FINDINGS AND RECOMMENDATION OF ATARC’S CLOUD INNOVATION LAB

JANUARY, 2016

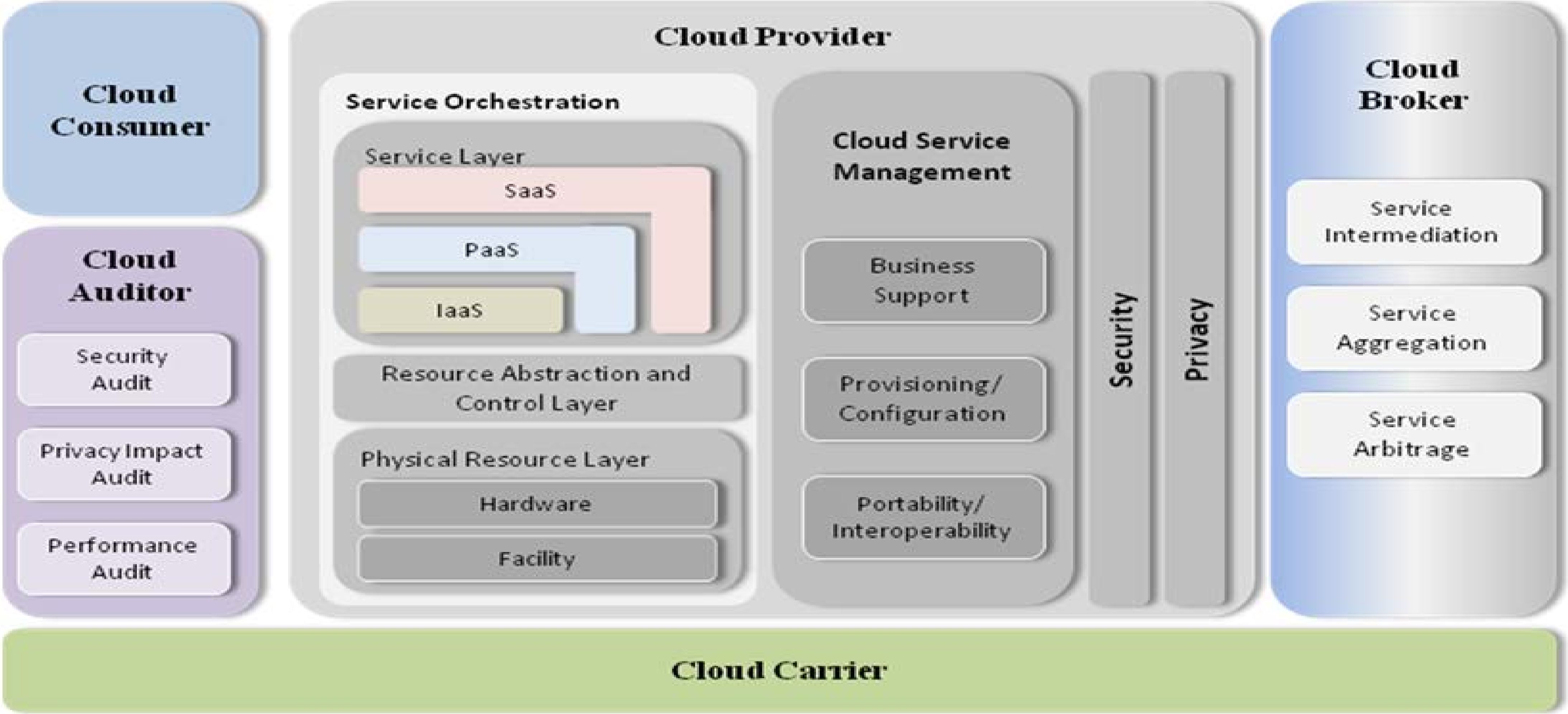
ATARC Cloud Innovation Lab

Table of Contents

- Roadmap
- Gaps and Emerging Challenges
- People and Cloud
- FedRAMP

Roadmap for Cloud Adoption

NIST Cloud Reference Model



Roadmap for Cloud Adoption

- Decision makers contemplating cloud computing adoption face a number of challenges relating to policy, technology, guidance, security, and standards.
- To achieve success in moving to the crowd leaders must address these challenges head on, while recognizing and avoiding the pitfalls that cause good ideas to fail.

Roadmap for Cloud Adoption

- Challenges
  - Moving from a CapEx to OpEx operating model
  - Cultural / Change management
  - Policies, regulations, and perceptions around security and ownership
    - FedRAMP compliance
  - Integration of cloud services in to existing infrastructure (ICAM, AD, Service Management, Change Management, SOC, etc).
    - Need both resources and innovation solutions.
  - Potential for cloud vendor lock-in

Roadmap for Cloud Adoption

- Migration Challenges
  - Anticipating cost: Reasonable cost estimates may be a challenge. Historical data indicates you cost may be higher than your most conservative estimate.
  - Documentation: No initial cloud package is 100% complete. You will have documentation challenges
  - Unanticipated discoveries: You will find configurations and processes that you have no idea what they do
  - Legacy software: You will find non-supported software that cannot be updated. You may have to change the technology.
    - Example - Solaris is not supported in the cloud.
  - Common services: Your agency common services (ICAM, FW rule sets) may not support your applications out of the box.

Roadmap for Cloud Adoption

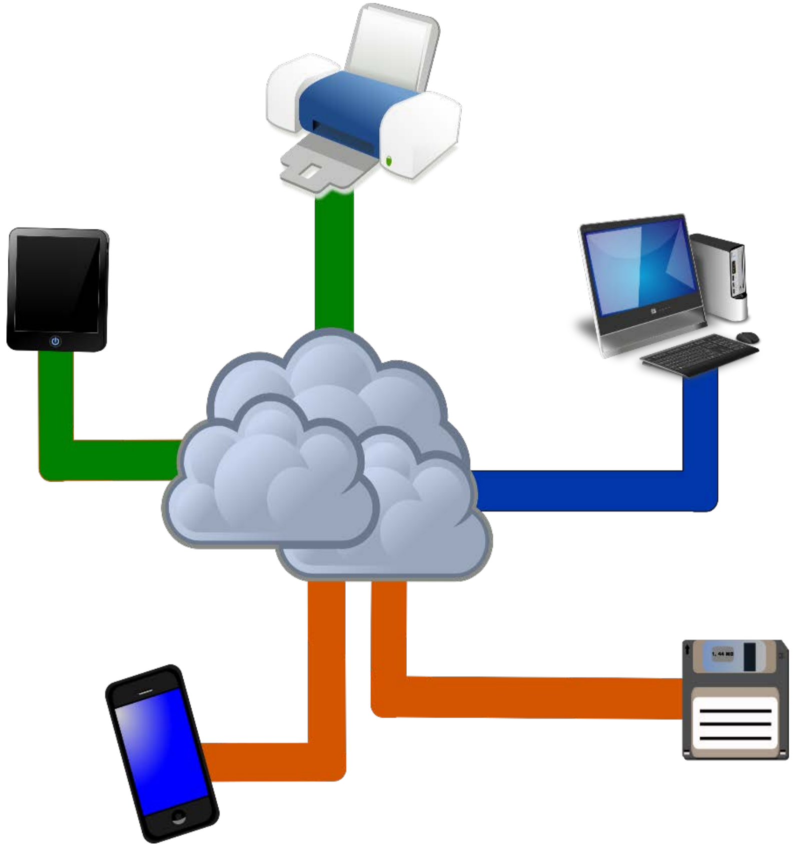
- Opportunities
  - Develop and deploy new processes, systems and offerings to make them more competitive
  - Reduce operational costs – licensing, overhead and capital investments
  - Rationalize applications
  - Improve mission delivery through more effective and agile IT

Roadmap for Cloud Adoption

- Recommendations
  - Agencies should take a phased approach to cloud migration
    - Each organization has its own threshold for risk and this determines your migration approach
    - Understand what gaps in requirements you are willing to accept
    - Not waterfall, but with all requirements up front, start with low hanging fruit and learn from it, while continually looking for ways to automate
  - Your cloud migration must be multi-dimensional, recognizing that many factors will impact the success or failure of your project

What to consider as you plan your move to cloud

- Consider these factors as you plan your move to cloud:
  - Acquisition
  - Change management
  - Scope management
  - Technology
  - Security
  - Metrics
  - Users and data



Acquisition

- **Acquisition and solution strategy**
  - Focus on being clear about your problem, without thinking about the solution (yet)
  - Document your goals and objectives in that context
  - Have a clear understanding of your desired final outcomes integrated in
- **Spend the time Developing a Strategic Roadmap first**
  - Don't default to the contractors you have –they might not have the expertise (or you probably would have solved these problems already)
  - Talk to your mission stakeholders, procurement officials, general council, and CIO
  - Create an aligned acquisition strategy that aligns to the strategic roadmap
  - Key to know what people what, what acquisition/lawyers will allow you to do, and what acquisition strategy will work for you organization.
- **Collaborate with industry**
  - Use "Market Research" as a way to have conversations
  - Educate industry before the procurement –if you want real solutions, they need to understand your real problems and desired outcomes
- **Consider enterprise-wide versus grass-roots –including values of each**
  - Enterprise-wide, shared solutions can solve multiple problems at once, but can sometimes be too hard to achieve in one step
  - Weigh using point solutions initially, leveraging internal groups that are passionate

Change Management

- **Come up with an inclusive strategy**
  - Needs to happen early, long before implementation
  - People are people –they act on emotion as much as anything else
  - Need to identify, then leverage supporters and detractors
- **Articulate the value of the changes**
  - Include stakeholders in the process
  - Find “change champions”
  - Focus on understanding what the stakeholders really want and need
- **Collect real data**
  - Existing documentation is a good, albeit often inaccurate baseline
  - Some staff could be hoarding information
  - Experts interviewing the people who have the information is the best way
  - This only works in conjunction with the people aspect of change management
- **Transition**
  - There needs to be overlap between the migration team and the support teams to ensure there is full support for a few weeks following a migration.
  - There needs to be better turnover and handoff to the support teams from the migration teams.
- ***Continuous throughout –not a one-shot deal***

Scope Management

- Collaboration: Current support and migration teams need to work collaboratively to implement an approach to accomplish the transition including performing a streamlined life cycle process.
- Budget: Contingency budget and schedule need to be factored into task orders with hard end dates to ensure those dates can be met if the scope of the task order should change based on due diligence after a task order is awarded.
- Schedule: The schedule must have time allotted for meeting with application and site owners to ensure complete information about the environments is captured in due diligence and common expectations are agreed to.
  - Create a base template schedule for migrations that include the following:
    - Set time for Due Diligence
    - Set time for meeting with application and site owners.
    - Migration design with the application and site owners to ensure the migration process will work with their applications and sites.
    - Ensure there is resource time reserved for both current support and migration teams to perform the necessary due diligence and migration approach design.

Technology

- Cloud is the driver, but remember it’s not all about cloud
- Shared platforms: Consider shared platforms as “offerings”
  - Directory management
  - Orchestration and provisioning
  - Brokering
  - Continuous monitoring
- Cloud is just one piece of the puzzle. Other things to consider include:
  - Mobile – Responsive Design – Content Management Systems – Portals – APIs
  - Application Platforms – Integration – Custom Development – Open Source -

Security

- **Consider security at the front-end**
  - Security should be considered as part of requirements
  - Data security, operational security, physical security
  - System should be built, integrated, and tested with security always a part
- **Determine Categorization for Confidentiality, Integrity, Availability**
- **Application Security/ Platform Security**
  - Use FEDRAMP and FISMA or equivalent
  - Still needed, even with FedRAMP
  - Delta between application and Infrastructure
  - Ensure Platform providers are truly secure – segmented, cleared access is critical
- **Security knowledge is not enough**
  - Need expertise in cloud security and cloud architecture
  - CCSK, CSSP, Cloud Security Alliance, etc.

Security (cont.)

- Conduct initial security evaluation of all internal and external dependencies
- Ensure security policies line up with the environment to which they are migrating
- Recommendations
  - Create a security interview process to include specific details on the application. Example- mapping out those dependencies and determining why and if they are needed.
  - Revalidated the classification of the data
  - Have a comprehensive change management process in place to include security review, back out procedures, communications plan, technical goals and objectives, expected downtime, testing plan and 508 compliance and security scans (static and transactional). Tools used in the cloud may be different than what are appropriate in data center.
  - Have a consistent SSL certificate management strategy
    - Certificates need to be managed and tracked appropriately. Key information needs to be maintained with certificates.
    - Individual/Singular certificates are difficult to track and manage.
    - Invest in certificate blocks, and replace certificates with new certificates when sites move to ensure all certificates have the same expiration and are all managed under the same certificate umbrella.

Metrics

- **Measurement should be part of your strategy**
  - Determine what to measure
  - Determine how often to measure (each metric)
  - Objective data helps with change management
- **Make sure metrics and messaging are targeted**
- **Establish a measurement baseline**
  - Measure those things you want to improve
  - Measure those things you are changing
  - Helps with understanding not just what, but how to measure
- **Put a governance structure in place to regularly review metrics**
  - Establish a "dashboard"
  - Review with a governance group
  - Ongoing measurement and analysis –how are we doing? Do we need more measurements?
- **Measurement and Analysis makes it easy to achieve, and to determine success**
  - Each phase may have different metrics

Users and Data

- **Everyone's users are different therefore you can't just go by what someone else did**
- **Users are the core of the "why" and "what" needs to be done–from the *data* to the *technologies***
- **Review the strategic goals of the agency, and build towards the strategic direction**
- **Your information could be getting to users via other systems**
- **Usability testing can be invaluable**
  - Understand IA, wording, design challenges, top tasks
  - Search data can be valuable
  - 508 compliance is very important and starts at the beginning
- **Once all this information is gathered, the "how" naturally results**
  - Technology is there just as a tool, not as a driver

USER

+

DATA

=

TECHNOLOGY

Candidates for Cloud

An application is a good candidate for cloud if it:

- Is in environments that do not leverage the cost and agility of real cloud capabilities
- Is an expiring contract
- Is at end of lifecycle
- Is a new website or application that should be designed and optimized for the cloud
- Requires up and down scaling to support variable processing requirements
- Relies on manually maintained web content as opposed to using intuitive web content management via Drupal or WordPress which puts content creation in the hands of the business owners
- Leverages agile development or DevOps
- Is a FISMA Low/Moderate websites/applications
- Needs to be brought up to security, privacy and Section 508 compliance standards
- Has performance issues and needs to be re-architected

Gaps and Emerging Challenges

Understanding Gaps and Emerging Challenges

To be successful agency leadership, CIOs and IT managers needs to understand where gaps and emerging challenges exist and manage to minimize the impact. Look out for:

- Gaps in expectation
  - Leadership. compliance, value, requirements
- Gaps in Understanding & Learning
  - Roles, Responsibilities, Services, Capabilities, Risk Ownership
- Gaps in Governance & Compliance
  - Security, Architecture, Services, Usage, Sprawl, Shadow IT

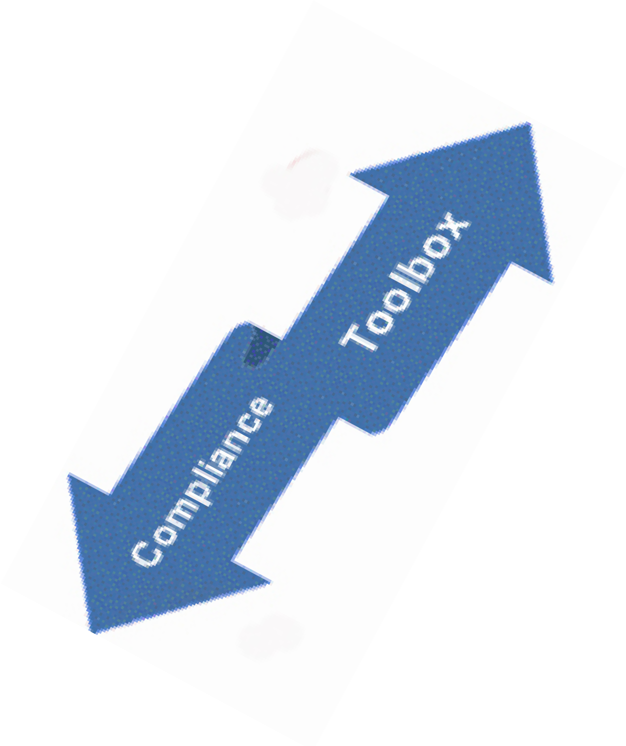
Gaps in Expectation

- **Leadership vs. agency managers**
  - Cloud Services & Capabilities
  - Reality vs Expectations
- **Compliance**
  - Security (Dept./Agency, FedRAMP, NIST 800-53r4)
  - Access Management (Shared Responsibility), Visibility of Controls (CDM/ISCM), Incident Response (Consumer vs Provider/Broker Roles)
- **Value**
  - Consumption and License cost (metered, usage based, vs. yearly)
  - Short term (time to market) vs. long term
  - What works now vs. how it is being used
- **Defined Requirements**
  - DC vs. cloud (performance)
  - Technology (H/w and virtual and Services)
  - Current needs vs. perceived long term needs

Gaps in Understanding & Learning

- Rapid change in technology marketplace
  - Resource challenges (consumer & supplier)
  - Niche products that cannot have broad test coverage
  - Traditional technologies that become “virtualized” or “cloud-ready” do not have all features or performance
  - Integrated testing is now an end-user task vs. a supplier task
- Roles and Responsibilities
  - Shared responsibility across provider, broker, consumer, tenant
- Organization’s IT policy do not align to cloud computing
  - Shared responsibility for security, compliance, incident response; ICAM, change and configuration management
- How do you keep up?
  - Understand how to do the assessment and see if you can actually operationalize.

Gaps in Governance and Compliance



- GRC frameworks and D/A Policies do not account for shared responsibilities
- Limitations in FISMA inventory management, controls management and POA&M management make it difficult to align D/A systems with FedRAMP systems
- Ongoing authorization and CDM/ISCM integration and report for cloud provider systems do not align with D/A OA and CDM/ISCM schedules or tools
- Ensuring that an agency-wide reference model has been established for consumption of cloud services
- Defined policies and SOPs for legacy approach, need to be updated/refined/fixed to address cloud
- Knowledge of risk management including minimizing legal and compliance issues
- ITIL methodology vs. cloud frameworks

Addressing Gaps and Emerging Challenges

To address all gaps, it starts with a common understanding and establish context as to how the D/A intends to use cloud

- Context: Not all cloud providers are created equal
  - Deployment models have impact on risk/trust, data types that can be housed/used
  - Differences exist between providers, service models and differences w/in service models
    - Distinctions/differences between IaaS, PaaS, SaaS may require different approaches: Example: SaaS - may need a DLP/Encryption GW
    - Usage Context: Determine users, where they are coming from, are they trusted, are their networks/devices trusted, what type of data are they interacting with, how are they interacting with that data
      - Informs decisions selecting Deployment Models (Public, Private, Community/FedRAMP), Service Models (IaaS, SaaS, PaaS), and the controls, compliance and governance needs
- Understanding & Learning: Education and Marketing Campaigns
- Governance & Compliance: SLAs, Security, Legal, contextual understanding (mission consumer, program
- Expectations: Setting and Managing
- Acquisition: Draw down accounts, options, etc

Intersection of People and Cloud

What’s driving organizational change

Democratization of IT:

- Cloud is here. It’s in every agency and being used today (average # of cloud services per agency? >1,000)
- Lack of tools to control Shadow IT
- Lack of visibility from IT into actual cloud usage
- Users bringing consumer behaviors to the workplace (e.g., use of Facebook, LinkedIn, Twitter, Slack, Evernote, Gmail and so on)
- Many users leveraging cloud for legitimate business use case while unaware of potential security risks they are posing

Resistance to change?

ORGANIZATIONAL BARRIERS:

- **Culture**: Where are decisions made within the organization? Is change embraced within the organization?
- **Awareness**: How do my mission needs align with various cloud service offerings? How are these systems secured?
- **Business Value**: Does it make sense to move my legacy systems to the cloud? What capabilities would benefit from moving to the cloud? What is my return on investment? We are in a new phase of market penetration, development and demand.

Defining Success

- **Identify the "Why":** How does cloud adoption further the agency's mission and vision: information sharing, data security and availability, cost reduction, increased productivity, etc.
- **Identify the "Fit":** How are decisions made within an Agency? Which levels and offices within the organization are involved in making the decision to move applications to and host data in the cloud? Security, IT, Users, Managers, Execs, Budget, Procurement/Purchasing
- **Identify the "Objectives"**: Cost reduction, user-experience, productivity, data / system availability, data integrity, system security, ease of purchase, job security, work-load, etc.
- **Identify the "Redundancy":** How do the functional area objectives converge and where do they conflict? Do these functional areas interact? If so, how and to what extent?
- **Identify the "Methods"**: What are the methods/ways to recognize organizations for embracing and implementing cloud? Internal and external?
- **Define "Success":** What metrics equate to success for their employees? Constituents? Partners?

FedRAMP’s Role in Cloud Adoption

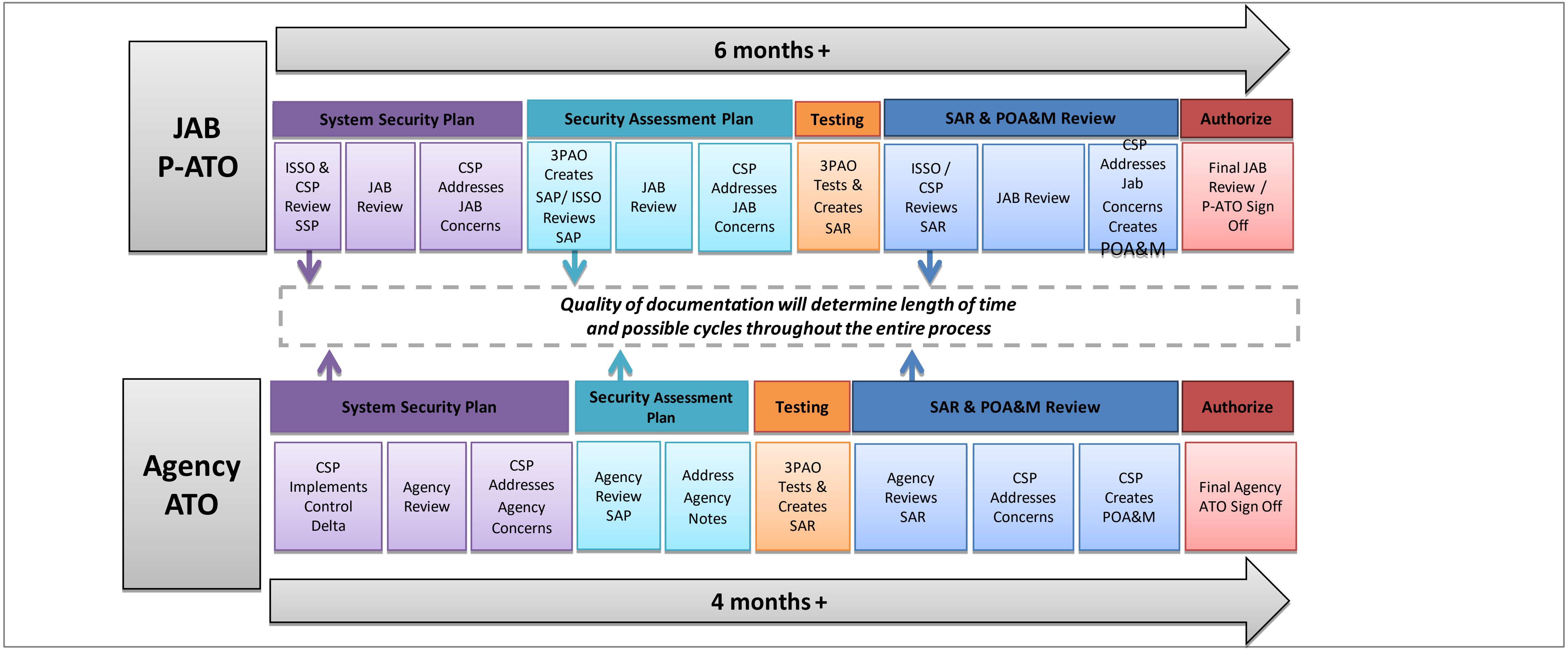
What is FedRAMP?

- FedRAMP - Federal Risk and Authorization Management Program
- Assess and authorize cloud computing products and services
- Based on FISMA standard 800-53
- Agencies use the FedRAMP review results to grant an Authorization to Operate (ATO)
- ATOs required for all systems at implementation or after significant changes to the system

FedRAMP 101

- **Cloud Service Provider initiates FedRAMP review**
  - Understand and document compliance with FedRAMP standards – documentation is key
  - Determine who will conduct review – Agency or JAB
  - Contract with an authorized Third Party Assessor (3PAO)
  - Establish relationship with FedRAMP Office
- **3PAO**
  - Conducts independent assessment of CSP submissions and reports to reviewer
- **Agency**
  - ATO can be granted ONLY by Agency SISO
  - Enforces continuous monitoring and ATO renewals
- **GSA**
  - Conducts CSP provided FedRAMP review

FedRAMP and Agency ATO Process and Notional Timeline



JAB P-ATO

6 months +

System Security Plan
- ISSO & CSP Review SSP
- JAB Review
- CSP Addresses JAB Concerns

Security Assessment Plan
- 3PAO Creates SAP/ ISSO Reviews SAP
- JAB Review
- CSP Addresses JAB Concerns

Testing
- 3PAO Tests & Creates SAR

SAR & POA&M Review
- ISSO / CSP Reviews SAR
- JAB Review
- CSP Addresses Jab Concerns Creates POA&M

Authorize
- Final JAB Review / P-ATO Sign Off

Quality of documentation will determine length of time and possible cycles throughout the entire process

Agency ATO

System Security Plan
- CSP Implements Control Delta
- Agency Review
- CSP Addresses Agency Concerns

Security Assessment Plan
- Agency Review SAP
- Address Agency Notes

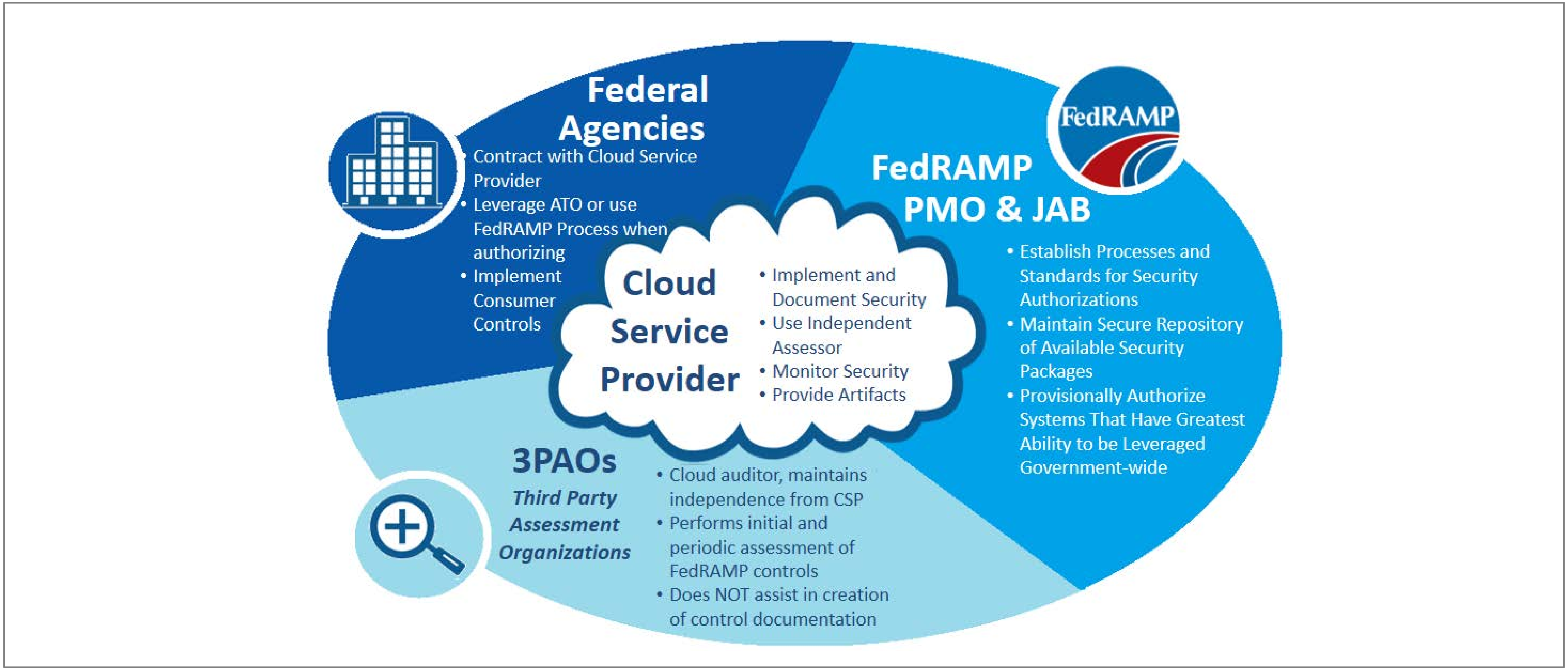
Testing
- 3PAO Tests & Creates SAR

SAR & POA&M Review
- Agency Reviews SAR
- CSP Addresses Concerns
- CSP Creates POA&M

Authorize
- Final Agency ATO Sign Off

4 months +

Who’s Involved



Federal Agencies

- Contract with Cloud Service Provider
- Leverage ATO or use FedRAMP Process when authorizing
- Implement Consumer Controls

FedRAMP PMO & JAB

- Establish Processes and Standards for Security Authorizations
- Maintain Secure Repository of Available Security Packages
- Provisionally Authorize Systems That Have Greatest Ability to be Leveraged Government-wide

Cloud Service Provider

- Implement and Document Security
- Use Independent Assessor
- Monitor Security
- Provide Artifacts

3PAOs

Third Party Assessment Organizations

- Cloud auditor, maintains independence from CSP
- Performs initial and periodic assessment of FedRAMP controls
- Does NOT assist in creation of control documentation

New Processes Implemented August 2015

- Continuous Monitoring
  - FedRAMP P-ATO Management and Revocation Guidance: Escalation processes and procedures as well as minimum mandatory escalation actions FedRAMP will take when a CSP fails to adhere to the requirements of the PATO.
  - Rev 4 Transition Guidance: The FedRAMP Joint Authorization Board updated the FedRAMP security controls baseline to align with the updated NIST SP 800-53 security controls as revised in Revision 4. The FedRAMP program management office (PMO) updated the FedRAMP security control baseline documentation and templates to reflect these changes.

Improving Initial CSP Submissions

- Quality Management
  - Ensure SSP + Attachments, SAP, SAR go through internal quality management processes.
    - See General Document Acceptance Criteria – FedRAMP.gov
- Content Management
  - Ensure system boundary is well-defined
    - What is in the boundary, what is excluded from the boundary.
  - Critical controls/”showstoppers” are in place and documented within SSP
    - Multi-Factor, Incident Response, Change Management, Contingency Planning, Self-Provisioning Portal, FIPS 140-2, etc.
  - Adhere to “FedRAMP SSP/SAP/SAR Initial Review Checklists”
    - Checklists located on FedRAMP.gov

Challenges and Mitigation Strategies

- **Process is confusing**
  - Visit fedramp.gov - has the best instructions including templates, weekly tips, monthly newsletter, schedule of presentations, training sessions
  - Ask questions before starting the submission process – fedramp.gov
  - Give Program suggestions about how to improve information dissemination

- **Must use FedRAMP not ISO or other audit frameworks**
  - FISMA is a law that the government is required to follow
  - Use experience with other frameworks to gage time/effort to do FedRAMP

Challenges and Mitigation Strategies, continued

- **Agencies require FedRAMP certification in order to bid**
  - Remind agencies that this is not a valid requirement
  - Agencies can require effort to obtain FedRAMP-based ATO
  - Report this to FedRAMP Office
  - New acquisition guidelines to be issued with OFPP in October 2015
- **Agencies not reusing ATOs**
  - Remind agency that this is a requirement of FedRAMP
  - Determine source of resistance
  - Talk to FedRAMP Office
  - Refer agency to *Agency Guide for FedRAMP Authorizations*
- **Agencies relying on ATOs conducted by JAB**
  - Agencies not conducting their own ATOs - cost and convenience

Success Factors

Preparation

- **Understand how to work with the government – keep up a dialogue with FedRAMP Office**
- **Understand NIST 800-53 requirements and how they apply to the cloud system**
- **Schedule a pre-meeting with FedRAMP Office – common issues include:**
  - Multi-factor authentication
  - FIPS 140-2 encryption standards wherever encryption is needed
  - What shared and corporate services are within the boundary
  - Clearly defined assets and hardware inventory
  - Mature patch management processes

Resources

- Invest in a security team
- Documentation and Testing usually require multiple meetings/versions before moving onto the next stage
- Appoint a lead for the FedRAMP process

Patience

- Realize that this is a process