



U.S. DEPARTMENT OF
ENERGY

Office of the Chief
Information Officer

Cloud computing and what it means for the Training Professional



Warren S. Udy, CISSP
Senior Cybersecurity Advisor
Office of the Associate CIO for Cyber Security
202-586-1746
warren.udy@hq.doe.gov



U.S. DEPARTMENT OF
ENERGY

Office of the Chief
Information Officer

What is Cloud Computing?





U.S. DEPARTMENT OF
ENERGY

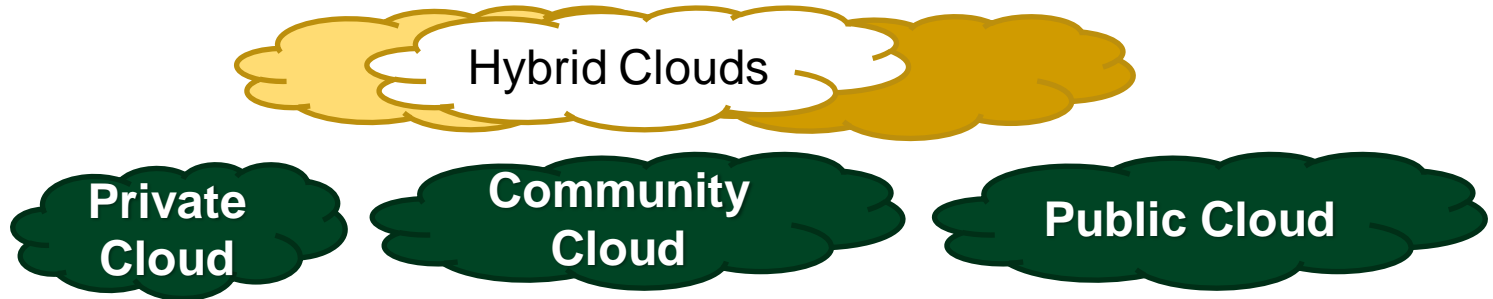
Office of the Chief
Information Officer

Google Data Center

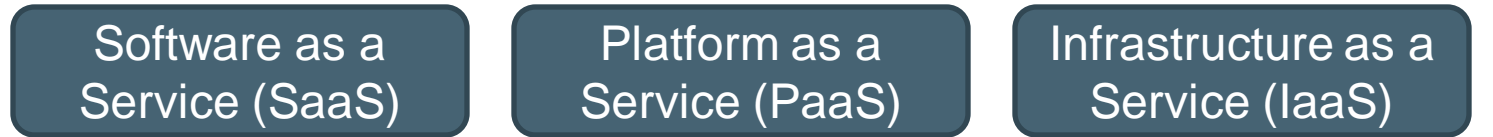


The NIST Cloud Definition Framework

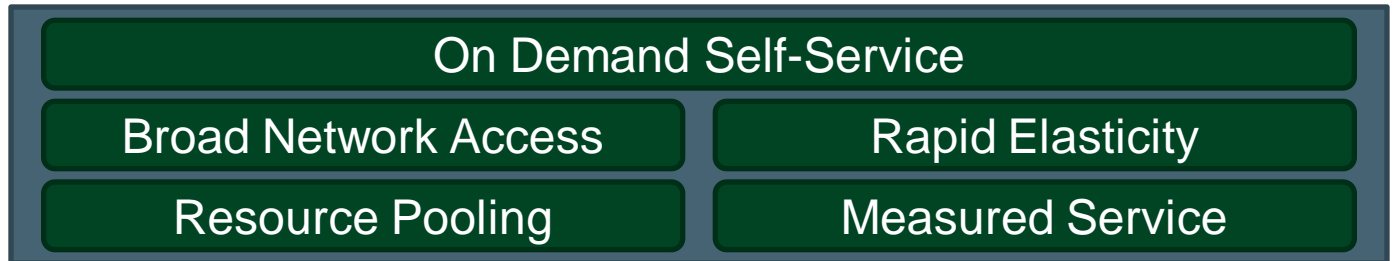
Deployment
Models



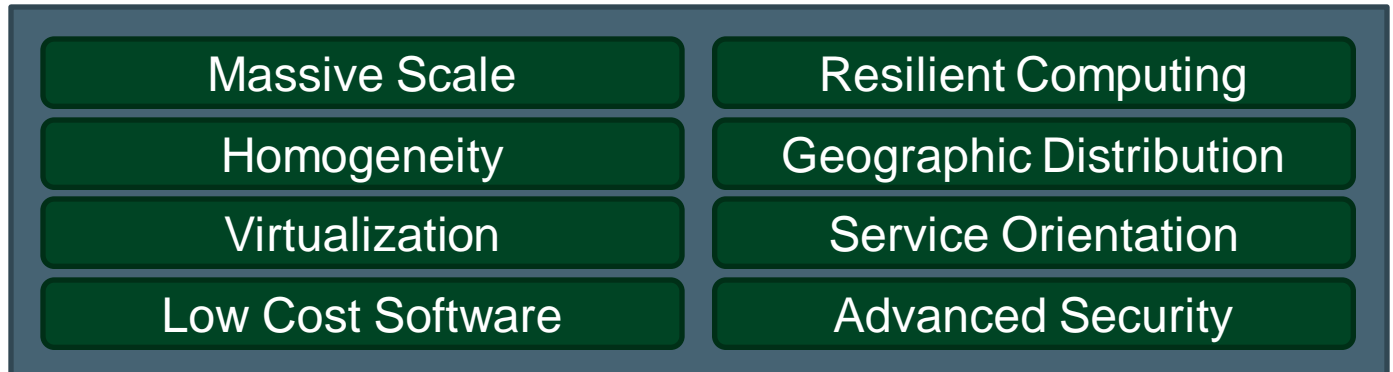
Service
Models



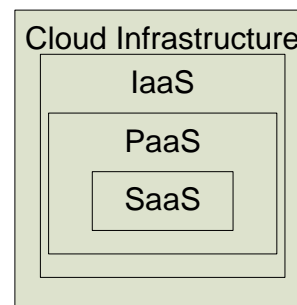
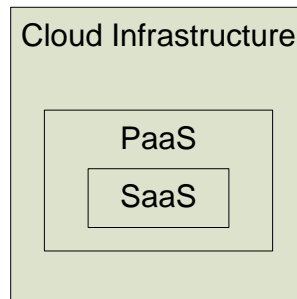
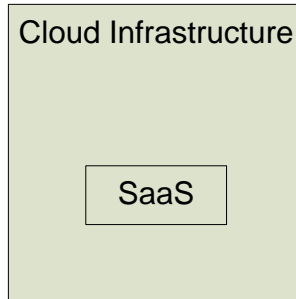
Essential
Characteristics



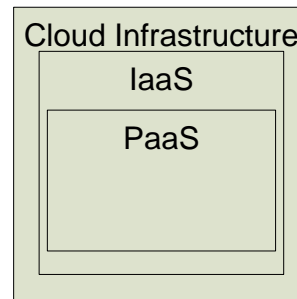
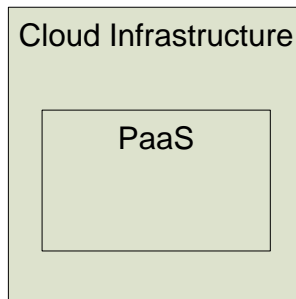
Common
Characteristics



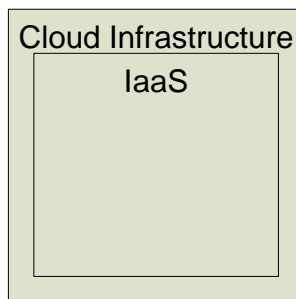
Service Model Architectures



Software as a Service
(SaaS)
Architectures



Platform as a Service (PaaS)
Architectures



Infrastructure as a Service (IaaS)
Architectures

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”**



Federal agencies will interact with FedRAMP in two ways:

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

• Office of Management and Budget Policy



• FedRAMP PMO



• ISIMC Guidance
• Cross Agency Coordination



FedRAMP

• FISMA Standards
• Technical Advisors
• Technical Specifications



**Joint Authorization
Board (JAB)**



• US-CERT Incident Coordination
• CyberScope Continuous Monitoring
Data Analysis



U.S. DEPARTMENT OF

ENERGY

Office of the Chief
Information Officer

Leveraging an Authorization

INNOVATIONS | **Federal Risk and Authorization Management Program (FedRAMP)**

Search CIO.gov

Search CIO.Gov GO >

Tuesday, January 4, 2011

SHARE

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

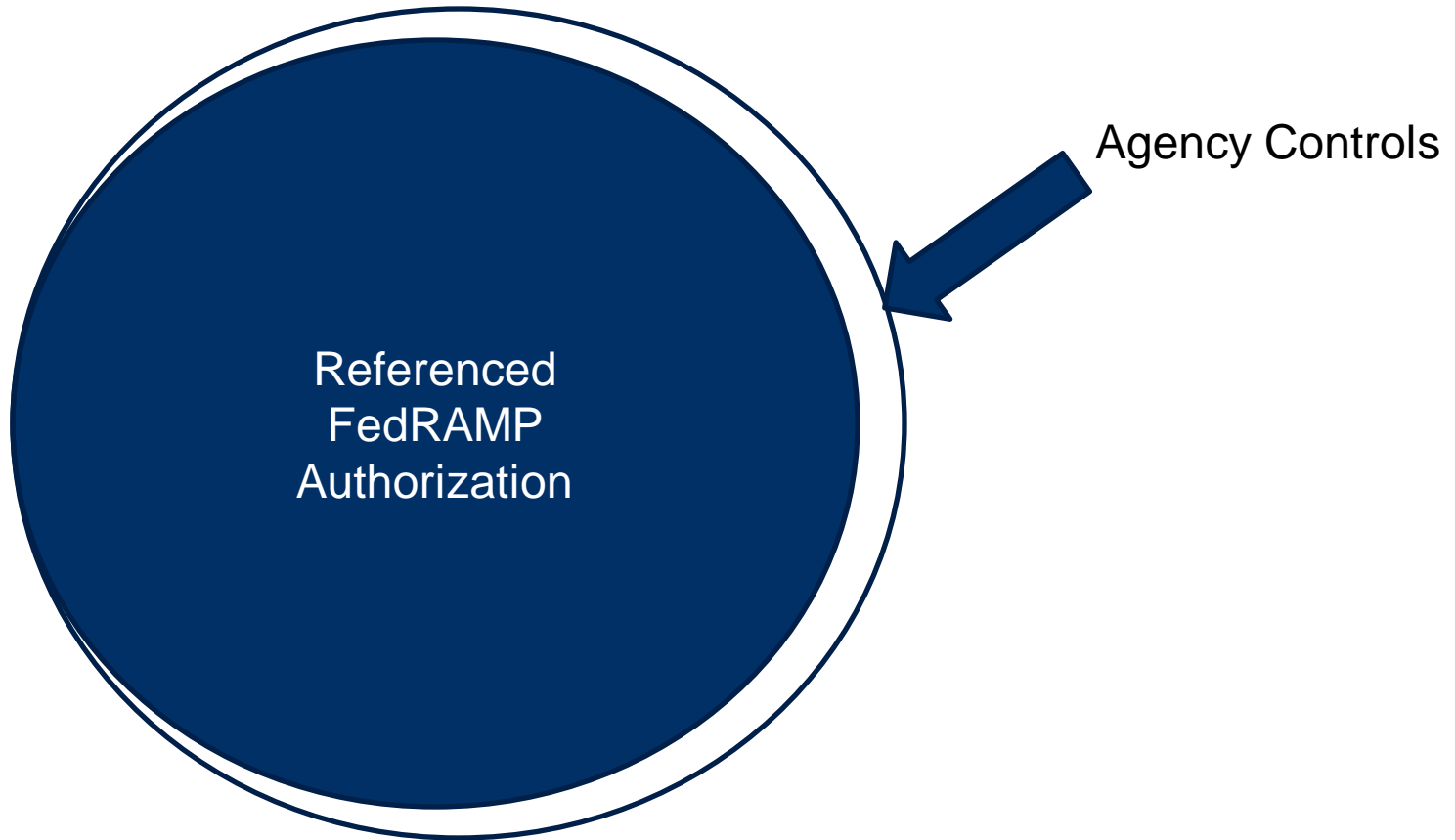
[Linda Cureton, CIO, NASA \(from wiki.nasa.gov:80\)](#)

I was having a healthy debate with my CTO for IT Chris C. Kemp. I'm not sure who won the CTO v.

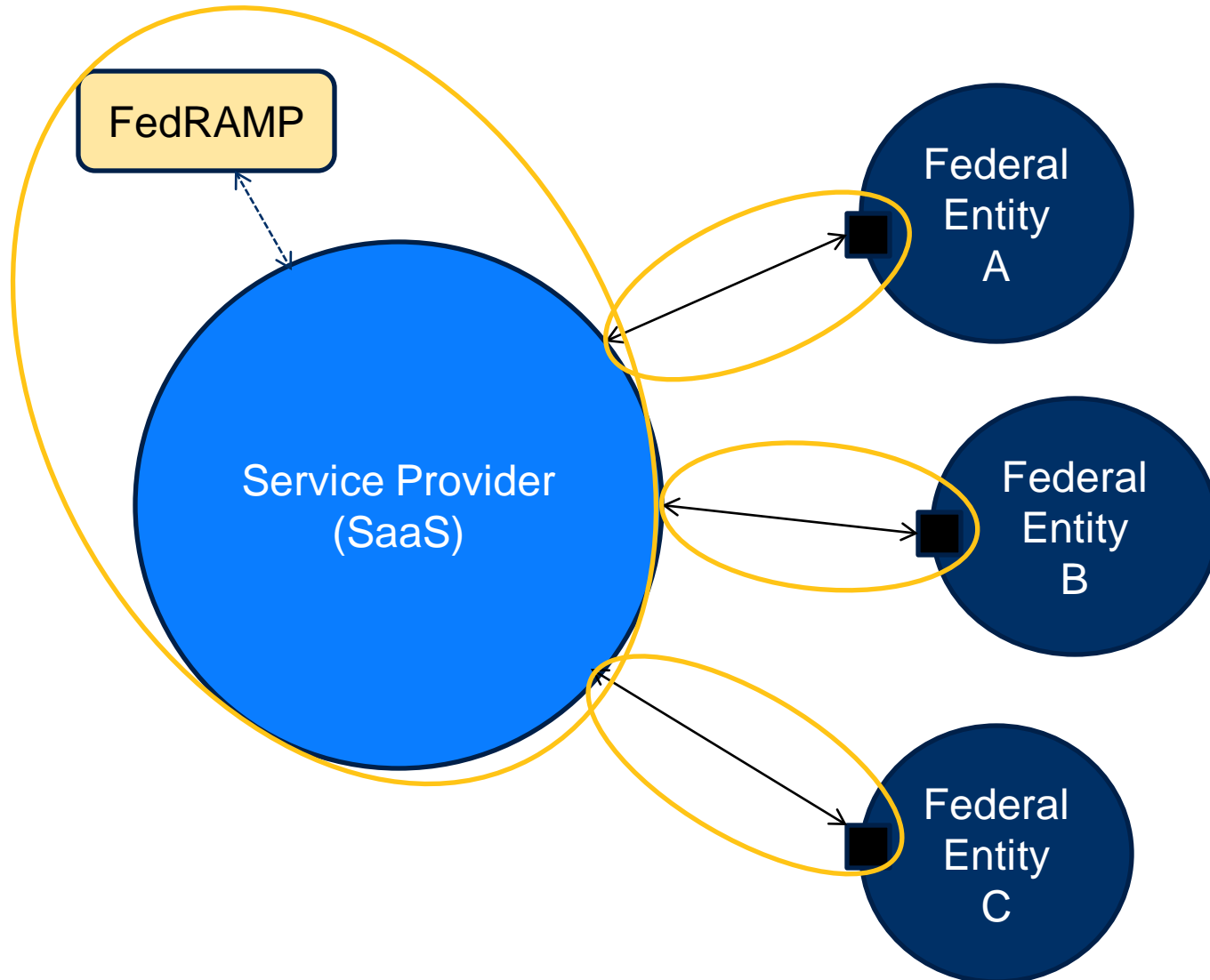
NIST 800-37 r1 – Leveraging.....

- *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.

Agency Authorization Package



Leveraged use of Authorization



Examples of Agency Controls

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

Awareness and Training (AT)

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
AT-1	Security Awareness and Training Policy and Procedures	AT-1	AT-1	AT-1 [Assignment: organization-defined frequency] Parameter: [at least annually]	None.
AT-2	Security Awareness	AT-2	AT-2	AT-2 [Assignment: organization-defined frequency] Parameter: [at least annually]	None.
AT-3	Security Training	AT-3	AT-3	AT-3 [Assignment: organization-defined frequency] Parameter: [at least every three years]	None.
AT-4	Security Training Records	AT-4	AT-4	AT-4b. [Assignment: organization-defined frequency] Parameter: [At least three years]	None.

The Anatomy of a Security Control

AT-3 SECURITY TRAINING

Control: The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) *[Assignment: organization-defined frequency] thereafter*.

Supplemental Guidance: The organization determines the appropriate content of security training based on assigned roles and responsibilities and the specific requirements of the organization and the information systems to which personnel have authorized access. In addition, the organization provides information system managers, system and network administrators, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training to perform their assigned duties. Organizational security training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. The organization also provides the training necessary for these individuals to carry out their responsibilities related to operations security within the context of the organization's information security program. Related controls: AT-2, SA-3.

Control Enhancements:

(1) **The organization provides employees with initial and *[Assignment: organization-defined frequency] training in the employment and operation of environmental controls.***

Enhancement Supplemental Guidance: Environmental controls include, for example, fire suppression and detection devices/systems, sprinkler systems, handheld fire extinguishers, fixed fire hoses, smoke detectors, temperature/humidity, HVAC, and power within the facility.

(2) **The organization provides employees with initial and *[Assignment: organization-defined frequency] training in the employment and operation of physical security controls.***

Enhancement Supplemental Guidance: Physical security controls include, for example, physical access control devices, physical intrusion alarms, monitoring and surveillance equipment, and security guards (deployment and operating procedures).

References: C.F.R. Part 5 Subpart C (5 C.F.R 930.301); NIST Special Publications 800-16, 800-50.

Priority and Baseline Allocation:

LOW: AT-3

MOD: AT-3

HIGH: AT-3

AT-3 SECURITY TRAINING

Control: The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [*Assignment: organization-defined frequency*] thereafter.

Supplemental Guidance: The organization determines the appropriate content of security training based on assigned roles and responsibilities and the specific requirements of the organization and the information systems to which personnel have authorized access. In addition, the organization provides information system managers, system and network administrators, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training to perform their assigned duties. Organizational security training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. The organization also provides the training necessary for these individuals to carry out their responsibilities related to operations security within the context of the organization's information security program. Related controls: AT-2, SA-3.





Additional Controls

Impact level	NIST Baseline Controls	Number of NIST Baseline Controls Eliminated	Additional FedRAMP Controls	Total Controls Agreed to By JAB
Low	115	12	13	116
Moderate	252	15	60	297

Areas with additional controls

Access Control (6)	Audit and Accountability (5)	Security Assessment and Authorization (1)	Configuration Management (4)
Contingency Planning (2)	Identification and Authentication (3)	Incident Response (1)	Maintenance (1)
Media Protection (1)	Risk Assessment (4)	System and Services Acquisition (4)	System and Communications Protection (11)
System and Information Integrity (1)			

Control Responsibility Options

- Single Entity has responsibility:
 - Cloud Provider 
 - Leveraging Entity 
- Both Entities have joint responsibility:
 - Cloud Provider + Leveraging Entity 
- Both Entities have individual responsibility
 - Cloud Provider 
 - Leveraging Entity 

- Cloud computing is really not that different than our current data centers
- Understanding the boundaries and who does what is critical to properly documenting controls.
- All cloud computing systems will require some training requirements.

Have fun with cloud computing..... Smile and they will wonder why.....

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

Mischel Kwon , Former Director of US-CERT

QUESTIONS?



Cloud Transition Checklist

NO, YOU WON'T NEED AN UMBRELLA.

Kloster

