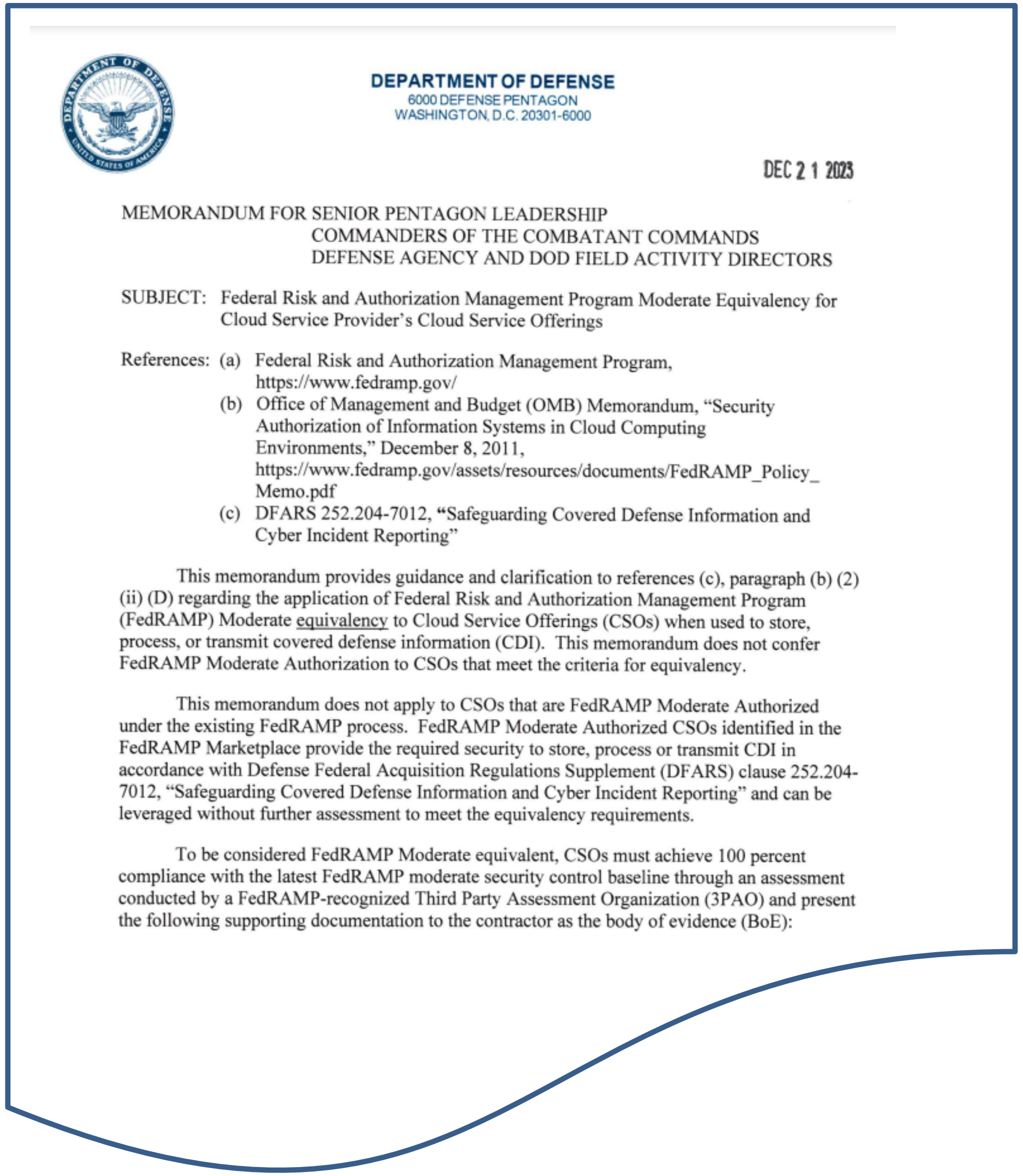
DFARS 7012 FedRAMP Equivalency DoD CIO Memo

BoE – Body of Evidence required by CSP, Cloud Service Offerings to Contractors for DCMA DIBCAC

- System Security Plan
- Security Assessment Plan
- Security Assessment Report by FedRAMP 3PAO
- Plan of Action and Milestones
  - Continuous Monitoring Only

No POA&MS for 3PAO Validation Opinion: 2 Nation State

DFARS 7012 c) – g) incident reporting, malware, etc applies



DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

DEC 2 1 2023

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
COMMANDERS OF THE COMBATANT COMMANDS
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Federal Risk and Authorization Management Program Moderate Equivalency for Cloud Service Provider's Cloud Service Offerings

References: (a) Federal Risk and Authorization Management Program, https://www.fedramp.gov/
(b) Office of Management and Budget (OMB) Memorandum, "Security Authorization of Information Systems in Cloud Computing Environments," December 8, 2011, https://www.fedramp.gov/assets/resources/documents/FedRAMP_Policy_Memo.pdf
(c) DFARS 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting"

This memorandum provides guidance and clarification to references (c), paragraph (b) (2) (ii) (D) regarding the application of Federal Risk and Authorization Management Program (FedRAMP) Moderate equivalency to Cloud Service Offerings (CSOs) when used to store, process, or transmit covered defense information (CDI). This memorandum does not confer FedRAMP Moderate Authorization to CSOs that meet the criteria for equivalency.

This memorandum does not apply to CSOs that are FedRAMP Moderate Authorized under the existing FedRAMP process. FedRAMP Moderate Authorized CSOs identified in the FedRAMP Marketplace provide the required security to store, process or transmit CDI in accordance with Defense Federal Acquisition Regulations Supplement (DFARS) clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting" and can be leveraged without further assessment to meet the equivalency requirements.

To be considered FedRAMP Moderate equivalent, CSOs must achieve 100 percent compliance with the latest FedRAMP moderate security control baseline through an assessment conducted by a FedRAMP-recognized Third Party Assessment Organization (3PAO) and present the following supporting documentation to the contractor as the body of evidence (BoE):

https://dodcio.defense.gov/Portals/0/Documents/Library/FEDRAMP-EquivalencyCloudServiceProviders.pdf

Approved for Public Release

Cloud Service Provider (CSP) Services and Government Standards Summary
Industry as Customer/Tenant with Government Sensitive Data Specifications

Product	Cloud Type	FedRAMP Authorization	ITAR/EAR* Foreign Restricted	NIST 800-53/171
Product A Commercial	Public	High/JAB	No	Yes + 7012 Memo
Product B Moderate	Government	High/DISA SaaS Moderate	No	Yes ?
Product C High	Government	High/Treasury	Yes	Yes ?
Product D Commercial	Public	Moderate/JAB	No	Yes ?
Product E Government	Government	High/JAB	Yes	Yes

Cloud Service Provider and Tenant(s) Share Configuration & Operations

Approved for Public Release

FedRAMP & OSCAL

Overall SSP Checks

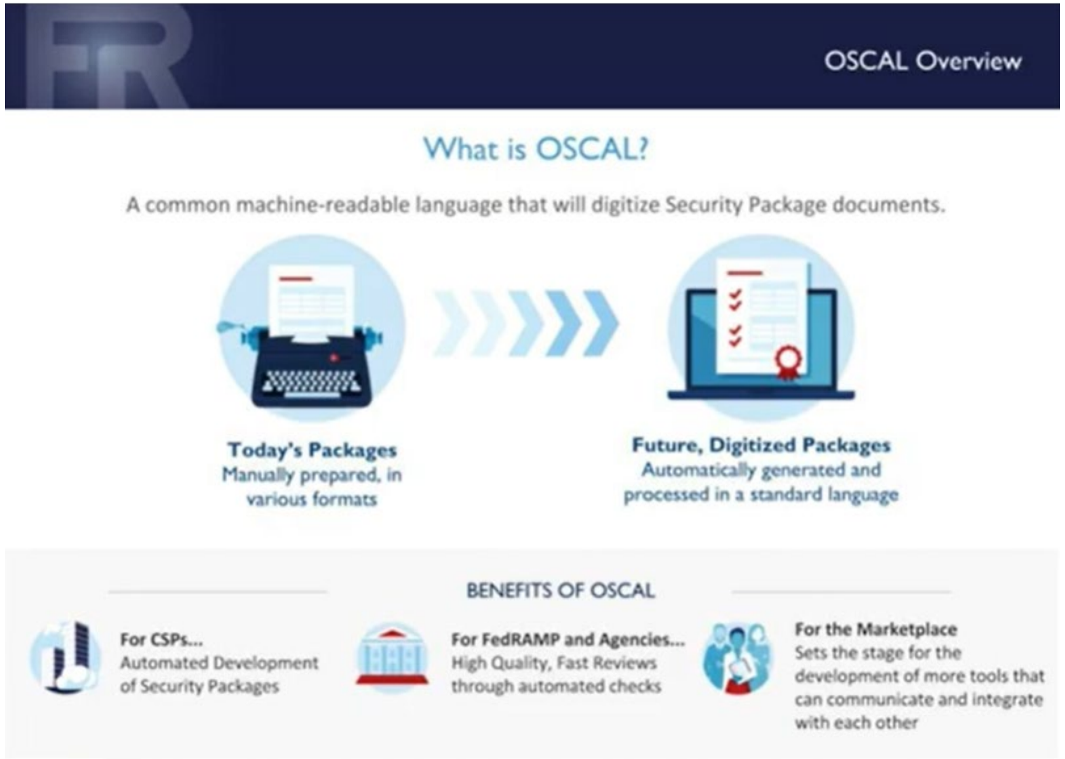
- ☐ 1a Is the correct SSP Template used?
- ☐ 1b Is the correct Deployment Model chosen for the system?
- ☐ 2 Do all controls have at least one implementation status checkbox selected?
- ☐ 3 Are all critical controls implemented?
- ☐ 4a Are the customer responsibilities clearly identified in the CIS-CRM Tab, as well as the SSP Controls (by checkbox selected and in the implementation description)? Are the CIS-CRM and SSP controls consistent for customer responsibilities? A sampling of seven controls involving customer roles is reviewed.
- ☐ 4b Does the Initial Authorizing Agency concur with the CRM (adequacy and clarity of customer responsibilities)?
- ☐ 5 Does the Roles Table (User Roles and Privileges) sufficiently describe the range of user roles, responsibilities, and access privileges?
- ☐ 6 In the control summary tables, does the information in the Responsible Role row correctly describe the required entities responsible for fulfilling the control? (50% complete, control mapping will complete this work in 18F/fedramp-automation#51)

.

.

.

- ☐ 16



OSCAL Overview

What is OSCAL?

A common machine-readable language that will digitize Security Package documents.

Today's Packages
Manually prepared, in various formats

Future, Digitized Packages
Automatically generated and processed in a standard language

BENEFITS OF OSCAL

For CSPs...
Automated Development of Security Packages

For FedRAMP and Agencies...
High Quality, Fast Reviews through automated checks

For the Marketplace
Sets the stage for the development of more tools that can communicate and integrate with each other

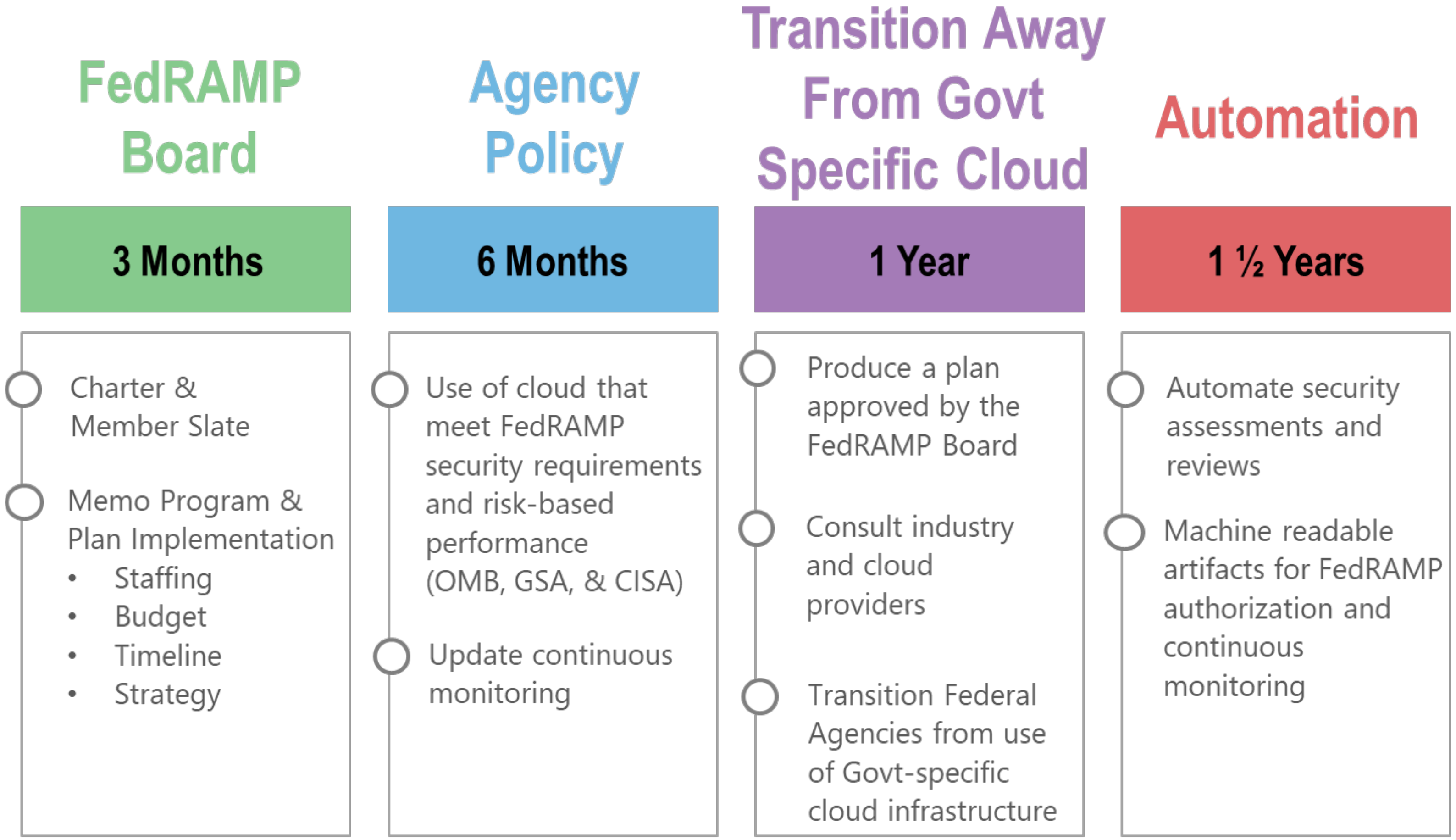
Approved for Public Release

OMB FedRAMP Modernization Memo

Replaces ~12 year dated Office of Management and Budget (OMB) Memorandum With intention to Strengthen the FedRAMP Cloud Authorization Program

<u>Key Areas</u>

- Risk Profiles & Evolving Cyber Risks
- Increase Agency Use/Re-use of FedRAMP cloud products and services
- Streamline the FedRAMP Authorization Process w/industry best practices
- Information sharing on threats and best practices
- NIST RMF & Standards
  - Reference to sw provenance



FedRAMP Board

3 Months

- Charter & Member Slate
- Memo Program & Plan Implementation
  - Staffing
  - Budget
  - Timeline
  - Strategy

Agency Policy

6 Months

- Use of cloud that meet FedRAMP security requirements and risk-based performance (OMB, GSA, & CISA)
- Update continuous monitoring

Transition Away From Govt Specific Cloud

1 Year

- Produce a plan approved by the FedRAMP Board
- Consult industry and cloud providers
- Transition Federal Agencies from use of Govt-specific cloud infrastructure

Automation

1 ½ Years

- Automate security assessments and reviews
- Machine readable artifacts for FedRAMP authorization and continuous monitoring

Approved for Public Release

https://www.fedramp.gov/2024-06-04-fedramp-governance/
https://www.fedramp.gov/assets/resources/documents/FedRAMP-Program-Roadmap-2024-2025-Public-Artifact.pdf