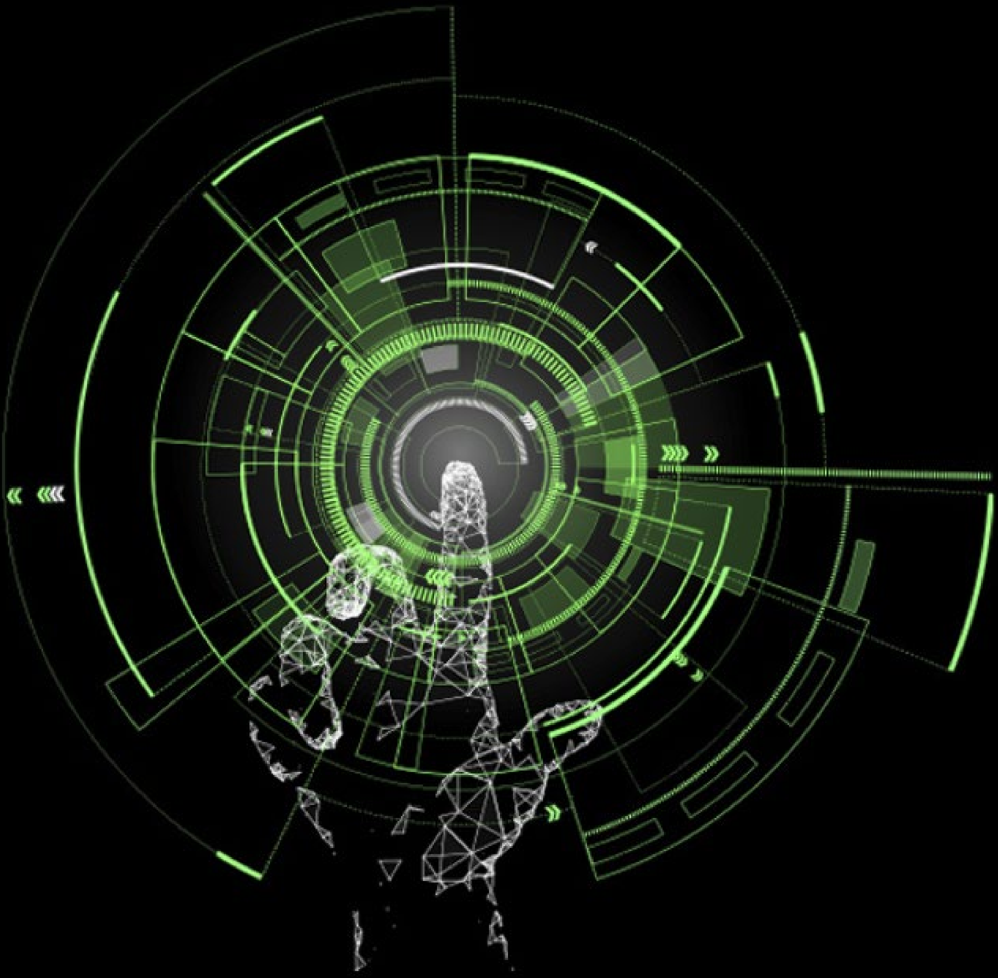
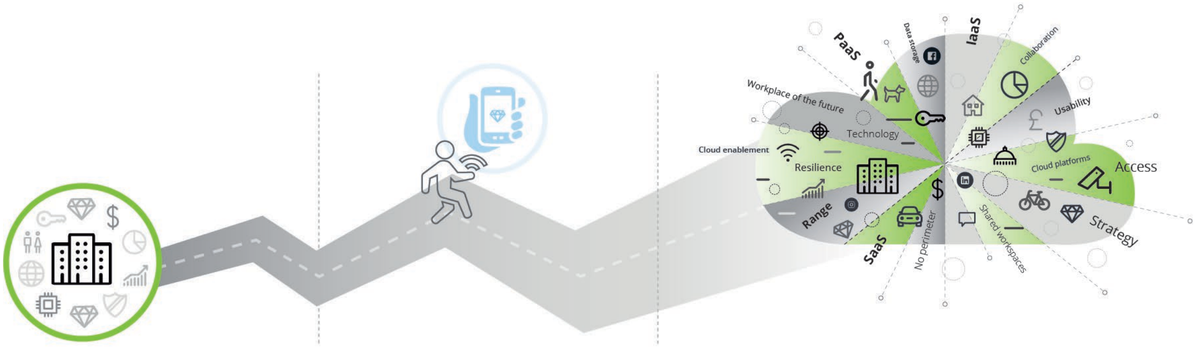
Deloitte.



The path to FedRAMP authorization for Cloud Service Providers

So, what is FedRAMP?

Spurred by the U.S. Government's Cloud First policy, the Federal Risk and Authorization Management Program (FedRAMP[1]) is a security assessment and authorization process that created with the goal of providing a **consistent** and **efficient** mechanism for applying security and measuring risk in cloud resources used by Federal agencies.



Is FedRAMP applicable to your organization?

- FedRAMP authorizations are required for **multi-tenant clouds** that are storing Federal agency Data or Metadata.
- FedRAMP is also a commonly used standard for cloud security by the U.S. government and supporting contractors. **Even if your cloud is not multi-tenant, or is indirectly supporting an agency, you may still be required to show proof of compliance,** even if it does not result in a FedRAMP authorization.

What are the benefits of achieving a FedRAMP authorization?

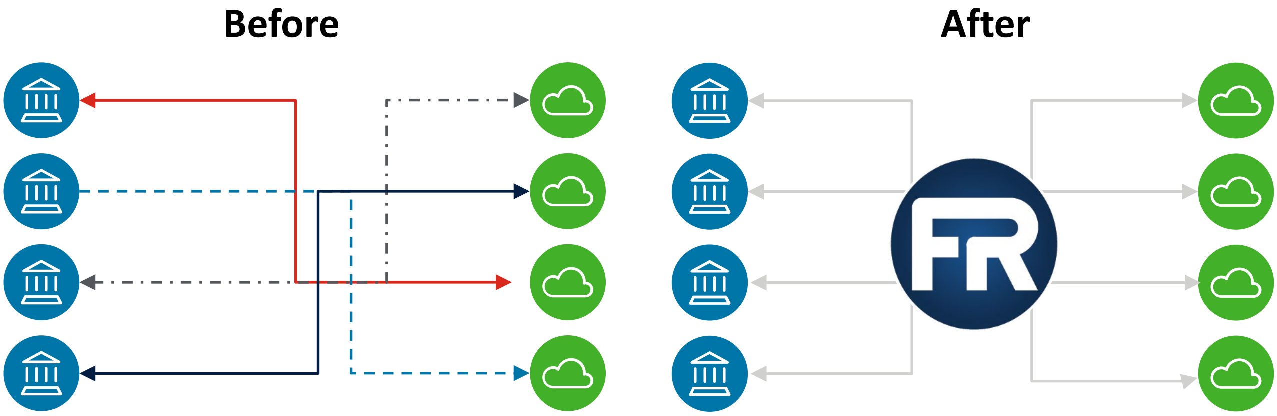
- FedRAMP authorizations are **required for many U.S. Government cloud contracts.**
- FedRAMP authorizations are **re-usable** and **scalable**, as FedRAMP Security Packages may be re-used as the basis for future authorizations and **may be built on top of each other** using Infrastructure and Platform as a Service (IaaS and PaaS) technologies.
- Lastly, a FedRAMP authorization is a widely recognized security milestone, even outside of the public sector.

Copyright © 2023 Deloitte Development LLC. All rights reserved

[1] See www.FedRAMP.gov for more information on the FedRAMP program.

How does it work?

Despite recently becoming a law, **FedRAMP does not operate on its own**. It is a program that layers on top of the Risk Management Framework (RMF) and Authorization to Operate (ATO) processes employed by U.S. Government agencies when evaluating whether to use software and services. By issuing cloud-specific guidance and acting as a middleman, FedRAMP makes ATO's more consistent, trustworthy, and re-usable across each agency.



This means that when your organization is providing a multi-tenant cloud service to the U.S. Federal Government, you will be seeking two authorizations:

- An **agency ATO**, coming from your sponsoring agency (or a provisional ATO, which we will explain later) will allow you to do business with your contracting agency
- A **FedRAMP authorization**, coming from the FedRAMP Program Management Office (PMO), will publicly acknowledge your service as a FedRAMP authorized cloud service offering (CSO) and allow prospective U.S. Government clients to perform a security review of your System

Copyright © 2023 Deloitte Development LLC. All rights reserved

What are my options?

The FedRAMP process is tailored to your offering as a Cloud Service Provider (CSP). Specific requirements vary based on the type of data stored in your System and how many agencies want to use it.

Impact levels

Three different FedRAMP impact levels are available to CSP's, depending on the sensitivity of the data that they store (see FIPS-199).

Impact level	Required security controls[1]
Low	156
Moderate	323
High	410

Working with the Department of Defense (DoD)? You might be required to implement certain network architecture changes and comply with additional DoD Cloud Security Requirements Guide (SRG) controls:

DoD Cloud SRG Impact Level	Additional security controls
Moderate + IL2	None
Moderate + IL4	38
Moderate + IL5	47

Paths to authorization

CSPs may move through the FedRAMP process via agency sponsorship, or via the Joint Authorization Board (JAB).

The **Agency Sponsorship** path is the standard process used by CSPs that have few or just one contract with US Government agencies for their cloud product. This path is more flexible, and there is the opportunity for the agency to accept risks associated with vulnerabilities in your System and/or gaps in your security controls.

vs

The **JAB Path** is a special path to FedRAMP authorization that is designed for CSPs with interest from many different U.S. Government agencies. It is a more difficult process that allows for little or no risk acceptance but provides a much faster time to authorization by many agencies at once.

[1] Control counts derived from the FedRAMP Security Controls Baseline (revision 5): https://www.fedramp.gov/assets/resources/documents/FedRAMP_Security_Controls_Baseline.xlsx

Copyright © 2023 Deloitte Development LLC. All rights reserved

What are the FedRAMP Security Controls?

FedRAMP Security Control Families:

- AC—Access Control
- AT—Awareness and Training
- AU—Audit and Accountability
- CA—Security Assessment & Authorization
- CM—Configuration Management
- CP—Contingency Planning
- IA—Identification & Authentication
- IR—Incident Response
- MA—Maintenance
- MP—Media Protection
- PE—Physical and Environmental Protection
- PL—Planning
- PS—Personnel Security
- RA—Risk Assessment
- SA—System & Services Acquisition
- SC—System & Communications Protection
- SI—System & Information Integrity
- SR – Supply Chain Risk Management

Examples of Critical FedRAMP Requirements:

Keeping Track of Federal Data and Metadata

- Federal data and metadata should stay within the authorization boundary, except when moving to another federally authorized system.

Complying with Federal Information Processing Standard (FIPS) 140 Requirements

- Encryption modules in-use within the authorization boundary must be FIPS 140 validated.

Consistency in Configuration Management

- FedRAMP requires you to utilize DoD Security Technical Implementation Guides (STIGs) for infrastructure supporting the environment, alongside automated monitoring for configuration drift.

Implementing Multi-Factor Authentication (MFA)

- MFA is required for access to the authorization boundary, regardless of whether users are an administrator or a customer.

Establishing Effective Vulnerability Management

- FedRAMP requires authenticated vulnerability scans of infrastructure within the authorization boundary on a monthly basis, and remediation of vulnerabilities in 30/90/180 days for High/Medium/Low risk vulnerabilities, respectively.

FedRAMP documentation Requirements

- FedRAMP's documentation requirements are massive, including a 400+ page System Security Plan (SSP), FIPS-199 assessment, Continuous Monitoring Plan, Incident Response Procedures, Contingency Plan, and security policies/procedures for 17 control families.

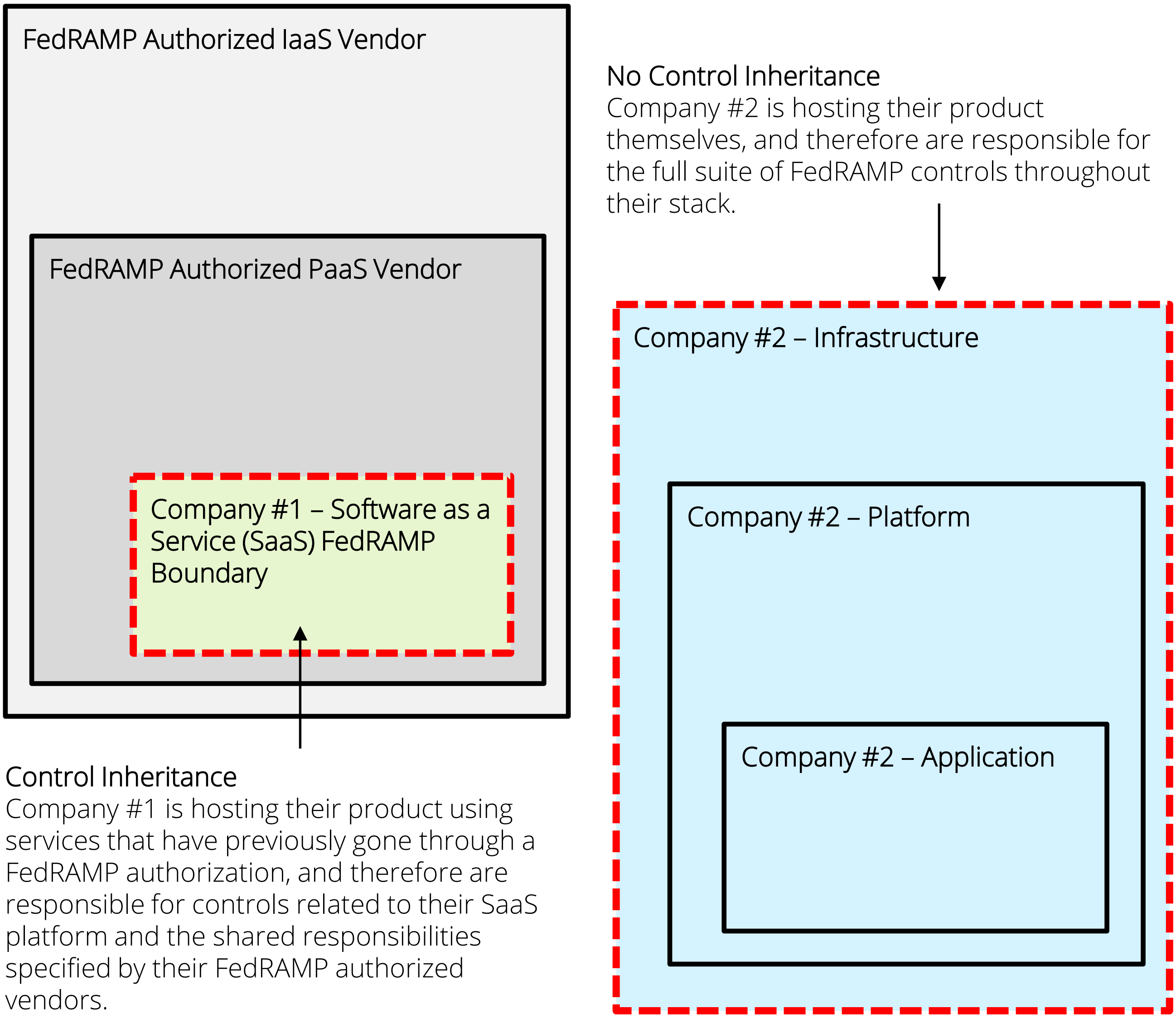
Monthly Continuous Monitoring (ConMon) Commitments

- Once authorized, FedRAMP requires reporting on security controls and Plans of Action and Milestones (POA&M's) on a monthly basis with each sponsoring agency (or the JAB).

Copyright © 2023 Deloitte Development LLC. All rights reserved

Am I responsible for everything?

Not necessarily! Because FedRAMP authorizations are managed by a central body, FedRAMP authorizations may be stacked upon one another. Hyperscale cloud providers like Amazon Web Services, Microsoft Azure, and Google Cloud Platform provide building blocks for your solution that are compliant out of the box:

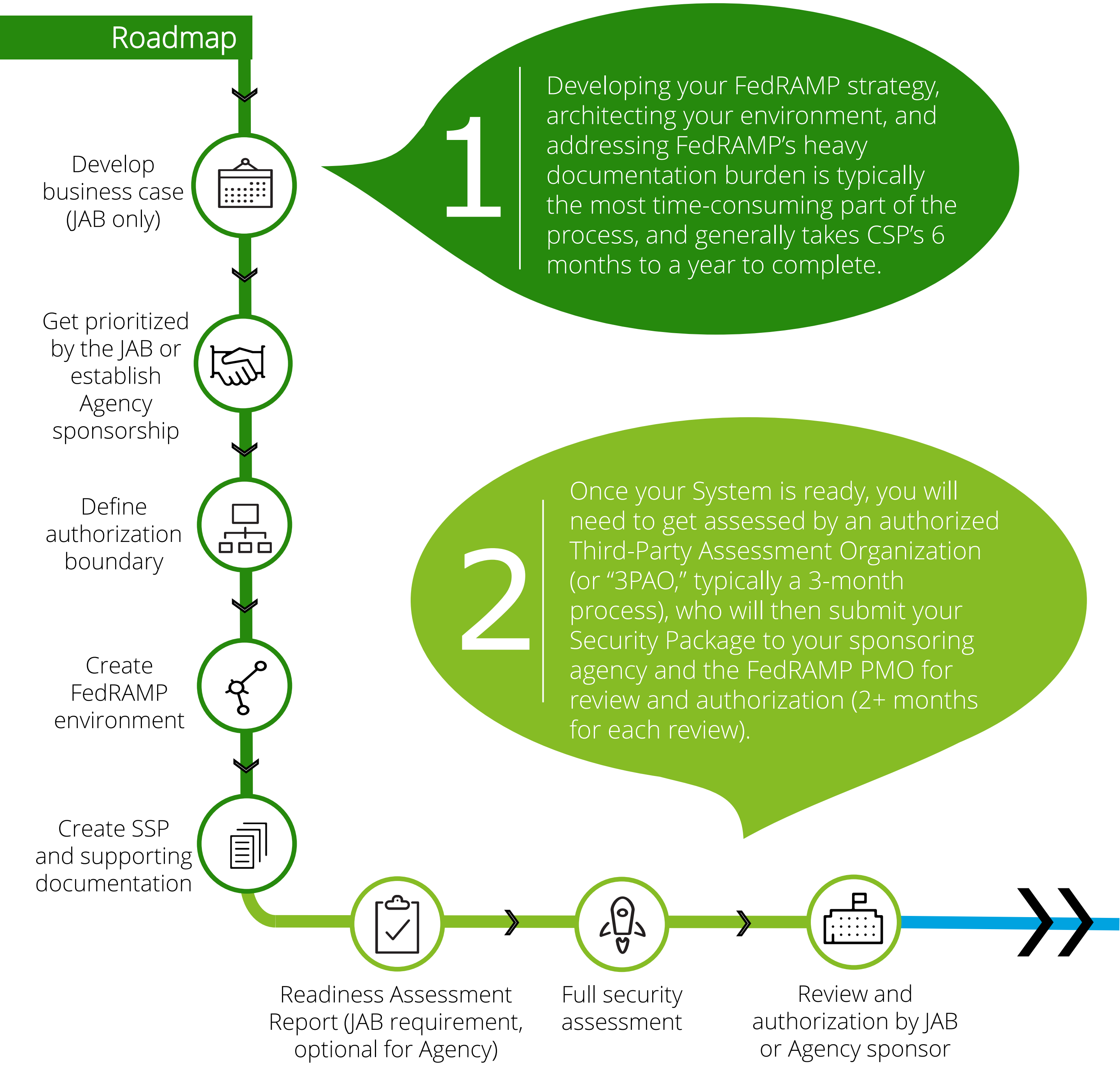

FedRAMP Authorized IaaS Vendor
FedRAMP Authorized PaaS Vendor
Company #1 – Software as a Service (SaaS) FedRAMP Boundary
Company #2 – Infrastructure
Company #2 – Platform
Company #2 – Application

No Control Inheritance
Company #2 is hosting their product themselves, and therefore are responsible for the full suite of FedRAMP controls throughout their stack.

Control Inheritance
Company #1 is hosting their product using services that have previously gone through a FedRAMP authorization, and therefore are responsible for controls related to their SaaS platform and the shared responsibilities specified by their FedRAMP authorized vendors.

Copyright © 2023 Deloitte Development LLC. All rights reserved

Okay, so how do I get authorized?...



Roadmap
Develop business case (JAB only)
Get prioritized by the JAB or establish Agency sponsorship
Define authorization boundary
Create FedRAMP environment
Create SSP and supporting documentation
Readiness Assessment Report (JAB requirement, optional for Agency)
Full security assessment
Review and authorization by JAB or Agency sponsor

1 Developing your FedRAMP strategy, architecting your environment, and addressing FedRAMP's heavy documentation burden is typically the most time-consuming part of the process, and generally takes CSP's 6 months to a year to complete.

2 Once your System is ready, you will need to get assessed by an authorized Third-Party Assessment Organization (or "3PAO," typically a 3-month process), who will then submit your Security Package to your sponsoring agency and the FedRAMP PMO for review and authorization (2+ months for each review).

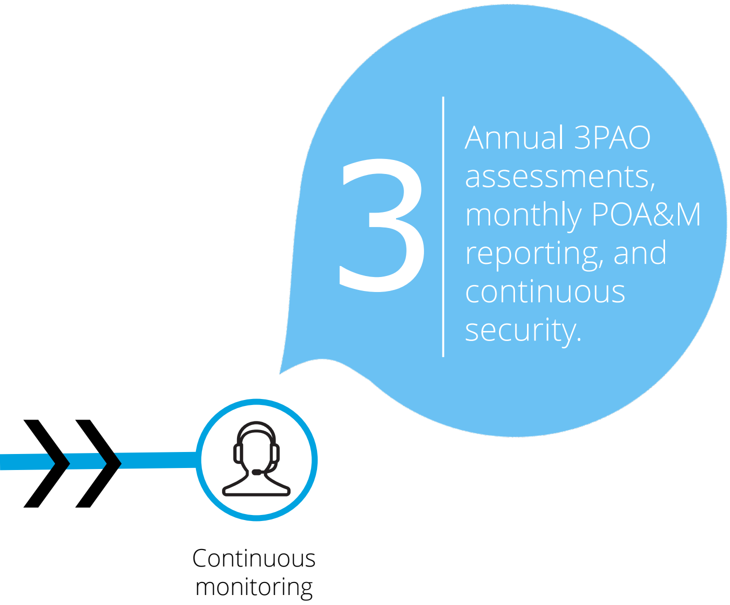
Copyright © 2023 Deloitte Development LLC. All rights reserved

…and how do I maintain my authorization?

During and after your 3PAO assessment, you will be responsible for “Continuous Monitoring” or “ConMon” requirements for the duration of your security authorization.

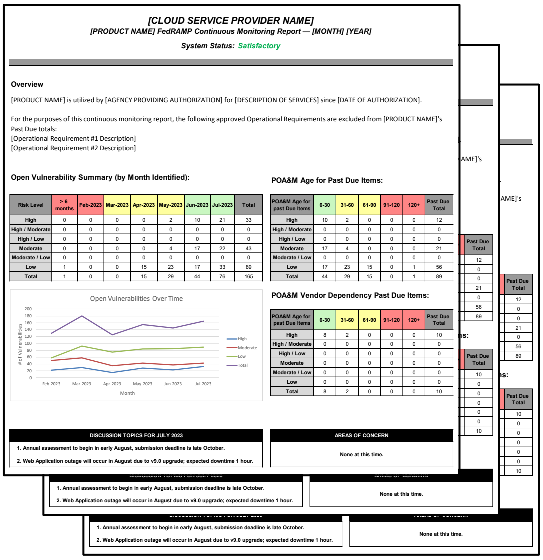
ConMon requirements are both operational and reporting focused, and they help your sponsoring agency understand the ongoing security health of your organization:

- Annual 3PAO assessments and assessments of significant changes (typically prior to implementation)
- Monthly reports of authenticated vulnerability scans
- Remediation tracking of open risks in the format of "Plans of Action and Milestones" (POA&Ms)



3 | Annual 3PAO assessments, monthly POA&M reporting, and continuous security.

Continuous monitoring



[CLOUD SERVICE PROVIDER NAME]
[PRODUCT NAME] FedRAMP Continuous Monitoring Report — [MONTH] [YEAR]
System Status: Satisfactory

Overview

[PRODUCT NAME] is utilized by [AGENCY PROVIDING AUTHORIZATION] for [DESCRIPTION OF SERVICES] since [DATE OF AUTHORIZATION].

For the purposes of this continuous monitoring report, the following approved Operational Requirements are excluded from [PRODUCT NAME]'s Past Due totals:
[Operational Requirement #1 Description]
[Operational Requirement #2 Description]

Open Vulnerability Summary (by Month Identified):

Risk Level	> 6 months	Feb-2023	Mar-2023	Apr-2023	May-2023	Jun-2023	Jul-2023	Total
High	0	0	0	0	2	10	21	33
High / Moderate	0	0	0	0	0	0	0	0
High / Low	0	0	0	0	0	0	0	0
Moderate	0	0	0	0	4	17	22	43
Moderate / Low	0	0	0	0	0	0	0	0
Low	1	0	0	15	23	17	33	89
Total	1	0	0	15	29	44	76	165

Open Vulnerabilities Over Time

POA&M Age for Past Due Items:

POA&M Age for past Due Items	0-30	31-60	61-90	91-120	120+	Past Due Total
High	10	2	0	0	0	12
High / Moderate	0	0	0	0	0	0
High / Low	0	0	0	0	0	0
Moderate	17	4	0	0	0	21
Moderate / Low	0	0	0	0	0	0
Low	17	23	15	0	1	56
Total	44	29	15	0	1	89

POA&M Vendor Dependency Past Due Items:

POA&M Age for past Due Items	0-30	31-60	61-90	91-120	120+	Past Due Total
High	8	2	0	0	0	10
High / Moderate	0	0	0	0	0	0
High / Low	0	0	0	0	0	0
Moderate	0	0	0	0	0	0
Moderate / Low	0	0	0	0	0	0
Low	0	0	0	0	0	0
Total	8	2	0	0	0	10

DISCUSSION TOPICS FOR JULY 2023

1. Annual assessment to begin in early August, submission deadline is late October.
2. Web Application outage will occur in August due to v9.0 upgrade; expected downtime 1 hour.

AREAS OF CONCERN

None at this time.

1. Annual assessment to begin in early August, submission deadline is late October.
2. Web Application outage will occur in August due to v9.0 upgrade; expected downtime 1 hour.
None at this time.
1. Annual assessment to begin in early August, submission deadline is late October.
2. Web Application outage will occur in August due to v9.0 upgrade; expected downtime 1 hour.
None at this time.

Copyright © 2023 Deloitte Development LLC. All rights reserved

How can Deloitte help me get there?

Deloitte can advise and assist with various FedRAMP needs.

3PAO Assessment and Advisory

- Perform full security assessments or Readiness Assessment Report (RAR) (Requires independence)
- Perform gap assessments against FedRAMP standards
- Direct assistance in design and implementation of security controls, including documentation support
- Assist in navigating through the authorization process

Security, architecture, and engineering

- Architecture guidance and hands-on-keyboard support
- Infrastructure as code development
- Automation implementation
- Project management oversight of architecture builds

Vulnerability management

- Establishing a sustainable, consistent vulnerability management process
- Establishing effective patching plans and development processes to remediate vulnerabilities

Platform Hosting Services

- Hosting services on Deloitte's PaaS
- Accelerate your path to authorization by inheriting Deloitte's controls at the platform and infrastructure layers

Note: If performing the 3PAO assessment, Deloitte can advise the company in readiness activities, however it cannot assume any management roles including remediation.

Copyright © 2023 Deloitte Development LLC. All rights reserved

Frequently Asked Questions

Are FedRAMP assessments difficult? What gets assessed? Generally speaking, FedRAMP assessments are much more comprehensive and stringent than similar commercial examinations that focus on a particular product. A FedRAMP assessment requires comprehensive security control testing, authenticated vulnerability scanning, and a penetration test to all be performed by your 3PAO.

What's my system scope? The scope of your FedRAMP requirements (your "Authorization Boundary") follows the Federal Data and Federal Metadata (to include security data) that will be stored within your System.

Does FedRAMP provide reciprocity with other standards? Yes. FedRAMP Low provides one-way reciprocity with StateRAMP Low, and FedRAMP Moderate provides one-way reciprocity with StateRAMP Low, Low+, Moderate, and DoD Cloud SRG IL2.

What are the independence requirements for 3PAO's? Your 3PAO must remain independent[1] of the CSP's they are assessing. In other words, if a firm is conducting your FedRAMP assessment, they generally cannot support your organization from an advisory perspective.

Hold on, wasn't the National Institute of Standards and Technology (NIST) 800-53 standard just updated to revision 5? Yes! Revision 5 to the NIST 800-53 standard has been released and FedRAMP has recently completed their public comment period on revised FedRAMP templates against the new standard, expected to go live in 2023. This new standard brings with it new requirements for Supply Chain and Privacy controls.

[1] A full list of 3PAO requirements, including independence requirements, can be found in the 3PAO Obligations and Performance Guide: https://www.fedramp.gov/assets/resources/documents/3PAO_Obligations_and_Performance_Guide.pdf

Copyright © 2023 Deloitte Development LLC. All rights reserved

Let’s Talk

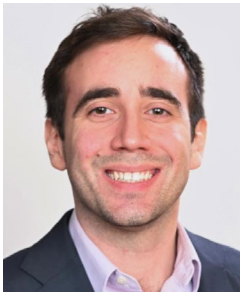
Have a question that isn’t addressed here, or want to understand the services we can provide for your organization? Let’s get in touch!

Matt Bogusch

Managing Director
Deloitte & Touche LLP
mbogusch@deloitte.com

Scott Maker

Managing Director
Deloitte & Touche LLP
smaker@deloitte.com



Joe Bartos

Senior Manager
Deloitte & Touche LLP
jobartos@deloitte.com

Copyright © 2023 Deloitte Development LLC. All rights reserved

Deloitte.

This document contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this document.

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2023 Deloitte Development LLC. All rights reserved