FedRAMP

OSCAL-Enabled FedRAMP Automation

NIST Virtual Conference

Feb 2 - 3, 2021

GSA

info@fedramp.gov

fedramp.gov

Agenda

I. Introduction & Overview: FedRAMP's Automation Efforts
II. Automation Roadmap
III. Automated Reviews
IV. Resources & Questions

Responding to What We're Hearing

In FY19, FedRAMP focused on gathering the voice of our customer to inform our future plans

Feedback Channels

We engaged with our customers via the following feedback channels

- Ideation Challenge
- Small Business Engagement
- ACT-IAC ATO Working Group
- Customer Journey Mapping

What We're Hearing

- Automation — Improve manual processes associated with the end-to-end authorization process
- More opportunities to connect with stakeholders — Increase outreach and involvement with all stakeholders in service of helping them understand and implement the FedRAMP process
- Further guidance and clarity into the process and security requirements
- Simplify the process
- Grow the marketplace — Increase options for cloud services available to Federal Agencies
- Reuse — Increase reuse of Agency ATOs (Industry preferred)

FedRAMP Next Generation

Open Security Controls Assessment Language (OSCAL) A set of formats (expressed in XML, JSON, and YAML) that provide machine-readable representations of control catalogs, baselines, system security plans, and assessment plans/ results.

FedRAMP OSCAL Baselines & Security Package Materials

The development of the FedRAMP baseline and security package materials in OSCAL.

Next Step: Refine OSCAL syntax and work with GRC tools to ingest OSCAL packages.

Automated Validations and Open Source Conversion Tools

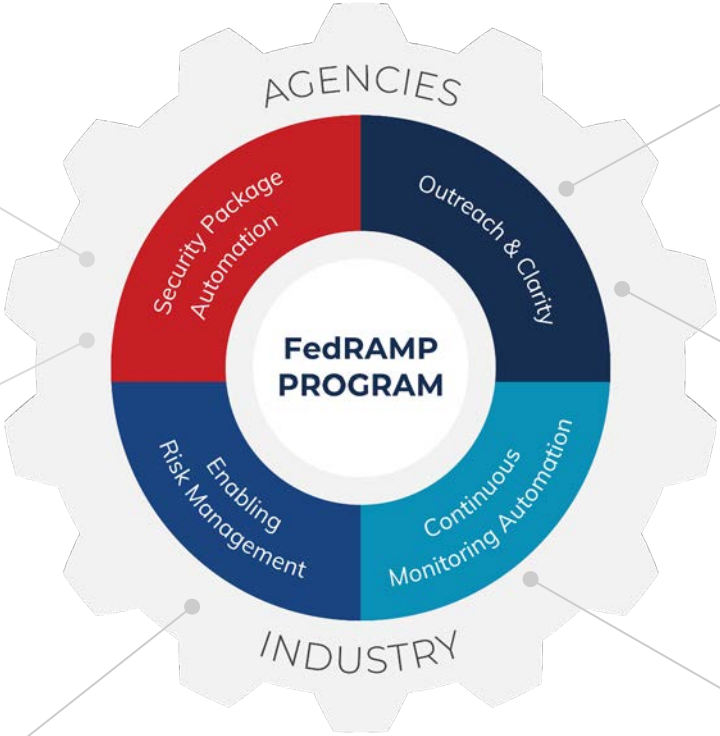
To encourage adoption of OSCAL, FedRAMP is developing conversion tools and OSCAL scripts that will allow Agencies to utilize OSCAL templates and significantly reduce the time to review security deliverables.

Next Step: Pilot validations and tools with users.

Threat-Based Authorization Approach

Teamed with DHS CISA .govCAR to score security controls on how well they protect, detect and respond to real-world threats.

Next Step: Apply methodology to rebaseline FedRAMP Ready and Annual assessment (up to moderate) requirements.



FedRAMP Guidance Updates

Updated multiple program guidance documents and templates to promote clarity and simplicity based on agency/industry feedback.

Next Step: Continue streamlining and refining FedRAMP Guidance.

Agency Liaison Program

Established a voluntary community of trained individuals that will serve as a unified voice across Federal agencies as they teach and facilitate FedRAMP processes and procedures.

Next Step: Conduct 4 FedRAMP Liaison meetings in FY21 and prepare Liaisons to conduct 1 training event at their own agency.

Web Services API Specifications

The development of an Application Programming Interface (API).

Next Step: Provide a service for programmers to push and pull data from FedRAMP (i.e. vulnerability information in OSCAL formats).

Security Package Automation

OSCAL Baselines & Security Package Materials

The Challenge: The security deliverables associated with government authorization packages are implemented in a way that are time consuming and manual to develop, review, and maintain.

The Solution: FedRAMP partnered with NIST to develop a standard machine-readable language, Open Security Control Assessment Language (OSCAL), and apply it to the NIST control catalogue, FedRAMP baselines, and security deliverables.

Benefits:

- Provides a common language that enables the automation of developing, reviewing and maintaining FedRAMP security deliverables.
- Enables FedRAMP to be directly incorporated into a continuous integration and deployment framework, aligned with current industry practices.
- Provides the opportunity for tools, scripts, APIs, and programs to be developed to create further efficiencies associated with cost and time. (Example: Governance, Risk, and Compliance (GRC) Integration, Review Script)

Automated Validations

The Solution: FedRAMP is developing a set of validation rules that will be created in OSCAL to enable automated package reviews.

Benefits:

- Decreases the level of effort to initially review automation packages
- Provides industry faster feedback to enable faster package reviews as a whole

Additionally, FedRAMP is working with other stakeholders, including DOJ CSAM and DOD eMASS to ingest OSCAL files.

OSCAL Roadmap

NIST and FedRAMP Goals

NIST and FedRAMP remained aligned with their goals by maintaining a continuous partnership throughout the development of OSCAL

NIST's Goals for OSCAL

- **Provide** a common/single machine-readable language, expressed in standard formats, for:
  - multiple compliance & risk management frameworks (e.g. NIST SP 800-53, ISO/IEC 27001 & 2, COBIT 5)
  - software & service providers to express implementation guidance against security controls
  - sharing how security controls are implemented (SSP)
  - sharing security assessment plans (SAP)
  - sharing security assessment results/reports (SAR & POA&M)
- **Enable** automated traceability from selection of security controls through implementation and assessment

FedRAMP's Goals for Automation

- **Expedite** the creation, assessment, and adjudication of security artifacts
- **Shift level-of-effort away** from compliance, and toward risk management
- **Enable automation** for Cloud Service Providers (CSPs), Accredited Third Party Assessment Organizations (3PAOs), and the FedRAMP PMO/JAB
- **Enable** stakeholder tool development and innovation

Potential Applications and Benefits

Benefits & Potential Applications for CSPs

CSPs may wish to consider adopting OSCAL to ease the burden of security management.

Potential Applications	Benefit
Automate the collection and correlation of SSP content	• Build workflows around SSP development and maintenance • Generate system inventory • Automatically populate or update POA&M content
Provide a machine-readable SSP to assessors and authorizing officials	• Enables assessors to expedite their assessments • Enables adjudicating officials to expedite their reviews • Enables adopting Agencies to import SSP content into GRC tools
Auto-generate machine readable input to scanning tools	• Reduces or eliminates manual entry and entry error
Auto-generate Control Information Summary (CIS) and Customer Responsibility Matrix (CRM)	• Under OSCAL these are simply generated "views" of the full SSP control content • Eliminates effort and errors compared to copy the current copy and paste maintenance
Import FedRAMP-published review rules and apply them	• Enables CSPs and 3PAOs to self test prior to package submission • Enables AOs and FedRAMP to streamline entire adjudication process • Enable faster communication among FedRAMP stakeholders

Benefits & Potential Applications for 3PAOs

3PAOs may wish to consider adopting OSCAL for assessment benefits.

Potential Applications	Benefit
Automate Assessment planning and pre-validation	• Enables automatic SSP validation checks
Auto-generate interview list	• Reduces time to develop interview list for specific CSP teams and list of controls
Auto-generate machine readable input to scanning tools	• Reduces or eliminates manual entry and entry error
Auto-generate Test Case Workbook (TCW) content from scanning tool output	• Reduces time / effort to copy and paste information manually, and reduces errors • Under OSCAL Risk Exposure Table (RET) and many other tables are simply “views” of the TCW content
Easily export residual risks from SAR to POA&M	• Reduces time / effort to copy and paste information manually, and reduces errors
Import FedRAMP-published review rules and apply them	• Enables CSPs and 3PAOs to self test prior to package submission • Enables AOs and FedRAMP to streamline entire adjudication process • Enable faster communication among FedRAMP stakeholders

Benefits & Potential Applications for Agencies

Agencies may wish to consider adopting OSCAL for assessment benefits.

Potential Applications	Benefit
Directly ingest FedRAMP packages into GRC tools	• Ensure accurate content by avoiding copy/paste errors • Dramatically reduce time and level of effort compared to copy/paste • Use workflow tools to expedite internal adjudication
Adopt validation resources, and tailor to your organization	• Run organizationally tailored validation on top of FedRAMP validation • Generate organizationally tailored "views" of FedRAMP packages
Adopt or create OSCAL tools for legacy system authorization packages	• Expedite internal authorization package development and maintenance • Expedite internal assessment and authorization activities • Ability to mandate OSCAL-based authorization packages from external assessors • Ability to share OSCAL-based security content with external stakeholders • Enable dashboards covering both legacy and cloud-base systems

FedRAMP's OSCAL Efforts to Date

FedRAMP partnered with NIST on OSCAL in 2018

2018

- **Summer -** Embedded FedRAMP SME with NIST to ensure OSCAL met FedRAMP's needs

2019

- **Spring -** Provided initial SSP syntax draft
- **Fall -** Published first guidebook for generating an OSCAL-based FedRAMP SSP
  - Including an example OSCAL-based FedRAMP SSP Template

2020 2021

- **Spring -** Provided initial SAP, SAR and POA&M syntax drafts
  - Published guidebooks for adopting OSCAL-based FedRAMP SAP, SAR, and POA&M
  - Including example OSCAL-based FedRAMP SAP, SAR and POA&M Templates
- **Summer -** Published tools to render OSCAL content into our Word-based templates
- **Summer -** Obtained GSA 10x research funding to investigate and prototype automated validation rule capabilities
  - Intend to publish those rules for other organizations to use with their tools
- **Currently** preparing OSCAL tooling to expedite our NIST 800-53 Rev 5 transition
- **Currently** aligning our guidebooks and templates with the December 2020 OSCAL RC-1 syntax

FedRAMP's OSCAL Efforts Going Forward

What to expect from FedRAMP

- Swift deployment of FedRAMP Rev 5 materials following the JAB's approval of the baselines
    - Also enables agility for future changes to 800-53 or our baselines
- Aligning the FedRAMP guidebooks and templates with the full OSCAL 1.0.0 release
- First publication of presentation transforms
    - Enables anyone to view OSCAL-based FedRAMP content in the same presentation format as our current templates
- First publication of validation rules
    - Initially focusing on package completeness and conformity

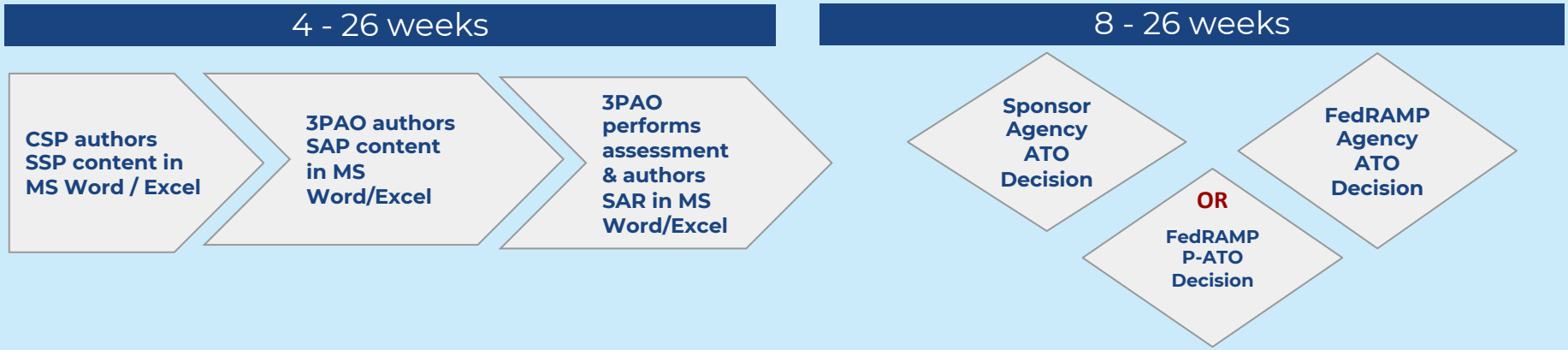
FedRAMP's OSCAL Efforts Going Forward

Based on stakeholder interactions, FedRAMP is looking forward to the following in 2021

- First FedRAMP packages delivered in OSCAL (SSP, SAP, SAR, and POA&M)
- First ConMon deliverables in OSCAL
- First 3PAOs using OSCAL:
  - to accept and handle your OSCAL-based FedRAMP SSP
  - to provide OSCAL-based SAP and SAR content
- Large CSPs offering IaaS providers offering OSCAL-based CRM content to SaaS customers
  - CRM content will use the OSCAL *Inheritance and Responsibility* Model, due out mid-year
- GRC tools used by many Agencies will be able to import OSCAL-based FedRAMP packages
- OSCAL-enabled expedited processing for CSPs pursuing FedRAMP+ with DoD

Automated Reviews

What's Working Well & Areas for Improvement



What's Working Well

- Internal review process: The internal process in place for package reviews functions smoothly
- Collaboration: The team is able to solve package review issues quickly, and their collaborative approach to package review is synergetic.
- Role Clarity / Team Structure: The review team is well organized and communication between agency reviewers is clear and efficient.

Areas for Improvement

- Formatting check for entire package is time consuming
- Validating consistency throughout documentation
- Tracking of CSP package remediations
- Format of tools and materials is not conducive to reviews or CSP working styles (CIS, diagrams)

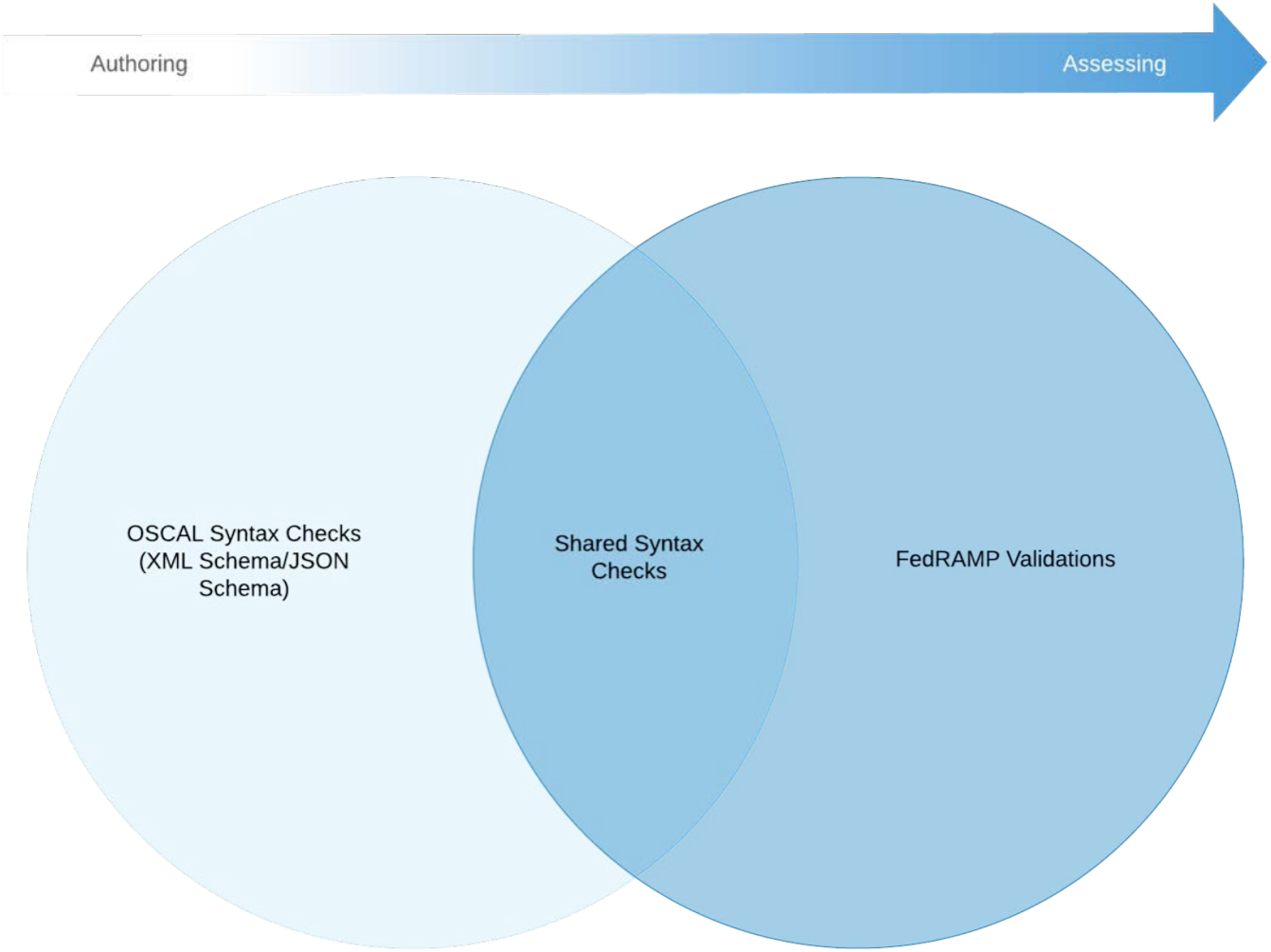
Automated Reviews

What kinds of questions does the SSP author need to answer?

- Is all the necessary front-matter complete?
- For the security controls:
  - Do I know all the minimum necessary controls for the system?
  - Are all my responses correct?
  - Are all the metadata points for all these controls correct?
  - Am I correctly referencing other FedRAMP products I use in this system?
- For all the attachments:
  - Have I attached them correctly?
  - Have I labelled them correctly?

Automated Reviews

Why do we need automated validations for FedRAMP?



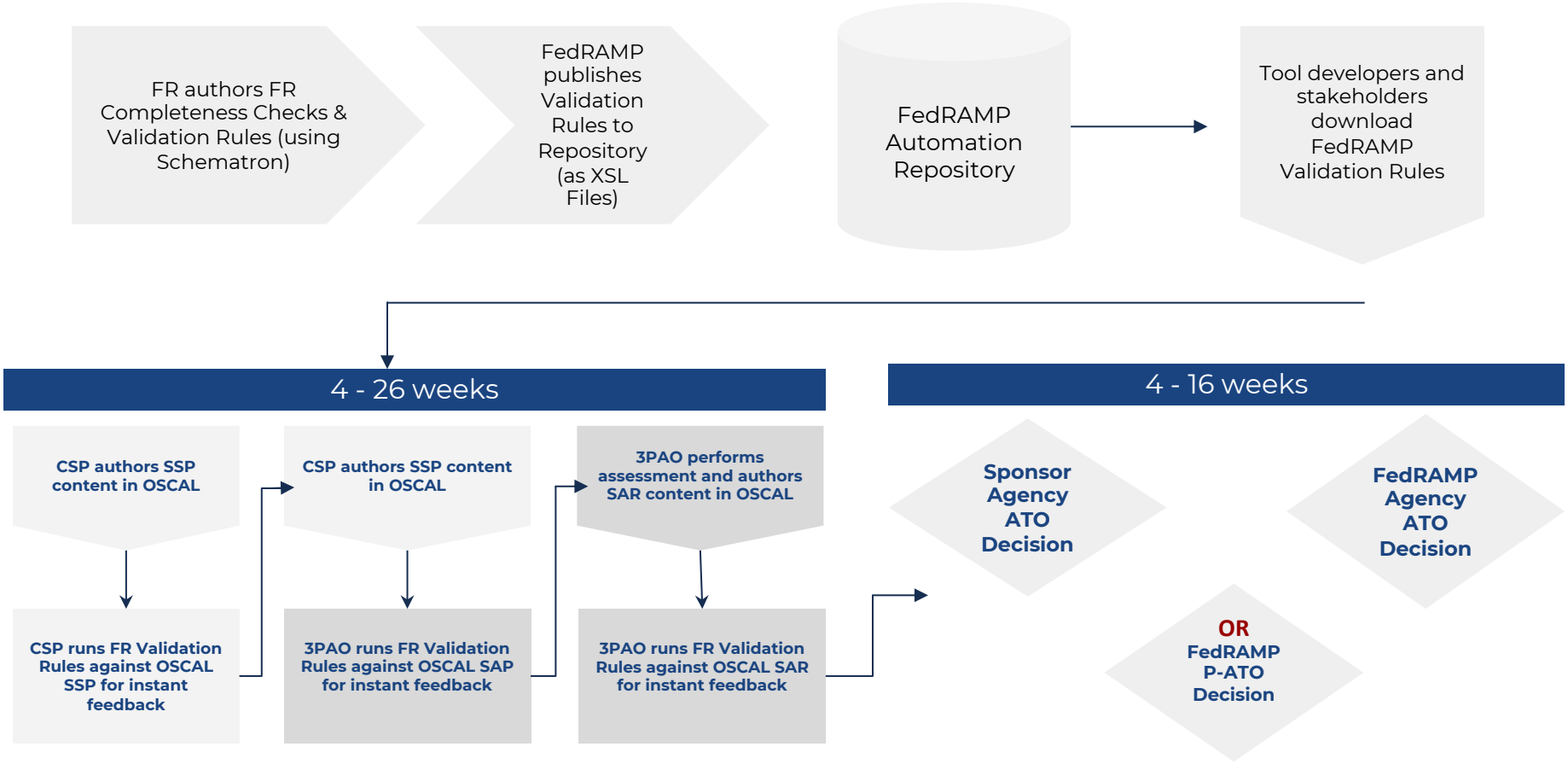
Automated Reviews

What does OSCAL change about the process?

- Complement what works and take the pain away:
  - Encode assessment data ***and*** the assessment information lifecycle
  - Structured content
    - Aggressive content deduplication: check once, reference everywhere
    - Machine readability brings targeted and holistic validation
    - Improved internal review processes
    - Enhanced collaboration abilities
    - Expedited package formatting, consistency, and CSP fixes
  - Layered automation and progressive enhancement
    - Standardize the feedback loop internally and externally
    - Perform just in-time consistency checks at multiple touchpoints
    - Serialize the brains of FedRAMP and 3PAO staff

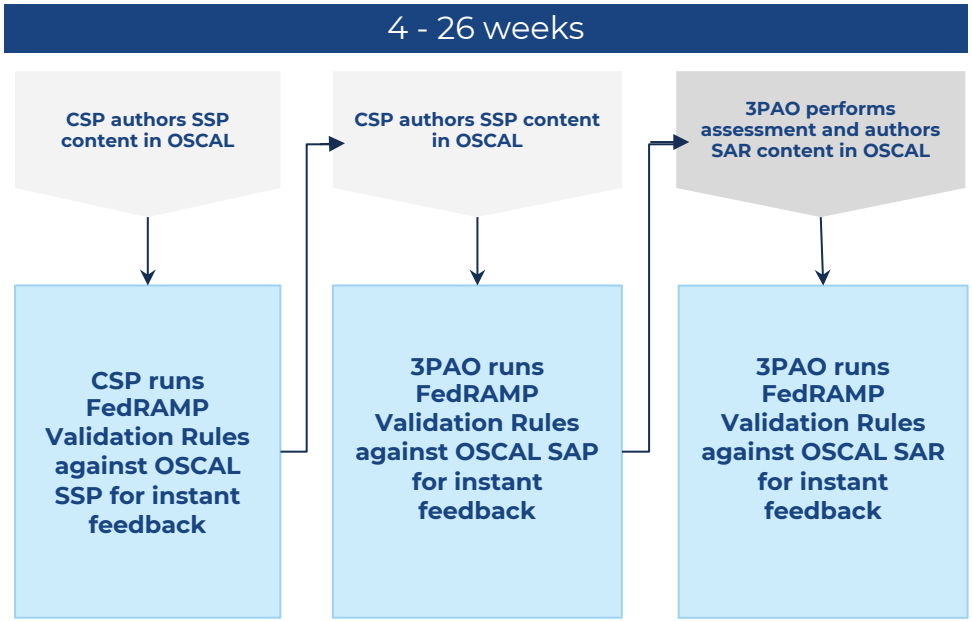
Proposed Future Process

The following image reflects the proposed future state, which is an **OSCAL-enabled review process** that allows all stakeholders to utilize OSCAL for instant feedback, resulting in faster ATO decisions



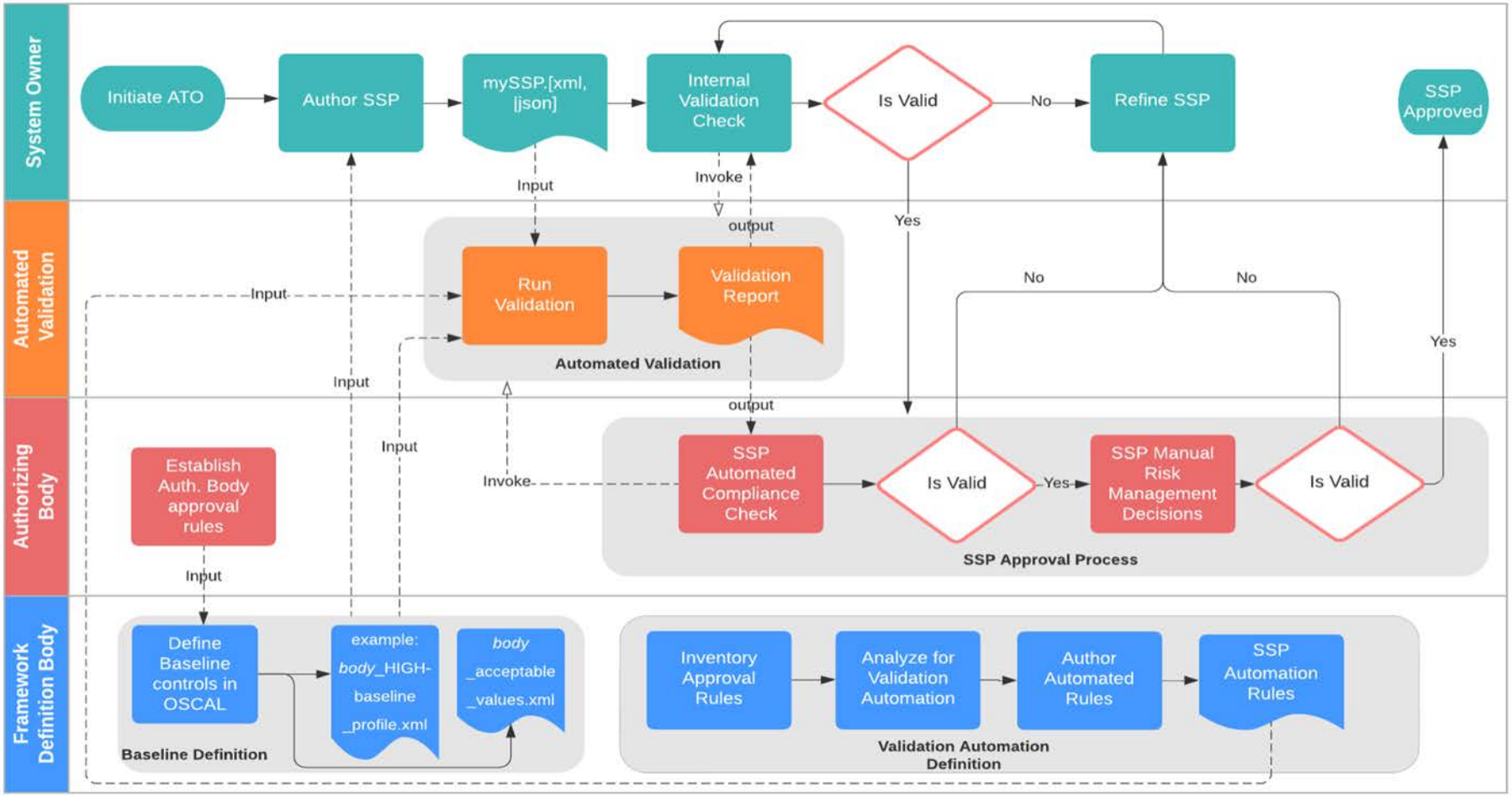
How will FedRAMP's automated validations work?

- Authors create the SSP in OSCAL
- Pipeline loads important dependencies and the SSP
  - Official defaults and required presets from OSCAL
  - Specific defaults and required presets from FedRAMP
- Pipeline determines the security sensitivity level of the SSP
  - Load the required catalog profile for a FedRAMP baseline
- Process the validation rules
  - Define variables with queries to locate relevant item(s)
  - Perform existence checks on certain fields, assembles, and attributes
  - Check for acceptable or required values
  - Cross-reference fields between different fields and assemblies
- Generate results report in a machine-readable standard for document validation (SVRL or XML)



Automated Reviews

How flexible is the FedRAMP Validations approach?



Resources

NIST and FedRAMP Repositories

FedRAMP Resources

For information on how to apply OSCAL to FedRAMP

FedRAMP Automation GitHub:

https://github.com/gsa/fedramp-automation

To include:

- Guidebooks for creating OSCAL-based FedRAMP Content
- SSP, SAP, SAR & POA&M OSCAL Templates
- Additional Technical Resources

Complete Vendor Resource Summary:
https://github.com/GSA/fedramp-automation/raw/master/documents/FedRAMP_OSCAL_Vendor_Resources.pdf

NIST Resources

Developers Brown Bag:

https://pages.nist.gov/OSCAL/contribute/dev-lunch/

NIST OSCAL GitHub:
https://github.com/usnistgov/OSCAL

NIST Project Website:
https://www.nist.gov/oscal

Gitter OSCAL Lobby:

https://gitter.im/usnistgov-OSCAL/Lobby

Thank You

Learn more at **fedramp.gov**

Contact us at **info@fedramp.gov**

@FEDRAMP