FedRAMP

FedRAMP Automation

NIST Briefing
March 1, 2022

GSA

info@fedramp.gov
fedramp.gov

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.

GOALS

1

Grow the FedRAMP Marketplace:

Continue to partner with government and industry to promote the adoption of secure cloud services across the federal government

2

Transform Processes:

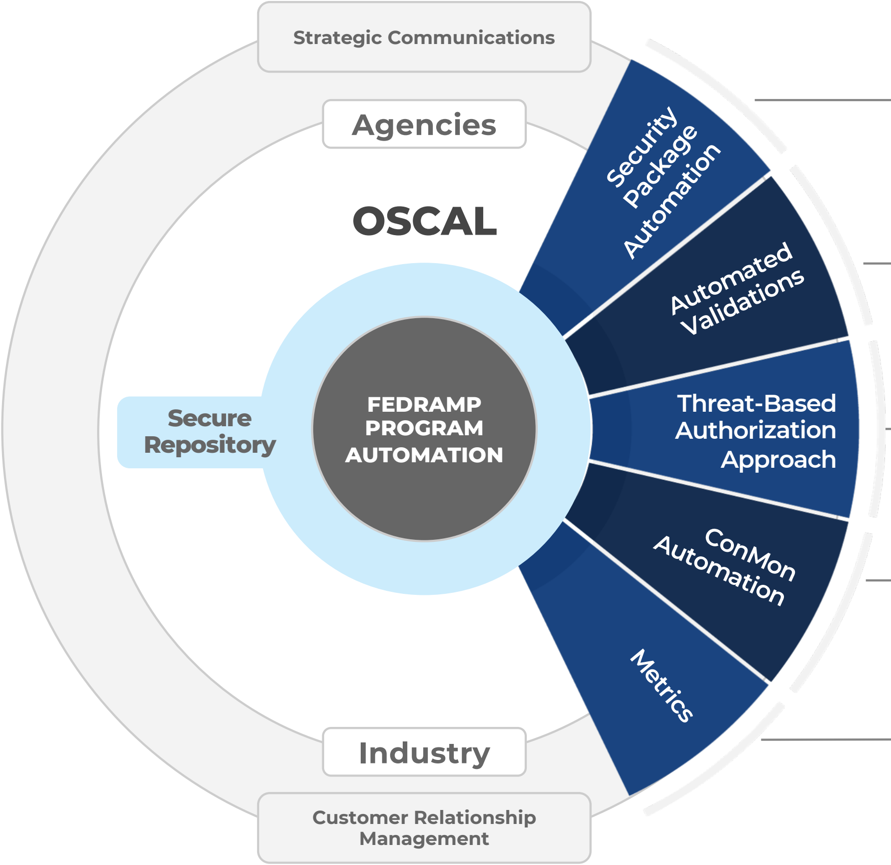
Incorporate automation and process improvements to improve the efficiency and stakeholder experience of the end-to-end FedRAMP process with the ability to accommodate future growth

3

Promote Knowledge Sharing:

Provide more opportunities for dialogue and feedback by hosting additional events for collaboration, feedback, training and exchange of ideas and practices

Automation Focus Areas


Strategic Communications
Agencies
OSCAL
Secure Repository
FEDRAMP PROGRAM AUTOMATION
Industry
Customer Relationship Management
Security Package Automation
Automated Validations
Threat-Based Authorization Approach
ConMon Automation
Metrics

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

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.

OSCAL Baselines & Security Package Materials

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.

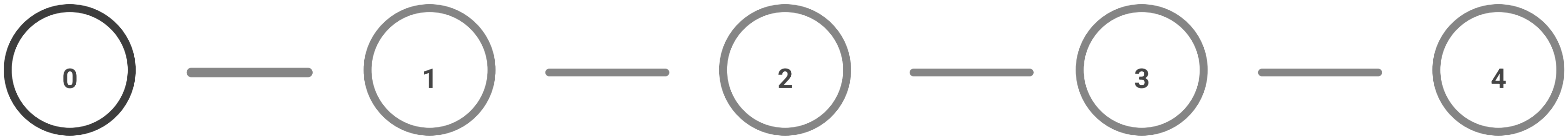
- As 10x explores ideas, they whittle down projects to move through four phases, where they continue to research and iterate on it.
- Not every idea moves through all four phases of funding. Some graduate from the program at earlier points.
- Deliverables have included a research report, a product or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

TOTAL

268

Projects funded by 10x

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.

10x ASAP Tool Demo

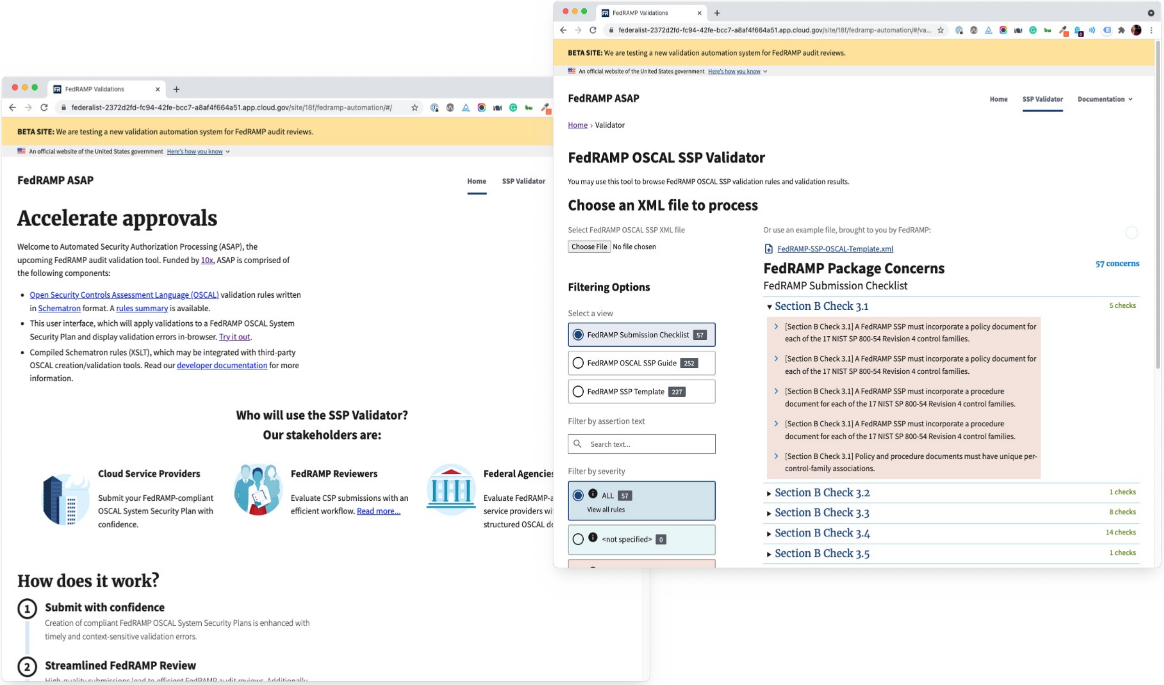
A tool for users to:

- Browse and filter rules
- Validate SSP documents
- Demonstrate embeddability of rules engine

Intended Users:

- Drafters, auditors

[Try it: go.usa.gov/xz3MV](go.usa.gov/xz3MV)


FedRAMP Validations
federalist-2372d2fd-fc94-42fe-bcc7-a8af4f664a51.app.cloud.gov/site/18f/fedramp-automation/#/

BETA SITE: We are testing a new validation automation system for FedRAMP audit reviews.

An official website of the United States government Here's how you know

FedRAMP ASAP
Home
SSP Validator

Accelerate approvals

Welcome to Automated Security Authorization Processing (ASAP), the upcoming FedRAMP audit validation tool. Funded by 10x, ASAP is comprised of the following components:

- Open Security Controls Assessment Language (OSCAL) validation rules written in Schematron format. A rules summary is available.
- This user interface, which will apply validations to a FedRAMP OSCAL System Security Plan and display validation errors in-browser. Try it out.
- Compiled Schematron rules (XSLT), which may be integrated with third-party OSCAL creation/validation tools. Read our developer documentation for more information.

Who will use the SSP Validator?
Our stakeholders are:

Cloud Service Providers
Submit your FedRAMP-compliant OSCAL System Security Plan with confidence.

FedRAMP Reviewers
Evaluate CSP submissions with an efficient workflow. Read more...

Federal Agencies
Evaluate FedRAMP-a
service providers wi
structured OSCAL d

How does it work?

1. **Submit with confidence**
   Creation of compliant FedRAMP OSCAL System Security Plans is enhanced with timely and context-sensitive validation errors.
2. **Streamlined FedRAMP Review**
   High-quality submissions lead to efficient FedRAMP audit reviews. Additionally,

FedRAMP Validations
federalist-2372d2fd-fc94-42fe-bcc7-a8af4f664a51.app.cloud.gov/site/18f/fedramp-automation/#/va...

BETA SITE: We are testing a new validation automation system for FedRAMP audit reviews.

An official website of the United States government Here's how you know

Home › Validator

FedRAMP OSCAL SSP Validator

You may use this tool to browse FedRAMP OSCAL SSP validation rules and validation results.

Choose an XML file to process

Select FedRAMP OSCAL SSP XML file
Choose File No file chosen

Or use an example file, brought to you by FedRAMP:
FedRAMP-SSP-OSCAL-Template.xml

Filtering Options

Select a view
● FedRAMP Submission Checklist 57
○ FedRAMP OSCAL SSP Guide 252
○ FedRAMP SSP Template 227

Filter by assertion text
Search text...

Filter by severity
● ALL 57
View all rules
○ <not specified> 0

FedRAMP Package Concerns

57 concerns

FedRAMP Submission Checklist

▾ Section B Check 3.1 — 5 checks
- [Section B Check 3.1] A FedRAMP SSP must incorporate a policy document for each of the 17 NIST SP 800-54 Revision 4 control families.
- [Section B Check 3.1] A FedRAMP SSP must incorporate a policy document for each of the 17 NIST SP 800-54 Revision 4 control families.
- [Section B Check 3.1] A FedRAMP SSP must incorporate a procedure document for each of the 17 NIST SP 800-54 Revision 4 control families.
- [Section B Check 3.1] A FedRAMP SSP must incorporate a procedure document for each of the 17 NIST SP 800-54 Revision 4 control families.
- [Section B Check 3.1] Policy and procedure documents must have unique per-control-family associations.

▸ Section B Check 3.2 — 1 checks
▸ Section B Check 3.3 — 8 checks
▸ Section B Check 3.4 — 14 checks
▸ Section B Check 3.5 — 1 checks

Phase 4: Developing Automated Validations

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

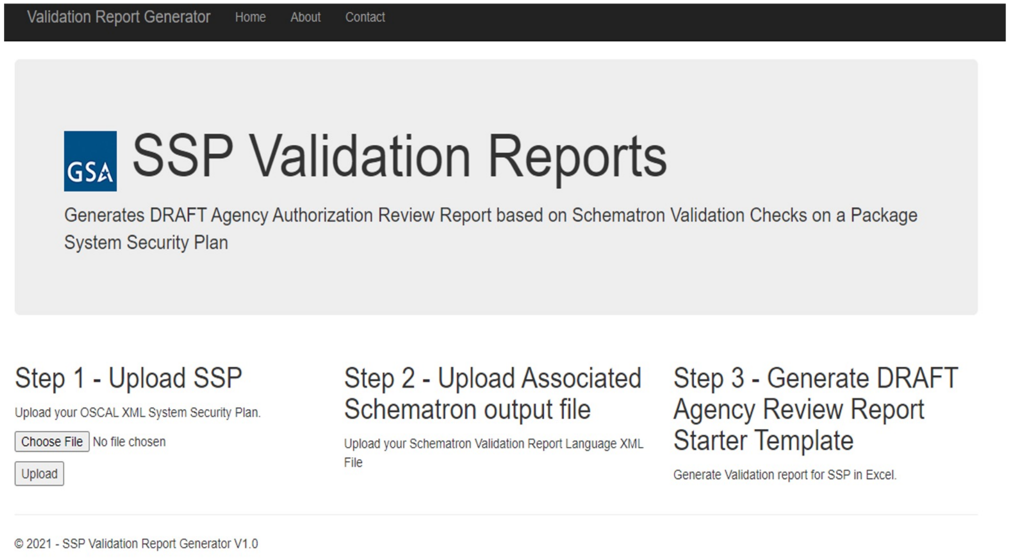
- 10x partnership with Centers for Medicare & Medicaid Services (CMS).
- Work with CMS as they sponsor a structured FedRAMP application from a pioneering Cloud Service Provider (CSP).
- Provide pre-assessment support to a CSP, so they can submit fully-compliant ATO documentation.
- Support the cultivation 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)



SSP Validation Reports

Generates DRAFT Agency Authorization Review Report based on Schematron Validation Checks on a Package System Security Plan

Step 1 - Upload SSP

Upload your OSCAL XML System Security Plan.

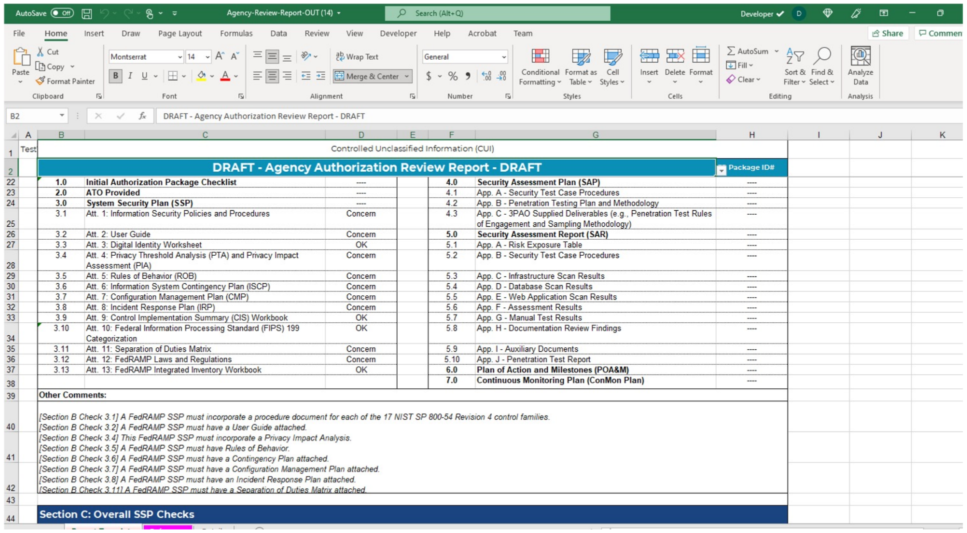
Step 2 - Upload Associated Schematron output file

Upload your Schematron Validation Report Language XML File

Step 3 - Generate DRAFT Agency Review Report Starter Template

Generate Validation report for SSP in Excel.

© 2021 - SSP Validation Report Generator V1.0



DRAFT - Agency Authorization Review Report - DRAFT

Test

Controlled Unclassified Information (CUI)

DRAFT - Agency Authorization Review Report - DRAFT					Package ID#
1.0	**Initial Authorization Package Checklist**	----	**4.0**	**Security Assessment Plan (SAP)**	----
2.0	**ATO Provided**	----	4.1	App. A - Security Test Case Procedures	----
3.0	**System Security Plan (SSP)**	----	4.2	App. B - Penetration Testing Plan and Methodology	----
3.1	Att. 1: Information Security Policies and Procedures	Concern	4.3	App. C - 3PAO Supplied Deliverables (e.g., Penetration Test Rules of Engagement and Sampling Methodology)	----
3.2	Att. 2: User Guide	Concern	**5.0**	**Security Assessment Report (SAR)**	----
3.3	Att. 3: Digital Identity Worksheet	OK	5.1	App. A - Risk Exposure Table	----
3.4	Att. 4: Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA)	Concern	5.2	App. B - Security Test Case Procedures	----
3.5	Att. 5: Rules of Behavior (ROB)	Concern	5.3	App. C - Infrastructure Scan Results	----
3.6	Att. 6: Information System Contingency Plan (ISCP)	Concern	5.4	App. D - Database Scan Results	----
3.7	Att. 7: Configuration Management Plan (CMP)	Concern	5.5	App. E - Web Application Scan Results	----
3.8	Att. 8: Incident Response Plan (IRP)	Concern	5.6	App. F - Assessment Results	----
3.9	Att. 9: Control Implementation Summary (CIS) Workbook	OK	5.7	App. G - Manual Test Results	----
3.10	Att. 10: Federal Information Processing Standard (FIPS) 199 Categorization	OK	5.8	App. H - Documentation Review Findings	----
3.11	Att. 11: Separation of Duties Matrix	Concern	5.9	App. I - Auxiliary Documents	----
3.12	Att. 12: FedRAMP Laws and Regulations	Concern	5.10	App. J - Penetration Test Report	----
3.13	Att. 13: FedRAMP Integrated Inventory Workbook	OK	**6.0**	**Plan of Action and Milestones (POA&M)**	----
			7.0	**Continuous Monitoring Plan (ConMon Plan)**	----

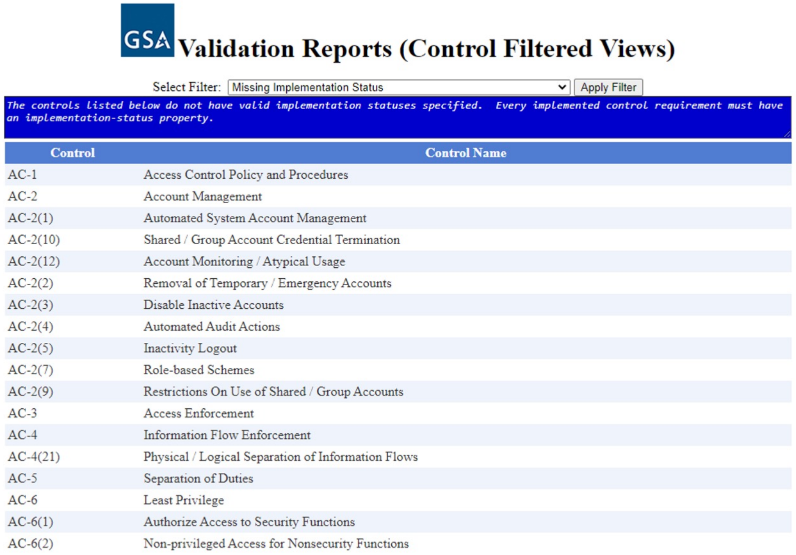
Other Comments:

[Section B Check 3.1] A FedRAMP SSP must incorporate a procedure document for each of the 17 NIST SP 800-54 Revision 4 control families.
[Section B Check 3.2] A FedRAMP SSP must have a User Guide attached.
[Section B Check 3.4] This FedRAMP SSP must incorporate a Privacy Impact Analysis.
[Section B Check 3.5] A FedRAMP SSP must have Rules of Behavior.
[Section B Check 3.6] A FedRAMP SSP must have a Contingency Plan attached.
[Section B Check 3.7] A FedRAMP SSP must have a Configuration Management Plan attached.
[Section B Check 3.8] A FedRAMP SSP must have an Incident Response Plan attached.
[Section B Check 3.11] A FedRAMP SSP must have a Separation of Duties Matrix attached.

Section C: Overall SSP Checks

Agency Authorization Review Report Tool (cont)

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)



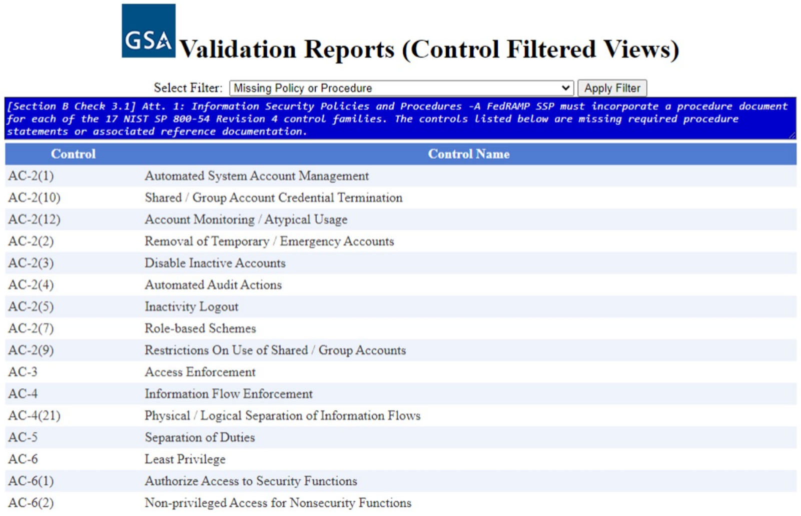
Validation Reports (Control Filtered Views)

Select Filter: Missing Implementation Status

The controls listed below do not have valid implementation statuses specified. Every implemented control requirement must have an implementation-status property.

Control	Control Name
AC-1	Access Control Policy and Procedures
AC-2	Account Management
AC-2(1)	Automated System Account Management
AC-2(10)	Shared / Group Account Credential Termination
AC-2(12)	Account Monitoring / Atypical Usage
AC-2(2)	Removal of Temporary / Emergency Accounts
AC-2(3)	Disable Inactive Accounts
AC-2(4)	Automated Audit Actions
AC-2(5)	Inactivity Logout
AC-2(7)	Role-based Schemes
AC-2(9)	Restrictions On Use of Shared / Group Accounts
AC-3	Access Enforcement
AC-4	Information Flow Enforcement
AC-4(21)	Physical / Logical Separation of Information Flows
AC-5	Separation of Duties
AC-6	Least Privilege
AC-6(1)	Authorize Access to Security Functions
AC-6(2)	Non-privileged Access for Nonsecurity Functions

Missing Implementation Status



Validation Reports (Control Filtered Views)

Select Filter: Missing Policy or Procedure

[Section B Check 3.1] Att. 1: Information Security Policies and Procedures -A FedRAMP SSP must incorporate a procedure document for each of the 17 NIST SP 800-54 Revision 4 control families. The controls listed below are missing required procedure statements or associated reference documentation.

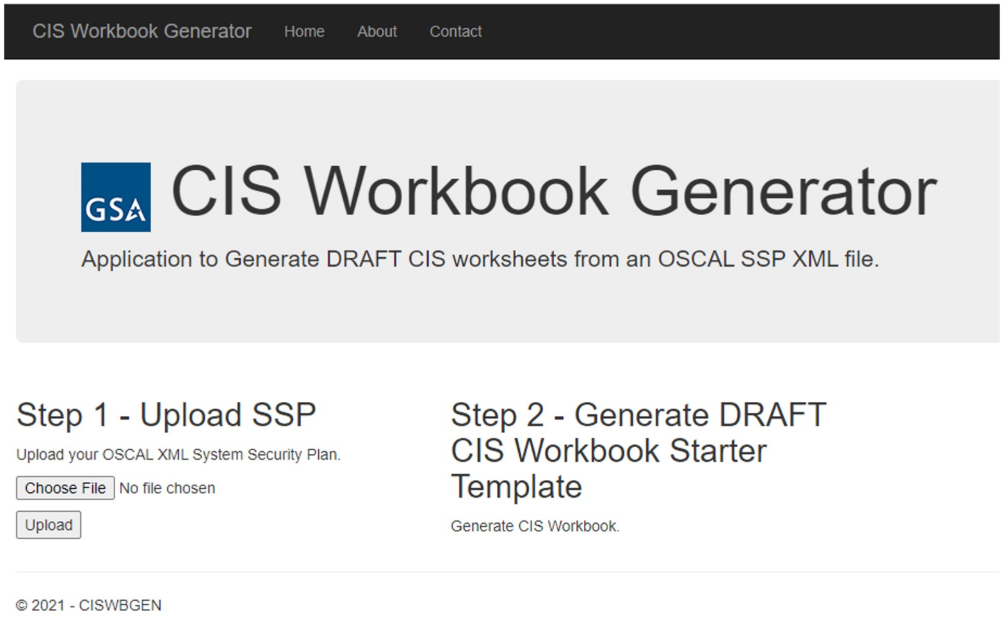
Control	Control Name
AC-2(1)	Automated System Account Management
AC-2(10)	Shared / Group Account Credential Termination
AC-2(12)	Account Monitoring / Atypical Usage
AC-2(2)	Removal of Temporary / Emergency Accounts
AC-2(3)	Disable Inactive Accounts
AC-2(4)	Automated Audit Actions
AC-2(5)	Inactivity Logout
AC-2(7)	Role-based Schemes
AC-2(9)	Restrictions On Use of Shared / Group Accounts
AC-3	Access Enforcement
AC-4	Information Flow Enforcement
AC-4(21)	Physical / Logical Separation of Information Flows
AC-5	Separation of Duties
AC-6	Least Privilege
AC-6(1)	Authorize Access to Security Functions
AC-6(2)	Non-privileged Access for Nonsecurity Functions

Missing Policy or Procedures

Control Filtered View (Reports)

CIS Workbook Generator

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



CIS Workbook Generator

Application to Generate DRAFT CIS worksheets from an OSCAL SSP XML file.

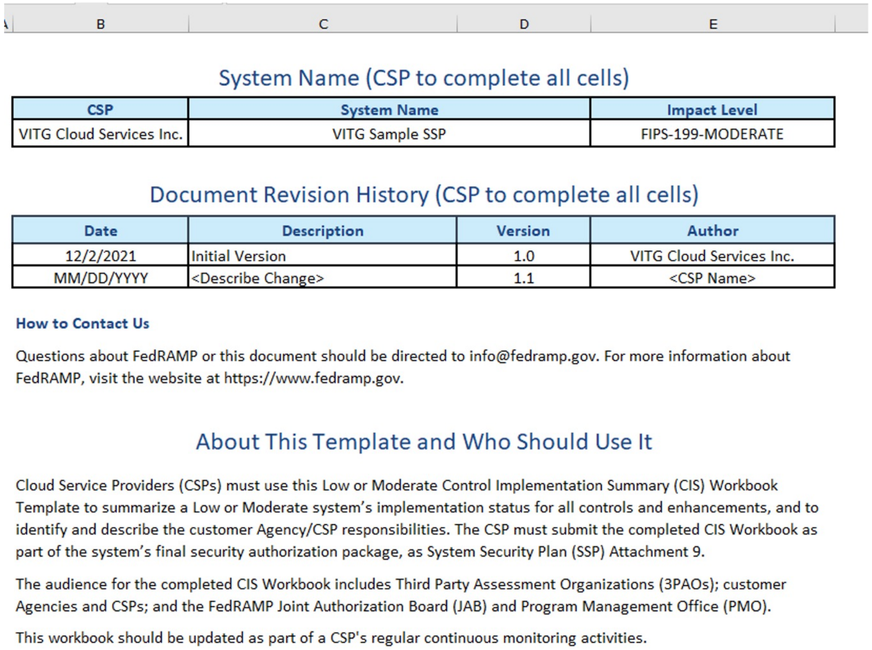
Step 1 - Upload SSP

Upload your OSCAL XML System Security Plan.

Step 2 - Generate DRAFT CIS Workbook Starter Template

Generate CIS Workbook.

© 2021 - CISWBGEN



System Name (CSP to complete all cells)

CSP	System Name	Impact Level
VITG Cloud Services Inc.	VITG Sample SSP	FIPS-199-MODERATE

Document Revision History (CSP to complete all cells)

Date	Description	Version	Author
12/2/2021	Initial Version	1.0	VITG Cloud Services Inc.
MM/DD/YYYY	<Describe Change>	1.1	<CSP Name>

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

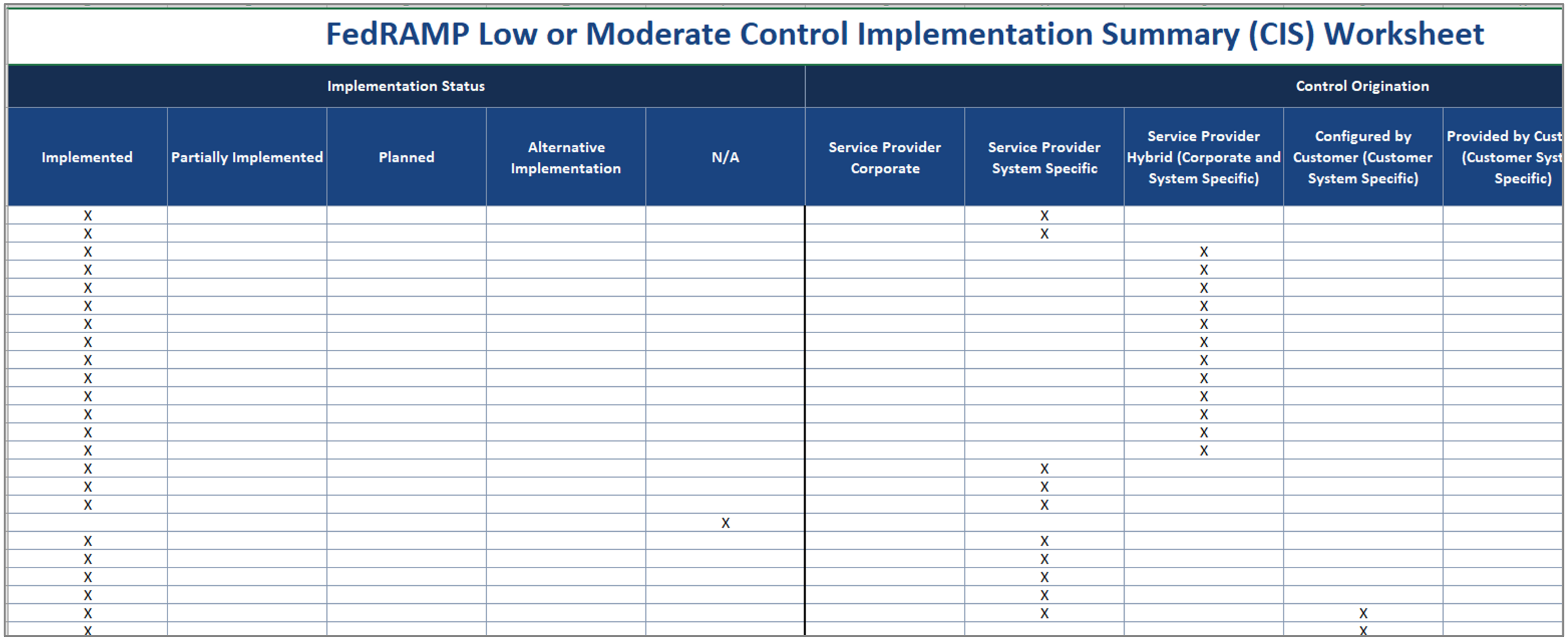
Cloud Service Providers (CSPs) must use this Low or Moderate Control Implementation Summary (CIS) Workbook Template to summarize a Low or Moderate system's implementation status for all controls and enhancements, and to identify and describe the customer Agency/CSP responsibilities. The CSP must submit 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.

CIS Workbook Generator (cont.)

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



FedRAMP Low or Moderate Control Implementation Summary (CIS) Worksheet

Implementation Status					Control Origination				
Implemented	Partially Implemented	Planned	Alternative Implementation	N/A	Service Provider Corporate	Service Provider System Specific	Service Provider Hybrid (Corporate and System Specific)	Configured by Customer (Customer System Specific)	Provided by Cust (Customer Syst Specific)
X						X			
X						X			
X							X		
X							X		
X							X		
X							X		
X							X		
X							X		
X							X		
X							X		
X							X		
X							X		
X							X		
X							X		
X						X			
X						X			
X						X			
				X					
X						X			
X						X			
X						X			
X						X			
X						X		X	
X								X	

Resources

FedRAMP GitHub Public Repositories

https://github.com/GSA/fedramp-automation - Primary FedRAMP automation repository.

https://github.com/GSA/fedramp-automation/tree/master/documents - FedRAMP OSCAL implementation guidance.

https://github.com/GSA/fedramp-automation/tree/master/dist/content/baselines/rev4 - FedRAMP OSCAL 800-53 Revision 4 baselines.

https://github.com/GSA/fedramp-automation/tree/master/src/validations - FedRAMP OSCAL Schematron phase 1 validations.

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