RegScale

SOLUTION BRIEF

FEDRAMP 20x · CR26 CONTINUOUS MONITORING

Vulnerability Data Your Agency Customers Can Read Themselves

On December 7, 2026, FedRAMP retires severity-driven vulnerability management and replaces it with Vulnerability Detection and Response (VDR) and Vulnerability Evaluation and Reporting (VER). From that date, every cloud service offering is measured against the new rules.

What the Rules Actually Say

VDR

Vulnerability Detection and Response

How you find vulnerabilities inside the authorization boundary and how fast you act once you do. Remediation timing follows real exposure and exploitability, not a scanner's severity label.

VER

Vulnerability Evaluation and Reporting

How you justify each rating and how you disclose it. Evaluations have to be reproducible and evidence-backed, and shared with agency customers and AOs continuously rather than monthly.

What Changes on the Ground

The severity-driven regime

- Every High and Critical finding inherits the same 30-day clock
- An isolated test database is treated like an internet-facing load balancer
- Compensating controls earn no formal credit toward the deadline
- Agency customers wait on a monthly spreadsheet someone has to build

Under VDR and VER

- Clocks run from days to months based on actual exposure and exploitability
- Reachability and asset criticality are inputs to the rating, not footnotes
- Evidence-backed mitigation lowers the rating and moves the deadline
- Agency customers and AOs read live posture themselves, continuously

There is no phase-in.

A provider still running severity-driven remediation after December 7 is running two programs at once: the one the scanner reports and the one FedRAMP measures. That gap surfaces in your next review, in front of the agency customers whose missions depend on your authorization.

RegScale

SOLUTION BRIEF

How We Do It

RegScale evaluates findings against the CR26 risk rules and hands the result to Trust Center over an authenticated, read-only pipeline. Your agency customers and their Authorizing Officials read live posture from that pipeline. Nobody on your security team compiles a package to make it happen.

Dedicated OAuth 2.0 service account · read-only · scoped to the authorized security plans you designate

1 Scoped Service Account Authentication

Trust Center authenticates as a dedicated, audited, non-interactive service account. Access is strictly read-only and limited to the security plans you authorize, so the pipeline can never write back into your system of record.

2 Continuous Machine-Readable Ingestion

On a recurring scheduled sync, Trust Center retrieves the monthly VDT (Vulnerability Data Template), AVI (Assessment Validation Infrastructure), and HLO (High-Level Obligations) JSON documents RegScale generates, satisfying the VDR-TFR-MHR machine-readable reporting requirement without a manual export step.

3 Live Federal Agency Customer Dashboards

Trust Center ingests real-time PAI ratings (N1 through N5 counts), overdue metrics, and classifier exposure. Built-in multi-tenancy ensures each federal customer sees only the Cloud Service Offerings they subscribe to.

4 Authorizing Official Self-Service Monitoring

AOs and ISSOs get their own continuous monitoring portal to inspect compliance posture, 192-day risk acceptances (MAV), and partial mitigation reduction ladders on demand, without asking your security team to build a custom export.

Start With a CR26 Readiness Workshop

A working session that maps your current detection, evaluation, and reporting practice against the VDR and VER rules, shows what RegScale automates for you, and names what your team still has to close before December 7, 2026.

FedRAMP

FedRAMP Class D (High) Certified Platform

sales@regscale.com

regscale.com

Sept 2026 · v1