UCSF
University of California
San Francisco

Securing Data in the Cloud

Jamie Lam
UCSF School of Medicine
Dean's Office Information Services Unit

7/13/2016

Agenda

- Introduction
- The Basics of Cloud Computing
  - Benefits and Risks
  - Types of Cloud computing services
  - Cloud computing at UCSF
- Considerations when using a cloud vendor
  - Vendor responsibilities vs. your responsibilities
- Governance of cloud computing at UC & UCSF
  - UC Cloud Services
  - Appendix DS and HIPAA BAA
  - Cloud governance at UCSF

Introduction

Who Am I and what is ISU?

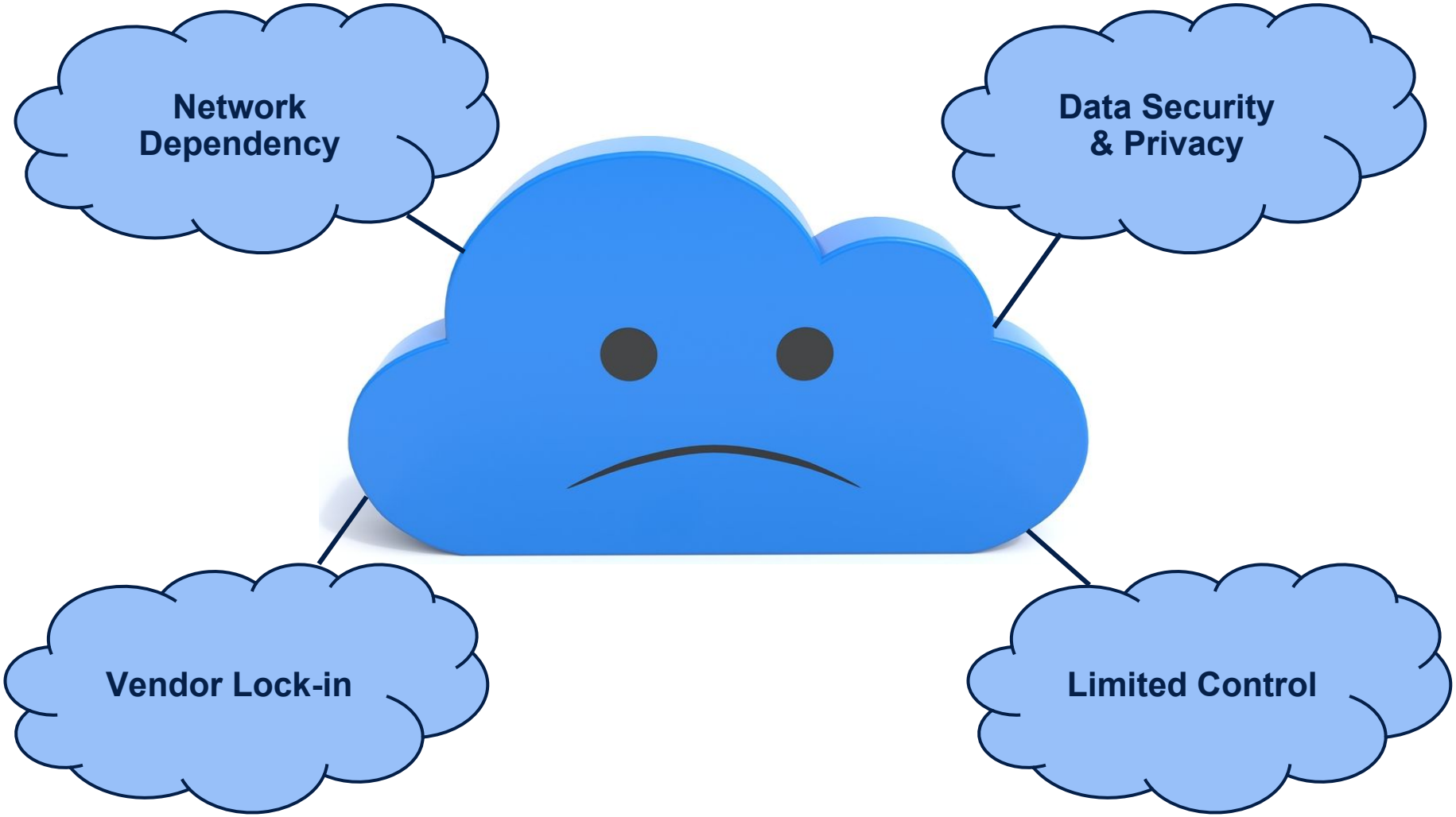
- Jamie Lam, UCSF School of Medicine Data Security Compliance Manager
  - Reports to UCSF School of Medicine Information Services Unit (ISU)
  - ISU serves to be a single point of contact (SPOC) for UCSF innovators and provides end-to-end services: Discovery -> Development -> Security Review -> Deployment -> Support

The Basics of Cloud Computing

Benefits of cloud computing

Cost reduction, Availability, Flexible Scalability

Risks of Cloud Computing



Types of Cloud Computing Services

Infrastructure as a Service (IaaS)

- Virtualization, storage, and networking
- Examples: Amazon Web Services (AWS), Rackspace Hosting
- Typical users: System administrators
- Host it

Platform as a Service (PaaS)

- Operating environment and services for application deployment
- Examples: Salesforce, Google App Engine
- Typical users: Developers
- Build it

Software as a Service (SaaS)

- Fully functional application
- Examples: Google Docs, Dropbox
- Typical users: Business end user
- Consume it

Cloud Computing at UCSF

Infrastructure as a Service (IaaS)

- UCSF Library infrastructure migration to AWS
  - Almost done!
- UCSF Anesthesia infrastructure migration to AWS
  - Architecting design with IT Security and AWS

Platform as a Service (PaaS)

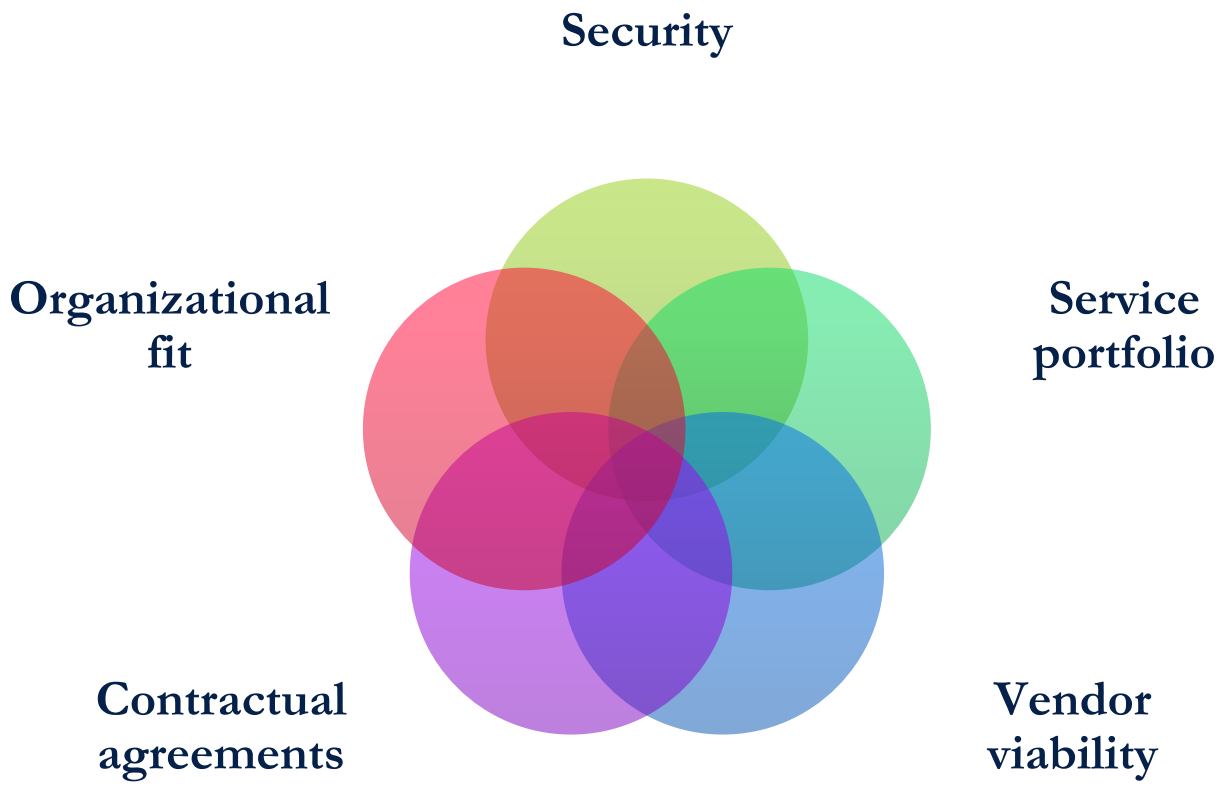
- UCSF uses custom Salesforce application development to meet specific needs that cannot be filled by the enterprise systems
- Program management in Dean's Office, Information Services Unit
- Over 70 applications developed

Software as a Service (SaaS)

- Enterprise
  - Qualtrics, Docusign
- Many departmental applications
  - Image Share, Healthloop, Radiologue

Considerations when using a cloud vendor

What should I look for in a cloud vendor?



Other considerations for cloud vendors

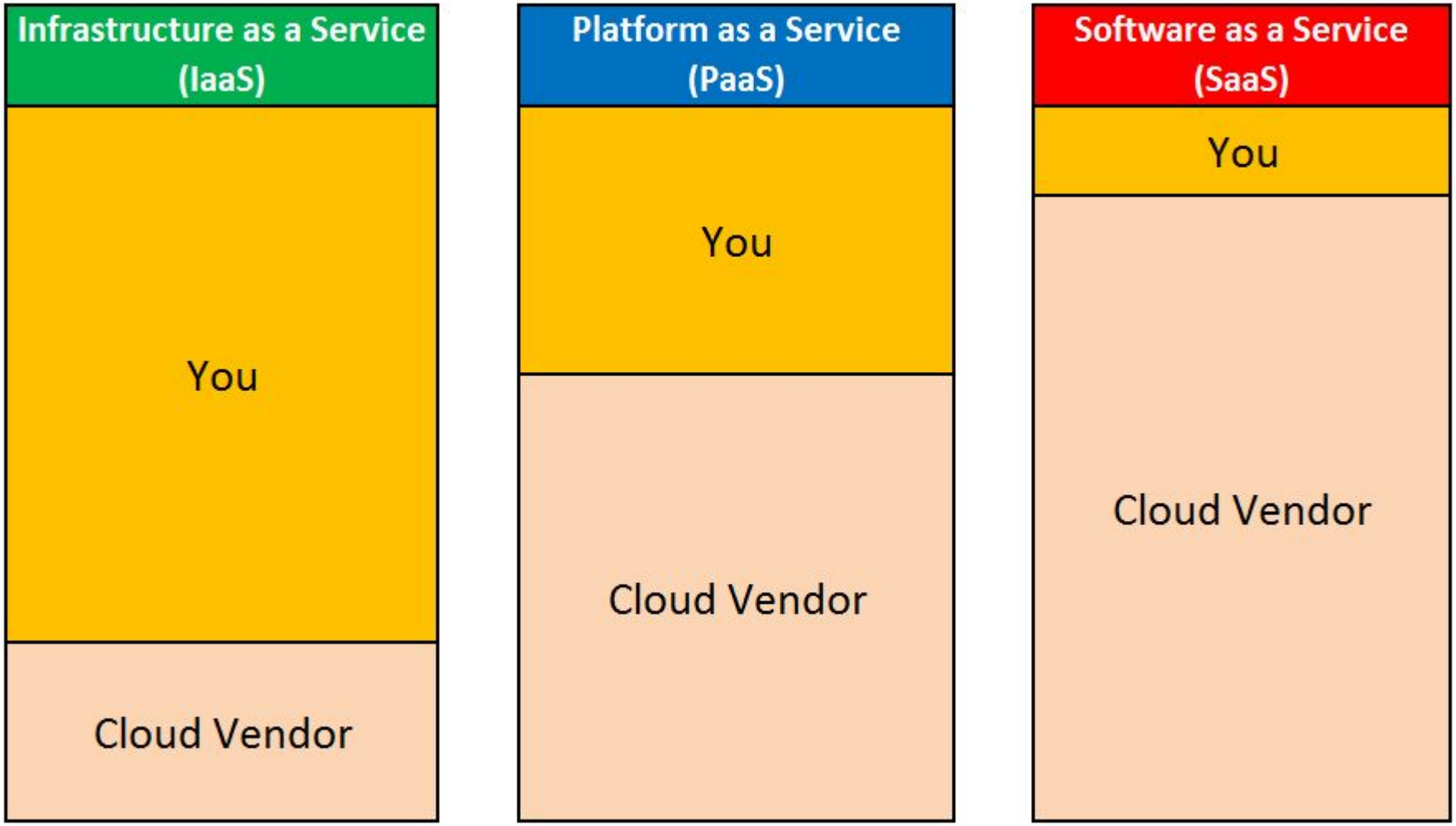
- Who owns the data?
- Who can access it?
  - Does the vendor use subcontractors who may also have access to your data?
  - Where are they working from?
- Where is the data being stored? Can your data be stored overseas?
  - Check backups and data replication sites too
- What happens to your data at the end of the contract?
  - Do you need to get the data back? If so, in what format?
  - Data destruction

Understand your responsibilities

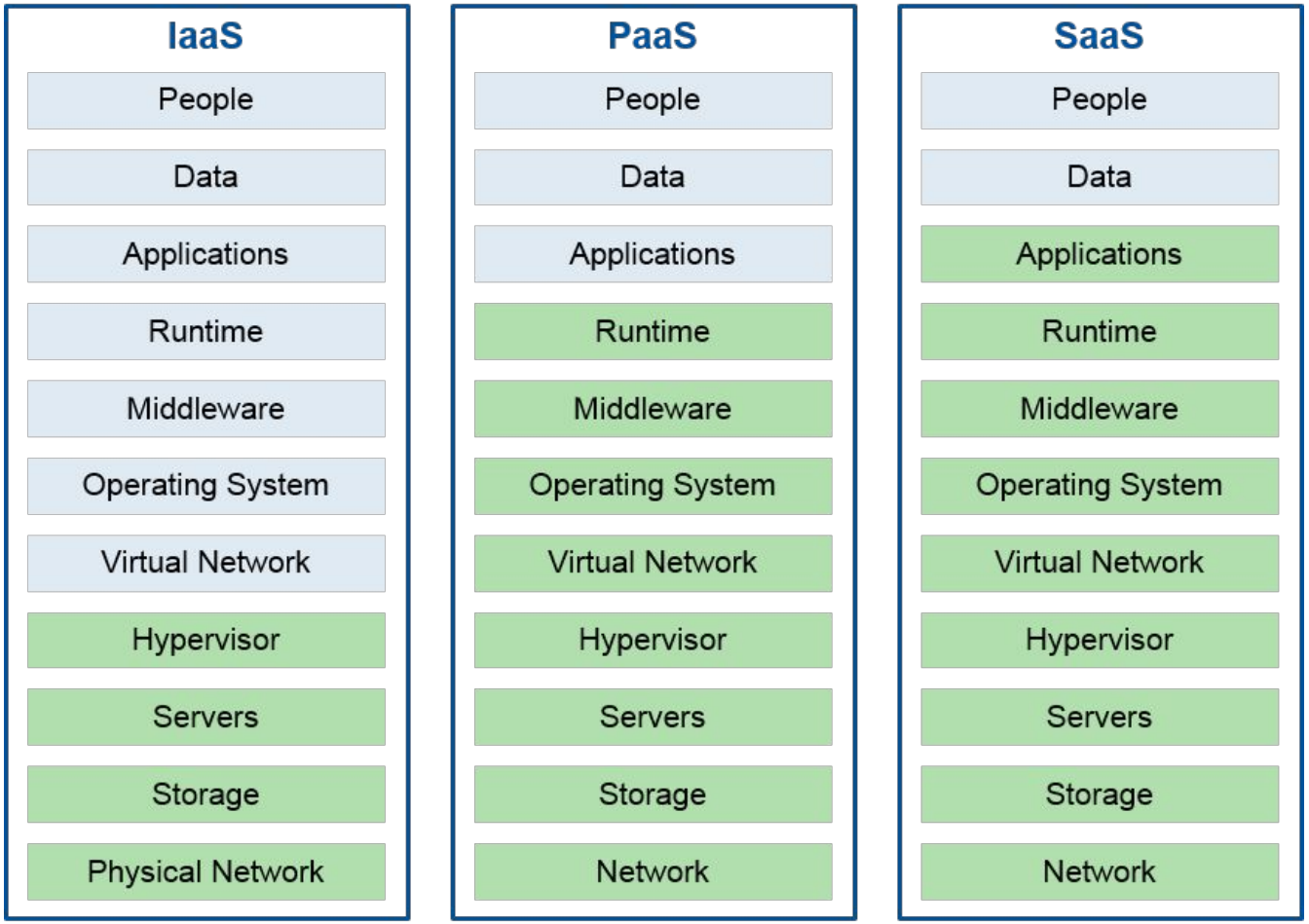
Gartner predicts, “Through 2020, 95 percent of cloud security failures will be the customer’s fault.”
- Top Strategic Predictions for 2016 and Beyond: The Future Is a Digital Thing.

- Only a small percentage of security incidents impacting enterprises using the cloud have been due to vulnerabilities that were the provider’s fault.
- You need to understand what you are buying and where the lines are drawn of what the vendor is supposed to do and what you are supposed to do.
- Confirm vendor’s responsibilities and make sure that they are contractually obligated to perform those responsibilities.

Responsibility Chart



Security Handoff Points



Source: Gartner (April 2016)

People and Data

Data

- What data are you moving to the cloud environment?
  - Consider data security requirements based on data classification
- Where does the data go?
  - Consider security of data at rest and in transit
  - Consider business workflow and when data leaves the system

People

- Access control
  - Authentication method & Password controls
  - Access authorization and termination procedures
  - Role based access
- Configure application to meet your campus's security policy

Governance of cloud computing at UC & UCSF

UC Cloud Services

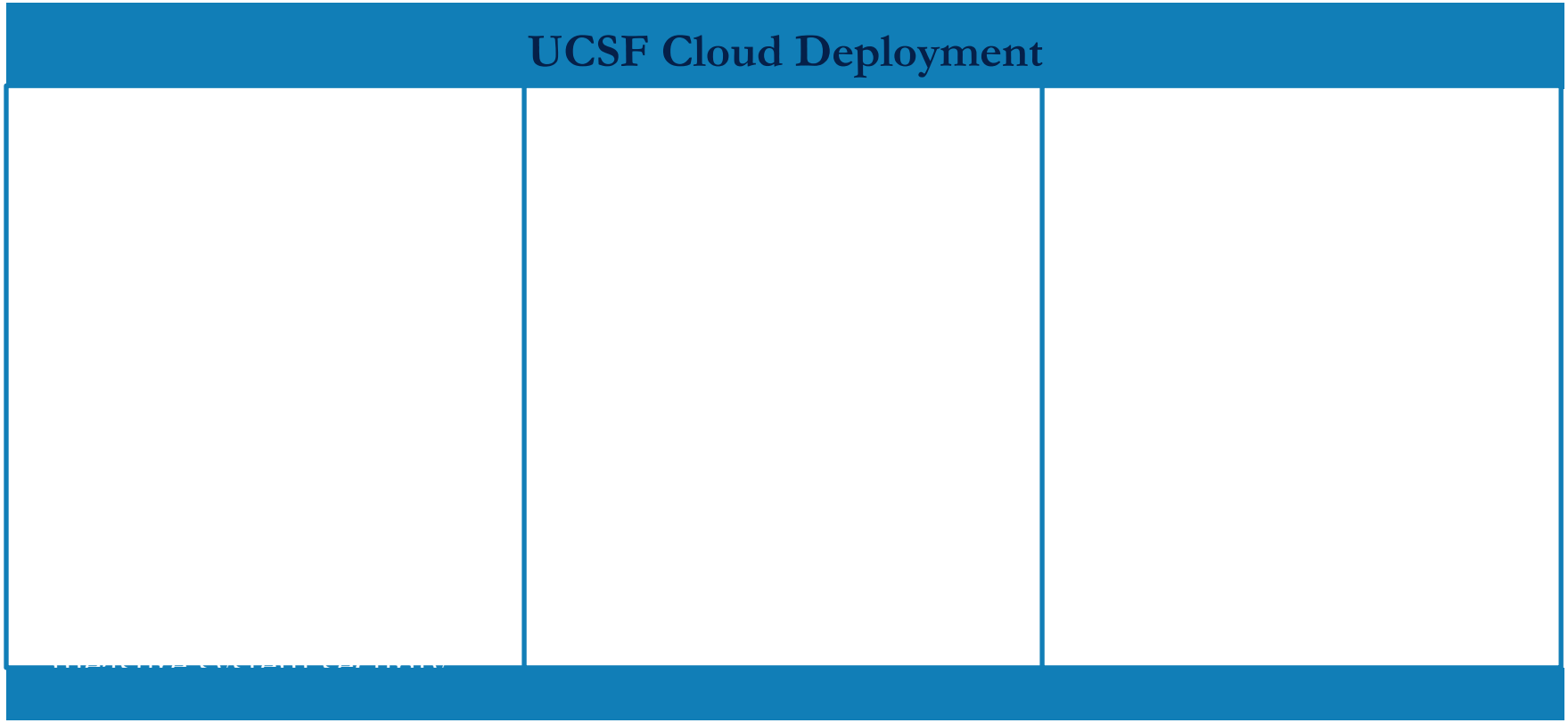
Existing systemwide contracts
http://www.ucop.edu/cloud-services-contracts/contracts-guidance/index.html

Service & service type	UC-wide contract	HIPAA Business Associate Agreement	Deployment guidance & implementation examples
Amazon web services Enterprise infrastructure	√	√	View the deployment guidance
Box File sharing/sync	√	√	View the deployment guidance
Google Apps for Education User productivity	√		View the deployment guidance
Microsoft Azure Enterprise infrastructure	√	√	View the deployment guidance
Microsoft Office 365 User productivity	√	√	*Coming soon*
SalesForce Business applications	√	√	View the deployment guidance

- Read the deployment guidance!
  - Understand your responsibilities
  - You may / may not be allowed to store sensitive data
    - Check your campus' cloud storage and usage guidelines
    - Work with your location contact(s)

Cloud Computing at UCSF

Multiple groups are involved in a successful cloud service deployment at UCSF



What is an Appendix – Data Security?

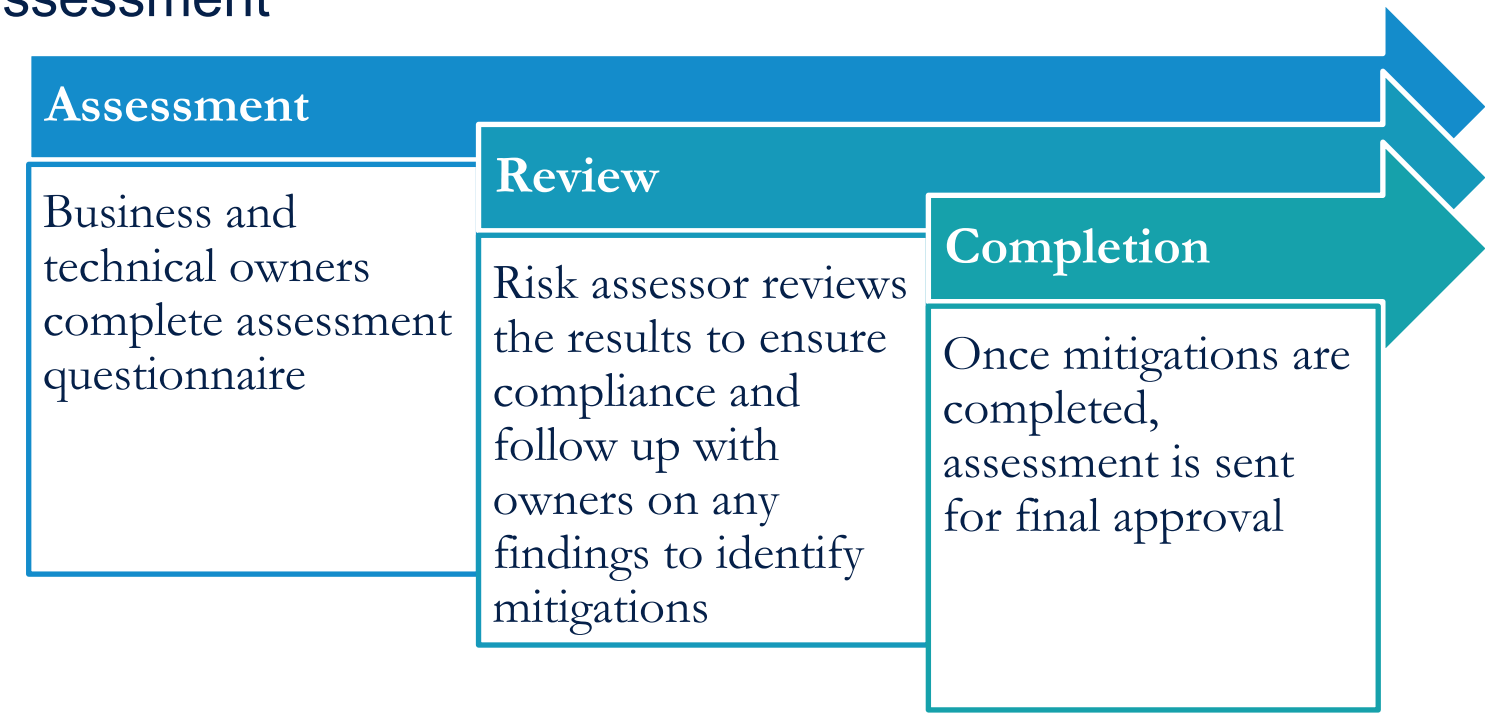
- UC has a common Appendix for Data Security & Privacy
- Provisions that all UC locations should use for contracts involving UC information
- Important because it highlights what the vendor can do with our information. Supplier cannot:
  - Access, use, or disclose data outside the scope of work
  - Access, use, or disclose for Supplier's benefit (even derivative information)
  - Disclose under court order without notifying UC
  - Move UC information outside USA without UC approval
- Let procurement know if your vendor may have access to your data

What is a BAA and what does it cover?

- HIPAA Regulations require the University, as a covered entity, to have a business associate agreement (BAA) whenever a non-University person or entity provides services to the University involving the use or disclosure of the University's protected health information (PHI).
  - Vendor has legal liability for security of data – with restrictions*
  - Vendor meets the requirements under HIPAA, including 45 CFR §§ 164.314 and 164.504(e)
  - Sets forth restrictions on use and disclosure of Customer Data constituting PHI by the vendor
  - Vendor signs HIPAA BAAs with downstream “subcontractors” that are also business associates of your institution
  - Requires notification of breaches and unauthorized use and disclosure of PHI
  - Vendor is financially liable for costs associated with security breach as a result of vendor’s failure to adhere to data security provisions in the BAA

System Risk Assessment

- A security risk assessment of information resources is required by UCOP policy. Also required by other regulations such as HIPAA.
- All new or changed systems at UCSF go through a system risk assessment



Questions?

University of California
San Francisco