CHECKLIST

anchore

FedRAMP 20x Vulnerability Detection and Response Checklist

For Containers and SBOMs

FedRAMP made its new vulnerability rules, Vulnerability Detection and Response (VDR) and Vulnerability Evaluation and Reporting (VER), mandatory for every certified cloud service by **December 7, 2026**, following CISA Binding Operational Directive 26-04. Use this checklist to see where your program stands for containerized workloads and for the code outside containers: virtual machine and host filesystems, source repositories and third-party software.

Work through each part and check what your program already does. Anything unchecked is a gap to close before December 7, 2026. The boxes are fillable, so you can complete and share this copy with your security, engineering and compliance teams.

Key Dates

DATE	WHAT HAPPENS
June 10, 2026	CISA issues BOD 26-04
June 16, 2026	FedRAMP Notice 0014 moves mandatory VDR and VER adoption to December 7, 2026
August 7, 2026	Agency policies must support BOD 26-04 remediation
December 7, 2026	VDR and VER mandatory for all certified offerings; agencies begin following BOD 26-04 timelines
Through March 7, 2027	Grace period: offerings not following the rules keep certification only under a corrective action plan, with notice to all agencies
After March 7, 2027	FedRAMP revokes certification for offerings not following the rules (Notice 0015)



PART 1

SBOM Inventory and Detection Coverage

Evaluation can only be as complete as detection, and detection can only be as complete as the SBOM. The VDR rules expect persistent detection across every resource in the boundary, containerized or not.

- [ ] Every container image in the boundary has an SBOM, stored centrally as the inventory of record.
- [ ] Code outside containers has an SBOM too: virtual machine and host filesystems, packaged applications, source repositories and build artifacts.
- [ ] SBOMs from vendors and third-party software are imported in SPDX or CycloneDX, validated and monitored alongside your own.
- [ ] SBOMs are organized by application and version, so every finding maps to the service agencies use.
- [ ] Detection runs at every stage: source repositories, CI/CD builds, container registries and running workloads.
- [ ] New CVEs are matched against every stored SBOM as feeds update, without rescanning the original artifact.
- [ ] Private registries are scanned with credentials, so no image is skipped.
- [ ] Vulnerability matching uses distro-specific feeds to cut false positives, and false-positive decisions are documented.
- [ ] Related vulnerabilities are grouped by application and version so one fix closes many findings.
- [ ] Coverage gaps (resources with no SBOM, unscanned images) are tracked and closed like any other finding.



PART 2

Evaluation

Every detected vulnerability needs an evaluation inside the window set by your certification class. CVSS severity alone no longer sets priority (VER rules).

- [ ] You know your certification class and measure time from detection to evaluation against its window.
- [ ] Internet reachability is determined for each affected resource: can a payload from the internet reach it, even indirectly.
- [ ] Likely exploitability is evaluated with CISA KEV status, EPSS scores and CISA SSVC exploitation data.
- [ ] Exploitation is assumed automatable unless you hold evidence otherwise, matching BOD 26-04's automatability factor.
- [ ] Affected or not-affected status is recorded per deployment as a VEX annotation, so the reasoning travels with the SBOM.
- [ ] Every finding carries a Potential Agency Impact (PAIN) rating from N1 to N5.
- [ ] Your PAIN method is written down. FedRAMP does not prescribe one, so the method itself is what an assessor reviews.
- [ ] Inputs your team has not answered yet default to the strictest value, so nothing slips while it waits for review.
- [ ] Each evaluation records who made it, when and on what evidence.

Potential Agency Impact (PAIN) Ratings

RATING	POTENTIAL AGENCY IMPACT OF EXPLOITATION
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 disruptive effect on more than one
N5	Debilitating effect on more than one agency

CISA SSVC Data and Decisions Behind Your PAIN Method

Because FedRAMP leaves the PAIN method to you, a consistent and documented method is what holds up in an assessment. Anchore Enterprise puts CISA SSVC exploitation and automatable data, KEV and EPSS on every finding and records SSVC decisions, so each rating your team assigns rests on documented inputs. Any SSVC input your team has not set defaults to its strictest value.

SSVC DECISION POINT	VALUES	SOURCE
Exploitation	None, Public PoC, Active	CISA SSVC data, KEV
Automatable	Yes, No	CISA SSVC data
Technical Impact	Partial, Total	Your team
Mission Prevalence	Minimal, Support, Essential	Your team, per application
Public Well-Being Impact	Minimal, Material, Irreversible	Your team, per application
Agencies impacted	One agency, more than one agency	Your team, per application

Mission Prevalence and Public Well-Being Impact combine into SSVC's Mission and Well-Being rating (Low, Medium, High). With exploitation, automatability and technical impact, that produces the SSVC decision (Track, Track*, Attend or Act). Your team then applies agencies impacted to assign a PAIN rating from N1 to N5, and your certification class to set the remediation deadline, using the method you have documented. Findings on the KEV keep CISA's due date.



PART 3

Remediation and Deadlines

Remediation timeframes now follow the PAIN rating, internet reachability, likely exploitability and your certification class (VDR rules). The POA&M is retired.

- [ ] Remediation deadlines are set from the finding's current PAIN rating, reachability, exploitability and class, not from CVSS severity.
- [ ] Findings in the CISA KEV catalog are remediated by the catalog's due date, including when they are mitigated but not fully remediated.
- [ ] At Class C and D, internet-reachable, likely exploitable findings rated above N3 are handled as FedRAMP reportable incidents until mitigated to N3 or below.
- [ ] Partial mitigations that lower a rating are recorded, and the rating history shows current, past and next target ratings.
- [ ] Findings not fully remediated within 192 days of evaluation are reported as accepted vulnerabilities, each with a named owner and explanation.
- [ ] Exceptions carry expiration dates, and alerts fire before a deadline lapses.
- [ ] Each finding is routed to the owning team with its deadline and the reason it matters.

PART 4

Reporting and Evidence

The VER rules replace monthly scan uploads and POA&M spreadsheets with a human-readable monthly report plus machine-readable detail that agencies can filter automatically.

- [ ] A monthly human-readable vulnerability report is produced from the same data as your machine-readable records.
- [ ] Per-finding details include internet reachability, likely exploitability and PAIN rating history.
- [ ] Accepted vulnerabilities are reported with a named owner and explanation.
- [ ] Reports validate against FedRAMP's published JSON schemas.
- [ ] SBOMs export in SPDX or CycloneDX, with VEX and VDR documents that show which vulnerabilities affect the service and why.
- [ ] Evidence can be regenerated on demand through an API, rather than assembled by hand.
- [ ] One system of record feeds security, engineering and compliance, not a separate compliance-only process.



PART 5

Hardened Images, Pipeline Gates and KSI Evidence

Fewer vulnerabilities in means fewer evaluations later. FedRAMP 20x measures these practices through Key Security Indicators rather than control narratives.

- [ ] Containers build from approved, hardened base images, checked against DISA STIG or CIS benchmarks.
- [ ] Images are redeployed from version-controlled builds rather than modified in place (KSI-CMT-RMV), with minimal packages to shrink the attack surface (KSI-CNA-MAT).
- [ ] Policy gates in CI/CD stop images with KEV findings, secrets, malware or unapproved base images before release, so changes are validated automatically throughout deployment (KSI-CMT-VTD).
- [ ] A Kubernetes admission controller blocks unscanned or non-compliant images from running.
- [ ] Every change to a deployed image is logged and traceable to a build (KSI-CMT-LMC).
- [ ] Image and infrastructure-as-code configurations are persistently evaluated and tested (KSI-MLA-EVC).
- [ ] Image integrity is validated with cryptographic methods, such as verifying signatures before deployment (KSI-SVC-VRI).
- [ ] Third-party and open source software is automatically monitored for upstream vulnerabilities (KSI-SCR-MON), and supply chain risks are identified and mitigated (KSI-SCR-MIT).
- [ ] SBOMs from authoritative sources feed an automatically generated, real-time inventory of information resources (KSI-PIY-GIV).
- [ ] If you still report under Rev 5, reuse the same evidence through the related NIST 800-53 controls FedRAMP lists for each KSI, such as RA-5 for KSI-SCR-MON and CM-8 for KSI-PIY-GIV.

ANCHORE ENTERPRISE

How Anchore Helps

Anchore Enterprise covers detection, exploitability context and evidence for container images, filesystems, source repositories and imported SBOMs.

CHECKLIST AREA	AVAILABLE TODAY	COMING SOON
SBOM inventory and detection	SBOMs for images, filesystems and source repositories; SPDX and CycloneDX import; continuous re-evaluation as feeds update	
Evaluation	CISA KEV, EPSS and SSVC data on every finding; SSVC decisions with internet reachability, Mission Prevalence and Public Well-Being Impact inputs; VEX annotations	
Remediation	Time-based allowlists with alerts; fix recommendations; Jira and Slack routing	KEV due dates applied automatically
Reporting	Scheduled reports; SBOM, VEX and VDR export; REST API	
Hardening and gates	FedRAMP, NIST, DISA STIG and CIS policy packs; CI/CD gates; admission control	

Speak With Our Security Experts

Contact Us