

# Federal Risk and Authorization Management Program (FedRAMP)

## FedRAMP 3PAOs: Technical Requirements

Arnold Johnson

Senior IT Security Specialist

National Institute of Standards & Technology





- **Technical Requirements**
- **Demonstration of Technical Capability**

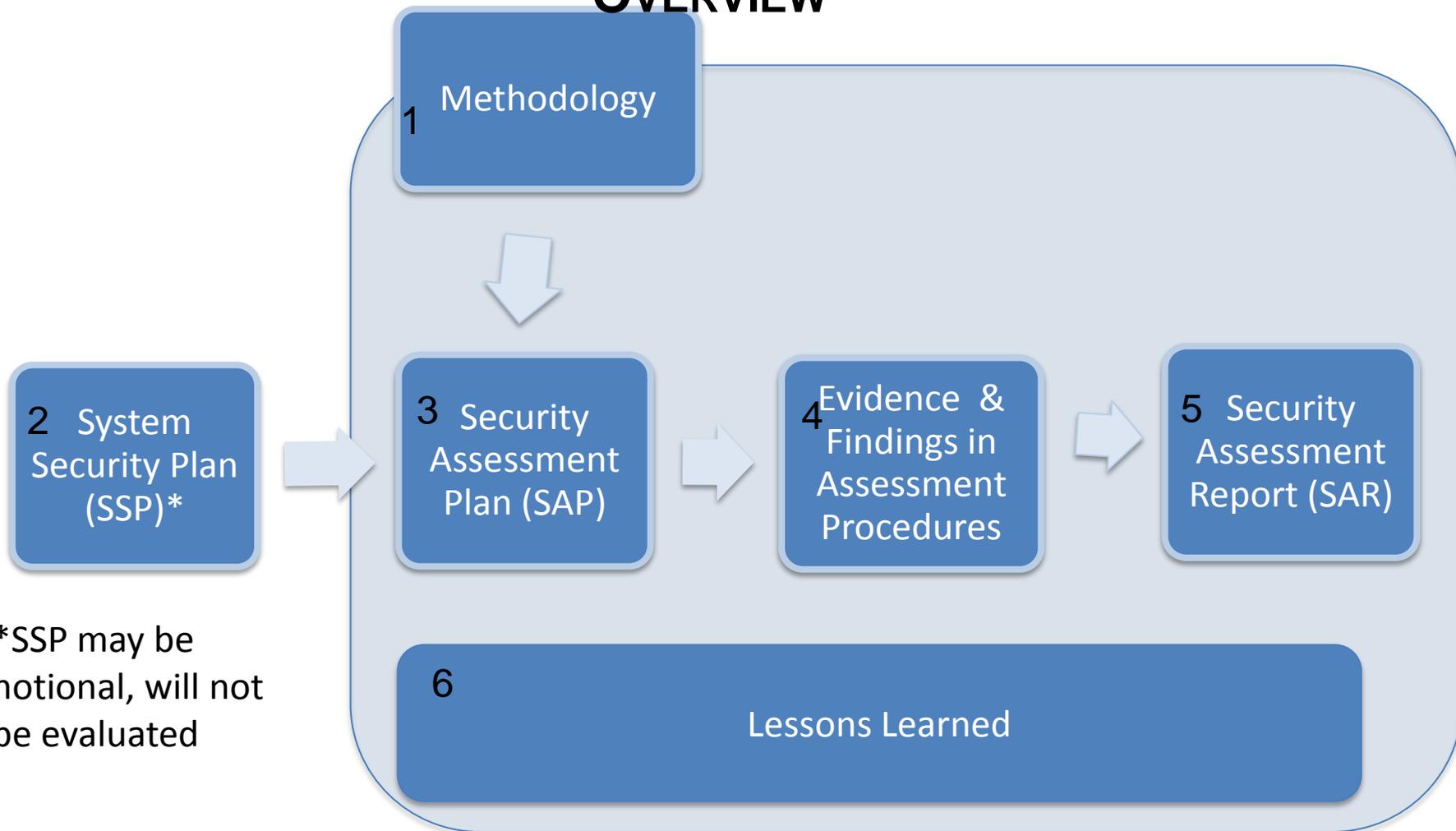




## 3PAO Technical Requirements – Part 2

- Prepare Security Assessment Plan (SAP) for each assessment consistent with program requirements
- Review assessment plan with CSP
  - Appropriate for the computing environment
- Conduct security assessment following SAP
- Prepare Security Assessment Report (SAR) consistent with FedRAMP program requirements

## OVERVIEW





## 1. Methodology

- Cross Reference to Applicant's Quality System
- Explain how program requirements and supporting NIST concepts and principles integrated into applicants quality system
- Describe applicant's methodologies used in security assessment of cloud-based information system technologies and practices
- Describe applicant's process to generate Security Assessment Plan
  - Exemplified in SP 800-53A (starting point)
  - Cloud service model (IaaS / PaaS / SaaS) considerations
  - Cloud deployment model (Public/Private/Hybrid/Community)



## 2. System Security Plan (SSP)

- Sample System Security Plan
  - FedRAMP SSP Template
    - Abbreviated template provided for applicant
  - Applicant selected cloud-based system
    - Previously assessed
    - Equivalent experimental system
  - Applicant selected
    - Service model -- (SaaS)
    - Deployment model -- Applicant's choice
  - Moderate impact
  - Security controls: AC-2, AC-17, AU-2, CM-6, CP-9, IR-4, RA-5, SC-9, SI-2
  - Capable of fully implementing controls
  - Sufficient detail to enable complete SAP (e.g., technologies)

SSP may be notional, will not be evaluated



## 3. Security Assessment Plan (SAP)

- Use applicant developed SSP
- Address all controls in SSP
- Use FedRAMP assessment procedures
  - abbreviated set provided for applicant
- Assessment procedures expected to be extended as appropriate to accommodate system specific technologies and practices



## 4. Assessment Evidence and Findings

- From simulated execution of SAP
- Recorded in FedRAMP provided abbreviated assessment procedures (blank blocks/columns)
  - Assessment Cases (series of assessment actions)
  - Security Assessment Case Reporting Forms (summary)
  - Evidence & findings returned with application
- Include several examples of potential results from satisfied to *varying* degrees of other than satisfied
- Minimum two (2) examples for each control judged to be “other than satisfied”



## 5. Security Assessment Report (SAR)

- Abbreviated version FedRAMP SAR provided
- Develop complete SAR from
  - Simulated execution of SAP
  - Assessment procedure evidence and findings
- Impact/risk of “other than satisfied” findings

