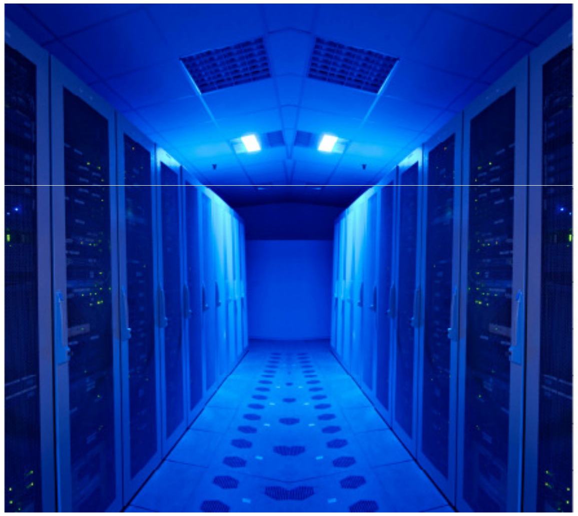
U.S. DEPARTMENT OF ENERGY

Office of the Chief Information Officer

How to Use the Federal Risk and Authorization Management Program (FedRAMP) for Cloud Computing



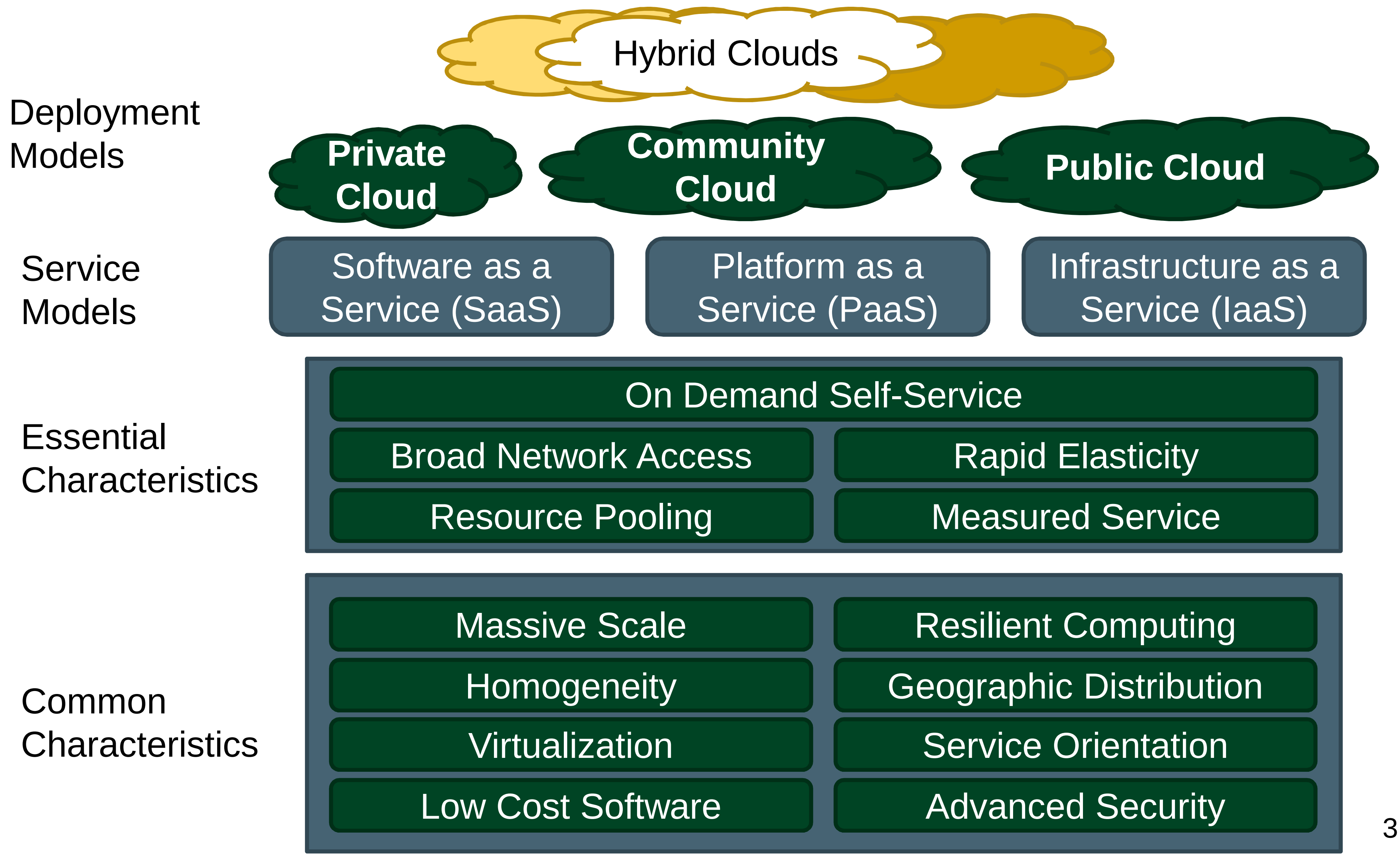
Warren S. Udy, CISSP
Senior Cyber Security Advisor
Office of Cyber Security
301-903-5515
warren.udy@hq.doe.gov

Five Stages of Grief

(or how is a cyber professional to deal with cloud computing?)

1. Denial and Isolation
2. Anger
3. Bargaining
4. Depression
5. **Acceptance**

The NIST Cloud Definition Framework



Hybrid Clouds

Deployment Models

- Private Cloud
- Community Cloud
- Public Cloud

Service Models

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

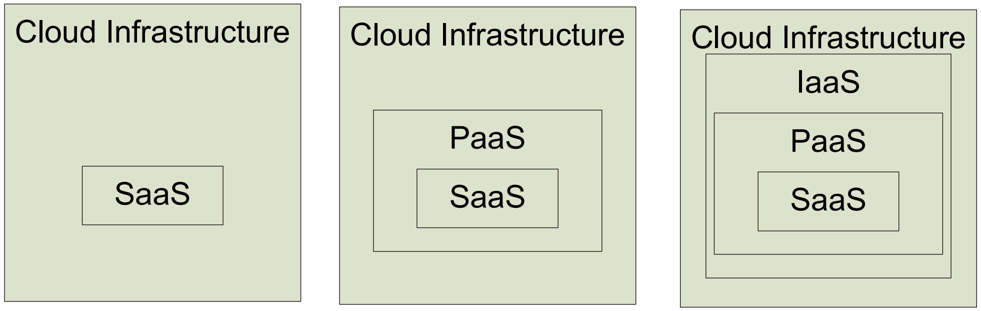
Essential Characteristics

- On Demand Self-Service
- Broad Network Access
- Rapid Elasticity
- Resource Pooling
- Measured Service

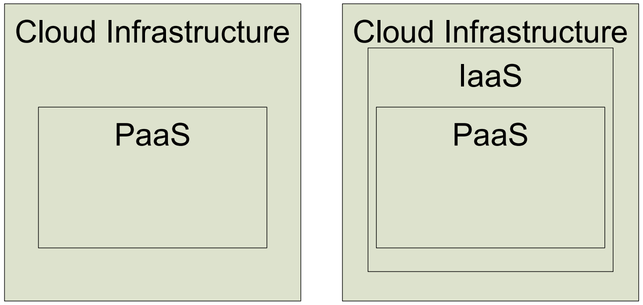
Common Characteristics

- Massive Scale
- Resilient Computing
- Homogeneity
- Geographic Distribution
- Virtualization
- Service Orientation
- Low Cost Software
- Advanced Security

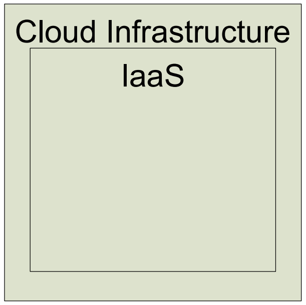
Service Model Architectures



Software as a Service (SaaS) Architectures



Platform as a Service (PaaS) Architectures



Infrastructure as a Service (IaaS) Architectures

NIST SP 800-37 - Changes in Rev 1

Two new concepts were added to NIST SP 800-37r1:

- Concept of Joint Authorization
- Concept of Leveraged Authorization

Federal Risk and Authorization Management Program (FedRAMP)

- Provides a standard approach to Assessing and Authorizing cloud computing services and products
- Allows joint authorizations and continuous monitoring services for Government and Commercial cloud computing systems
- Results in a common security risk model that can be leveraged across the Federal Government
- “Approve once, and use often"

Government use of FedRAMP

Federal agencies will interact with FedRAMP in two ways:

- Sponsoring a multi-agency cloud provider
- Leveraging a FedRAMP authorized system

Elements of FedRAMP

- Joint Authorization Board (JAB)

? (Sponsor)

- JAB Technical Representatives
  - Day-to-day involvement in the process and the review of the authorizations.
  - Recommend approval to the Authorizing Officials
- FedRAMP Operations Office
  - Day-to-day support of the authorization process
  - Interacts with federal Offices
  - Interacts with the service providers

Joint Authorization Board

DOD DHS GSA

(Plus Sponsoring Agency)

Sponsoring a Provider

What does it mean to sponsor a provider?

- Must have two sponsors to confirm multi-agency
- If your agency is the secondary agency sponsor, you are only confirming that the provider will be used by multiple agencies – NO other support or interaction is needed
- Agency has a contractual relationship with the provider
- Feels that the provider can have government wide utilization (multi-agency)
- Agency CIO is willing to sponsor (Join JAB)
  - Provide a Technical Representative to review authorization and advise the CIO on the authorization decision
  - Participate in the joint authorization

If my agency sponsors a provider and they can not meet the FedRAMP standards what happens?

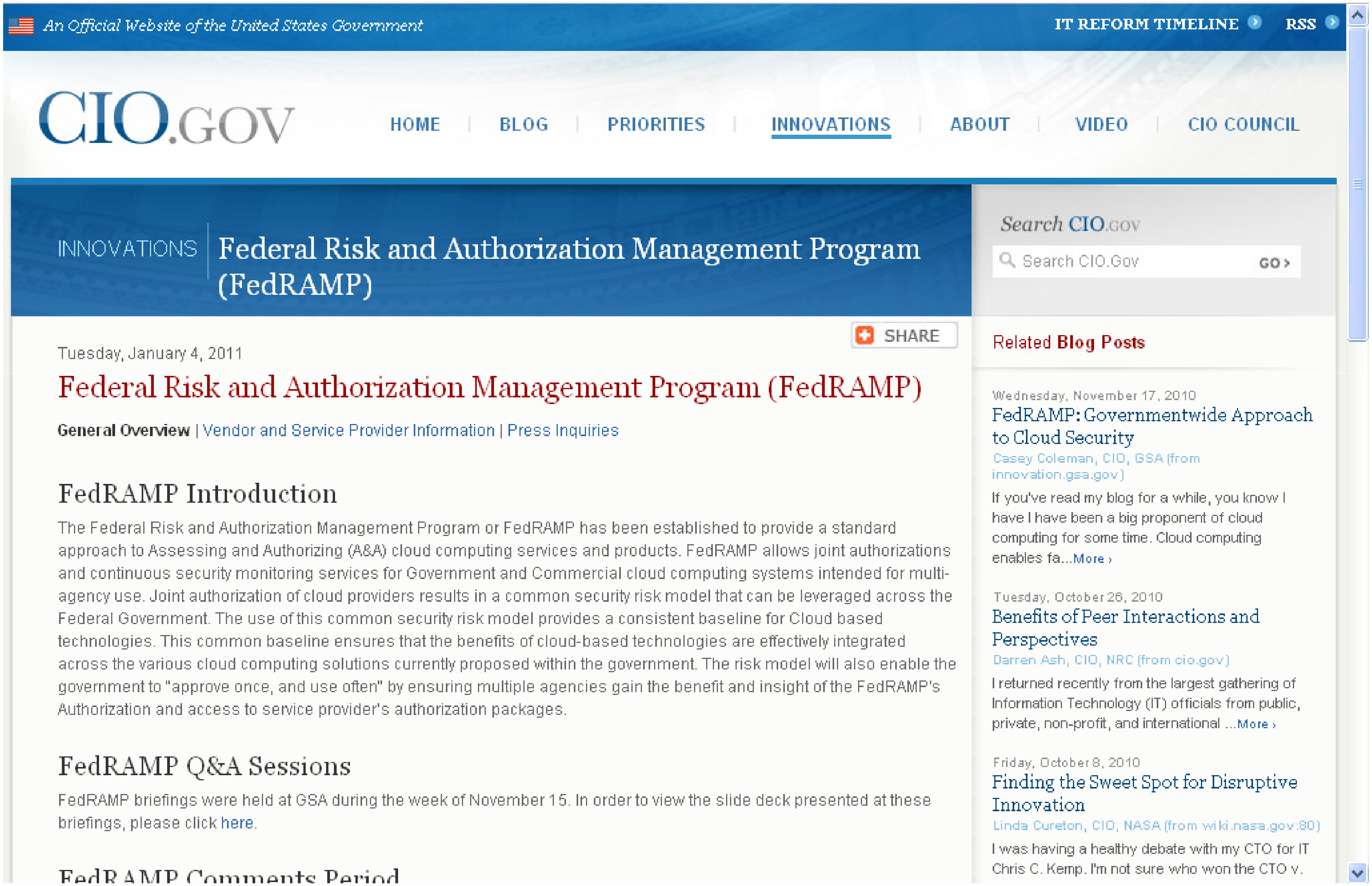
- Remember that the provider will **fund** the needed documentation of the controls and the independent assessments
- The first step in the process will be to document how the provider will comply with the controls.
  - Answers will be high level
  - Workbook with answers will be reviewed by FedRAMP and the JAB Tech Reps
  - May require face-to-face meeting to understand risks and its implications.
- By the end of this initial step agencies should know if the provider can complete the process.

Remember…….

- Agencies sponsoring a provider can add controls if needed
- Agency will utilized limited resources for the initial reviews of the workbook
- If you don’t like what the provider provided (read free documentation), the agency is free to initiate their own authorization

Leveraging an Authorization

www.fedramp.gov



An Official Website of the United States Government
IT REFORM TIMELINE
RSS
CIO.GOV
HOME | BLOG | PRIORITIES | INNOVATIONS | ABOUT | VIDEO | CIO COUNCIL
INNOVATIONS
Search CIO.GOV
Search CIO.Gov
GO ›
SHARE

Federal Risk and Authorization Management Program (FedRAMP)

Tuesday, January 4, 2011

Federal Risk and Authorization Management Program (FedRAMP)

General Overview | Vendor and Service Provider Information | Press Inquiries

FedRAMP Introduction

The Federal Risk and Authorization Management Program or FedRAMP has been established to provide a standard approach to Assessing and Authorizing (A&A) cloud computing services and products. FedRAMP allows joint authorizations and continuous security monitoring services for Government and Commercial cloud computing systems intended for multi-agency use. Joint authorization of cloud providers results in a common security risk model that can be leveraged across the Federal Government. The use of this common security risk model provides a consistent baseline for Cloud based technologies. This common baseline ensures that the benefits of cloud-based technologies are effectively integrated across the various cloud computing solutions currently proposed within the government. The risk model will also enable the government to "approve once, and use often" by ensuring multiple agencies gain the benefit and insight of the FedRAMP's Authorization and access to service provider's authorization packages.

FedRAMP Q&A Sessions

FedRAMP briefings were held at GSA during the week of November 15. In order to view the slide deck presented at these briefings, please click here.

FedRAMP Comments Period

Related **Blog Posts**

Wednesday, November 17, 2010
FedRAMP: Governmentwide Approach to Cloud Security
Casey Coleman, CIO, GSA (from innovation.gsa.gov)
If you've read my blog for a while, you know I have I have been a big proponent of cloud computing for some time. Cloud computing enables fa...More ›

Tuesday, October 26, 2010
Benefits of Peer Interactions and Perspectives
Darren Ash, CIO, NRC (from cio.gov)
I returned recently from the largest gathering of Information Technology (IT) officials from public, private, non-profit, and international ...More ›

Friday, October 8, 2010
Finding the Sweet Spot for Disruptive Innovation
Linda Cureton, CIO, NASA (from wiki.nasa.gov:80)
I was having a healthy debate with my CTO for IT Chris C. Kemp. I'm not sure who won the CTO v.

U.S. DEPARTMENT OF ENERGY
Office of the Chief Information Officer

How does my agency leverage an authorization?

FedRAMP web site will list two types of authorizations:

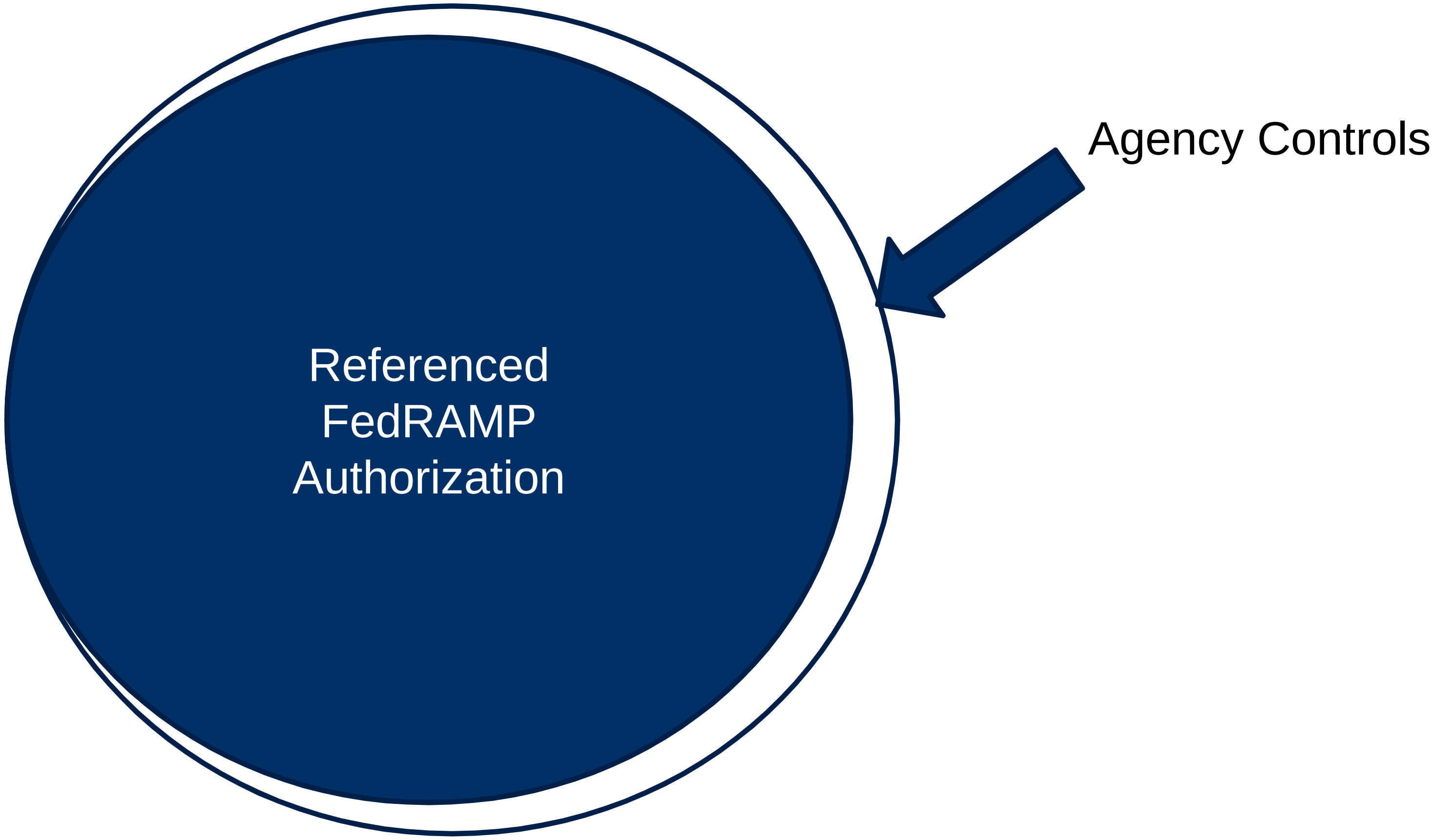
- Those who have completed the FedRAMP authorization process
- Those authorized by other federal entities that could be used by multiple agencies
  - These could have used the FedRAMP set of controls
  - Most likely authorized only by one agency and with baseline controls
- FedRAMP will provide document access to only FedRAMP authorized systems
- Site will help agencies get access to other listed systems

NIST 800-37 r1 – Leveraging…….

- ***leveraged authorization, is employed when a federal agency chooses to*** accept some or all of the information in an existing authorization package generated by another federal agency ***based on a need to use the*** same information resources (e.g., information system and/or services provided by the system).
- The leveraging organization reviews the organization’s authorization package as the basis for determining risk to the leveraging organization.
- Considers risk factors such as the authorization results, the environment of operation, the criticality/sensitivity of the information to be processed, stored, or transmitted, as well as the overall risk tolerance of the leveraging organization.

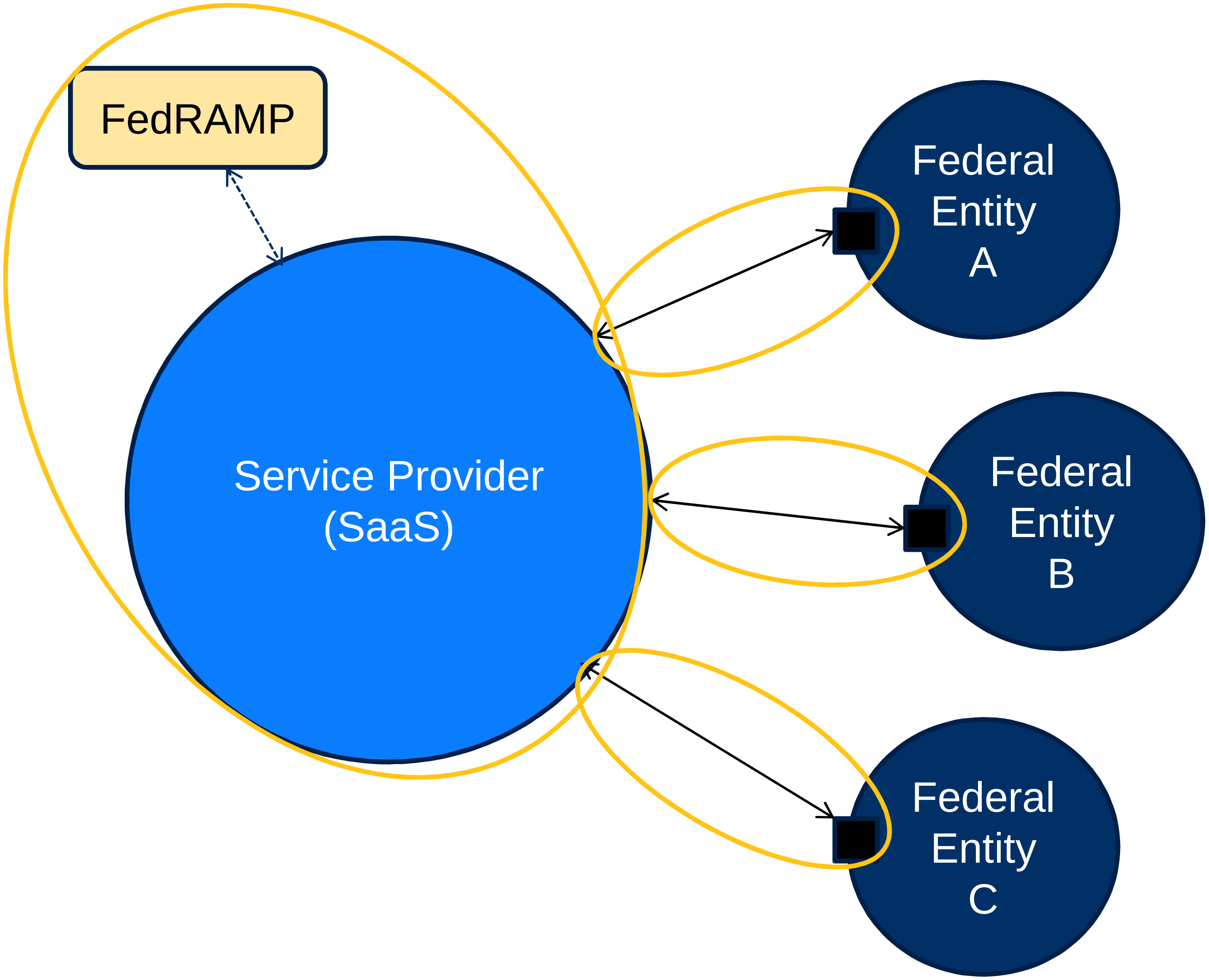
U.S. DEPARTMENT OF ENERGY
Office of the Chief Information Officer

Agency Authorization Package


Agency Controls

Referenced FedRAMP Authorization

Leveraged use of Authorization



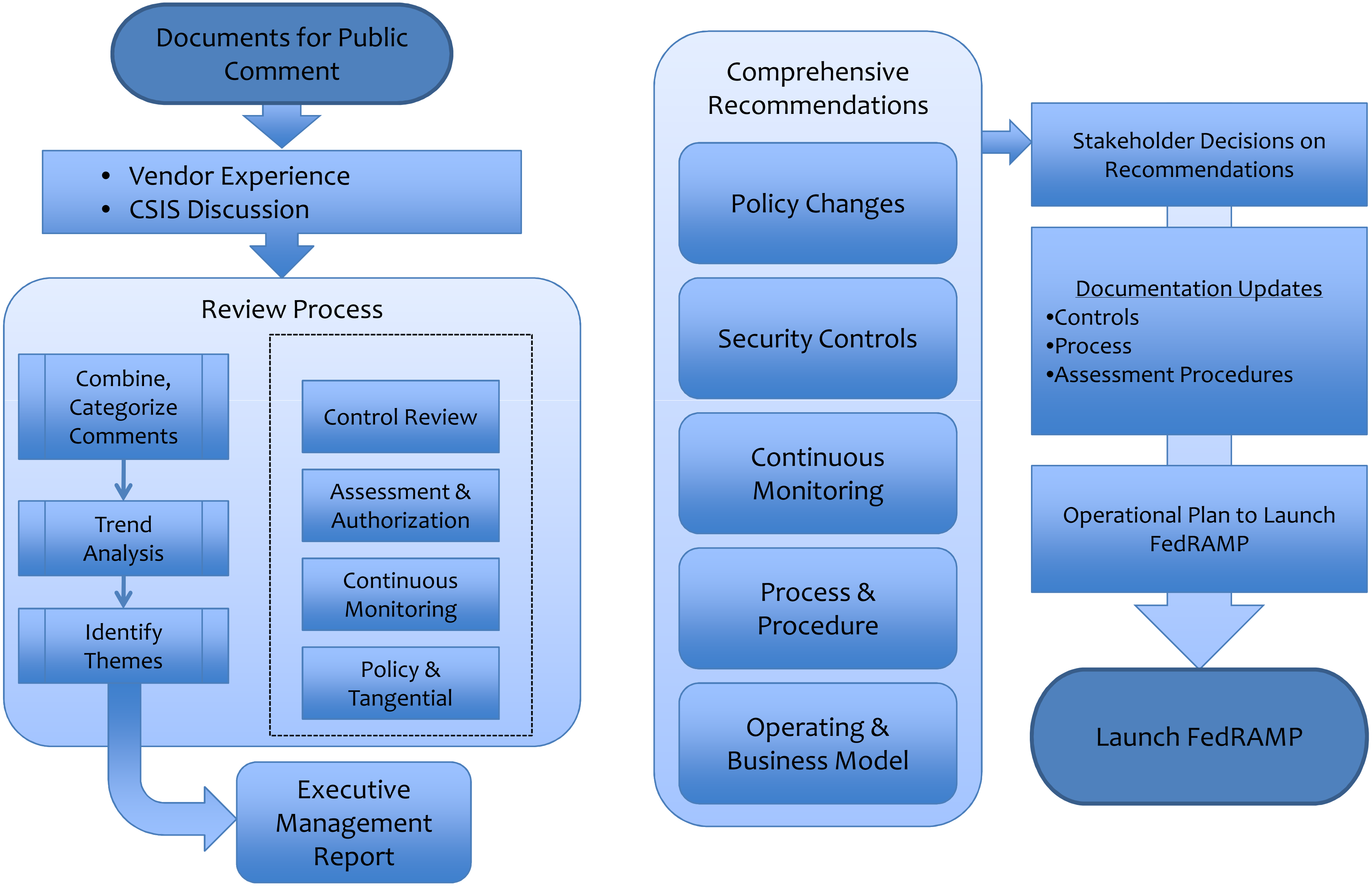
U.S. DEPARTMENT OF
ENERGY
Office of the Chief
Information Officer

Examples of Agency Controls

- FIPS-199 determination of the data.
- Initial Privacy Review of the data.
- Perform user cyber training.
- Provisioning of actual users.
- Termination of users.
- Continuous review of agency controls.

Where Are We Today?

High-Level Review Process



Documents for Public Comment

- Vendor Experience
- CSIS Discussion

Review Process

Combine, Categorize Comments

Trend Analysis

Identify Themes

Control Review

Assessment & Authorization

Continuous Monitoring

Policy & Tangential

Executive Management Report

Comprehensive Recommendations

Policy Changes

Security Controls

Continuous Monitoring

Process & Procedure

Operating & Business Model

Stakeholder Decisions on Recommendations

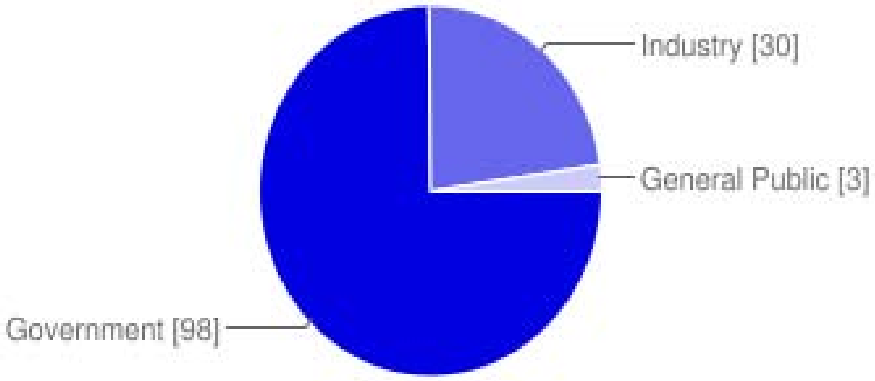
Documentation Updates

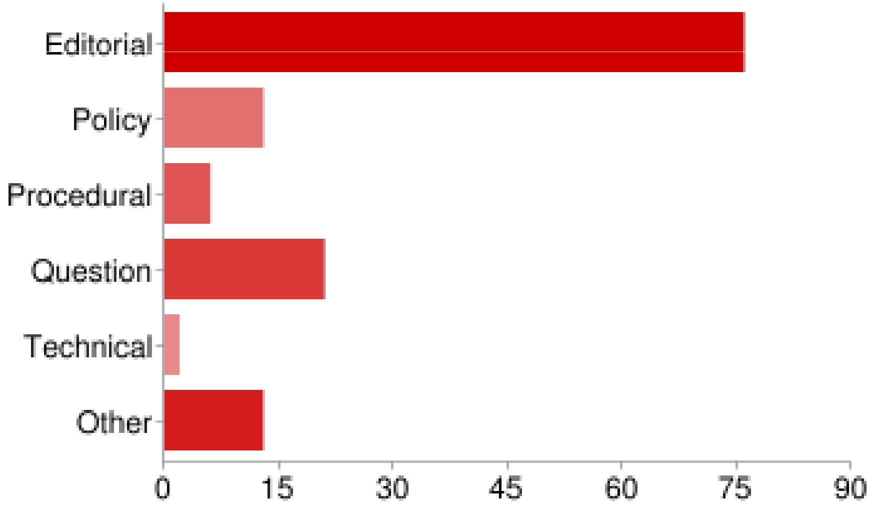
- Controls
- Process
- Assessment Procedures

Operational Plan to Launch FedRAMP

Launch FedRAMP

Summary of FedRAMP Comments





Organization Type		
Government	98	75%
Industry	30	23%
General Public	3	2%

Comment Type		
Editorial	76	58%
Policy	13	10%
Procedural	6	5%
Question	21	16%
Technical	2	2%
Other	13	10%

- Comment period was extended to **Monday, January 17, 2011.**

FedRAMP Tiger Teams

- FedRAMP Security Controls
- Assessment and Authorization
  - FedRAMP A&A processes
  - Security Control Baseline
  - IV&V and Independent 3rd Party Assessment
- Continuous Monitoring
  - Vulnerability Scanning and Penetration Testing
  - Change Management
  - Incident Handling
  - Continuous Monitoring and Reporting
- Policy
  - FISMA Reporting
  - Trusted Internet Connection (TIC)
  - Privacy
  - FedRAMP Operating and Business Model

PMO Update - IaaS Award

Cloud Storage Awardees:

- Apptis, Inc.
- AT&T
- Autonomics Resources
- CGI Federal Inc.
- Computer Literacy World
- Computer Technology Consultants
- Eyak Tech LLS
- General Dynamics Information Technology
- Insight Public Sector
- Savvis Federal Systems
- Verizon Federal Inc.

Vendor		Cloud Storage	Virtual Machines	Web Hosting
1	Apptis, Inc.	X	X	
2	AT&T	X	X	
3	Autonomic Resources		X	
4	CGI Federal Inc.		X	X
5	Computer Literacy World	X	X	X
6	Computer Technology Consultants	X	X	X
7	Eyak Tech LLC	X	X	X
8	General Dynamics Information Technology		X	
9	Insight Public Sector	X		
10	Savvis Federal Systems		X	X
11	Verizon Federal Inc.		X	
Total Awards by Lot		6	10	5

Now that we have FedRAMP, how does DOE interact with it?

Implement a DOE interaction Office

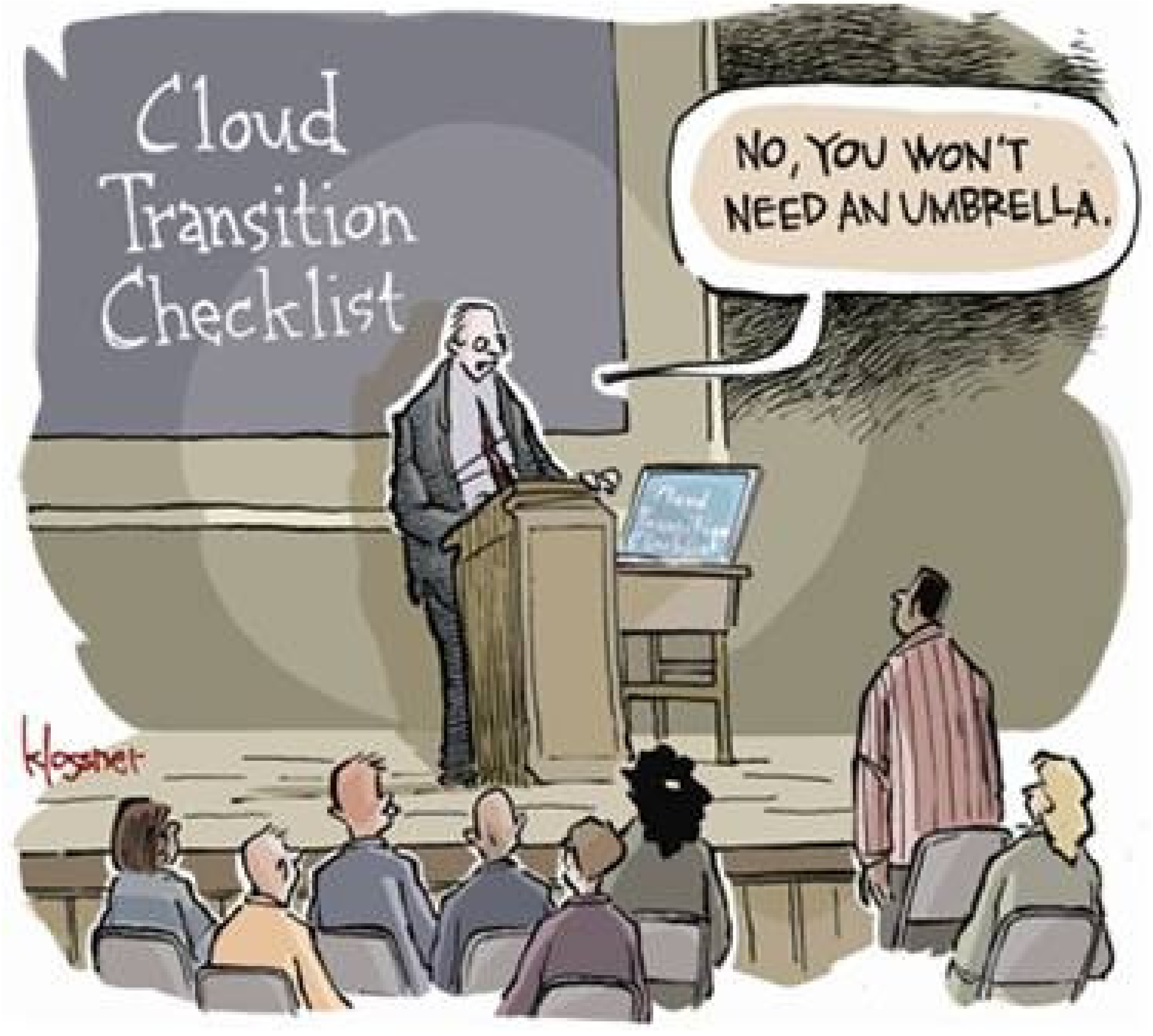
- Reviewing a draft charter
  - Leveraging on the FedRAMP concepts
  - Include a Joint authorization for DOE only systems
  - Governance model
  - Determine what systems DOE sponsors
  - Assist any DOE element to take advantage of a FedRAMP authorized system
- Jump start systems for cloud use……

QUESTIONS?

Words of Wisdom……

“I realized that security is more of a people and process problem than a technical problem”

Mischel Kwon , Former Director of US-CERT


Cloud Transition Checklist
NO, YOU WON'T NEED AN UMBRELLA.
klossner