



Account for Anything™



APRIO RISK ASSURANCE & ADVISORY SERVICES · CSP ENABLEMENT GUIDE

A Guide for Certified Cloud Service Providers (CSPs): Rev5 to FedRAMP 20x

An introduction to FedRAMP's Consolidated Rules for 2026 (CR26) with practical guidance for Providers already serving Federal Agencies.

A NOTE ON THIS GUIDE

This guide reflects FedRAMP's Consolidated Rules for 2026 (CR26) and related public notices as understood as of July 31, 2026. It is an educational resource prepared by Aprio, not official FedRAMP guidance, and not legal, regulatory, or compliance advice. Confirm all date sensitive data at fedramp.gov before relying on it.

What's inside this guide

Chapter 1	Setting the stage	03
Chapter 2	Inside the new model	05
Chapter 3	Where Rev5 and 20x converge	10
Chapter 4	Convert opportunistically	13
Chapter 5	Coordinating with your Agency Authorizing Official (AO)	17
Chapter 6	How your assessment will differ	20
Chapter 7	Your path to 20x	26
Appendix A	Combined dated timeline	29

IF YOU READ NOTHING ELSE

FedRAMP 20x is not new vocabulary layered on the old model. The model itself is inverted. Rev5 led with compliance: Providers documented a process and assumed security followed automatically. 20x leads with security: prove the outcome continuously and compliance follows as a byproduct. The how, meaning, implementation, monitoring, and evidence, is yours to design. FedRAMP states the outcome and stops there. For a team that wants a checklist, this open design space reads as new ambiguity. For a technically strong security team, that same open design space is the advantage.

Connect with our team today to discuss your FedRAMP journey: 3PAO@aprio.com.

CHAPTER ONE

Setting the stage

If you're already FedRAMP authorized, the good news is you've done the hard part. The authorization, assessment, and documentation you've spent years building won't disappear. What changes is the model FedRAMP uses to evaluate security effectiveness and maintain trust in your environment over time.

That model is set by CR26, FedRAMP's Consolidated Rules for 2026, which is the single rulebook governing FedRAMP's entire modernization effort. It covers both the Rev5 and 20x Certification Paths at once and spells out the terms under which a cloud service provider (CSP) may move from one Path to the other. CR26 not only defines Key Security Indicators (KSIs) that anchor the 20x model, but it also defines the program rules alongside them, in the same document. That distinction matters because a meaningful share of what changes for a Rev5 CSP comes from the program rules directly, not from adopting KSIs. This guide comes back to that repeatedly.

1.1 FedRAMP 20x, in brief

FedRAMP 20x is FedRAMP's modernized certification model. It replaces long narrative security documents with automated, continuously verified evidence, organized around specific, testable outcomes called KSIs. The model was piloted through 2025 and formalized on June 24, 2026, when FedRAMP published CR26.

CR26 does not retire Rev5. If you hold a current Rev5 Agency authorization, CR26 governs your certification for as long as you remain on Rev5, whether or not you pursue 20x immediately. Rev5 itself has a fixed horizon, covered in Appendix A, so *as long as you remain on Rev5* is not the same as *indefinitely*.

KEY POINT

CR26 is not a reauthorization event. Your Rev5 authorization remains valid and continues to follow its normal annual assessment timeline. Your Marketplace listing, authorization boundary, and Agency's acceptance of your package all carry over automatically in the updated FedRAMP Marketplace.

1.2 Why FedRAMP is modernizing

FedRAMP publishes five specific goals for 20x, and two of them get directly at a specific problem: a CSP building a separate, government-specific version of its cloud solution to obtain authorization to process federal information. FedRAMP's stated goals call for leveraging existing industry investments in security by inheriting best-in-class commercial security frameworks, and enabling rapid, continuous innovation without artificial checkpoints that halt progress. Its core concepts add a third piece: a cloud service's effective security posture should never be reduced just to satisfy a security control.

Put together, that's the actual mechanism. Under Rev5, FedRAMP itself often assigned the specific technical approach, or the exact parameter value behind a control, based on standards set before commercial cloud existed in its current form. That produced requirements that frequently didn't match how a modern commercial cloud operates. 20x's stated goals point the other way: let Providers carry forward the commercial security investment they've already made, instead of forcing an architecture change just to satisfy a control that's often outdated.

20x asks a different core question than Rev5 did. Rev5 asked what a Provider would do, while 20x asks what is true about a Provider's system right now and demands proof rather than a written promise. A Provider states the security outcome, proves that outcome against the Provider's real, live architecture, and certification follows directly from the proof.

In practice, 20x replaces narrative documentation and control implementation statements, reviewed by a person once at a single point in time, with continuous, automated evidence of the system's current state.

Done well, a CSP can run one secure commercial cloud and keep delivering new capabilities, features, and offerings into the federal space just as the CSP delivers to private sector, rather than freezing a government-specific environment that falls behind the underlying commercial product from which it was originally cloned.

1.3 Some Providers will have an easier transition

At first glance, FedRAMP 20x can look like a single modernization effort that affects every Provider in roughly the same way. In practice, this won't be the case.

Two Providers can read the same rulebook, pursue the same Certification Class, and face dramatically different levels of effort. The difference is not compliance maturity but automation maturity.

Automation maturity is the degree to which security controls are continuously enforced, continuously validated, and capable of producing evidence as a byproduct of normal operations. Providers with higher automation maturity will discover that much of what 20x requires already exists as a byproduct of normal operations.

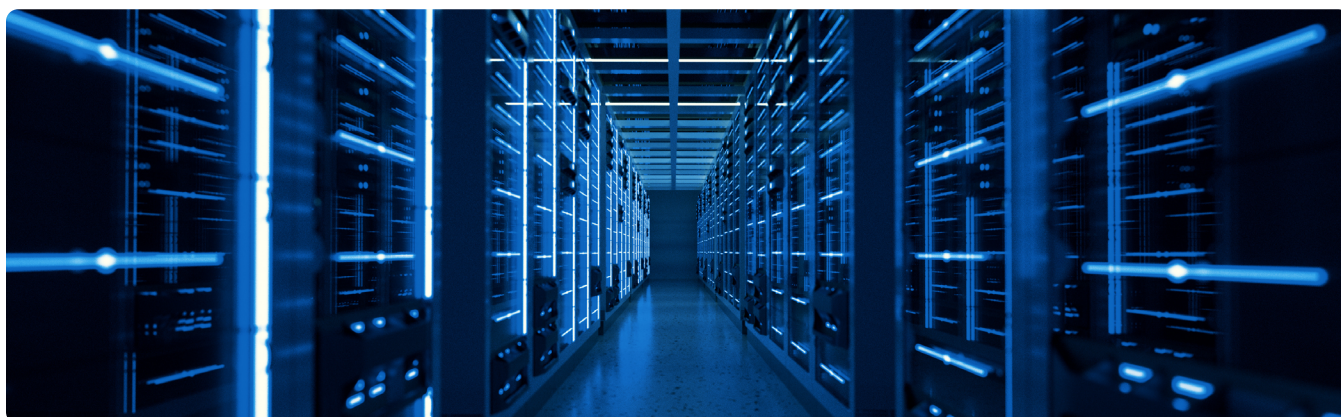
A CSP operating a lift and shift application may face substantial reengineering before 20x becomes practical. Likewise, organizations whose controls are still heavily dependent on manual activities, human review, spreadsheets, and assessment-specific evidence collection may find that 20x becomes less of a documentation project and more of an engineering initiative. The effort shifts from writing compliance narratives to building the automation, instrumentation, and operational practices needed to demonstrate security continuously.

This distinction appears repeatedly throughout this guide. Understanding where your organization falls on that spectrum is one of the most important things you can do before planning a transition to 20x.

One reality worth understanding early

One of the strongest predictors of 20x effort is how much of your security program already produces evidence automatically. Common indicators of automation maturity include:

- Infrastructure as Code (IaC)
- Centralized identity and automated provisioning Just-in-Time (JIT) access
- Policy-as-code
- Structured, centralized logging
- Continuously validated configurations
- Machine-readable security data
- Automated security testing and validation



CHAPTER TWO

Inside the new model

For many Rev5–certified CSPs, the transition to CR26 can feel more dramatic than it is. Much of the uncertainty comes from unfamiliar terminology and references rather than entirely new security expectations. Understanding the language of the new model is the first step to seeing how existing Rev5 practices align to 20x.

As you explore the framework, you will encounter new terms, acronyms, and reference codes that serve as the building blocks of the model. Once those foundations are understood, the larger shift becomes clearer: FedRAMP is moving from prescribing specific controls to defining the security outcomes that must be achieved. Rather than centering assessments on the implementation of individual NIST 800–53 controls, 20x focuses on KSI and the evidence that demonstrates those outcomes are being met.

That evolution also changes how compliance is proven. While documentation remains important, the new model places greater emphasis on objectives, repeatable evidence generated through technical controls, automation, and operational data. The result is a transition from proving security through paperwork to proving security through measurable outcomes and demonstrable results.

This chapter introduces the concepts, references, and mindset changes that form the foundation of the 20x approach.



2.1 New vocabulary

Existing Term	CR26 Term	What it Means for You
FedRAMP Authorization	FedRAMP Certification	This status pertains to your Marketplace listing. Historical use of “authorization” caused confusion, since only Agencies are able to authorize a CSO. If you are familiar with the NIST Risk Management Framework (RMF), this is a return to two distinct gates: FedRAMP certifies, while the Agency authorizes. Under 20x, you will need to update the language in your Trust Center, sales materials, and contracts. This does not impact your CSO architecturally.
Agency Authority to Operate (ATO)	Still ATO, unchanged	Not renamed and not absorbed into “certification.” Your Agency’s own risk-acceptance decision remains a separate instrument from your FedRAMP Certification, issued by a different party. <i>See Chapter 5, Coordinating With Your Agency AO.</i>
Impact Level (Low / Moderate / High)	Certification Class (B / C / D; Class A is new)	Low, Moderate, and High baselines are now termed Class B, C, and D, respectively. Class A replaces the concept of FedRAMP Ready, but at a much lower and more achievable bar than previously imposed.
3PAO	Independent Assessor	Same organization, same position in the process, new label. What changes is the assessment methodology itself, formalized as Independent Verification and Validation. <i>See below and Chapter 6, How Your Assessment Will Differ.</i>
No prior equivalent	Independent Verification and Validation (IV&V)	A formal methodology, not just a description. Your assessor now confirms both that you implemented what you documented and that the implementation produces the intended result in your live system, not only that you wrote it down correctly. Applies to Rev5 assessments and 20x alike. <i>See Chapter 6, How Your Assessment Will Differ.</i>
SSP, SAR, Control Implementation Summary, Customer Responsibility Matrix	Certification Package (Certification Package Overview, Security Decision Record, Secure Configuration Guide)	Here’s some welcome news! Gone are the days of writing thousands of pages of security policies, procedures, and control implementation statements. Documentation changes for 20x are significant. While the underlying concepts may be present in your Rev5 package, the presentation and content change immensely.
Continuous Monitoring (ConMon)/Monthly deliverables	Ongoing Certification Report	Monthly POA&M reviews are done, the kind where deviation requests and vendor dependencies got relitigated month after month with every Agency separately. Agencies now review ConMon data on their own schedule and make their own risk-based decisions about how you are handling vulnerabilities. <i>See Chapter 3, Where Rev5 and 20x Converge.</i>
Significant Change Request (approval required first)	Significant Change Notification, SCN (Notification after the fact, optional today)	20x empowers CSPs to keep modernizing, shipping new services, features, and functionality to the government, all under an approved change control process. 20x does not eliminate significant change tracking, it replaces the manual notification-and-review process with automated, continuous validation, so new capabilities do not mean stopping for a new round of paperwork or a manual review gate each time. <i>See Chapter 4, Convert Opportunistically.</i>
Secure Repository/connect.gov	Trust Center	Whereas Rev5 required security package uploads to a government-run repository, under 20x CSPs host their own Trust Center. General service information is public with no login required, and Agencies get fast, on-demand access to sensitive security data instead of the old slow manual request process.

2.2 How the reference codes work – *three letter codes*

By now you have likely encountered mentions of KSIs, and you may have already noticed one or more three-letter codes running through FedRAMP’s recent publications. That’s not incidental. Every rule and every KSI under CR26 is built from three segments, for the same reason: automation. **Machine readability** is one of 20x’s central goals, and a consistent three-part code lets a system parse and cross-reference every requirement in the program without a person in the loop.

Take KSI-IAM-AAM. The first segment, KSI, identifies the kind of item: a Key Security Indicator. The second, IAM, identifies its family: Identity and Access Management. The third, AAM, distinguishes the specific item: Automating Account Management.

This structure spans the entire program: approximately 50 KSIs, roughly 250 rules, and more than 350 defined three-letter codes in total. Treat these counts as ballparks, not fixed numbers as CR26 continues to be actively tweaked, and both the codes and their totals are still moving.

As previously stated, CR26 is the blueprint for the entire program, not only the security requirements or the KSIs themselves. It also governs process: how evidence gets presented, who is responsible for what, and how each part of the program operates. The same automation goals apply here too, so these underlying rules carry their own three-letter codes. Minimum Assessment Scope (MAS), Significant Change Notification (SCN), and Vulnerability Detection and Response (VDR) are three FedRAMP rules you’ll see throughout this guide. We’re calling out these three specifically because they’re either already required today or available to you now, even before you transition to the 20x Path.

While CR26 defines more than 350 three-letter codes across KSIs, rules, notices, and supporting program elements, only a subset appears in this guide. For convenience, the codes referenced throughout this playbook are summarized below.

AFR – Authorization by FedRAMP (KSI family)	CED – Cybersecurity Education (KSI family)	CMT – Change Management (KSI family)
CNA – Cloud-Native Architecture (KSI family)	IAM – Identity and Access Management (KSI family)	INR – Incident Response (KSI family)
MAS – Minimum Assessment Scope (FedRAMP Rule)	MLA – Monitoring, Logging, and Auditing (KSI family)	NTC – Public Notice (announcement numbering)
PIY – Policy and Inventory (KSI family)	RFC – Request for Comment (proposed rule numbering)	RPL – Recovery Planning (KSI family)
SCN – Significant Change Notification (FedRAMP Rule)	SVC – Service Configuration (KSI family)	TPR – Third-Party Resources (KSI family)
VDR – Vulnerability Detection and Response (FedRAMP Rule)	VER – Vulnerability Evaluation and Reporting (FedRAMP Rule)	

2.3 Outcomes over prescription – *KSIs vs. NIST 800-53 controls*

Chapter 1, Setting the Stage, explained why FedRAMP is modernizing: removing the incentive for Providers to build a government-specific version of their commercial cloud solutions. One example of that needed modernization is how Rev5 has historically assigned control parameter values.

A Rev5 control frequently specified not just what to achieve but a good part of how, meaning FedRAMP-assigned parameter values, specific mechanisms, sometimes a named technical approach. A KSI states the outcome and stops there. How you implement it, and how you monitor, evidence, and manage it over time, is left to you.

In some cases, commercial cloud services had moved to more modern security approaches while federal deployments remained tied to older FedRAMP-prescribed values. The issue was not security, but flexibility: a mandated parameter can prevent Providers from adopting newer approaches that achieve the same outcome more effectively. FedRAMP's own reasoning for removing most of these assigned values is that a fixed value acts as a ceiling as much as a floor. If a required value says something must happen at least every 30 days, that becomes the norm for every Provider, even one whose commercial service could reasonably do it daily. Under CR26, Providers set and justify their own parameters instead.

That tradeoff deserves honest discussion, not just the upside. There is no single FedRAMP-approved value to hit the way there was sometimes a specific parameter under Rev5. On the plus side, CSPs now have real room to implement in a manner consistent with their own risk level and tolerance, rather than a number set for the entire program regardless of fit. On the downside, there's no longer a defined threshold telling you exactly what to do, and some CSPs may have preferred Rev5's simpler "just tell me what you want" approach, even with its one-size-fits-all cost.

2.4 From paperwork to proof – *automation > documentation*

You should read this section's title as "Automation is greater than documentation." Under Rev5, compliance and security were related but functionally separate pursuits, and compliance was the one managed day-to-day. You wrote a policy, documented how a control was implemented, an assessor checked the documentation against the requirement, and security was assumed to follow if the paperwork was right. That assumption is exactly where "compliant but not secure" comes from: a system could pass its assessment by satisfying what was written down while still carrying real exploitable gaps, because the thing being directly proven was adherence to a document, checked once a year, not the live state of the system.

The KSI model reverses the object of proof. The primary thing being demonstrated is the security outcome itself, proven continuously against the live system. Compliance (i.e., the certification, the Security Decision Record or SDR, and the evidence bundle) falls out of demonstrating that the outcome holds. If it holds and you can show it, you are compliant. If it does not, no amount of documentation saves you, because the result is computed from live evidence, not written by a person describing intentions.

WHAT THIS CHANGES, ORGANIZATIONALLY

Under a compliance-first model, FedRAMP is a cost center whose output is documentation, funded to keep selling to the Government, with security as a hoped-for side effect. Under a security-first model, FedRAMP is an extension of the security program the company should be running regardless of any federal customer. You are funding real security engineering that happens to also produce your certification, not a separate function generating paperwork with limited benefit to your actual security posture.

It also changes the question leaders should be asking. A compliance-first frame produces a process question: are we current on our filings and due dates. A security first frame produces the sharper, more honest version of that same question: is our security working right now and can we prove it?

Of note, CR26 and eventually the full transition to 20x does not mean less work, at least initially. Your documentation time will decrease but it is likely your architecture, development, and overall technical security activities will increase, but this is where your time should be spent anyway. No documentation is going to keep adversaries at bay. Strengthen your technical posture, build security you can continuously prove, and the compliance package is the byproduct, rather than building the compliance package and hoping security is underneath it somewhere.



CHAPTER THREE

Where Rev5 and 20x converge

Everything in this chapter is mandatory, and none of it is contingent on a decision about 20x. Whether you stay on Rev5 until it is sunset or plan to pursue a 20x Certification in the future, these obligations apply regardless of the Path you choose.

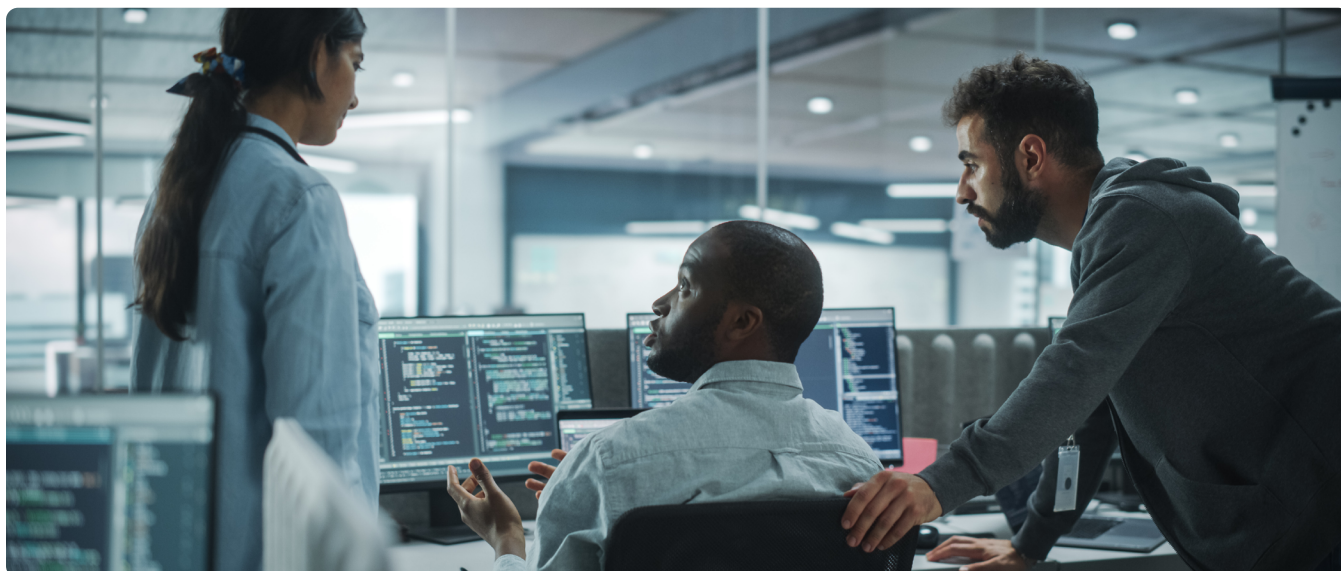
This is where Rev5 and 20x converge. The items in this chapter are not tied to a decision about which authorization model you pursue; they are program-wide obligations that apply throughout the transition period and affect authorized CSPs either today or at a defined point in their assessment lifecycle.

Some of these obligations are already in effect. Others are triggered by a specific milestone in your assessment cycle rather than a fixed calendar date. The documentation stack changes discussed below are an example. You may not encounter them until a future assessment, but once that assessment arrives, the requirement applies. None of the obligations in this chapter are waiting for you to choose a Path first.

Two carry significant consequences if missed, including potential risk to the authorization itself. To help you prioritize, the items are presented in order of urgency, with the most time-sensitive actions first. Every date in this chapter, and every other date referenced throughout this guide, is also collected in Appendix A.

A QUICK NOTE BEFORE DIVING IN

Several items below are referenced by an NTC or RFC number, such as NTC-0012 or RFC-0026. NTC (Notice) is FedRAMP's numbering system for finalized rule announcements. RFC (Request for Comment) identifies the proposed version of a rule before it is finalized as a notice. Unlike KSIs, FedRAMP Rules, and other coded references discussed in this guide, NTC and RFC numbers do not indicate a security topic or control area. They are simply tracking numbers assigned in publication order. You will see these identifiers used as shorthand throughout this chapter and the rest of the guide.



1 A dedicated security email is already required

FedRAMP Security Inbox (FSI) has been mandatory for every Rev5 CSP listed in the Marketplace since January 5, 2026. It requires a dedicated, monitored email address, meeting specific authentication standards, routed to a senior security official who can respond on the organization's behalf. This email address is listed in the Marketplace as your "security email."

FedRAMP is already enforcing this requirement; this is not a future deadline. In addition, FSI has a live escalation ladder. Public notification of noncompliance began on March 1, 2026, while complete removal from the Marketplace began on May 1, 2026. Removal plus a three-month ban on certification began on July 1, 2026. If you have not set this up, treat it as the single most urgent item in this chapter, since enforcement is already active.

2 A Secure Configuration Guide is already required

This has been mandatory for all Rev5 cloud services, Certified, In Process, and Ready, since March 1, 2026. It supplements your existing Customer Responsibility Matrix (CRM) rather than replaces it. FedRAMP provides no template, so it is on you to produce the Secure Configuration Guide in a form that communicates your configuration clearly to your Agency users. This requirement is part of the broader baseline rebuild covered later in this chapter, but it does not wait for your next assessment. It is active now.

3 Vulnerability scanning moves from monthly to continuous

Rev5 vulnerability management has run on the same rhythm for years: scan once a month, log what you find, and carry it forward onto a POA&M until someone eventually closes it out. That rhythm is gone. NTC-0014 requires persistent, risk-based vulnerability management evaluated against actual exposure and exploitability, not a monthly snapshot and a running spreadsheet of open items. This process is one of the larger operational shifts in this entire guide, not a paperwork update, but a real change to how your security team works day-to-day.

NTC-0014 formalizes this shift through the Vulnerability Detection and Response (VDR) and Vulnerability Evaluation and Reporting (VER) requirements. Compliance becomes mandatory on December 7, 2026. The grace period for correction runs through March 7, 2027. After that date, a non-compliant certification can be revoked.

In practice, this changes both detection and reporting. Just as importantly, remediation decisions are no longer driven primarily by severity. CR26 evaluates vulnerabilities based on actual exposure, reachability, exploitability, and potential Agency impact, creating different outcomes for two vulnerabilities with the same CVSS score.

- Detection moves off a flat monthly cadence to a risk-based detection model with different frequencies based on asset characteristics and drift potential.
- Each vulnerability is evaluated for internet-reachability and exploitability, not scored on severity alone.
- Known Exploited Vulnerabilities (KEV), according to CISA's KEV catalog, must be remediated by CISA's own due dates regardless of mitigation status. This approach overrides the risk-based math for anything on that list.
- Non-KEV vulnerabilities can be mitigated rather than fully remediated, if the mitigation genuinely removes the internet-reachable or automatable exposure.

- A human-readable report of this activity is required at least monthly, alongside ongoing reporting to every relevant party.
- Per vulnerability tracking is expected to include detection time and source, reachability and exploitability status, current and historical Potential Agency Impact N-rating (PAIN) rating, remediation progress, overdue status with an explanation, and final disposition.

4 Incident reporting windows shrink to as little as 15 minutes

Reporting timeframes are now tiered by Certification Class, and the former *Potential Adverse Impact* rating is renamed PAIN. The most severe rating for a Class D service carries an initial report window as short as 15 minutes. Providers must now name the Agencies likely affected by an incident, and the former requirement to report Agency and customer incidents directly to CISA has been removed. If your incident response runbook still uses the prior terminology or assumes a direct CISA report, it needs to be updated now. As of this writing, FedRAMP has not published a separate deadline for this notice; it is expected to take effect under CR26's overarching January 1, 2027 mandatory date. (NTC-0012).

5 Your Rev5 baseline gets rebuilt, but not with KSIs

NTC-0013 is FedRAMP's effort to rebuild the Rev5 baseline without requiring adoption of the KSIs which pertain only and directly to the 20x Path. While many modernization efforts are being introduced through CR26, FedRAMP also recognized that some improvements should benefit every CSP, including those CSPs that remain on the Rev5 Path. NTC-0013 brings many of those improvements into the traditional Rev5 framework while preserving the familiar NIST SP 800-53 control structure.

If you stay on Rev5, your control baseline does not change. You are still assessed against the same NIST SP 800-53 controls at your assigned impact level. What changes is who defines many of the implementation details within that baseline. As discussed in Section 2.3, historically, FedRAMP assigned numerous ODPs, essentially determining the strength and rigor with which controls must be implemented. Under a rebuilt baseline, Providers are responsible for defining parameters and justifying those threshold decisions.

This is not a one-time judgment call. For each parameter FedRAMP previously assigned, the CSP must establish and justify its chosen value based on mission needs, business requirements, applicable laws and regulations, industry standards, or other governing requirements. Those decisions must be documented for review by assessors and Agencies.

The changes extend beyond parameters. Rev5 previously included implementation restrictions that reflected older technology assumptions. FedRAMP has rescinded its requirement for a specific network segmentation method, allowing Providers to use approaches better aligned with modern cloud architecture. This approach reflects the broader direction of the rebuilt baseline: fewer prescribed implementations and greater responsibility for CSPs to demonstrate why their chosen approach is sufficient.

The documentation model is changing as well. The legacy SSP, SAR, Control Implementation Summary, and Customer Responsibility Matrix are being replaced by the Certification Package Overview, Security Decision Record, and Secure Configuration Guide. Together, these changes modernize the Rev5 baseline while keeping its underlying control framework intact.

This rebuilt baseline becomes effective at your first independent assessment that completes after January 1, 2027. Completion date, not start date, determines applicability. An assessment that begins in 2026 but concludes after January 1, 2027 will be evaluated against the CSP-defined updated baseline. If your next assessment is already scheduled, confirm with your assessor whether its expected completion date falls before or after that threshold.

6 Your documentation stack is restructured on a different clock than Item 5

The documentation stack that Rev5 CSPs have used for years is being replaced. The System Security Plan (SSP), including its appendices, the Security Assessment Plan (SAP), and the Security Assessment Report (SAR) are being consolidated into two persistently maintained documents: the Certification Package Overview (CPO) and the Security Decision Record (SDR). The POA&M is also being retired and replaced by separate vulnerability tracking and reporting mechanisms under CR26.

The CPO is the high-level description of the cloud service offering. It contains service metadata, public-facing details, and an executive assessment summary supplied by the assessor. The SDR is the authoritative implementation record, capturing applicable controls, parameter values, implementation details, and the mechanisms used to satisfy requirements, alongside the assessor's independent verification and validation findings. Where disagreements exist between the CSP and assessor, those differences remain visible in the same record.

Neither document comes with a FedRAMP-provided template. Like the Secure Configuration Guide discussed earlier in this chapter, FedRAMP defines the required content through a machine-readable JSON schema and leaves presentation and formatting to the CSP.

Both documents must exist in two forms: human-readable and machine-readable (JSON). The narrative documentation does not disappear; it is simply paired with a structured counterpart that must remain consistent with it. Nothing requires a GRC or compliance automation platform to manage this relationship, but maintaining both versions manually becomes increasingly difficult at scale.

These documentation changes are mandatory and apply to assessments that start after January 1, 2027. Once you transition, the SAP and SAR disappear from the FedRAMP-required minimum package. Assessment planning and assessment results do not disappear. Instead, your assessor's work is recorded directly in the CPO and SDR instead.

One final reality check: FedRAMP sets the floor, not the ceiling. Even after this transition, an AO can still request traditional artifacts such as SAP, SAR, screenshots, or other supporting evidence in addition to the FedRAMP minimum package. Before you transition, confirm with your AO what documentation they expect to receive.

7 Continuous monitoring data must reach every Agency you serve

If your service has more than one Agency customer, you are now expected to share your continuous monitoring data with all of them, not only your original authorizing Agency. In practice, that means one shared reporting cycle covering every Agency at once, rather than separate one-to-one relationships, traditionally a monthly meeting open to all Agencies simultaneously, shifting under CR26 toward a quarterly cadence, and shared distribution of vulnerability data and ConMon artifacts to every Agency at the same time. See also [RFC-0026](#).

BEFORE YOU LEAVE THIS CHAPTER

FedRAMP uses January 1, 2027 as the trigger for items 5 and 6, but not in the same way. The NTC-0013 baseline rebuild in Item 5 applies to assessments that are completed after that date. The CPO/SDR transition in Item 6 applies to assessments that start after that date. For assessments spanning the cutoff, those two rules can point in different directions. Keep that distinction in mind as you plan your transition timeline.

CHAPTER 4

Convert Opportunistically

Everything in Chapter 3, *Where Rev5 and 20x Converge*, is mandatory. The two changes in this chapter are not mandatory, but they are available to you now, and worth understanding before you decide to wait.

4.1 Significant change notification

Since February 27, 2026, Rev5-certified Providers have had the option to move from the traditional Significant Change Request (SCR) process, where FedRAMP's approval is required before a system change, to a Significant Change Notification (SCN) process, where you notify FedRAMP after completing certain categories of change. Delivering a new capability or feature no longer means waiting months for government pre-approval before you can deploy it. This directly serves the broader goal introduced in Chapter 1, *Setting the Stage*: without a fast, notification-based path for shipping changes, a CSP has a real incentive to maintain a separate, slower moving government version of its service, just to avoid the old approval lag. SCN removes that incentive, letting one commercial offering serve both markets at the same pace. SCN has no adoption window and no tie to your assessment cycle. You can switch to SCN whenever it fits your change cadence.

This option does not jeopardize your authorization on its own, but adopting it carries several concrete obligations:

- Formally notify FedRAMP that you are switching by submitting the SCN intake form.
- Classify each change using FedRAMP's four fixed categories, each separately defined by FedRAMP and carrying its own process, as shown below.
- Coordinate with your Agency customers first. FedRAMP places this responsibility on the Provider directly. Thus, ensuring this change in process doesn't surprise an Agency is on you. If your government contracts specify the traditional SCR process by name (i.e., uncommon, since most contracts don't get into this level of procedural detail), adopting SCN doesn't override that language, the contract itself needs to be amended separately, or you risk a conflict between what FedRAMP allows and what you're contractually bound to.
- Keep historical SCNs available alongside your authorization data, roughly 12 months or until your next annual assessment completes, whichever your Agency expects. This specific duration has moved before and could again, confirm the current figure against fedramp.gov rather than treating either number as settled.

The table below defines each of FedRAMP's four fixed SCN change categories and what triggers each one.

Change Type	Definition
Routine Recurring	Regular, ordinary maintenance (e.g., addressing known flaws or vulnerabilities) that doesn't meaningfully affect your risk posture.
Adaptive	A change that can be verified with minor updates to existing automated validation and doesn't require major changes to procedures or documentation.
Transformative	A change substantive enough to affect existing risk determinations, typically a major new feature or capability that changes how a customer uses the service.
Impact	A change that's likely to shift your cloud service offering's actual impact level itself (e.g. Categorization changes from Moderate to High).

Each change type carries its own downstream obligation:

- Routine recurring changes need no formal notification at all;
- Adaptive changes require notifying Agency customers within 14 days, after the fact;
- Transformative changes require advance notification and your independent assessor's involvement before you proceed; and
- Impact changes cannot use SCN at all and instead trigger a new full assessment.

Each notification must also document a summary of customer impact, including any change to the customer's own configuration responsibilities and a plan and timeline for verifying the affected KSIs or controls. Providers must separately maintain auditable records of how each change was evaluated, available to FedRAMP on request.

4.2 Minimum assessment scope – smaller Boundary, different Rules

A FAMILIAR REV5 ARGUMENT GETS A BETTER ANSWER

Remember arguing that your ticketing system didn't process federal data and had no real ability to affect it, only to be told to bring it inside your authorization boundary anyway because it might contain federal metadata? Under Rev5, that argument is usually lost. Minimum Assessment Scope (MAS), optional for Rev5 CSPs from January 12, 2026, gives you a real basis for making that argument.

What MAS actually changes

Previous Rev5 boundary guidance focused on the movement of federal information and metadata throughout the system. For many CSPs, MAS creates an opportunity to reduce what must be assessed, monitored, and evidenced.

Under Rev5, boundary guidance required accounting for the flow of all federal information and metadata through the system, explicitly including logs, audit trails, and vulnerability reports about the system itself, not just the federal data the system processed.

MAS narrows that test. The operative question is no longer whether a resource handles information about the system. The question is whether the resource is likely to handle federal customer data or could affect the confidentiality, integrity, or availability (CIA) of that data. The anchor shifts from the system's information generally to the customer's data specifically.

What may move out of scope

MAS creates legitimate candidates for exclusion that often generated debate under Rev5. Examples include:

- Ticketing systems that do not handle federal customer data and cannot affect it,
- Public-facing uptime monitoring services,
- External attack surface scanners that observe only internet-facing assets, and
- Monitoring tools that only collect publicly available information.

FedRAMP's own scope guidance treats these types of services differently because they do not have privileged access, do not hold non-public information, and cannot directly affect federal customer data.

What stays in scope

MAS is not a free pass to remove security tooling from your boundary. Systems with privileged or authenticated access to production environments remain security-relevant and remain in scope. Examples include:

- Internal vulnerability scanners,
- SIEM platforms,
- Security monitoring solutions,
- Administrative management tools, and
- Any system capable of affecting federal customer data

If a resource can affect the CIA of federal data, MAS does not change that outcome.

Allowed does not mean accepted

MAS changes FedRAMP's certification boundary. However, it does not guarantee Agency acceptance of every excluded system or non-authorized supporting tool. Before making a significant boundary or tooling decision, discuss the approach with your AO and Agency stakeholders.

More flexibility doesn't eliminate Agency preference

MAS changes more than what may be excluded; it can also expand the technologies a Provider may use.

For internal functions that do not handle federal customer data and cannot affect its CIA, MAS may support the use of non-FedRAMP authorized solutions. Historically, many Providers defaulted (or were forced) to FedRAMP authorized products simply because boundary expectations were unclear or overstated.

That does not mean Agencies will be comfortable with every exclusion or non-authorized supporting tool. MAS changes what must be included within the certification boundary, but Agencies remain free to evaluate broader architectural and supply chain decisions as part of their own risk analysis in support of authorization decisions. In practice, initial signs suggest that some Agencies appear more comfortable with these exclusions than others.

If a system handles federal customer data or can affect its CIA, the analysis changes entirely. Those systems remain squarely in scope.

Client-side software

Client-side software follows a related but distinct logic. An agent, application client, or mobile application installed on an Agency's systems are not considered a cloud service under FedRAMP's definition. As a result, it sits outside the authorization boundary by rule, not by judgment call. That does not mean security responsibilities disappear, but that FedRAMP does not define the obligations that apply to this software, given it resides outside the traditional cloud service boundary.

This remains an area worth watching. FedRAMP has been explicit about reducing fragmented Agency-specific requirements in favor of broader federal consistency, so additional guidance is likely as the framework continues to mature.

The biggest change may be boundary documentation

This next shift may be the most impactful of all because it reverses one of Rev5's primary focus areas.

Under Rev5, the authorization boundary was everything. Traditional authorization packages required exhaustive diagrams and narratives documenting where federal data was processed, stored, or transmitted; every data flow entering and leaving the boundary; authentication methods; ports, protocols, services, inventories, protective mechanisms, and detailed justifications for every connection.

MAS reflects an acknowledgment that cloud environments do not operate as static diagrams.

Infrastructure is created and retired continuously. Cloud services expand, contract, and evolve throughout the year. Maintaining a boundary representation frozen at a single point in time was already becoming a poor reflection of how modern environments operate. Under MAS, the documentation requirement becomes conceptually simpler:

- Identify the information resources that belong to the cloud service offering,
- Document the information flows between those resources, and
- Document the applicable security categories.

Simpler documentation, however, does not mean less validation.

For 20x systems, those inventories and relationships are validated continuously through automated mechanisms such as KSI-PIY (Policy and Inventory) and KSI-TPR (Third-Party Resources). For Rev5 CSPs adopting MAS, the same concepts are validated through IV&V, where assessors verify that documented inventories and information flows accurately reflect the live environment.

Before adopting MAS, understand the obligations

Before deciding whether and when to move from traditional Rev5 boundary guidance to MAS, understand what you are signing up for:

1. Identify the information resources that handle federal customer data or could affect its CIA. That collection becomes your cloud service offering.
2. Document information flows and security categories for each resource.
3. Document all in scope third-party resources, including their usage, configuration, justification, and any mitigations or compensating controls.
4. Include relevant metadata, including metadata about federal customer data, within scope.
5. Document excluded resources separately for Agency context without pulling them into certification scope. This is optional.

MAS adoption is itself a significant change

A smaller assessment boundary does not mean a smaller change process. Adopting MAS requires updating your authorization approach and therefore constitutes a significant change. The transition must proceed through the applicable SCR or SCN process, be evaluated by your independent assessor, be communicated to FedRAMP, and be reflected in your authorization data.

MAS can significantly reduce scope, but moving to MAS is not simply updating a diagram. It is a formal change to how your cloud service offering is defined and assessed.

CHAPTER 5

Coordinating with your Agency Authorizing Official (AO)

Continuing on Rev5 keeps you on a path that is both Agency-authorized and FedRAMP-certified. The Authorization half, the part that belongs to your AO, runs on an ongoing relationship built on coordination, not automation. FedRAMP 20x is genuinely new. As the rest of this guide shows, the program is modernizing at every level, vocabulary, documentation, assessment method, and the philosophy behind what gets proven and how.

This shift is a huge improvement for the industry. It is also a real change, landing on Providers, Agencies, and assessors at the same time, and change at this scale brings a learning curve for everyone involved, not a failure on anyone's part. Staying aligned with your Agency now protects three things: a shared, current understanding of where the program stands, a security posture strong enough to protect federal data through the transition, and honest visibility into where you are headed so both sides can make informed decisions.

The conversations you have with your Agency today also lay the foundation for an eventual move to 20x. Once 20x is fully in place, its automation reduces the need for scheduled meetings. Agencies pull what they need asynchronously, on their own schedule, rather than waiting on a recurring call.

What brings your Agency into the conversation

20x is new, so make sure you and your Agency are on the same page.

1. Your next assessment

Confirm early whether it completes before or after January 1, 2027, since that date determines whether the Rev5 Balance work applies. This is covered fully in Chapter 6, How Your Assessment Will Differ.

2. Adopting Significant Change Notification (SCN)

Moving from the traditional approval process to SCN is a mindset change for your Agency, not just a filing for you. Be ready to walk them through what SCN is, what changes for them, and what SCN asks of them moving forward. Even after adopting SCN, remember that some categories of change still require upfront communication and your assessor's involvement ahead of the change itself, Transformative changes specifically. See Chapter 4, Convert Opportunistically, for the full category breakdown.

More common than it seems

An unresponsive AO is not a sign you are doing something wrong. A few things help:

- Confirm you are reaching the right person, since day-to-day contact often runs through an ISSO or AODR, not the AO directly.
- Attach the ask to a touchpoint you already have, such as a ConMon review or assessment, rather than a cold request.
- Try your mission side program contact as a second channel.
- Document your outreach in writing, on a schedule, whether you get a reply or not.

If communications are genuinely stalled, FedRAMP is a reasonable escalation point.

3. Justifying your own parameter values under the Rev5 Balance work

FedRAMP does not require advance approval before you set these. The values live in your SSP, and soon in your SDR, for review by FedRAMP and your Agency as part of normal package review, no prerequisite step is required. It's still worth raising this change proactively, as this will be the first time many Agencies will see a Provider-justified value instead of a FedRAMP-assigned number, and an early conversation heads off a documented, defensible choice reading as a surprise.

4. Standing up 20x pilot tooling

Keep your production authorization boundary and any 20x pilot work in clearly separate environments. Any move from sandbox to production is its own change and should be on your Agency's radar before it happens, not after.

5. Filing to move officially to 20x

This only comes up when you decide to switch Certification Paths, which is not a decision to make without your Agency's input first. FedRAMP's own rule text allows holding a Rev5 Agency Authorization and a 20x Program Certification for the same service concurrently, but calls it strongly discouraged given the added complexity and confusion. There is little upside to running both on purpose. Treat this as a one Path decision, made with your Agency.

6. A reportable incident

The one trigger here that you do not plan around, but the mechanics changed under CR26, so you are impacted regardless of Certification Path/Type. Incident response windows are set by two things: the incident's severity rating and your Certification Class. Class D is tightest, Class C sits in the middle, Class A and B are the most lenient. Every incident gets a Potential Agency Impact N-rating, or PAIN for short, on a five-point scale:

- N1: Minimal effect on one or more Agencies
- N2: Narrow effect on one or more Agencies
- N3: Disruptive effect on one Agency
- N4: Debilitating effect on one Agency or a disruptive effect on more than one Agency
- N5: Debilitating effect on more than one Agency

Most readers of this guide are running a Rev5 Moderate service, now Class C. Here is your actual clock:

Rating	Initial Report	Ongoing Reports	Final Report
N5, N4, N3	1 hour	Every 6 hours	Within 6 hours of recovery
N2	24 hours	Every 24 hours	Within 1 business day
N1	1 business day	Every business day	Within 1 business day

It's important to know your reporting requirements *before* an incident, not during one.

7. A Corrective Action Plan (CAP)

A CAP is not new to CR26, it has been a FedRAMP remediation tool under Rev5, and it remains available under 20x. What's new is the automatic Agency notification built into a CR26 CAP. Every CAP now comes with notice to all your Agency customers as a matter of course.

8. Key role change

Your FedRAMP Security Inbox routes to a specific, named senior security official. A change there is worth flagging directly rather than letting your Agency discover it through an unanswered email, the same applies for a change in independent assessors.



CHAPTER 6

How your assessment will differ

For every authorized CSP reading this guide, Rev5 is simply the ground you are standing on. No Agency has yet signaled 20x as a live Path for an existing authorization, and until one does, staying on Rev5 is the reality, not a decision revisited every quarter. This guide treats that reality as the starting point: run Rev5 well, right now, while keeping a controlled, deliberate path toward 20x open for when the moment is actually right.

That reality does not insulate your next assessment from CR26-introduced changes. CR26 redefines the entire FedRAMP program, not just the 20x and Rev5 Paths individually, so your next assessment will not look like the ones before it. This chapter covers what changes and the mechanics of where your package goes once it is done.

WORTH REINFORCING HERE

For an authorized Rev5 CSP, June 11, 2027 is largely a non-event. That date closes the door to new Rev5 certification applications. It does not trigger a new requirement, assessment change, or compliance obligation for Providers that already hold a Rev5 authorization. Carry on, business as usual.

6.1 Methodology

Your assessor's role hasn't changed. It's still an independent organization engaged to evaluate your cloud service and, for an Agency Certification, provide a recommendation your AO can act on. What has changed is how that assessment is performed, which transition requirements apply based on your assessment timeline, what gets examined, how deeply it is examined, and where the line between Provider and assessor responsibilities now sit.

Method

Formalized under CR26 as Independent Verification and Validation (IV&V), introduced in Chapter 2, Inside the New Model. Under the traditional model, your assessor read a narrative document, sampled evidence, and issued a report built around what was written down. IV&V asks two separate questions:

1. **Verification:** Did you implement what you documented?
2. **Validation:** Does that implementation produce the intended result, tested against your live, running system?

Timing

January 1, 2027 is a key date throughout CR26, but it doesn't work the same way every time it's used. Sometimes a rule kicks in if your assessment hasn't started yet. Other times it kicks in if your assessment is scheduled to complete after that date. Same date, two different tests, and which one applies changes what you're on the hook for. Check each rule against your own assessment schedule individually rather than assuming one answer covers all of them, the stakes here are real enough that missing this distinction could mean missing a requirement entirely.

Rule	Trigger	Covered In
NTC-0013	Assessment completes after Jan 1, 2027	Chapter 3, Where Rev5 and 20x Converge, item 5
CPO/SDR (doc stack)	Assessment starts after Jan 1, 2027	Chapter 3, Where Rev5 and 20x Converge, item 6
IV&V methodology	Assessment starts after Jan 1, 2027	This section

An example timeline for illustrative purposes: Consider an assessment that starts December 2026 and is scheduled to complete February 2027. NTC-0013 rebuild applies (assessment completes after Jan 1, 2027), but the assessment is still conducted using the traditional assessment methodology and the traditional SSP/SAP/SAR structure, (assessments starts before Jan 1, 2027). The next assessment after that one is the first to get IV&V, CPO, and SDR together.

Scope

When we think about cybersecurity assessments, two dimensions directly inform intensity, depth and breadth. CR26 changes both, and it changes them differently.

Depth changes on the controls you already have implemented. IV&V is the mechanism. Under the traditional model, an assessor reviewed point-in-time evidence, backed by a narrative explaining why that evidence proved compliance. CR26 asks providers to define and justify their own parameter values, build controls that enforce configuration and functionality automatically, and maintain monitoring capable of producing evidence close to real time. Manual processes that satisfied Rev5 in the past will not satisfy IV&V going forward. The practical effect is a real jump in the depth of understanding, proof, and knowledge required, not only from your security team, but from your assessor as well.

Breadth changes too, on what gets checked at all. Regardless of Certification Path, be it 20x or Rev5, CR26 expects every applicable FedRAMP rule to be assessed, not only the NIST 800-53 controls you're used to. Applicable is the operative word here. FedRAMP's own text is explicit: if a rule doesn't apply to you, the information isn't required.

For instance, the mandatory requirements outlined in Chapter 3, FSI, Secure Configuration Guide, VDR/VER, and ConMon data sharing, apply regardless of any choice you've made. Certification Data Sharing, introduced in this chapter's Submission section, is mandatory too, just on its own later clock. MAS and SCN apply only if you've adopted them. If you're still on the legacy boundary guidance and the traditional SCR process? Then the associated CR26 requirements wouldn't apply to you yet.

All of this sits on top of the NIST 800-53 control walkthrough you already know, but assessment execution looks different regardless. Assessor checks of the program level rules introduced by CR26 run relatively quick compared to the deep IV&V work happening on your controls. For instance, confirming you've adopted MAS correctly (a rule) is a much lighter lift than proving a control's live effectiveness. That said, a rule can still become genuinely complex. Sticking with the same example, a MAS boundary spanning many third-party resources and tangled information flows is no longer a "quick validation" and instead can take real assessor time to trace, even when the rule itself is simple to state.

Independence

The line is narrower than it's ever been. Assessors can walk you through what a rule or KSI requires, flag unclear evidence, and discuss better ways to test something. This means you can expect real, substantive help from your

assessor. Gone are the checklist-junkie days of Rev5 assessors. What assessors cannot do is hand you a specific implementation and then guarantee it will pass. That's exactly why advice to loop your assessor in early is worth taking, most of what you'd want from them is on the allowed side of that line.

6.2 Artifacts

With CR26, three distinct factors determine your artifact requirements, meaning the documentation stack you maintain and your assessor's contribution to your security package. Those factors are timing, your adoption choices, and your Agency's expectations. Each will be discussed in this section.

To set the stage, given this is a 20x transition guide developed for CSPs that have an existing Agency authorization under the Rev5 Path, and given the bulk of the Marketplace holds Moderate authorization (now Class C certification), let's assume every reader starts with a Rev5 package built on the traditional SSP doc stack.

1. Timing

CR26 dictates when your Rev5 SSP doc stack is no longer sufficient and a CPO/SDR takes its place. That date is January 1, 2027. As covered in Chapter 3, if your assessment is scheduled to start after January 1, 2027, you're required to have a CPO and SDR instead of your traditional Rev5 doc stack, and your assessor's output moves into the CPO/SDR going forward. If your assessment is scheduled to start before January 1, 2027, you continue on your Rev5 doc stack, and your assessor's output continues to be provided via the traditional SAP and SAR you already know.

2. Adoption choices

Whether you've adopted MAS and/or SCN carries its own documentation impacts, and each change what your assessor is checking and reporting on as a result. Adopting MAS replaces your traditional, exhaustive Authorization Boundary Diagram with a narrower set of records, your actual in scope information resources, their information flows and security categories, and justification for any in scope third-party resource, and your assessor's job shifts from validating an exhaustive static diagram to validating that narrower, live inventory instead.

Adopting SCN adds its own documentation, a customer impact summary and a KSI or control verification plan for each notification, plus auditable records of how each change was evaluated, and gives your assessor a standing role reviewing Transformative changes in advance, rather than approving a Significant Change Request after the fact. Neither adoption is tied to the January 1, 2027 date. Both are available now and change your package whenever you choose to adopt them.

3. Agency requirements

This third factor sits outside FedRAMP's rules entirely. Even once you know your timing and your MAS/SCN status, your specific Agency may still expect documentation beyond FedRAMP's requirements. FedRAMP's floor is the bare minimum FedRAMP requires, and this becomes a live factor around January 1, 2027 specifically. Even if you, as the CSP, are ready and required to transition to CR26's CPO/SDR structure, your Agency may not be there yet.

Your Agency may require additional artifacts to accompany the minimum FedRAMP package, such as maintaining legacy documents in the short run, to support the Agency's risk-based determination to

Assume questions, not resistance

Communication is key during this transition. Lean on your assessor to understand the requirements and the new framework to help craft the right story. If needed, reach out to FedRAMP for help communicating with your Agency directly.

reauthorize your cloud solution. Individual Agency requirements are the wild card this guide can't calibrate for you. This is the justification for the consistent message throughout this guide to engage both your Agency and your assessor sooner rather than later.

Let's talk about the assessment's impact on your documentation

Once CPO and SDR apply to you, the mechanics of how they're built are worth understanding, Chapter 3 already covers your content that lives in each document. This section focuses on the assessment's impact on the documents.

In the SDR, your assessor's findings are incorporated directly by the assessor, not paraphrased by you. Each applicable control carries a defined set of fields. You author most of them: your ODPs, implementation status (don't worry, not the "who what when why and how" days of old), the mechanisms or activities that address the control, and your own verification and validation, meaning the evidence you maintain that your implementation is appropriate and working as intended. Your assessor authors two fields directly: the IV&V and their own findings from testing your controls against your live system. You can add responses or clarifications to what your assessor wrote, but the fields are theirs to populate and not yours to summarize on their behalf.

In the CPO, your assessor supplies an overall assessment summary. Think of it as the closest thing left to the executive summary in a legacy Rev5 SAR without that report's rigid structural requirements. It covers what the assessor examined, what evidence supported those findings, where implementation matched what was documented, where implementation fell short, and if applicable, anything the two of you still disagree on. That last category (i.e., disputed findings) gets documented as-is rather than forced to resolution before publication.

It's worth being honest about the mechanics here rather than overstating them: FedRAMP's own rule simply states the assessor must verify that the provider didn't change content they (i.e., the assessor) generated. There's no published technical safeguard, no signature or hash, confirmed specifically for these fields. Instead, it rests solely on the assessor's ongoing diligence as the persistently maintained record gets updated, not a one-time memory check months after the fact.

KEY POINT

It's worth stepping back and looking at the bigger picture. Everything in this section points toward 20x's underlying goal of structured, machine-readable, near-continuous evidence, and CR26 does not expect every Rev5 CSP to reach that destination overnight. That's why the timing table above exists. The phased deadlines move CSPs, assessors, and Agencies toward automation at a pace that makes practical business sense rather than forcing the entire ecosystem to change at once.

Let's talk about evidence

One more discussion point around artifacts in this new world. The evidence itself, not just the documents that hold it, changes dramatically under CR26 and eventually 20x. Gone are the days of walking control by control through interview sessions focused on alignment between documentation and interviewees while capturing a screenshot as proof. A static screenshot showing a setting was configured once is no longer treated as sufficient proof of compliance on its own.

Remember: FedRAMP prioritizes security over compliance now, not the other way around.

So, instead of looking in the rearview, your assessments become more forward focused. Your assessor will ask to observe controls operating live where possible. That means a real-time walkthrough of configuration logic,

the automated check firing, and the control behaving as documented. You cannot escape documentation entirely. Static evidence still has a role as support for what is observed live, but no longer as a replacement for the demonstration.

Remember the 80 hours you spent responding to your assessor’s 250-plus item request list by uploading screenshots into a homegrown portal? You do not get that time back one-for-one. Instead, more of that effort shifts into live interaction with your assessor and demonstrations of controls in operation. Whatever your assessor observes is documented in whichever assessment artifacts apply to your phase of the transition: the traditional SAR if your assessment starts before January 1, 2027, or the CPO and SDR if it starts after.

6.3 Tools aren’t required, but...

FedRAMP does not require a specific GRC platform, compliance automation solution, or any other tool. Nothing in CR26 mandates a vendor, a product category, or even the use of automation software, but the practical reality becomes harder to ignore with each new transition requirement.

One requirement sits outside the CPO/SDR discussion above and follows its own timeline. **Machine-readable authorization package requirements** become mandatory on September 30, 2026. Noncompliance after that date triggers public notification. A grace period extends through September 30, 2027, after which a noncompliant certification is removed from the Marketplace.

Within that requirement, the actual burden is narrower than “everything must become machine-readable.” Fully structured, JSON-validated-against-a-schema content applies to a specific set of artifacts that should already sound familiar: the CPO, SDR, incident reports, vulnerability reports, public certification data, and the policy index. Those artifacts already have published JSON schemas under CR26, and that requirement applies regardless of Class or Path.

For most of the remaining content, the change is less dramatic. Narrative explanations, implementation descriptions, and other prose-based materials remain semi-structured text for Classes A, B, and C. The larger shift is in format rather than structure. Traditional DOCX and XLSX files give way to simpler text-based formats that can be versioned, compared, and processed more easily.

At first glance, plain text and markdown may feel like a step backwards from a formatted Word document.

Choose a platform that can keep up with change

FedRAMP has become one of the most forward-leaning cybersecurity programs in the federal government. If the last 20 months are any indication, the program is moving quickly toward automation, structured data, and continuously validated security.

When evaluating a GRC or compliance automation platforms, focus on two key capabilities: future adaptability and data portability.

- Can it maintain the same information in both human-readable and machine-readable form?
- Can it produce artifacts aligned to FedRAMP’s published JSON schemas?
- Is it built around continuously maintained records or periodic audit cycles?
- Can your data be exported cleanly if you change tools later?
- Does it preserve FedRAMP’s native structure and identifiers, or translate everything into proprietary control IDs?
- How does it accommodate new schemas, artifacts, and reporting requirements when FedRAMP changes?

Many platforms normalize frameworks into their own internal control catalog. That can simplify multi-framework compliance, but it also creates dependence on the vendor’s translation layer. As FedRAMP or other frameworks move toward structured certification data, portability matters.

In practice, however, they support the new assessment model far better. Text-based formats show exactly what changed between reviews, allow assessors to compare versions quickly, and can be reliably processed by both Provider and assessor systems. That matters when authorization records are maintained continuously rather than reviewed as static snapshots once or twice a year. The goal is not to turn every narrative into structured data. The goal is to make continuous review practical.

Class D (equates to High under Rev5) Providers face a higher bar. Comprehensive machine-readable authorization data is expected across both initial and ongoing authorization activities, maintained at the individual service level rather than as a single package. Significant changes are incorporated in a recurring schedule rather than managed through traditional package updates.

If you are pursuing Class D, treat machine readability as a major implementation effort rather than a documentation adjustment.

None of these requirements explicitly demand a GRC platform or compliance automation solution. At the same time, maintaining structured artifacts, machine-readable records, schema validation, synchronized human-readable content, and continuously updated authorization data without automation becomes increasingly difficult and resource-intensive as the transition progresses. The rules stop short of requiring tools, but the practical realities do not.

6.4 Submission

The contents of your package are not the only things changing. Where that package lives and how FedRAMP accesses it are changing as well.

Today, Rev5 certification materials are maintained in USDA Connect, FedRAMP's repository, alongside any additional materials your sponsoring Agency requires through its own processes. That's the model most readers of this guide operate under today.

20x changes the destination, not just the format. Instead of uploading certification materials into a FedRAMP-managed repository, Providers maintain a Trust Center that they host themselves. The public-facing portion contains general information about the service. The restricted portion, available only to FedRAMP and authorized Agency customers, becomes the home for your certification materials, including your CPO, SDR, and any other information required for oversight.

Which model applies to your next assessment depends on two things. First, your timing relative to the January 1, 2027 transition dates discussed throughout this chapter. Second, your Agency's expectations. Even where FedRAMP allows a particular submission approach, Agencies may still require supplemental materials or maintain existing processes during the transition period. Before assuming which destination applies to your next assessment, confirm both.

Every Rev5 Provider ultimately moves to a Trust Center model. The compliance deadline is August 1, 2027. A grace period extends through February 1, 2028, but it should be viewed as a cure period, not additional implementation runway. Treat August 1, 2027 as the real deadline.

Until then, USDA Connect remains a valid submission channel.

CHAPTER SEVEN

Your path to 20x

By this point, you already know what changes are mandatory. Most of them apply regardless of how quickly you move toward 20x. FSI, the Secure Configuration Guide, VDR/VER, ConMon data sharing, the NTC-0013 rebuild, CPO/SDR, IV&V, and Certification Data Sharing all arrive on their own timelines. MAS and SCN, covered in Chapter 4, remain the only optional items in this guide.

The question is no longer what changes. The question is how far and how fast you should move toward 20x itself. The following is a set of questions to work through with your team, Agency(ies), and/or assessor to help inform your transition decisions.

ONE FACTOR PREDICTS MORE THAN ALL THE OTHERS

One question influences nearly every answer in this chapter: *is your service fundamentally cloud native, or is it a lift and shift application running on compliant infrastructure?*

Cloud native services often discover that much of the evidence 20x wants already exists. Identity, deployment, logging, configuration management, and operational security frequently produce machine-readable evidence as a byproduct of normal operations. Lift and shift services often discover they must build the automation, instrumentation, and operational processes first. That distinction influences nearly every other decision in this chapter.

1. How much of your security posture is already automated and continuously verifiable?

FedRAMP's target is that most 20x requirements ultimately rely on automated validation rather than human review. If a security activity is currently performed through a spreadsheet, manual process, or documented procedure rather than a system capable of validating and reporting on its own, that represents new engineering work rather than simply reformatting existing evidence.

One answer predicts more of that work than almost anything else: how identity is handled. Services that rely on an external identity provider with IdP-enforced MFA, centralized account management, and automated provisioning often begin much closer to 20x than those that manage authentication directly inside the application. In-app identity tends to pull access control, account management, logging, and evidence collection along with it.

Most organizations answer this question based on intuition rather than evidence. A structured inventory of identity, deployment, logging, monitoring, and configuration domains quickly turns that intuition into a realistic transition plan. If a major domain requires substantial reengineering, especially identity, treat that effort as its own project rather than a task hidden inside a broader modernization budget.

2. When is your next independent assessment?

January 1, 2027 affects more than one requirement. Depending on when your assessment begins, different portions of the CR26 transition become applicable, including the NTC-0013 rebuild, CPO/SDR adoption, and IV&V requirements.

Do not treat "before or after 2027" as a single test. Compare your actual assessment dates against the timelines discussed in Chapter 6, How Your Assessment Will Differ.

If your next assessment falls close to those transition dates, completing required modernization work with an eventual 20x Certification in mind can often reduce duplicate effort later.

3. Can you support Rev5 and a 20x build at the same time?

Moving early almost always means operating two tracks simultaneously for a period of time.

That often includes maintaining an active Rev5 Certification while building automation capabilities, Trust Center content, continuous evidence collection, and 20x assessment materials in parallel. It may also mean assessor support across both efforts and engineering resources divided between today's requirements and tomorrow's.

None of that should be budgeted as if existing teams can simply absorb the work alongside their current responsibilities. Cost has always been the largest barrier to FedRAMP. 20x does not eliminate that cost so much as relocate it, from years of documentation effort to engineering effort focused on automation, instrumentation, and continuous validation. Budget accordingly.

4. Is "wait and see" actually a viable strategy?

Waiting itself isn't open-ended. Rev5 remains available only through December 31, 2028. That means every organization considering 20x is operating within a finite planning window regardless of anything else in this chapter. Waiting may absolutely be the correct decision, but it should be a conscious choice and not the default one.

There is one advantage to moving earlier. FedRAMP has repeatedly demonstrated a willingness to incorporate public feedback, pilot results, and implementation experience into the program itself. Organizations participating earlier are positioned to influence how unresolved questions and future refinements ultimately land rather than merely adapting to them after the fact.

5. Is a specific Agency asking for 20x?

This question extends beyond your current sponsoring Agency. Some Agencies are already showing greater interest in automation, continuous validation, and machine-readable security data. If expanding beyond your existing federal customer base is part of your strategy, that demand signal belongs in this decision alongside everything else.

A transition that may look marginally beneficial for a single Agency relationship can look widely different when viewed through the lens of future market access.

6. Does 20x support your broader federal growth strategy?

This one is about growth. Some Agencies are gravitating toward a 20x posture specifically, independent of what your current sponsor prefers. If federal growth beyond your current customer is part of your strategy, that pull belongs in this decision alongside everything else here.

The question behind all the others

While it's impossible to boil this transition down to a single element, **your application architecture** comes very close. How much of that combined posture already produces the evidence 20x wants, and how much still has to be built, comes down almost entirely to one architectural fact: whether your application was designed cloud native or lifted and shifted onto compliant infrastructure after the fact.

A cloud native build, containers or serverless, identity delegated to a managed provider, infrastructure defined and deployed as code, structured logging shipped to a central store, inherits a large share of what 20x asks for as a byproduct of how it was built, not as new work. Much of that evidence is already sitting there, queryable through native cloud APIs, whether anyone built it with FedRAMP in mind or not. An application that was lifted and shifted onto the same FedRAMP authorized hosting doesn't get that same benefit. The infrastructure underneath is compliant. The application running on it was never designed to produce this kind of evidence, and being hosted well doesn't retroactively fix that.

There's a common perception in the market that 20x is cheaper than Rev5 since it trades a massive documentation stack for automation instead. That perception may hold for CSPs already running cloud native or well-architected applications, where security is present and the remaining work is mostly configuration and wiring, connecting evidence that already exists to what 20x wants to see. The lower cost perception most certainly does not hold for a CSP running a dated, lift and shift application. In this case, transition imposes something re-architecture and/or reengineering work that is likely significantly more extensive and expensive than the documentation burden it replaces. Whether 20x actually saves you money depends entirely on which starting point you're working from, and assuming the general market perception applies to your specific application without analysis is the exact mistake we're trying to avoid here.

Treat that distinction as the lens every question above runs through, not a seventh item alongside them. It's what turns Question 1's automation estimate into a real number, what sets the actual scope of Question 3's parallel build, and what determines how much of Question 4's runway you need.



APPENDIX A

Combined dated timeline

The table below contains the important dates from CR26 current as of July 31, 2026. Lines with bolded text are the most important dates for the readers of this guide.

Date	What happened or will happen	What it means for you
Jan 5, 2026	FedRAMP Security Inbox (FSI) becomes mandatory.	Already in effect, with an active escalation ladder.
Jan 12, 2026	Minimum Assessment Scope (MAS) becomes optional for Rev5.	Adopt whenever it fits your change cadence.
Feb 27, 2026	Significant Change Notification (SCN) becomes optional for Rev5.	Same basis as MAS.
Mar 1, 2026	Secure Configuration Guide becomes mandatory. FSI noncompliance begins public notification.	Active now, does not wait for your next assessment.
May 1, 2026	FSI noncompliance escalates to full Marketplace removal.	Confirm your Security Email is active.
Jun 24, 2026	CR26 released.	FedRAMP published the Consolidated Rules for 2026, introducing Classes A–D, Trust Centers, CPOs, SDRs, MAS, SCN, and other major changes.
Jul 1, 2026	FSI noncompliance escalates to removal plus a three-month certification ban.	The final rung of an already active ladder.
Jul 4, 2026	Optional early adoption of CR26 processes opens.	Voluntary. See Chapter 3.
Jul 6, 2026	Marketplace listings open under CR26 terminology.	Confirm your listing reflects the new terminology.
Jul 28, 2026	FedRAMP Ready becomes legacy.	New FedRAMP Ready submissions are no longer accepted. CSPs should pursue Class A instead.
Aug 3, 2026	FedRAMP 20x Class A pipeline opens.	FedRAMP begins accepting Class A certification applications.
Aug 10, 2026	Temporary Rev5 Program Certification pipelines open.	Certain Ready Conversation and Lost Sponsor CSPs may pursue Rev5 Program Certification with any Agency sponsor.
Aug 31, 2026	Class B and Class C 20x pipelines open.	The realistic starting point for most Moderate CSPs.
Dec 7, 2026	NTC-0014 vulnerability rules (VDR/VER) become mandatory.	Applies now, regardless of Path. See Chapter 3.
Jan 1, 2027	CR26 becomes mandatory for all stakeholders.	New certifications, annual assessments, incident reporting, MAS, SCN, CPOs, SDRs, and other CR26 requirements become the baseline expectation moving forward.
Mar 7, 2027	NTC-0014 grace period ends.	Noncompliant certifications may be revoked.

Date (ctd.)	What happened or will happen (ctd.)	What it means for you (ctd.)
Jun 11, 2027	FedRAMP stops accepting new Rev5 applications.	Does not affect your existing certification.
Aug 1, 2027	Trust Center and SDR maintenance deadlines arrive.	Rev5 CSPs should be operating under the new Certification Data Sharing and Security Decision Record model. Treat this as the real Trust Center transition deadline.
Nov 1, 2027	Machine-readable package requirements take fuller effect for Rev5.	Class D faces the fullest requirement. See Chapter 6.
Feb 1, 2028	Final CR26 grace periods expire.	CSPs not meeting applicable CR26 requirements risk losing certification. This is the ultimate CR26 compliance backstop date.
Through Dec 31, 2028	CR26 remains the stable baseline, while Rev5 is available on an ongoing basis through at least this date.	CSPs should expect migration to future Consolidated Rules before this date.

CONFIRM AGAINST CURRENT FEDRAMP GUIDANCE

FedRAMP issued multiple versioned corrections to CR26 within the first weeks after release, tracked in a dedicated CR26 changelog. Confirm specifics at fedramp.gov/2026 before acting on any of these, particularly close to an assessment. CR26 continued to change after its June 24, 2026 release. A package or runbook built against the June 24 text may already reflect a superseded rule. Confirm specifics at fedramp.gov/2026, fedramp.gov/2026/changelog, and github.com/FedRAMP/ rules before acting on any date sensitive item.

