Доставка на софтуер - особености и процеси

Тема №4

Разпространени стандарти и регулации, гарантиращи определени характеристики на даден продукт и услуга

Част 2: FedRAMP

Съдържание

1 Въведение

Федералната програма за управление на риска и оторизациите (FedRAMP) е създадена през 2011 г., с цел предоставяне на ценово ефективен, базиран на управление на риска подход за приемане и използване на облачни услуги от федералното правителство на САЩ. FedRAMP дава възможност на агенциите да използват модерни технологии в областта на облачните услуги, като се акцентира върху сигурността и защитата на федералната информация. FedRAMP е законово установен стандартизиран подход за оценка на сигурността, оторизация и непрекъснато мониториране на облачни продукти и услуги, които обработват некласифицирана федерална информация.

FedRAMP създава и управлява основен набор от процеси, за да гарантира ефективна и повторяема облачна сигурност за правителството. Също така установява списък на услуги и техните доставчици, за да насърчи използването и запознаването с облачните услуги, като в същото време улеснява

сътрудничеството в правителството чрез открит обмен на знания, сценарии на употреба и тактически решения.

1.1 Предимства

- Намалява дупликацията на усилия, несъответствията и неефективността на разходите.
- Създава обществено-частно партньорство за насърчаване на иновациите и развитието на по-сигурни информационни технологии.
- Позволява на федералното правителство да ускори приемането на облачните технологии, създавайки прозрачни стандарти и процеси за оторизации за сигурност и позволявайки на агенциите да използват оторизациите за сигурност на общо правителствено равнище.

1.2 Цели

- Да увеличи използването на сигурни облачни технологии от страна на правителствените агенции.
- Да подобри рамката, чрез която правителството осигурява и упълномощава облачни технологии.
- Да изгражда и насърчава тесни партньорства с участниците във FedRAMP.

1.3 Законова база

FedRAMP стандартизира изискванията за сигурност при упълномощаването и непрекъснатата киберсигурност на облачни услуги в съответствие с FISMA, OMB Circular A-130 и политиката на FedRAMP, както и с FedRAMP Authorization Act, като част от National Defense Authorization Act (NDAA).

Законът за модернизация на сигурността на федералната информация (Federal Information Security Modernization Act / FISMA) изисква от агенциите да защитават федералната информация. Съответно FedRAMP прилага FISMA изискванията в контекста на облачния софтуер.

Офисът за управление и бюджет (Office of Management and Budget / OMB) уточнява, че когато агенциите прилагат FISMA, те трябва да използват стандартите и насоките на Националния институт по стандарти и технологии (National Institute of Standards and Technology / NIST).

FedRAMP използва стандартите и насоките на Националния институт по стандарти и технологии (NIST) с цел предоставяне на стандартизирани изисквания за сигурността на облачни услуги, програма за оценка на съответствието, стандартизирани пакети за упълномощаване и договорен език, както и хранилище за пакети за упълномощаване.

FedRAMP Authorization Act установява правителствена програма, предоставяща стандартизиран и преизползваем подход към оценката на сигурността и упълномощаването на облачни продукти и услуги за обработка на не класифицирана информация, използвана от агенциите.

Компаниите доставчици на облачни услуги (Cloud Service Provider / CSP) се стремят да получат така наречената FedRAMP оторизация, даваща им зелена светлина за предоставяне на услугите си към правителствения сектор на САЩ. Начините за получаване на такава оторизация ще разгледаме след малко. При вземането на бизнес решение относно типа на FedRAMP оторизация, която е най-подходяща за дадена услуга, е важно да се обмисли общата стратегия за клиентите от федералното правителство. Също така е важно да се разбере готовността на организацията относно процеса на FedRAMP оторизация. Доставчик на облачни услуги трябва да бъде готов да демонстрира дали услугата му е вече работеща или се разработва, както и обема на текущото търсене на услугата на федералния пазар.

2 Участници в процеса на оторизация

Освен доставчика на облачната услуга като основен и очевиден участник в процеса, има и няколко други ключови участника, които имат съществен принос в постигането на FedRAMP оторизация.

2.1 FedRAMP Program Management Office (PMO)

Отговорен за предоставянето на единен процес на заинтересованите страни, FedRAMP PMO е ключов партньор за CSP (Cloud Service Providers), които извършват изследвания или търсят оторизация от FedRAMP за своя CSO (Cloud Service Offering). Неговите отговорности включват:

- грижа за процеса на упълномощаване от FedRAMP
- координация с JAB (Joint Authorization Board) за приоритизиране на доставчиците с цел постигане на JAB Provisional Authorization to Operate (P-ATO) - след малко ще изясним този термин
- подкрепа за управление на проекти за CSP и агенции
- предоставяне на услуги, които могат да бъдат преизползвани в целия федерален сектор, като предоставя сигурно хранилище на оторизациите от FedRAMP

2.2 Joint Authorization Board (JAB)

JAB (Joint Authorization Board) е основното управленско и вземащо решения тяло на FedRAMP. JAB включва Главните информационни офицери (CIO) на Департамента по национална сигурност (DHS), Администрацията за обществените услуги (GSA) и Министерството на отбраната (DoD). JAB определя и установява базовите контроли за сигурността на FedRAMP и критериите за акредитация на Организациите за оценка от трета страна (3PAO). JAB работи тясно с FedRAMP PMO, за да гарантира, че базовите контроли за сигурността на FedRAMP се въвеждат в последователни и повторяеми процеси за оценка на сигурността и оторизация на CSO (Cloud Service Offerings).

CSP (Cloud Service Providers), които вземат бизнес решение да преследват JAB P-ATO за своя CSO, се приоретизират чрез FedRAMP Connect. По време на този процес на приоритизация, JAB се стреми да оторизира облачни услуги, които счита, че са най-вероятно да бъдат използвани в целия правителствен сектор. Това се разглежда подробно в Критериите за приоретизация на JAB на FedRAMP. За CSO, които постигат P-ATO, JAB също се грижи, че тези системи поддържат приемлив рисков профил чрез Непрекъснато мониториране (ConMon).

2.3 Федерални агенции

Доставчиците на облачни услуги (CSP), които вземат бизнес решение да работят директно с агенция с цел получаване на Оторизация за Опериране (Authorization to Operate / ATO), ще си сътрудничат с агенцията през целия процес на оторизация от FedRAMP. Агенциите дефинират своите специфични политики и процедури, допълнително към изискванията на FedRAMP, и са отговорни за прегледа на пакетите за сигурност, разработени от CSP. Най-накрая, Оторизиращия представител (Authorizing Official / AO) на агенцията трябва да приеме риска, свързан с използването на облачна услуга, чрез издаването на Оторизация за Опериране за тяхната агенция. Агенциите трябва също така да извършват непрекъснат мониторинг на всяка оторизирана система в употреба, като преглеждат месечни и годишни артефакти, предоставяни от CSP.

Оторизиращият представител (AO) на агенция е високопоставен федерален служител, който носи окончателната отговорност за вземането на рисково обосновано решение за предоставяне на Оторизация за Опериране (ATO) за предлаганата от CSP услуга. Решението се формализира в писмо за Оторизация за Опериране, предоставено на CSP и на FedRAMP PMO. Оторизиращите представители имат достатъчна видимост в рамките на своята организация, за да разберат въздействието и разходите от индивидуален CSO върху средата на сигурността и операциите на агенцията.

Първоначалната ATO от агенцията не представлява приемане на риск от страна на цялото правителство. Също така, първоначалната оторизираща агенция не носи отговорност за извършването на непрекъснат мониторинг от името на всички федерални агенции. Всяка агенция трябва да издаде ATO за своето собствено използване на CSO и да преглежда артефактите чрез непрекъснат мониторинг, за да осигури, че нивото на сигурността е задоволително за продължаваща употреба от страна на агенцията. CSP с множество клиенти-агенции трябва да установи сътруднически подход към Непрекъснатия мониторинг.

2.4 Third Party Assessment Organizations (3PAOs)

Като независими трети страни, Организациите за оценка от трета страна (3PAO) извършват начални и периодични оценки на облачни услуги, за да гарантират тяхното съответствие с изискванията на FedRAMP. CSP, които преследват FedRAMP оторизация, трябва да осигурят оценка от независима трета страна за техните CSO.

За процеса на оторизация от JAB, CSP трябва да избере 3PAO, призната от FedRAMP, която отговаря на необходимите изисквания за качество, независимост и познание на FedRAMP, за да извършва задължителните независими оценки на сигурността.

За процеса на оторизация от агенция, повечето оценки се извършват с използването на признатата от FedRAMP 3PAO. Въпреки това агенция може да избере да използва своята Организация за независима верификация и валидация (Independent Verification and Validation / IV&V) за оценка на CSO.

По време на началната оценка, оценителите са отговорни за разработването на План за оценка на сигурността (Security Assessment Plan / SAP) и Доклад за оценка на сигурността (Security Assessment Report / SAR). Организациите за оценка от трета страна, признати от FedRAMP, могат да се намерят в платформата FedRAMP Marketplace.

Ако агенция избере да използва собствения си екип за независима верификация и валидация или оценител от трета страна, който не е признат от FedRAMP като 3PAO, Оторизиращият представител на агенцията трябва да заяви и докаже независимостта на организацията за оценка. Освен това, организацията за оценка трябва да използва предоставените от FedRAMP шаблони.

3 Стратегия за получаване на оторизация

Съществуват два подхода за получаване на Оторизация от FedRAMP: Оторизация чрез JAB или Оторизация чрез агенция. Трябва да се вземат предвид редица фактори, за да се определи подходяща стратегия за оторизация.

3.1 Търсенето: Широко срещу Специфично

Търсенето е ключов фактор за CSP, които вземат решение между преследване на JAB P-ATO или ATO от агенция-партньор. Обикновено FedRAMP оценява CSO като с търсене в широк мащаб или в конкретна ниша. Търсенето в широк мащаб отразява доказан или потенциален интерес към услугата от страна на няколко агенции, докато търсенето в конкретна ниша отразява специфичната полезност или приложимост на услугата за конкретна агенция. При оценка кой тип оторизация да се търси, CSP трябва да може да уточни типа търсене, тъй като CSO с широко търсене са по-подходящи за JAB P-ATO, а CSO с търсене в ниша са по-подходящи за ATO от агенция.

3.2 Съществуващи или Потенциални Партньори от Агенцията

Първата стъпка за постигане на Оторизация от FedRAMP чрез агенция е CSP да установи партньорство с федерална агенция. Някои CSP може вече да имат агенция или агенции, които са заинтересовани да оторизират техните CSO, защото вече използват услугата или използват on-premise версия и желаят да преминат към облачна. Други CSP може да имат потенциални клиенти, които са заинтересовани от тяхната услуга или пък да реагират на Заявки за предложения (Requests for Proposals / RFPs), които включват изисквания за FedRAMP съответствие. Важно е да се обсъжда FedRAMP рано в процеса. PMO може да сътрудничи с CSP в разговори с агенции, за да отговори на въпроси или опасения относно процеса на оторизация.

3.3 Тип облачен модел

CSP трябва да уточни дали техният CSO е правителствен, обществен, частен или съществува като хибриден облак, спрямо дефинициите в NIST SP 800-145 при определянето на облачния модел.

- **Правителствен (Government-Only Community):** Облакът съдържа само данни на правителството. Клиентите могат да бъдат федерални, щатски, местни, племенни, териториални, научни центрове, финансирани от федералното правителство, подизпълнители, работещи от името на правителството, или лаборатории.

- **Публичен (Public):** Обществениият облак поддържа както правителствени, така и неправителствени клиенти. Това съответства на традиционния модел на облачни услуги, но потенциално представлява по-голям риск за федералното правителство.

- **Частен (Private):** Облаци за частна употреба, предназначени за единични организации и изцяло внедрени във федерални съоръжения, не подлежат на изискванията на FedRAMP и са единственото изключение от задължителното прилагане на FedRAMP за всички федерални агенции. За частни облаци, базирани на IaaS/PaaS вместо да са внедрени във федерално съоръжение, агенцията трябва да използва процеса на FedRAMP, но PMO на FedRAMP не преглежда пакети за частни облаци, не предоставя FedRAMP Оторизационно обозначение (FedRAMP Authorized designation) и не ги публикува в Marketplace, тъй като концепцията за "повторна употреба" не се прилага.

- **Хибриден (Hybrid):** Комбинация от облачни инфраструктури (частни, правителствени или публични). Всеки облак е уникална единица, но е свързан с други облаци, за да предоставя услуги на организация (например, "cloud bursting" за балансиране на товара между облаци).

3.4 Нива на Въздействие

Стандартът за обработка на федерална информация (FIPS) 199 предоставя стандартите за категоризиране на информация и информационни системи, което е процесът, който CSP използват, за да осигурят, че техните услуги отговарят на минималните изисквания за сигурност при обработка, съхранение и предаване на федерални данни. Категориите се базират на потенциалното въздействие, което определени събития биха имали върху способността на организацията да изпълни своето предназначение, да защити активите си, да изпълни законовите си отговорности, да поддържа ежедневните си функции и да защитава лицата.

Важно е CSP да разберат нивото на въздействие на своите услуги и съответната им категоризация при разработване на стратегия за оторизация. CSO се категоризират в едно от три нива на въздействие (ниско, умерено и високо) и в рамките на три цели за сигурността (конфиденциалност, цялост и наличност).

3.4.1 Нива на Въздействие

- **Ниско Ниво на Въздействие**
  Подходящо е за CSO, при което загубата на конфиденциалност, цялост и наличност би довела до ограничени неблагоприятни ефекти върху операциите, активите или лицата на агенцията. FedRAMP в момента има две базови линии (baselines) за системи с данни с ниско въздействие: LI-SaaS Baseline и Low Baseline. LI-SaaS Baseline взема предвид SaaS приложения с ниско въздействие, които не съхраняват лични данни извън това, което обикновено се изисква за осъществяване на вход (т.е. потребителско име, парола и имейл адрес). Необходимата документация за сигурност е консолидирана, а броят на контролите, които се изискват за тестване и проверка, се намалява спрямо стандартното оторизиране на Low Baseline.

- **Умерено Ниво на Въздействие**
  Системите с умерено въздействие представляват около 80% от услугите на CSP, които получават Оторизация от FedRAMP. Това е подходящо за CSO, при което загубата на конфиденциалност, цялост и наличност би довела до сериозни неблагоприятни ефекти върху операциите, активите или лицата на агенцията. Тези ефекти могат да включват значителни щети на оперативните активи на агенцията, финансови загуби или вреди за лица, които не са свързани със загубата на живот или физически щети.

- **Високо Ниво на Въздействие**
  Високо въздействие е обикновено свързано със системи за прилагане на закони и спешни услуги, финансови системи, системи за здравеопазване и всяка друга система, при която загубата на конфиденциалност, цялост или наличност се очаква да има тежко или катастрофално неблагоприятно въздействие върху операциите, активите или лицата на организацията. FedRAMP въвежда високата базова линия, за да вземе предвид най-чувствителните, некласифицирани данни на федералното правителство в облачни среди, включително данни, които засягат защитата на живота и срещу финансова разруха.

3.4.2 Цели за сигурността

- **Конфиденциалност:** Достъп и разкриване на информацията включва средства за защита на личната неприкосновеност и специализирана информация.

  Пример: Достъпът до личната информация на Джон Доу е достатъчно ограничен с цел privacy.

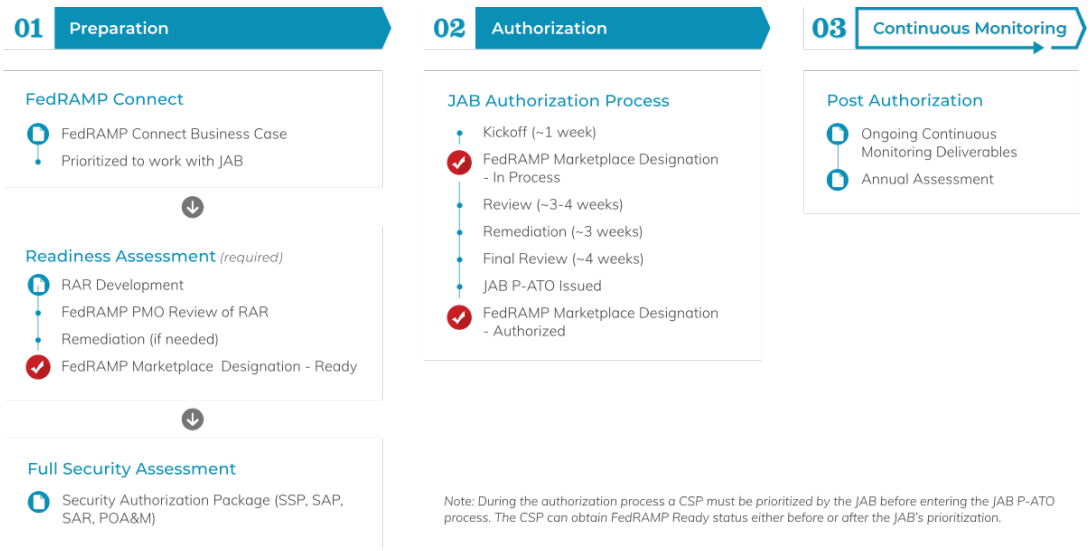
- **Цялост:** Съхранената информация е достатъчно защитена срещу модификации.

  Пример: Сюзън Смит няма подходящ достъп и не може да променя информация на Джон Доу.

- **Наличност:** Навременен и надежден достъп до информацията е гарантиран.

  Пример: Джон Доу може надеждно да достъпва сигурни работни данни.

4 JAB Оторизация



Фиг. 1: Процес за JAB Оторизация

4.1 Фаза 1: Подготовка

4.1.1 FedRAMP Connect

JAB инвестира значително в създаването на обширен пазар от доставчици и има капацитет да оторизира само ограничен брой CSO на година въз основа на текущите ресурси и финансиране. За да се гарантира ясна възвращаемост на ресурсите, използвани за упълномощаване на CSO за федералното правителство, JAB оценяват CSO чрез процес, наречен FedRAMP Connect. По време на този процес CSO разработват business case и се оценяват и подреждат по приоритети за работа с JAB въз основа на критерии за приоритизация. Най-важният критерий за приоритизация от страна на JAB е да се докаже общодържавното търсене на CSO.

JAB приоритизира до 12 CSO годишно, за да работят по постигане на JAB Authorization. След като е приоритизиран, CSP има 60 дни да стане FedRAMP Ready (ако вече не е). Бъдейки приоритизиран за работа с JAB и бидейки определен за FedRAMP Ready от FedRAMP PMO, представляват първата фаза на процеса на JAB Authorization.

4.1.2 FedRAMP Ready

FedRAMP Ready обозначението е задължителна за всяко CSP, търсещо JAB P-ATO, и се препоръчва преди търсенето на ATO от агенция. Въпреки че получаването на FedRAMP Ready не е гаранция,

че CSO ще бъде оторизиран, CSO, които са FedRAMP Ready, имат предимство при приоритизацията, тъй като федералното правителство има по-ясно разбиране за техните технически възможности и вероятността за успех в процеса на оторизация. При планирането на процеса на оторизация за FedRAMP, CSP трябва да има предвид, че обозначението FedRAMP Ready е валидно само за една календарна година след одобрението от FedRAMP PMO.

За да започнат работа с JAB, CSP трябва да постигнат обозначение FedRAMP Ready за своето CSO. За постигане на FedRAMP Ready, CSP трябва да работи с FedRAMP-recognized Third Party Assessment Organization (3PAO), за да завърши Readiness Assessment на своето предложение за услуга. Докладът за оценка на готовността (Readiness Assessment Report / RAR) документира възможността на CSP и предоставя на JAB информация за текущото състояние на сигурността на CSO.

След приключване на оценката, 3PAO може да предостави доклад за оценка на готовността (Readiness Assessment Report / RAR) на PMO, ако 3PAO може да удостовери готовността на CSO за процеса на упълномощаване. Ако има някакви проблеми, идентифицирани от PMO по време на прегледа, CSP получава обратна връзка за това, което трябва да бъде коригирано, за да се счита CSP за FedRAMP Ready. След като PMO одобри RAR, CSO се обозначава като FedRAMP Ready в FedRAMP Marketplace. Освен че е задължително при преследването на JAB P-ATO, бидейки обозначен като FedRAMP Ready в Marketplace предоставя ценна видимост пред потенциални клиенти от агенции, които проучват CSO, отговарящи на техните организационни изисквания.

4.1.3 Пълна оценка на сигурността

След като CSO е приоритизиран да работи с JAB и е обявен за FedRAMP Ready, CSP финализира Плана за сигурност на системата (System Security Plan / SSP) за предложението за услуга и се свързва с FedRAMP-recognized 3PAO. 3PAO разработва План за оценка на сигурността (Security Assessment Plan / SAP), провежда пълна оценка на предложението за услуга и произвежда Доклад за оценка на сигурността (Security Assessment Report / SAR). CSP участва в дейностите по оценка в съответствие с SAP. Накрая CSP разработва План за действие и ключови точки (Plan of Action and Milestones / POA&M), за да следи и управлява системните рискове за сигурност, идентифицирани в SAR. SSP, SAP, SAR и POA&M трябва да бъдат завършени с помощта на шаблоните на FedRAMP и трябва да бъдат представени заедно. JAB няма да преглежда документите един по един. Вместо това целият пакет за сигурността, заедно с първото предоставяне на данни за непрекъснато наблюдение, ще бъде разглеждан в цялост и трябва да бъде представен на PMO поне 2 седмици преди среща с JAB. След това FedRAMP PMO ще работи с CSP и FedRAMP-recognized 3PAO, за да извърши проверка на пълнотата и да координира срещата с JAB.

4.2 Фаза 2: Упълномощаване

Процесът на JAB Authorization използва гъвкава методология с множество стъпкови проверки и принципът "fail fast". Започва се с JAB Kickoff. По време на този етап CSP, 3PAO и FedRAMP съвместно преглеждат системната архитектура, възможностите относно сигурността и състоянието на рисковете на CSO. Въз основа на резултата от Kickoff Meeting, JAB издава решение "да" или "не" за продължаване на процеса на оторизация. Kickoff обикновено е комбинация от брифинги и неформални въпроси и отговори. След Kickoff JAB провежда подробен преглед на пакета за оторизация на сигурността. Очаква се от CSP и 3PAO да подкрепят JAB ревюиращите лица, като отговарят на въпроси и коментари навреме и участват в редовни срещи. След като бъде завършен този процес, JAB издава официално решение за оторизация и, ако е благоприятно, издава Provisional Authorization to Operate (P-ATO).

CSP-та могат да бъдат премахнати (решение "не") от процеса по всяко време поради редица причини, въпреки че това се дължи главно на основен архитектурен проблем или друга неизправност, която не може да бъде решена по време на фазата на оторизация.

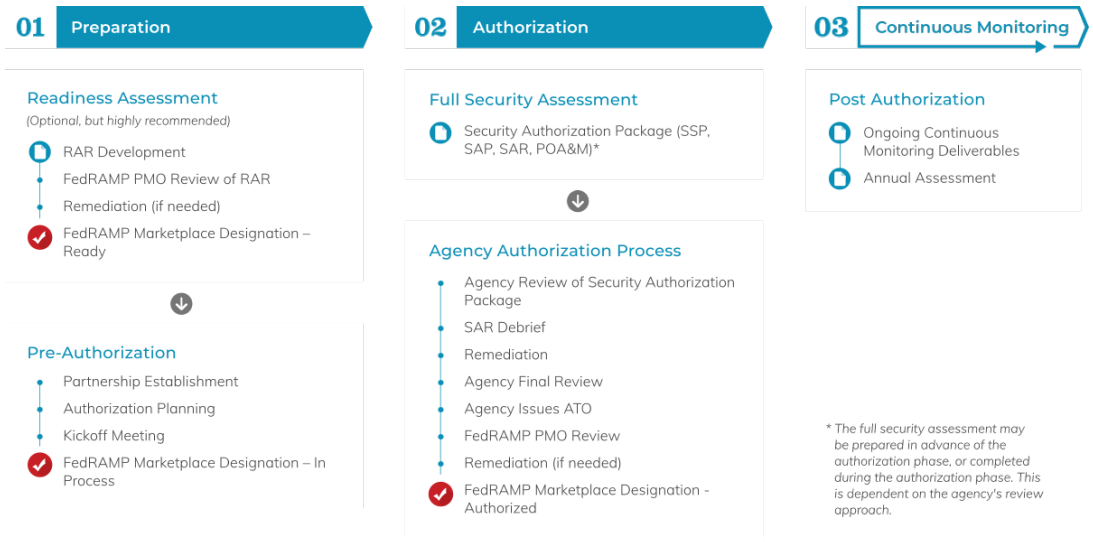
JAB P-ATO означава, че всички три агенции на JAB са прегледали пакета за сигурност и го считат за приемлив за федералната общност. В съчетание с това агенциите преглеждат JAB P-ATO и свързания в него пакет за сигурност и го одобряват за използване от техните агенции. По този начин агенцията издава своето собствено упълномощаване за използване на продукта. JAB P-ATO не е приемане на риск, а гаранция за агенциите, че рисковия профил на системата е прегледана и одобрена от DoD, DHS и GSA. Всяка агенция трябва да преглежда и издава собствено ATO, което покрива използването на облачната услуга в рамките на агенцията.

4.3 Фаза 3: Продължителен мониторинг

След издаването на JAB P-ATO CSP трябва да поддържа състоянието на сигурността си, съответстващо на изискванията на FedRAMP, според първоначалната оценка и процес на оторизация. Това се постига чрез Непрекъснато Наблюдение на системата на CSP. Описано в NIST SP 800-137, целта на Непрекъснатото Наблюдение е да осигури: (1) оперативна видимост, (2) управление на промените и (3) изпълнение на задълженията по реагиране на инциденти през целия живот или използване на системата.

За системите с JAB P-ATO, JAB действа като централизирано PMO за дейностите по Непрекъснато Наблюдение за тези системи, предоставяйки на агенциите артефакти и стандартен процес за оценка и управление на системите с JAB P-ATO.

5 Оторизация чрез Агенция



Фиг. 2: Процес за Оторизация чрез Агенция

5.1 Фаза 1: Подготовка

5.1.1 FedRAMP Ready

FedRAMP Ready е опционален за процеса на Оторизация чрез агенция, но се препоръчва. Процедурата е същата като разгледаната по-рано при P-ATO чрез JAB.

5.1.2 Предварителна оторизация

5.1.2.1 Установяване на партньорство В тази фаза на предварителното упълномощаване CSP формализира своето партньорство с агенция, отговаряща на изискванията, изложени в FedRAMP Marketplace за оторизация на облачни услуги. На този етап CSP трябва да има напълно работеща услуга и екип, който се е ангажирал с процеса на FedRAMP. CSP трябва да се свърже с FedRAMP PMO чрез процеса за приемане. Като допълнение, PMO ще генерира FedRAMP ID за CSO. Преди да идентифицира агенция-партньор, CSP трябва да определи категоризацията на сигурността на данните, които ще бъдат обработвани в системата. Този анализ ще информира CSP за това, коя степен на въздействие е най-подходяща за тяхната система. След като партньорството е на място, CSP трябва да потвърди своята степен на въздействие с агенцията, която ще извърши своята оценка на FIPS 199.

5.1.2.2 Планиране на оторизацията След установяването на партньорството CSP трябва да:

- Потвърди ресурсите, които ще вложи за процеса на оторизация

- Работи с агенцията за избор на 3PAO за оценка във Фаза 2 (предпочитано с FedRAMP-разпознат 3PAO, въпреки че CSP може да използва независими организации за оценка при ATO)
- Завърши обучение за CSP относно FedRAMP
- Определите подхода на агенцията за преглед на пакета за оторизация - Директен Линеен Подход (Just-In-Time), който се препоръчва или Всички Артефакти Паралелно
- Завърши Work Breakdown Structure (WBS) и да го изпрати на PMO за преглед.
- Работи с агенцията, за да завърши Искане за In Process, след което може да започне планирането на Kickoff Meeting.
- Започне работа по Kickoff Briefing Deck. Едно копие на завършената презентация трябва да бъде изпратено на FedRAMP PMO преди планирането на Kickoff Meeting.

5.1.2.3 Среща за Стартиране / Kickoff Meeting Последният етап в тази фаза е да се подготви и проведе Среща за Стартиране. Целта на Срещата за Стартиране е формално да започне процеса за Оторизация от агенцията, като се представят ключови членове на екипа, преглежда се CSO и се гарантира, че всички са наясно с общия процес и времевите рамки. Въпреки че FedRAMP PMO координира и улеснява Срещите за Стартиране, те в крайна сметка служат в полза на CSP и партньорството с агенцията.

След Срещата за Стартиране всички заинтересовани страни ще имат общо разбиране за:

- Общият процес за одобрение, milestones, резултатите, ролите и отговорностите и графика.
- Целта и функцията на CSO, границата на одобрението, потоците на данни, известните пропуски и плановете за отстраняване, специфичните изисквания на агенцията, контролите, които са отговорност на клиента, и области, които може да изискват одобрение на риска от агенцията.
- Процесът на агенцията за преглед на пакета за одобрение и вземане на решение за одобрение на основата на риска.
- Процесът на PMO за преглед на пакета за одобрение от гледна точка на повторно използване на правителството.
- Най-добрите практики и съвети за успех.

След завършването на това събитие, CSP може да получи достъп до сигурното хранилище на FedRAMP (освен ако нивото на въздействие на системата не е Високо). Освен това CSP, които вече не са с обозначение "In Process" в FedRAMP Marketplace, могат да бъдат включени, ако агенцията е доволна от брифинга и графика.

5.1.2.4 Обозначаване "In Process" CSP-тата се считат за FedRAMP In Process, докато активно работят за FedRAMP Оторизация, било то през JAB или чрез установено партньорство с агенция. Документът FedRAMP Marketplace Designations for Cloud Service Providers определя изискванията за постигане на този статус. След като са в процес, CSP-тата се показват в FedRAMP Marketplace с този статус.

5.2 Фаза 2: Оторизация

5.2.1 Пълен Преглед на Сигурността

По време на тази фаза, 3PAO тества системата на CSP. SSP трябва да бъде напълно разработен, а CSP трябва да се свърже с 3PAO, за да разработят SAP. Ако CSP е в партньорство с агенция, използваща подхода Just-In-Time е препоръчително агенцията да одобри SAP преди 3PAO да започне тестовете. По време на тестовете е критично да не се правят промени в системата и да се замрази от гледна точка на разработка. След завършване на тестовете, 3PAO ще разработи SAR, който подробно описва техните открития и включва препоръка за FedRAMP Оторизация. След това CSP ще разработи POA&M, базиран на откритията от SAR включващ обратната връзка от 3PAO, който описва план за справяне със заключенията от тестовете.

След като това бъде завършено, CSP и 3PAO трябва да работят за завършване на представянето на SAR Debrief. Целта на SAR Debrief е да помогне за информиране при рисковия преглед на агенцията относно CSO. По време на SAR Debrief, 3PAO представя резултатите от прегледа на сигурността, CSP представя плана и графика за справяне с остатъчния риск, и FedRAMP PMO описва оставащите milestones и съвети за успех. Въпреки че PMO координира и улеснява SAR Debrief, това е предназначено да бъде в полза на CSP и агенцията.

В края на SAR Debrief всички заинтересовани страни ще имат общо разбиране за:

- Подходът, методологията и графика на 3PAO за оценка
- Обхвата на тестовете
- Резултатите от оценката и остатъчния риск
- Плана и графика на CSP за справяне с остатъчния риск
- Заявления за отклонение, които изискват одобрение на агенцията (коригиращи мерки, фалшиви положителни резултати)
- Оперативно изисквани рискове, които изискват приемане на риск от агенцията (например, услуги или компоненти, от съществено значение за работата на CSO, но изключени от тестваната граница)
- Процеса на агенцията за преглед на пакета и вземане на решение за оторизация, базирано на риск
- Процеса на PMO за преглед на пакета от гледна точка на многократна употреба от страна на правителството
- Най-добри практики и съвети за успех

5.2.2 Процес на Оторизация от Агенцията

След като оценката и свързаните с нея резултати са завършени, агенцията ги преглежда и или ги одобрява, или изисква допълнителни тестове. След това се провежда финален преглед и, ако агенцията приеме риска, свързан с използването на системата, те предоставят Писмо за Оторизация на Операцията (ATO), подписано от Оторизиращия Представител.

След като агенцията издаде своето писмо за ATO, PMO извършва преглед на пакета за оторизация, за да се определи пригодността му за многократна употреба от правителството.

След получаване на писмото за ATO от PMO се извършват множество стъпки за постигане на обозначение FedRAMP Authorized. Няма да се спираме на тях.

След като CSO получи обозначение FedRAMP Authorized, FedRAMP Marketplace се актуализира, за да отрази това. PMO ще предостави пакета за сигурност на CSO, след като поиска и потвърди заявителя, на цялото федерално правителство с цел издаване на последващи ATOs за използването на услугата, базирано на техния собствен преглед на документацията за сигурност на CSO. Поради чувствителността на материалите, тази информация се контролира високо чрез използването на Формуляр за Заявка за Достъп до FedRAMP. Всеки формуляр изисква одобрение от PMO на FedRAMP, за да се прегледат документите.

5.3 Фаза 3: Непрекъснато Мониториране

След като Оторизацията на FedRAMP е завършена, CSP трябва да предостави ежемесечни материали за Непрекъснато Мониториране на агенциите, които използват техните услуги. Тези материали включват актуализиран POA&M, резултати/доклади от сканиране за уязвимости, заявки за отклонение, заявки за Значими Промени, съобщения за инциденти и годишен пакет за оценка. Всяка агенция, използваща услугата, преглежда месечните материали за Непрекъснато Мониториране. CSP с CSO, категоризирани от към въздействие като LI-SaaS, Ниско или Умерено, използват сигурното хранилище на FedRAMP за публикуване на месечните материали за Непрекъснато Мониториране. При категоризация като Високо, се използват свое собствено сигурно хранилище.

PMO на FedRAMP препоръчва на CSP, които имат повече от една клиентска агенция, да оптимизират процеса на Непрекъснато Мониториране и потенциално да минимизират повтарящи се усилия по такъв начин, че всяка агенция все още изпълнява своите задължения по отношение на

Непрекъснатото Мониториране. PMO предоставя подход за съвместно Непрекъснато Мониториране. Съвместното Непрекъснато Мониториране позволява на агенциите да споделят отговорността за надзора на Непрекъснатото Мониториране, а на CSP - създаването на централен форум за разглеждане на въпроси и постигане на консенсус по отношение на заявките за отклонение, Значимите Промени и Годишната Оценка, вместо да се координират с всяка агенция отделно.

Освен това CSP трябва да наеме 3PAO, за да извърши годишна оценка на сигурността и да гарантира, че рисковия профил на системата се поддържа на приемливо ниво през целия жизнен цикъл на системата. Годишната оценка, заедно с актуализираната документация за сигурност на пакета за одобрение, трябва да бъде качена в сигурните хранилища на FedRAMP.

6 Заключение

FedRAMP е един от добрите примери за добре структуриран и прагматичен подход за работа с правителствения сектор. Имайки предвид обема на пазара при софтуера за правителствени цели в САЩ и желанието за модернизация и преход към облака, познаването и съответствието с FedRAMP има потенциал да донесе не малко позитиви за организациите.