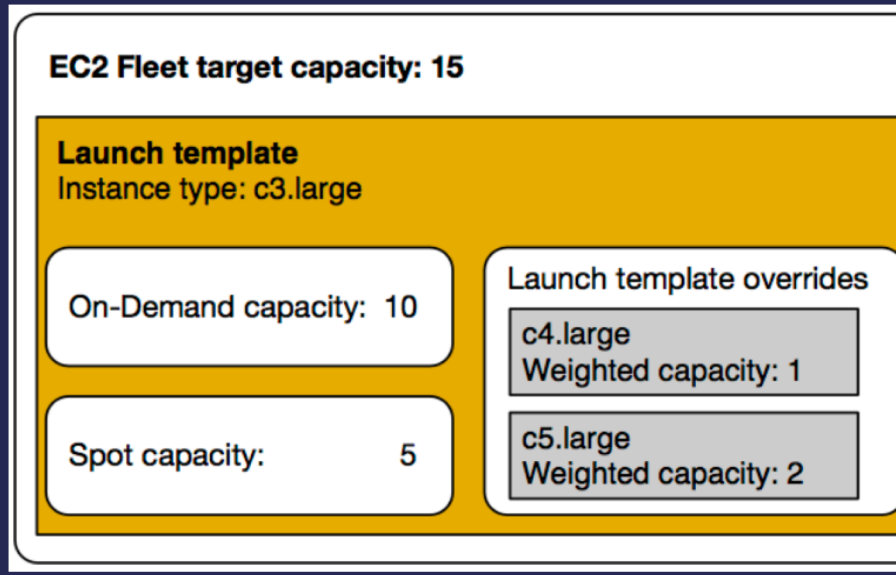
Leverage Native Services



So many services, so little time!

Eliminate management overhead!
Not all managed service will meet your exact needs.
Examples:

- **CloudFormation – Create your infrastructure in a reproducible, re-useable, and code-based method**
- **EC2 Fleet**
- **RDS and/or Serverless Aurora**
- **Elastic Beanstalk (for applications elasticity)**
- **DynamoDB**



Slide courtesy of A. Greaves

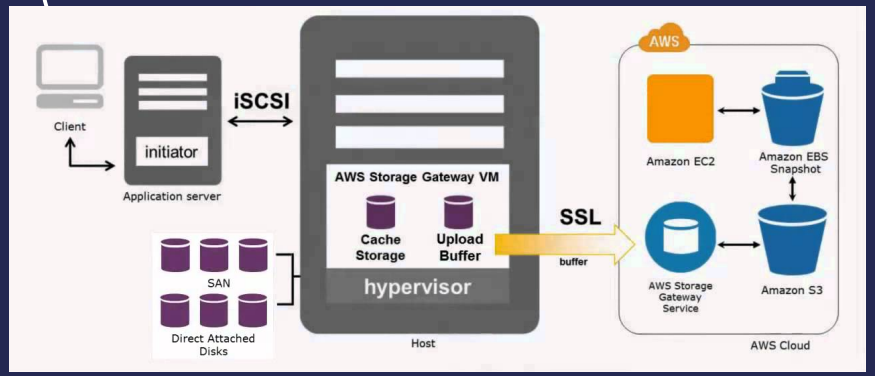
UC San Diego Health: AWS Cloud Strategy

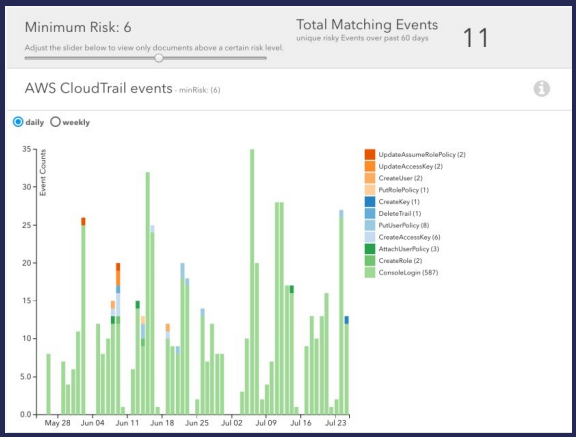
Phase I core infrastructure (Complete)

- **System Security Plan and Design document provisionally approved by security**
  - Pending organizational decisions on Logging, IDS/IPS (firewall-type)

Phase II focusing on customer defined service needs

- **Storage with S3**
  - Role transfer account -> S3
  - Customer buckets (filegateway endpoint as a NFS mount)
  - Filegateway Virtual tape library
  - StorageGateway application mounts (an iscsi) and S3
  - ***AWS Macie -** DLP and Bucket analytics service: *evaluating*
  - AD and MFA authentication, Duo MFA delete verification
- **AWS WorkSpaces VDI environment**
  - Proof of Concept in progress





Slide courtesy of A. Greaves

So, Instead of Being Competitive, We Collaborated

On the Health side,

- S3
- Access control
- Boundary security
- VPC/EC2 within an account
- Logging infrastructure
- Vulnerability/Compliance scanning

Collaboration, cont'd

On the Research IT side,

- Evident.io
- OpenVPN / Campus VPN / Campus IP space
- DUO MFA
- 2 more research project pilot participants
- User documents
- And more….

What's Next

- Continue to collaborate
- Compliance and Privacy Review
- Proof of Concept project to evaluate cost of outsourcing the maintenance of the environment
- "Packaging" compliance docs and code-sharing
- Handing off the Research IT side

In Summary

Collaboration

Questions?