## FY22 Program Vision

Modernize FedRAMP through automation and business process improvements to continue to grow and scale the program, while enhancing the experience of agencies and industry.

<table>
<thead>
<tr>
<th>GOALS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
</tr>
<tr>
<td>Grow the FedRAMP Marketplace:</td>
</tr>
<tr>
<td>Continue to partner with government and industry to promote the adoption of secure cloud services across the federal government</td>
</tr>
</tbody>
</table>
FedRAMP OSCAL Baselines and Security Package Materials
Developed and released the FedRAMP baselines and security package materials in OSCAL, accompanied with guidebooks.

Automated Validations
Developing a set of validation rules that will be created in OSCAL to enable automated package reviews (i.e. conduct low-level reviews such as completeness, consistency, adherence to formatting, etc.), as well as automated mark-ups and reviews.

Threat Based Profile
Conducted control scoring (up to FedRAMP Moderate baseline) with DHS CISA.govCAR. Evaluating methodology for application to FedRAMP annual assessment requirements.

WebServices API Specifications
Develop specifications of how to develop an API, which provides a service for programmers to push and pull data from FedRAMP (i.e. vulnerability information in OSCAL formats).

Measuring Success
Develop strategic metrics to demonstrate automation’s positive and measurable impact on the FedRAMP missions, goals, and stakeholder experience.
OSCAL & Automated Validations
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. This will enable FedRAMP to automatically conduct low-level reviews (i.e. completeness, consistency, adherence to formatting, etc.), as well as automated mark-ups and reviews.

**Benefits:**
- Tune and cost savings
- Submission of higher quality packages
- Allows review teams to focus on higher value assessments
- Ensures FedRAMP responds to industry feedback

Additionally, FedRAMP is working with other stakeholders, including DOJ CSAM and DOD eMASS to ingest OSCAL files.
Overview of the 10x Program

10x is crowdsourcing program used to collect ideas from federal employees and turn them into real products that improve the public's experience with the federal government.

- As 10x explores ideas, they whittle down projects to move through four phases, where they continue to research and iterate on it.
- Not every idea moves through all four phases of funding. Some graduate from the program at earlier points.
- Deliverables have included a research report, a product or platform, a complete redesign of a process, and more.

TOTAL

Projects funded by 10x

268
10x Program Phases

0. Evaluate Idea
   - Clarity
   - Alignment
   - Impact

1. Investigate
   - Major Red Flags
   - Demand.

2. Discover
   - Current State
   - Market fit
   - Regulatory requirements
   - Timeline
   - Funding Model

3. Develop
   - MVP
   - Recruit agency customer
   - Product roadmap
   - Business Plan

4. Scale
   - Additional customers
   - Largest possible audience
Developing Automated Validations

For a FedRAMP OSCAL SSP, there are over 100 validation rules, two thirds of which are capable of being automated.

- We implemented over 90% of the automatable validations.
- The related Schematron comprises about 4,700 lines of code at this time; corresponding unit tests comprise about 10,500 lines of code.
- The fourth and final 10x ASAP phase will include additional automated validations for OSCAL documents (SSP, SAP, SAR, POA&M).
  - While prior focus had been specifically on FedRAMP automation, the project will attempt to accommodate fundamental NIST RMF validations with overlays for FedRAMP and other RMF adaptations.

Project repository: https://github.com/GSA/fedramp-automation
Phase 3: Developing Automated Validations

The GSA 10x-sponsored ASAP project has proceeded through four phases.

Phase 3 funding was used to create a System Security Plan (SSP) validation framework.

- We embedded with FedRAMP to understand reviewer needs.
- We proved the efficacy of structured, machine-readable validation rules.
- We employed Schematron to allow the validation rules to be used in other applications.
- We ate our own dog food, and created a browser-based front-end to the validation framework.
A tool for users to:
- Browse and filter rules
- Validate SSP documents
- Demonstrate embeddability of rules engine

Intended Users:
- Drafters, auditors

Try it: go.usa.gov/xz3MV
Phase 4: Developing Automated Validations

In Phase 4, 10x ASAP will scale our solution to a CMS-sponsored FedRAMP application

- 10x partnership with Centers for Medicare & Medicaid Services (CMS).
- Work with CMS as they sponsor a structured FedRAMP application from a pioneering Cloud Service Provider (CSP).
- Provide pre-assessment support to a CSP, so they can submit fully-compliant ATO documentation.
- Support the cultivation of both FedRAMP and CMS-specific requirements, leading to a virtuous circle of improving efficiency.
Demo:
Prototype Tools
Agency Authorization Review Report Tool

Standalone tool that will generate a DRAFT Agency Authorization Review Report Workbook from an OSCAL SSP (LOW and MODERATE) and Schematron Validations Report Language Output File (SVRL)
Standalone tool that will generate a DRAFT Agency Authorization Review Report Workbook from an OSCAL SSP (LOW and MODERATE) and Schematron Validations Report Language Output File (SVRL)
CIS Workbook Generator

Standalone tool to Generate a CIS Workbook from an OSCAL SSP.

Step 1 - Upload SSP
Upload your OSCAL XML System Security Plan.
Choose File | No file chosen
Upload

Step 2 - Generate DRAFT CIS Workbook Starter Template
Generate CIS Workbook.

How to Contact Us
Questions about FedRAMP or this document should be directed to info@fedramp.gov. For more information about FedRAMP, visit the website at https://www.fedramp.gov.

About This Template and Who Should Use It
Cloud Service Providers (CSPs) must use this Low or Moderate Control Implementation Summary (CIS) Workbook Template to summarize a Low or Moderate system's implementation status for all controls and enhancements, and to identify and describe the customer Agency/CSP responsibilities. The CSP must submit the completed CIS Workbook as part of the system’s final security authorization package, as System Security Plan (SSP) Attachment 9.

The audience for the completed CIS Workbook Includes Third Party Assessment Organizations (3PAOs); customer Agencies and CSPs; and the FedRAMP Joint Authorization Board (JAB) and Program Management Office (PMO).

This workbook should be updated as part of a CSP’s regular continuous monitoring activities.
FedRAMP Low or Moderate Control Implementation Summary (CIS) Worksheet

<table>
<thead>
<tr>
<th>Implementation Status</th>
<th>Control Origination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implemented</td>
<td></td>
</tr>
<tr>
<td>Partially Implemented</td>
<td></td>
</tr>
<tr>
<td>Planned</td>
<td></td>
</tr>
<tr>
<td>Alternative</td>
<td></td>
</tr>
<tr>
<td>Implementation</td>
<td></td>
</tr>
<tr>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Service Provider</td>
<td></td>
</tr>
<tr>
<td>Corporate</td>
<td></td>
</tr>
<tr>
<td>System Specific</td>
<td></td>
</tr>
<tr>
<td>Service Provider</td>
<td></td>
</tr>
<tr>
<td>Hybrid (Corporate and</td>
<td></td>
</tr>
<tr>
<td>System Specific</td>
<td></td>
</tr>
<tr>
<td>Configured by</td>
<td></td>
</tr>
<tr>
<td>Customer (Customer</td>
<td></td>
</tr>
<tr>
<td>System Specific</td>
<td></td>
</tr>
<tr>
<td>Provided by Cust.</td>
<td></td>
</tr>
<tr>
<td>(Customer System</td>
<td></td>
</tr>
<tr>
<td>Specific)</td>
<td></td>
</tr>
</tbody>
</table>

FedRAMP.gov
FedRAMP GitHub Public Repositories


https://github.com/GSA/fedramp-automation/tree/master/dist/content/templates - FedRAMP OSCAL templates for SSP, SAP, SAR, POAM.

https://github.com/GSA/oscal-gen-tool - MVP tool to import, edit and export OSCAL SSPs, SAPs, SARs and POAMs.

https://github.com/GSA/oscal-ssp-to-word - MVP tool to convert OSCAL SSP to FedRAMP Word version of SSP.

https://github.com/GSA/oscal-sap-to-word - MVP tool to convert OSCAL SAP to FedRAMP Word version of SAP.

https://github.com/GSA/oscal-sar-to-word - MVP tool to convert OSCAL SAR to FedRAMP Word version of SAR.
Thank you!

Learn more at fedramp.gov

Contact us at info@fedramp.gov

@FEDRAMP