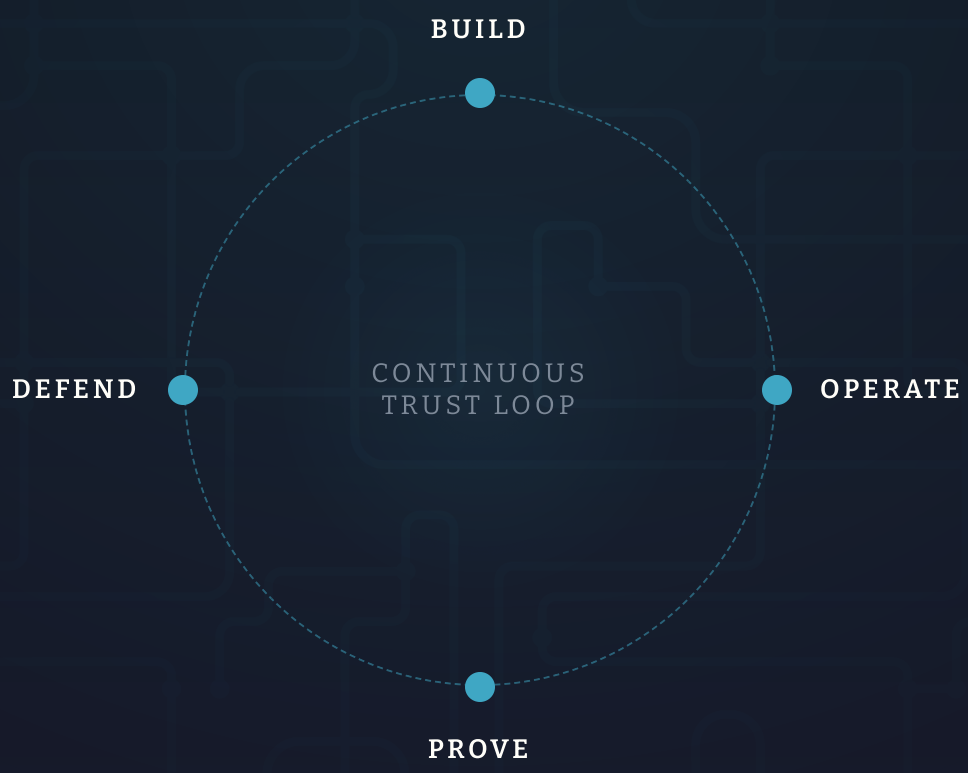
InfusionPoints

WHITE PAPER / 2026



FEDRAMP CR26 · A CSP PLAYBOOK

FedRAMP Just Changed the Rules.

Here's what cloud service providers need to do now, and how the Continuous Trust Platform gets you there.

FEDRAMP CLASS C (MODERATE) CERTIFIED

AWS PREMIER TIER PARTNER

ISO 9001 · ISO 27001

On June 24, 2026, FedRAMP launched its Consolidated Rules for 2026: CR26. It is the most significant restructuring of the FedRAMP program to date, and it applies to every cloud service provider with an existing certification or one in flight.

The rules took effect July 4, 2026, and early adoption is open. Mandatory compliance begins December 7, 2026; the window to enter a new Rev5 certification closes on June 11, 2027. The upside is shelf life: CR26 is the operating baseline through December 31, 2028, the first multi-year FedRAMP roadmap in years.

The nearest deadline is twelve weeks out. Every Rev5 certified service must be running the new vulnerability rules by December 7, 2026, with consequences including potential certification revocation as early as March 2027. The driver is CISA Binding Operational Directive 26-04, which assumes known vulnerabilities are already being exploited and treats slow remediation as a vulnerability itself. FedRAMP adopted that posture for certified CSPs through NTC-0014. A lapsed certification is not a compliance finding: it changes your Marketplace status, stalls agency renewals, and holds up active procurements. Expect a two-quarter engineering program, not a documentation sprint.

REV5 CERTIFIED TODAY	MID-ASSESSMENT	NOT YET CERTIFIED
Dec 7 is your critical path. Then decide whether to renew or move.	You will be judged under CR26, not the rules you entered under.	20x is your route. Assessor capacity is the constraint, not the paperwork.

Jul 4 '26	Dec 7 '26	Jan 1 '27	Jun 11 '27
RULES TOOK EFFECT	MANDATORY COMPLIANCE	NEW REV5 APPS + 20X	REV5 WINDOW CLOSES

THE CLOCK IS ALREADY RUNNING

The CSPs moving now will hold a clean listing through 2028. The ones who wait for their assessor to call will be explaining a corrective action plan in public.

What Changed, and Why It Matters

CR26 shifts how FedRAMP defines the relationship between a CSP, its security program, and the federal agencies it serves. The old model assumed a CSP's compliance documentation, including the SSP, appendices, and POA&Ms, *was* the security program. CR26 rejects that premise, replacing the documentation-as-security model with a **security-outcomes model**, where evidence of security posture matters more than the artifacts produced to describe it.

The terminology changes are structural, not cosmetic. These shifts have downstream implications for your contracts, marketing materials, procurement language, and internal processes. The time to update that language is now.

~~FedRAMP Authorization~~

▼ becomes

FedRAMP Certification

~~Low / Moderate / High~~

▼ becomes

Certification Classes A–D

Low & Li-SaaS → Class B · Moderate → Class C · High → Class D. Class A remains the pilot tier.

~~System Security Plan~~

▼ becomes

Certification Package Overview + Security Decision Record + Secure Configuration Guide

~~Continuous Monitoring~~

▼ becomes

Ongoing Certification

Maintaining status, not running monthly scans.

WORDS ARE CHEAP. EVIDENCE ISN'T.

Under CR26, your security posture is only as real as the evidence your architecture can produce on demand.

Two Paths Forward: 20x and Rev5

CR26 formalizes two certification paths, and choosing between them is the most consequential decision you'll make under the new rules. You need to understand both, even if you're on Rev5, because the direction of the program now points one way.

That direction is **FedRAMP 20x**. It reframes certification as a continuous, automated process: instead of assembling a document package and defending it at a point in time, you stand up machine-readable Key Security Indicators that prove your controls are working every day. The 20x pipelines opened in stages through August 2026, Class A first, then Class B and C, so the question isn't *whether* to move, but how quickly you can get your evidence architecture ready to enter one.

PATH A

PRIMARY PATH

FedRAMP 20x

The primary path for new certifications and the long-term direction of the program. Built for cloud-native services that demonstrate security outcomes through automation and machine-readable evidence rather than document-heavy packages.

It replaces the SSP: instead of a plan, you produce **Key Security Indicators**: measurable, outcome-focused evidence that controls are working, generated programmatically where possible.

- Class A pipeline · Aug 3, 2026
- Class B & C pipelines · Aug 31, 2026

PATH B

SUNSETTING

FedRAMP Rev5

Active during the transition, but with a hard end date: no new applications accepted after June 11, 2027. Existing certifications stay valid through at least Dec 31, 2028, but CR26 changes how you manage them:

- POA&Ms are eliminated, replaced by an **Accepted Weaknesses** list.
- Vuln management factors in exploitability, internet reachability, and impact, not just monthly scans.
- Reporting shifts to collaborative, agency-facing **quarterly** reports.
- Significant Change moves from **approval-based to notification-based**.
- Packages move from Word/Excel to simplified JSON, with OSCAL as an option.

Every current Rev5 Certified system must adopt these changes by **December 7, 2026**, now twelve weeks out.

Which path? Cloud-native and instrumented for automated evidence → 20x. Complex, heavily tailored infrastructure → Rev5 Class C/D, near-term only.

The Deadlines Are Enforcement Dates

This timeline is not aspirational. Each date below carries a consequence.

Jul 6, 2026
Marketplace listings opened for CSPs entering initial implementation under CR26.

Jul 28, 2026
FedRAMP Ready went Legacy. No new FedRAMP Ready submissions accepted after this date.

Aug 3, 2026
FedRAMP 20x Class A pipeline opened.

Aug 31, 2026
FedRAMP 20x Class B and C pipelines opened.

YOU ARE HERE · SEP 16, 2026

Dec 7, 2026
Every Rev5 certified CSO must have adopted the VDR and VER vulnerability rules. The first hard CR26 deadline, and the one that arrives soonest.

Jan 1, 2027
CR26 becomes mandatory for all new Rev5 applications; all active 20x Certified services must follow the rules or FedRAMP requests corrective action.

Mar 7, 2027
Grace period ends for VDR & VER laggards resulting Certification Revocation

Jun 11, 2027
FedRAMP stops accepting new Rev5 Certification applications.

Dec 31, 2028
CR26 itself expires and is replaced by the next consolidated ruleset.

⚠ THE DEADLINE MOST CSPS WILL MISS

FedRAMP's Vulnerability Detection & Response (VDR) and Vulnerability Evaluation & Reporting (VER) rules, the FedRAMP-side implementation of CISA BOD 26-04, carry their own deadline that applies to **every Rev5 certified CSO**, not just 20x pilots.

Why the date moved up. CISA Binding Operational Directive 26-04 directs agencies to assume exploitation of a known vulnerability is automatable, and to treat a lagging remediation process as a vulnerability in its own right. A binding directive cannot reach a private company, so FedRAMP issued NTC-0014 to adopt that model for certified CSPs through the VDR and VER rulesets. NTC-0014, not the directive, is what makes Dec 7, 2026 binding on you.

Any client still running legacy monthly scanning against RA-05, SI-02, or SI-04 now. Dec 7, 2026 is roughly twelve weeks out.

Which of These Is You?

Not every CR26 obligation lands on every provider, and the sequence depends on where you start. Answer these four to know which pages you need.

Do you hold a Rev5 certification today?

Yes	First deadlines apply December 7, 2026, with risk of certification revocation as soon as March 2027.
In flight	You will be assessed under CR26, not the rules you started under. Settle path and class before you re-enter the queue.
Not yet	20x is your route. Skip the Rev5 section and go straight to the 20x four.

How is your vulnerability data produced today?

Monthly scans	Your critical path. Dec 7 is a tooling change, and is the only CR26 obligation in 2026..
Continuous, not contextual	You need exploitability, internet reachability and impact scoring, not more scan frequency.
Contextual and continuous	You are likely close. Document the mapping to VER-EVA-AIA, VDR-CSO-FAV and VDR-CSO-DET so an assessor can follow it.

Can an agency pull your compliance data through an API today?

No	Certification Data Sharing becomes mandatory for existing CSPs on August 1, 2027, with grace period ending on February 1, 2028.
Exports only	Add programmatic access, access logging and historical snapshots. Static exports do not satisfy the rule.

Is your assessor qualified and booked for your target path?

Not engaged	Assessor capacity is the constraint most CSPs discover late. All three pipelines are open and the queue is filling.
Engaged for Rev5	Confirm they are qualified for 20x before you commit to a transition date.

If You Only Do Three Things

The nine items on the following pages are not equal. These three carry a date and a consequence. If your team is small, start here and treat the rest as sequencing.

P1 Get contextual vulnerability management running.

DEADLINE · DEC 7, 2026

It is the only CR26 obligation inside 2026, and the grace period closes Mar 7, 2027. Everything else on the list has a runway into 2027 or 2028. If monthly scanning is still your model, this is a tooling change with a twelve-week window, not a documentation task. Three rules drive it: assume exploitation of a known vulnerability is automatable, treat a lagging remediation process as a vulnerability in its own right, and prove detection verifies that controls operate as described.

P2 Decide your path and class, in writing.

DEADLINE · BEFORE ANY BOUNDARY OR TOOLING WORK

Every downstream choice inherits it: assessor selection, package format, evidence architecture, and how aggressive your incident and verification timelines are. The Rev5 option also has a fixed expiry, so leaving the decision open is itself a decision.

P3 Stand up programmatic access to your compliance data.

DEADLINE · ALREADY A MUST · GRACE ENDS AUG 1, 2027

It gates Ongoing Certification rather than sitting beside it. Agencies need API access, JSON-format data, access logging and historical snapshots. Build it once and the reporting obligations above it get much cheaper.

WHAT NOT TO START WITH

Do not open with document rewrites. The terminology updates matter for contracts, proposals and collateral, and they carry no assessment consequence and no deadline. Run them alongside the engineering work, not ahead of it. Once these three are moving, turn to the section that matches your path: Rev5 on page 8, 20x on page 9.

Rev5: What's Left

The three priorities cover the work that carries a date and a consequence. These five are the remainder of the Rev5 obligation, and all of them are due by December 7, 2026.

01 **Map every ruleset's own effective-date structure individually.**

CR26 doesn't move all at once, and the grace periods run past January. Significant Change Notification, Cryptographic Module Use, and Incident Evaluation and Communication run to Jun 1, 2027; Certification Data Sharing and the Security Decision Record run to Aug 1, 2027; the latest grace period in the ruleset reaches Feb 1, 2028. For an existing provider the Rev5 baseline rebuild (NTC-0013) applies at your first independent assessment after Jan 1, 2027. Build a dated calendar per ruleset from the published JSON rather than treating Jan 1, 2027 as one cliff.

02 **Prepare for the package format change. It changes your tooling, not just paperwork.**

The Certification Package moves from Word/Excel templates to simplified JSON, with OSCAL as an option. FedRAMP expects providers to populate these using automation from operational data. If your GRC process is shared drives and templates, you need a platform that produces structured, machine-readable output.

03 **Map every requirement that scales by your Certification Class.**

FedRAMP removed most FedRAMP-defined organizational requirements within the SP 800-53 baselines. Once your class is set, map everything that scales by it: incident timelines, verification cadences, assessment frequency, and KSI depth. Class B is the baseline; C and D carry more aggressive timelines. Same for FIPS-140, where you document your encryption use so agencies can evaluate it against their risk tolerance.

04 **Use the codified Presumption of Adequacy.**

Agencies must not require additional security information beyond FedRAMP's own rules unless the agency head determines a demonstrable need, and must notify FedRAMP when they do. If a customer agency has been asking for duplicative artifacts on top of your package, this is a legitimate basis to push back.

05 **Update every external reference to your certification status.**

Your website, proposals, and contract boilerplate should say FedRAMP Certification and reference your Certification Class (Low and Li-SaaS to Class B, Moderate to Class C, High to Class D). Zero technical lift and no deadline of its own.

20x: Four Things to Get Right

20x is no longer the experimental track. Under CR26 it's the primary path for every new CSP, and the direction existing Rev5 providers should be heading. The Class A pipeline opened August 3, 2026; Class B and C opened August 31, 2026.

01 **Design for Key Security Indicators, not a document.**

20x has no SSP. It has KSIs: measurable, machine-verifiable evidence that controls are working. A document describes intent; a KSI demonstrates what's happening continuously. Ask what data your environment can produce automatically to prove a control functions, and build the pipeline around generating it.

02 **Build the boundary around the reduced Minimum Assessment Scope.**

Most FedRAMP-defined org requirements are gone and the assessment scope is smaller, an explicit invitation to compete on program quality. A tightly scoped, well-reasoned boundary moves faster through 20x than one copied from a Rev5 package. Treat reduced scope as room to build something defensible.

03 **Build evidence generation as infrastructure, not a GRC afterthought.**

20x expects KSIs, vulnerability data, change records, and the package itself to come from automation, not a quarterly report. Your evidence pipeline is an engineering deliverable. Wire scanning, ticketing, change tracking, and package generation together programmatically from day one, or spend the months after your pipeline opens retrofitting automation onto a manual process.

04 **If you are moving from Rev5, start the transition plan now.**

FedRAMP has said that Rev5 providers should begin the move as soon as possible. New Rev5 applications stop on June 11, 2027, and the agency market shifts fully toward 20x after that. Providers who start now won't be scrambling when the cutoff passes.

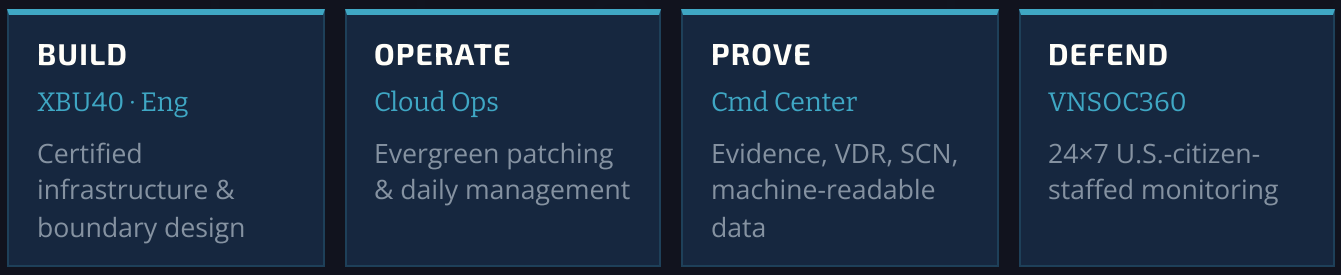
> THE COMMON THREAD
>
> 20x rewards CSPs who build security as a continuously demonstrable, automated practice, and penalizes those adapting a document-and-scan model to a framework designed to replace it. Treat these four as engineering decisions made early, not compliance tasks handled late.

How the Continuous Trust Platform Supports CR26

We didn't build our platform in response to CR26. We built it around one premise: trust in a federal cloud environment has to be **continuous**, not a point-in-time event you renew once a year. CR26 is FedRAMP catching up to that premise and writing it into the rules.

The shift from Rev5's document-and-scan model to an evidence-driven, always-on Certification model doesn't require us to reinvent anything. It validates the architecture we've run for nearly 20 years, without outside capital, for customers across DoD, DHS, HHS, and Treasury. The Continuous Trust Platform (CTP) runs it as a single engine.

FIGURE 2 · THE CTP ENGINE



BUILD XBU40 & Systems Engineering

The requirement. CR26 makes 20x the primary route, replacing the SSP with Key Security Indicators demonstrated programmatically. Building a compliant, 20x-ready environment from scratch is a multi-month effort most CSPs underestimate.

What we deliver. XBU40 is our FedRAMP Class C (Moderate) Certified cloud infrastructure, the foundation layer of CTP. Operate within its boundary and you inherit its certification posture and instrumented evidence generation, so your path to Class B or C starts from a stronger position. Our systems engineering practice makes the boundary and architecture decisions CR26 now rewards.

OPERATE Cloud Ops & Platform Foundation

The requirement. CR26 assumes the certified environment is being actively run, not documented once and left alone. A strong compliance layer on unmanaged infrastructure is the gap CR26 is designed to expose.

What we deliver. Managed Cloud Ops keeps XBU40, and any environment we operate, running the way the certification package says it does. Evergreen patching means the Security Decision Record and KSIs reflect reality, not a snapshot from your last assessment. This is where the loop closes back into Build and feeds straight into Prove.

PROVE Command Center · AuditShield · Trust Center

The requirement. CR26 eliminates the SSP/POA&M model. Packages move to structured JSON with OSCAL optional; Ongoing Certification shifts to quarterly reporting; Consumer Data Sharing now requires programmatic API access as a MUST.

What we deliver. Command Center, our GRC platform, turns what Build and Operate did into standing, defensible evidence. Its ALTO AI assistant, POA&M automation, SSP management, and OSCAL export are built around continuous, structured data. Trust Center is a tamper-evident, machine-readable repository built to satisfy Consumer Data Sharing directly. Paired with AuditShield's automated evidence pipeline across CMMC and FedRAMP, it replaces the manual monthly artifact cycle with an auditable evidence chain.

DEFEND VNSOC360

The requirement. VDR rules go well beyond monthly scanning. VER-EVA-AIA requires assuming exploitation is automatable unless proven otherwise; VDR-CSO-FAV treats a lagging VDR process as a vulnerability itself. Ongoing Certification assumes continuous awareness and a team that can act around the clock.

What we deliver. Command Center gives you the detection, tracking, and response workflow; VNSOC360, our 24×7 U.S.-citizen-staffed SOC, gives you the humans who run it. Our governing principle: agents observe and propose while humans approve. Humans in the loop, not merely on it. For a CSP without mature internal SOC capacity, VNSOC360 covers what the Dec 7 VDR/VER deadline demands.

THE MAPPING AT A GLANCE

CR26 REQUIREMENT	LAYER	CAPABILITY
20x Class B/C certification path (pipelines open Aug 31)	Build	XBU40 + Systems Engineering
Reduced Minimum Assessment Scope, boundary redesign	Build	Systems Engineering
Environment operated as certified, not just documented	Operate	Cloud Ops
SSP & POA&M elimination, JSON/OSCAL packages	Prove	Command Center
Consumer Data Sharing, programmatic data access	Prove	Trust Center
Continuous evidence for Ongoing Certification	Prove	AuditShield
Vulnerability Detection & Response · Significant Change Notification	Prove	Command Center
24×7 monitoring, triage, and incident response	Defend	VNSOC360

A different framework, one that rewards real security engineering.

CR26 rewards CSPs that have invested in security engineering, continuous evidence generation, and automation. It penalizes those who treated FedRAMP compliance as a document-production exercise. The deadlines are set and the pipelines are open. Providers with evidence pipelines already running will be the ones agencies can buy from six months out.

We've spent nearly 20 years building the capabilities CR26 is now formalizing as requirements. We can show you what CR26 means for your program, and what it takes to be ready before the December 7 VDR/VER deadline and the January 1 mandate.

Talk to us about your CR26 transition.

Bring your current path, class, and timeline. We'll map it against the deadlines that apply to you and show you where the Continuous Trust Platform closes the gaps.

INFUSIONPOINTS.COM →

THE RULES WON'T WAIT. NEITHER WILL YOUR COMPETITORS.

Six months from now, half your market will still be arguing about templates. The other half will be certified, listed, and winning the contracts you wanted.

BUILD • OPERATE • PROVE • DEFEND

ABOUT INFUSIONPOINTS, LLC

InfusionPoints helps government agencies and technology providers build, operate, prove, and defend secure, mission-ready cloud and AI environments: cloud engineering, cybersecurity, compliance automation, and 24×7×365 security operations by U.S. citizens on U.S. soil. The Continuous Trust Platform runs on XBU40 infrastructure, managed Cloud Ops, the Command Center GRC suite with Trust Center, the AuditShield evidence pipeline, and VNSOC360 SOC operations.

CERTIFIED SMALL HUBZONE BUSINESS CONCERN · AWS PREMIER TIER PARTNER
FEDRAMP CLASS C (MODERATE) CERTIFIED · ISO 27001 · ISO 9001 · CMMC

EMAIL
gary.daemer@infusionpoints.com

PHONE
336-990-0252

WEB
www.infusionpoints.com

613 Elkin Highway, North Wilkesboro, NC 28659 · Mission Obsessed, Outcome Focused.