



Lazarus Alliance
Proactive Cyber Security©

SERVICE.
INTEGRITY.
RELIABILITY.

FedRAMP Rev. 5 → 20x Transition Diagnostic

From Rev. 5 Documentation
to 20x Execution Proof.

A Practical, Evidence-Driven Path
to Continuous, Machine-Readable
FedRAMP Security.

Rev. 5

DOCUMENTS
ASSESSMENTS
POINT-IN-TIME
COMPLIANCE

20x

CONTINUOUS
EVIDENCE
MACHINE-READABLE
TRUST AT SCALE

SAME
MISSION.
A STRONGER
TOMORROW.



EVIDENCE
ARCHITECTURE



ASSESSOR-READY
JSON



ENGINEERING
VALIDATION



KSI HISTORY
PLAN



DUAL-RUN
OPERATING MODEL



QUARTERLY
REPORTING

GLOBAL
CYBERSECURITY
SOLUTIONS FOR A
MORE RESILIENT WORLD.

LazarusAlliance.com

FEDRAMP

Rev. 5 to 20x Transition Diagnostic

From documentation to continuous execution proof

DATED ROADMAP | EVIDENCE + SCHEMA | KSI HISTORY | DUAL-RUN OPERATIONS

Engagement outcome

An executable transition system that preserves the existing Rev. 5 program while building reusable, engineering-validated, machine-readable evidence for FedRAMP 20x.

Prepared by Lazarus Alliance

September 17, 2026



LazarusAlliance
Proactive Cyber Security©

FedRAMP Rev. 5 to 20x Transition Diagnostic

Move from document-based FedRAMP compliance to continuously provable FedRAMP security.

The FedRAMP Rev. 5-to-20x Transition Diagnostic evaluates how an existing FedRAMP program must change across architecture, evidence, engineering, assessment, and continuous reporting. The engagement produces a dated transition roadmap, reusable evidence architecture, assessor-ready JSON strategy, KSI history plan, and dual-run operating model designed to preserve the existing Rev. 5 program while building the evidence required for FedRAMP 20x.

Why now

FedRAMP states that Phase 5 will end new Rev. 5 Certifications and identifies June 11, 2027 as the planned date to stop accepting new Rev. 5 Certifications. FedRAMP also states that a transition path and timeline for existing Rev. 5 offerings will be provided by the end of Phase 5.

1. Transition Baseline & Target-State Decision

Start with the existing Rev. 5 authorization/certification environment and determine what can be reused, transformed, automated, replaced, retired, or newly implemented.

- Inventory the authorization boundary, SSP/control implementation material, assessment evidence, continuous monitoring sources, vulnerability processes, inventories, IAM, logging, SDLC, change management, incident response, supply-chain dependencies, policies, automation, and engineering telemetry.
- Establish the intended 20x target class and identify dependencies that affect transition sequencing.
- Trace current evidence to the systems that actually generate it, rather than treating the compliance repository as the source of truth.

Primary deliverable - Rev. 5 to 20x Transition Matrix

Every material program component is classified as Reuse | Transform | Automate | Replace | Retire | New Requirement.

This matters because a 20x Certification Package is fundamentally different from a traditional static package: FedRAMP describes it as Certification Data maintained over time and made available in human-readable and, where required, machine-readable forms.

2. Evidence & Schema Gap Review

This is the centerpiece of the diagnostic. The review does not merely map Rev. 5 controls to KSIs; it determines whether the client can actually produce the evidence 20x expects.

Diagnostic dimension	Question answered
Source	Where does the evidence originate?

Diagnostic dimension	Question answered
Authority	Is it generated from an authoritative system?
Automation	Can it be produced without manual audit preparation?
Frequency	Point-in-time, periodic, or persistent?
Verification	How is correctness established?
Validation	How do we prove the measure works?
History	Is historical evidence retained?
Schema	Can the result populate required FedRAMP JSON?
Human view	Can an agency or assessor understand it?
Machine view	Can another system consume it?
Ownership	Which engineering/security function owns it?
Failure state	What constitutes a failed validation?

The resulting Evidence Architecture Map becomes reusable infrastructure rather than a one-time assessment workbook. Where a rule specifies a FedRAMP JSON schema, machine-readable information must be valid against the corresponding schema.

Evidence & Schema Deliverables

- Evidence & Schema Gap Register
- FedRAMP 20x Data Dictionary
- Source -> Evidence -> KSI -> SDR -> JSON lineage map
- JSON schema validation report
- Remediation backlog
- Sample assessor-ready JSON objects

Architecture principle

One authoritative evidence source -> multiple compliance and assurance outputs. Do not build another parallel compliance repository.

3. KSI History Acceleration Plan

A technical deficiency can often be remediated quickly; missing historical telemetry cannot be manufactured retroactively. For each KSI, determine available history, retention period, granularity, completeness, integrity, automation, gaps, and the earliest qualifying date.

For Class C, current FedRAMP rules call for historical metrics in the Security Decision Record, including a 30-day summary, up to one year of summary history where available, and daily metric data up to one year where available. Class C also requires persistent-validation status history covering at least six months for all KSIs.

KSI Evidence Clock

KSI	Evidence source	Current history	Automation	Target history	Clock starts	Ready date
KSI-XXX	CI/CD	11 months	Yes	>=6 months	Existing	Ready
KSI-XXX	IAM	90 days	Partial	>=6 months	09/30/26	03/30/27
KSI-XXX	CMDB/API	None	No	>=6 months	11/15/26	05/15/27

Critical-path output

The KSI Evidence Clock converts a generic transition plan into a certification critical path by showing when evidence history becomes mature enough to support the target 20x posture.

4. Engineering Validation Review

This differentiates the engagement from firms treating 20x as another compliance-mapping exercise. Engineering teams participate directly in proving that automated measures are authoritative, repeatable, testable, and capable of generating durable evidence.

- Security objective -> measure -> implementation -> evidence generator -> validation method -> failure criteria -> alert/remediation -> independent assessment path.
- Evaluate whether evidence generation survives normal system changes, deployment changes, tooling changes, and personnel turnover.
- Test the validation logic itself, not merely the presence of an artifact.

FedRAMP has reported that successful 20x adoption requires deep engineering involvement and that faster reviews were associated with consistent machine-readable schemas, concise evidence context, clear failure criteria, assessor feedback adjacent to provider validation, and assessor review of validation code. For Class C, current rules require at least two automated methods for each KSI to persistently verify and validate KSI accuracy and completeness.

KSI Validation Engineering Specification

Per-KSI design

Objective -> Measure A -> Measure B -> Source -> Query/API -> Logic -> Threshold -> Pass/Fail -> Exception -> Evidence -> JSON -> Historical storage

5. Assessor-Ready JSON Proof Package

Do not stop at telling clients that JSON will be necessary. Produce representative working output using actual client evidence wherever practical.

- Certification Package Overview data
- Security Decision Record data

- KSI records
- Metric and history structures
- Evidence references
- Verification and validation results
- Assessment fields
- Ongoing Certification Report structure

FedRAMP requires the Security Decision Record in both human-readable and JSON formats, with implementation, verification, validation, independent verification/validation, and applicable artifact information. Current FedRAMP guidance also emphasizes human- and machine-readable package completeness and recommends validating package JSON using the applicable schema validator.

Execution-proof

We do not just tell you that your program needs machine-readable evidence. We prove that your existing security systems can produce it.

6. Rev. 5 / 20x Dual-Run Operating Model

Existing providers should not dismantle mature Rev. 5 processes before the 20x transition path is settled. The diagnostic establishes one evidence-producing security program with two reporting paths rather than two separate compliance programs.

Authoritative evidence layer	Rev. 5 assurance path	20x assurance path
Operational security systems, telemetry, APIs, repositories and engineering validation	SSP / SAP / SAR; POA&M; ConMon; annual assessment; agency evidence	KSI validation; SDR; JSON; historical metrics; ongoing reporting; persistent evidence

The operating model identifies which Rev. 5 processes remain necessary, which evidence feeds both regimes, what new 20x pipelines must be created, and when legacy processes can eventually be retired.

7. Dated Transition Roadmap

The roadmap is date-specific from delivery rather than expressed as generic phases. For an engagement beginning in September 2026:

Period	Outcome
Sep-Oct 2026	Rev. 5 baseline, target class, KSI/rule mapping, evidence inventory
Oct-Nov 2026	Evidence architecture and JSON/schema gaps resolved
Nov-Dec 2026	Automated validation pipelines established
Dec 2026	KSI history clock operational across target scope
Q1 2027	Dual-run Rev. 5/20x reporting and engineering validation

Period	Outcome
Q2 2027	Historical evidence maturation and assessor dry run
By Jun. 11, 2027	Transition position evaluated against final FedRAMP requirements
Quarterly thereafter	Executive + engineering + assessment readiness reporting

For Class D, the roadmap must remain explicitly adaptive. RFC-0033 states that Class D will significantly exceed Class C, with detailed requirements being developed through the Phase 4 pilot, and anticipates additional assurance-engineering, automation, availability, and FOCl requirements.

8. Durable Quarterly Transition Report

The diagnostic is designed to evolve naturally into recurring assurance. Each quarter, Lazarus Alliance delivers a concise executive and engineering report covering:

- 20x transition readiness
- KSI validation coverage
- Automated verification coverage
- Historical evidence maturity
- JSON/schema validity
- Evidence-source health
- Open engineering deficiencies
- Rev. 5 / 20x dual-run status
- Assessment findings
- FedRAMP rule changes
- Upcoming transition milestones
- Management decisions required

Class C also requires all KSIs to be included in an independent FedRAMP assessment at least annually, making quarterly evidence health a practical mechanism for preventing annual assessment preparation from becoming another scramble.

Tangible Outputs

These are concrete transition assets:

#	Deliverable
1	FedRAMP Rev. 5 -> 20x Transition Diagnostic Report
2	Dated Certification Transition Roadmap
3	Evidence Architecture & JSON Schema Gap Analysis
4	KSI Historical Evidence & Maturity Plan
5	Rev. 5 / 20x Dual-Run Operating Model
6	Assessor-Ready 20x Proof Package + Quarterly Reporting Model

Execution-Proof Differentiation

Traditional transition consulting	Lazarus Alliance approach
Map controls -> identify gaps -> recommend remediation	Map requirements -> identify authoritative evidence -> validate engineering implementation -> automate evidence -> validate schemas -> establish KSI history -> generate assessor-ready JSON -> prove the dual-run model -> measure readiness quarterly

Not another FedRAMP gap assessment.

From Rev. 5 documentation to 20x execution proof. Lazarus Alliance determines whether the security architecture can continuously produce the evidence FedRAMP 20x requires - and proves it through reusable evidence architecture, engineering validation, historical KSI metrics, schema-valid JSON, assessor-ready outputs, and a dated transition roadmap.

FedRAMP Reference Sources

The diagnostic should be refreshed against current FedRAMP 20x rules and RFCs at engagement start and at each quarterly reporting cycle.

FedRAMP 20x program: <https://www.fedramp.gov/20x/>

Using FedRAMP 20x packages: <https://www.fedramp.gov/2026/agencies/use/packages/20x/>

FedRAMP Certification rule: <https://demo.fedramp.gov/2026/providers/20x/rules/fedramp-certification/>

Security Decision Record rule: <https://preview.fedramp.gov/2026/providers/20x/rules/security-decision-record/>

Security Decision Record reference: <https://preview.fedramp.gov/2026/reference/20x/c/security-decision-record/>

Independent Verification and Validation: <https://www.fedramp.gov/2026/reference/20x/c/independent-verification-and-validation/>

RFC-0033 - 20x Phase 4 Development Tracks: <https://www.fedramp.gov/rfcs/0033/>

Class A Certification Package guidance: <https://help.fedramp.gov/hc/en-us/articles/55366564534043-What-must-be-in-a-Class-A-Certification-Package>