FedRAMP  
Federal Risk and Authorization Management Program  

Federal Computer Security Program Managers’ Forum  

Claudio Belloli  
FedRAMP Information Systems Security Manager  
GSA  

August 19, 2014
## FedRAMP: A brief history

<table>
<thead>
<tr>
<th>Year</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb 2010</td>
<td>Kundra Announces FedRAMP Security Working Group concept announced</td>
</tr>
<tr>
<td>Nov 2010</td>
<td>3PAO Concept Planned</td>
</tr>
<tr>
<td>Jul-Sep 2011</td>
<td>Tiger Teams Convene</td>
</tr>
<tr>
<td>Dec 2010</td>
<td>JAB Drafts Baseline</td>
</tr>
<tr>
<td>Jan 2011</td>
<td>3PAO Public Draft Released</td>
</tr>
<tr>
<td>Jun 2011</td>
<td>JAB Finalizes Baseline</td>
</tr>
<tr>
<td>Feb 2012</td>
<td>CONOPS published</td>
</tr>
<tr>
<td>May 2012</td>
<td>First Agency Authorization</td>
</tr>
<tr>
<td>Jun 2012</td>
<td>FedRAMP Launches</td>
</tr>
<tr>
<td>Dec 2012</td>
<td>OMB Releases Policy Memo</td>
</tr>
<tr>
<td>Jun 2014</td>
<td>Two-Year FedRAMP Operational Anniversary</td>
</tr>
</tbody>
</table>

- **Feb 2010**: Kundra Announces FedRAMP Security Working Group concept announced
- **Nov 2010**: 3PAO Concept Planned
- **Jul-Sep 2011**: Tiger Teams Convene
- **Dec 2010**: JAB Drafts Baseline
- **Jan 2011**: 3PAO Public Draft Released
- **Jun 2011**: JAB Finalizes Baseline
- **Feb 2012**: CONOPS published
- **May 2012**: First Agency Authorization
- **Jun 2012**: FedRAMP Launches
- **Dec 2012**: OMB Releases Policy Memo
- **Jun 2014**: Two-Year FedRAMP Operational Anniversary

- **Feb 2010**: Kundra Announces FedRAMP Security Working Group concept announced
- **Nov 2010**: 3PAO Concept Planned
- **Jul-Sep 2011**: Tiger Teams Convene
- **Dec 2010**: JAB Drafts Baseline
- **Jan 2011**: 3PAO Public Draft Released
- **Jun 2011**: JAB Finalizes Baseline
- **Feb 2012**: CONOPS published
- **May 2012**: First Agency Authorization
- **Jun 2012**: FedRAMP Launches
- **Dec 2012**: OMB Releases Policy Memo
- **Jun 2014**: Two-Year FedRAMP Operational Anniversary
FedRAMP is in Full Operations

- Repeatable processes for continuous monitoring activities
- Agency outreach
- Additional access controls in the secure repository
- Agency ATO’s accessible and leveraged by other agencies
- Guide to FedRAMP updated to reflect lessons learned in IOC
- Manual dashboards in use for internal, JAB and other stakeholder reporting
- Privatization of 3PAO Accreditation
  - A2LA selected as the accreditation body
FedRAMP Key Stakeholders & Responsibilities

**Federal Agencies**
- Contract with Cloud Service Provider
- Leverage ATO or use FedRAMP process when authorizing
- Implement consumer controls

**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

**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
Agency Responsibilities

• As of June 5, 2014, all cloud projects must meet the FedRAMP requirements when initiating, reviewing, granting, and revoking security authorizations
  – Use of FedRAMP security controls baseline
  – Use of mandatory templates
  – Provide FedRAMP PMO with ATO letters
  – Use FedRAMP repository for all ATOs where re-use is possible

• Agencies must enforce FedRAMP via contractual provisions
  – Template contract language available on FedRAMP.gov
  – Includes generic security section as well as control specific contract clauses

• Agencies must report to OMB via PortfolioStat cloud services that cannot meet FedRAMP requirements
FedRAMP Relationship to the NIST Risk Management Framework

1. **Categorize the Information System**
   - Low Impact
   - Moderate Impact

2. **Select the Controls**
   - FedRAMP Low or Moderate Baseline

3. **Implement Security Controls**
   - Use of an Independent Assessor (3PAO)

4. **Assess the Security Controls**
   - Describe in SSP

5. **Authorize Information System**
   - Provisional ATO
   - Agency ATO

6. **Monitor Security Controls**
   - Continuous Monitoring
FedRAMP Security Assessment Framework (SAF) and NIST Risk Management Framework
Timeline for the SAF

- **Document**
  - SSP
  - NIST RMF 1, 2, 3

- **Assess**
  - SAP
  - Testing
  - NIST RMF 4

- **Authorize**
  - SAR
  - POAM
  - NIST RMF 5

- **Monitor**
  - ConMon Reports
  - NIST RMF 6

- **JAB P-ATOs**
- **Agency ATOs**
- **CSP Supplied**

- **Timeframes**
  - ~6 wks
  - 4+ mos
  - 9+ mos
### SAF Process Area: Document

#### System Security Plan

<table>
<thead>
<tr>
<th>Categorize the Information System</th>
<th>Select the Security Controls</th>
<th>Implement the Security Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>- NIST RMF Step 1</td>
<td>- NIST RMF Step 2</td>
<td>- NIST RMF Step 3</td>
</tr>
<tr>
<td>- Determine impact level by using the FIPS 199 Form</td>
<td>- Use the FedRAMP low or moderate baseline security controls</td>
<td>- Use FedRAMP templates</td>
</tr>
<tr>
<td>- FedRAMP only supports Low and Moderate impact levels</td>
<td>- 125 controls for low</td>
<td>- Templates include considerations specific to cloud implementations</td>
</tr>
<tr>
<td></td>
<td>- 325 for moderate</td>
<td>- Implementation guidance in Guide to Understanding FedRAMP</td>
</tr>
</tbody>
</table>

FedRAMP only supports Low and Moderate impact levels.

FedRAMP templates include considerations specific to cloud implementations.

Implementation guidance in Guide to Understanding FedRAMP.
Assess the Security Controls

- NIST RMF Step 4
- Independent Assessors must be used
- FedRAMP accredits independent assessors through the 3PAO accreditation program
- Highly encourage all agencies to use accredited 3PAOs for FedRAMP assessments
- Use FedRAMP SAP template
- FedRAMP tailored test cases
- Create unique test cases for any CSP alternative implementations
Authorize

<table>
<thead>
<tr>
<th>Security Assessment Report</th>
<th>Plan of Action and Milestones (POA&amp;M)</th>
</tr>
</thead>
</table>

Authorize the Information System

- NIST RMF Step 5
- Independent Assessors provide a SAR detailing risks of the system
- CSP must create POA&M which determines timeline for remediation and/or mitigations of each risk identified in the SAR
- Authorizing official makes a risk based decision for authorization of CSP
- If CSP has risk posture that is acceptable, agencies will still have certain responsibilities for the authorization (e.g. multi-factor authentication, access control, TIC, etc.)
- Two types of authorizations: JAB Provisional ATOs and Agency ATOs
- CSP supplied packages will NOT have an authorization, but WILL have a SAR and POA&M
SAF Process Area: Monitor

Continuous Monitoring

Monitor Security Controls

- NIST RMF Step 6
- Risk Management Framework with cloud gets away from a “point in time” approach to security authorizations
- 3 key steps: Operational Visibility, Change Control, and Incident Response
- FedRAMP Continuous Monitoring Strategy and Guide defines the process for CSPs to meet continuous monitoring requirements through periodic reporting, making plans for changes to the system, and how to respond appropriately to incidents that may occur within a CSP system once authorized
# Overview: FedRAMP SAF Standardizes RMF for Cloud

<table>
<thead>
<tr>
<th>FedRAMP SAF Process</th>
<th>NIST SP 800-37 Step</th>
<th>FedRAMP Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Document</strong></td>
<td>1. Categorize System</td>
<td>Low and Moderate Impact Levels</td>
</tr>
<tr>
<td></td>
<td>2. Select Controls</td>
<td>Control Baselines for Low and Moderate Impact Levels</td>
</tr>
<tr>
<td><strong>Assess</strong></td>
<td>4. Assess the Security Controls</td>
<td>FedRAMP accredits 3PAOs 3PAOs use standard process and templates</td>
</tr>
<tr>
<td><strong>Authorize</strong></td>
<td>5. Authorize the System</td>
<td>ATOs with JAB P-ATO or Agency ATO CSP Supplied packages</td>
</tr>
<tr>
<td><strong>Monitor</strong></td>
<td>6. Continuous Monitoring</td>
<td>Use Continuous Monitoring Strategy and Guide</td>
</tr>
</tbody>
</table>
FedRAMP Authorization Paths

**JAB Provisional Authorization (P-ATO)**
- Prioritizes authorizing cloud services that will be widely used across government
- CIOs of DoD, DHS and GSA must agree that the CSP:
  - Strictly meets all the controls
  - Presents an acceptable risk posture for use across the federal government
- Conveys a baseline level of likely acceptability for government-wide use
- CSPs must use an accredited Third Party Assessor Organization (3PAO)
- FedRAMP PMO manages continuous monitoring activities; agencies review results

**Agency ATO**
- Issued by the agency only
- Agencies have varying levels of risk acceptance
- Agency monitors the CSPs continuous monitoring activities
- Option to use a 3PAO or independent assessor to perform independent testing

**CSP Supplied**
- Submitted directly by CSP to FedRAMP
- CSP without ATO
- CSP must use an accredited 3PAO
Authorization Process – JAB and Agencies

**JAB P-ATO**
- **System Security Plan**: ISSO & CSP Review SSP
- **CSP Addresses JAB Concerns**
- **Security Assessment Plan**: 3PAO Creates SAP/ISSO Reviews SAP
- **JAB Review**
- **Testing**: CSP Addresses JAB Concerns
- **3PAO Tests & Creates SAR**
- **SAR & POA&M Review**: ISSO / CSP Reviews SAR
- **Authorize**: CSP Addresses Jab Concerns Creates POA&M
- **Final JAB Review / P-ATO Sign Off**

**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

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

4 months +

6 months +
Authorization Progress to Date

JAB Provisional Authorizations
- 12 cloud services approved
- FedRAMP authorizations cover 250+ government contracts
- Agencies expected to update ATO memos for these services

Agency issued ATOs
- 5 cloud services authorized by agencies

FedRAMP Pipeline
- 25 cloud services in process for JAB Provisional or Agency Authorization
- 8 cloud services awaiting kick-off

FedRAMP Cost Savings
- $40 million in cost savings based on known FISMA reporting
Available P-ATOs and Agency ATOs

- Autonomic Resources (IaaS)
- CGI Federal (IaaS)
- AT&T StaaS (IaaS)
- Akamai CDN (IaaS)
- HP ECS-VPC (IaaS)
- Lockheed Martin SolaS-I (IaaS)
- Microsoft GFS (IaaS)
- Microsoft Azure (PaaS)
- IBM (PaaS)
- Oracle FMCS (PaaS)
- Economic Systems FHR Navigator (SaaS)
- CTC URHD (SaaS)
- Amazon US East West (IaaS)
- USDA (NITC) (IaaS)
- MicroPact Product Suite (PaaS)
- Salesforce (PaaS, SaaS)
- Amazon GovCloud (IaaS)
- MicroPact eCase (SaaS)
- AINS (PaaS, SaaS)
June Deadline and PortfolioStat

June 2014
- All CSPs used by Federal agencies need to meet FedRAMP requirements
  - Baseline security controls, independent assessment, use templates, make documentation available in the repository for leveraging
- Agencies must enforce FedRAMP with cloud providers via contracts

PortfolioStat Reporting
- New questions regarding FedRAMP
- Agencies must rationalize lack of FedRAMP compliance
- Agencies must identify plans to meet FedRAMP requirements

PortfolioStat Analysis
- PMO reviews PortfolioStat reporting by agencies
- Compare with other data points
- Provide OMB with analysis for Agency PortfolioStat session
FedRAMP Security Controls Baseline Update

Security Controls Baseline Update

- Extensive public comment period
- PMO and JAB reviews

FedRAMP Baseline

<table>
<thead>
<tr>
<th>Category of Changes</th>
<th># Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revision 3 Baseline</td>
<td>298</td>
</tr>
<tr>
<td>Withdrawn by NIST from Previous FedRAMP Baseline</td>
<td>(41)</td>
</tr>
<tr>
<td>Removed by Analysis FedRAMP Baseline</td>
<td>(8)</td>
</tr>
<tr>
<td>Not Selected in Rev. 4</td>
<td>(4)</td>
</tr>
<tr>
<td>Carryover Controls</td>
<td>245</td>
</tr>
<tr>
<td>Added by NIST</td>
<td>39</td>
</tr>
<tr>
<td>Added by analysis</td>
<td>41</td>
</tr>
<tr>
<td>Revision 4 Baseline</td>
<td>325</td>
</tr>
</tbody>
</table>
NIST SP 800-53 Rev 4 Update Overview

• Rev. 4 Documentation Update Effort
  – 15 total documents to be released
  – Updates affected 13 core FedRAMP templates and documents
  – Creation of 2 additional documents
  – Approximately 1250 pages of edits
  – 3000+ hours of work to complete

• Major Overhauls and New Documentation
  – CONOPS updated to FedRAMP Security Assessment Framework
  – Guide to Understanding FedRAMP including new lessons learned
  – Creation of test cases for 80 new controls due to NIST not updating test cases for 800-53 Revision 4
NIST SP 800-53 Rev 4 Templates

- All FedRAMP Rev-4 documents and template updates released on June 6, 2014
- PMO will follow NIST style of public comment period on documentation
- PMO will have periodic updates to documentation available for public comment periods with advance notice published on www.fedramp.gov

PMO is always open to suggestions for new formats, problems with documents, or other feedback on templates
## Transition Plan
- CSPs divided into 3 categories

### Detailed Transition Plan for CSPs
- Overview of controls selected for annual assessment
  - New controls (80)
  - Core controls (~40)
  - Controls selection based on risk management approach

### Overall level of effort:
- Normal annual assessment 100-120 controls
- Rev 4 transition ~150 controls

<table>
<thead>
<tr>
<th>Transition Timeframes</th>
<th>Initiation</th>
<th>In Process</th>
<th>Continuous Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Must use new requirements for authorization</td>
<td>Must update at first annual assessment</td>
<td>Must update at annual assessment – at least 6 months to plan</td>
</tr>
</tbody>
</table>
• CSPs in the in-process and continuous monitoring stages have to update to new baseline during annual assessment
  – Providers must implement new controls
• Documentation (SSP and supporting documents) must be updated using the new templates to indicate implementation of Rev 4 controls
  – Testing will be around 140/150 controls
    – Annual core controls
    – New Controls
    – Delta of Controls needed to be assessed due to changes to system
Authorization

- Tailoring of test cases is critical for unique architectural design
- Information security is a business issue
  - Technology is easy; business processes and procedures, guidelines and practices are what makes security work
- A risk is not mitigated because “it’s believed” a service is only available internally

Continuous Monitoring

- Same tools used for testing and on-going continuous monitoring
- Locking down the system critical to successful testing
- Planning significant change in advance
- Alignment of scanning, patching and testing schedules
Lessons Learned

CSP readiness tied to a number of factors

• Size of CSP infrastructure, alternate implementations, vulnerabilities or risks identified, type of service offering(s)
• Alignment of corporate business strategy to sell cloud services to the government
• Processes and procedures
• Able to address controls in preparation check list
  – Section 5.1 of the Guide to Understanding FedRAMP
Future: Increased Agency ATOs, Working Groups

Agency ATOs

- CSPs and agencies need to work together to initiate and grant authorizations
- CSPs need to analyze customer base
- Agency path best suited for majority of CSPs

Working Groups

- PortfolioStat reporting identified FedRAMP POCs
- Assist in cross-agency authorizations
- Increase guidance and address common issues
- Give platform for CSPs to reach out to agencies
Impact of FedRAMP

**Enables Cloud Security**

- Successfully proven the U.S. government can securely use all types of cloud computing
- Created a standards based approach to security through risk management
- Implements continuous diagnostics and mitigation (CDM) for cloud
  - On-going visibility into CSP risk posture
  - Trend analysis of vulnerabilities and incidents
- Establishing a new marketplace for cloud vendors

**Accelerates USG adoption of Cloud Computing**

- Enables agencies achieve cost savings and efficiency through cloud computing
- Accelerates time to market for cloud services when authorizations re-used
  - DOI leveraged 6 authorizations and conservatively estimates a cost savings of 50% per authorization
  - HHS estimates cost savings at over $1M for their authorization and leveraging of Amazon alone

**Ahead of the Curve**

- Commercial industry is looking to FedRAMP as a model for building standards based security for cloud services
- Other countries are also looking to FedRAMP for their security frameworks
Questions and Answers
For more information, please contact us or visit us the following website:

www.FedRAMP.gov
Email: info@fedramp.gov

Follow us on @ FederalCloud