Lazarus Alliance Launches FedRAMP Rev. 5-to-20x Transition Diagnostic Helping CSPs Build a Path to Continuous Assurance

New service evaluates evidence, JSON readiness, KSIs, engineering validation, and the operational changes required to transition from traditional FedRAMP to 20x



Lazarus Alliance Proactive Cyber Security services Logo

SCOTTSDALE, AZ, UNITED STATES, September 17, 2026 / EINPresswire.com/ -- Lazarus Alliance, Inc., a cybersecurity assessment and compliance firm, today announced the FedRAMP Rev. 5-to-20x Transition Diagnostic, a specialized engagement designed to help existing FedRAMP cloud service providers determine how their current security and compliance programs must evolve for FedRAMP 20x.

> A screenshot can show what a system appeared to be doing at a moment in time. Twenty-X pushes the industry toward something substantially more valuable."
>
> *Michael Peters - Founder and CEO*

The service addresses a transition that extends beyond conventional control mapping. FedRAMP 20x increasingly emphasizes persistently maintained security information, verification and validation, historical Key Security Indicator (KSI) metrics, and machine-readable certification data. Under the FedRAMP Consolidated Rules for 2026, providers must supply Security Decision Records in both human-readable and JSON formats, and machine-readable information must validate against applicable FedRAMP JSON schemas.

FedRAMP has also established significant transition milestones. The FedRAMP 20x Class B and Class C pipeline opened August 31, 2026; the Consolidated Rules for 2026 become mandatory for stakeholders beginning January 1, 2027, subject to individual rule applicability and effective dates; and FedRAMP plans to stop accepting applications for new Rev. 5 Certifications on June 11, 2027.

"The transition to FedRAMP 20x is not simply a matter of rewriting a System Security Plan or

remapping controls. The fundamental question is whether an organization can continuously prove that its security program is operating as represented, using evidence that is authoritative, reusable, machine-readable, and independently verifiable," said Michael Peters, CEO of Lazarus Alliance. "Our diagnostic is designed to answer that question early enough for engineering, security, and compliance teams to do something about it."



From Documentation to Execution Proof

The Lazarus Alliance FedRAMP Rev. 5-to-20x Transition Diagnostic examines the client's existing FedRAMP environment from both an assessment and engineering perspective.

Rather than producing only a traditional gap-analysis spreadsheet, the engagement is designed to establish an executable transition architecture. It evaluates existing Rev. 5 artifacts and processes against the evidence, data, validation, automation, and operating-model capabilities needed for 20x.

The diagnostic focuses on four questions:

* What can be reused? Existing Rev. 5 controls, evidence, telemetry, processes, and security investments are classified for reuse, transformation, automation, replacement, retirement, or new implementation.
* Can the environment produce 20x evidence? Lazarus Alliance evaluates authoritative evidence sources, APIs, security telemetry, validation mechanisms, historical data, and their ability to support FedRAMP's machine-readable schemas.
* Is sufficient history being created now? Existing KSI data retention and historical evidence are evaluated to identify when the organization can demonstrate the necessary operating history.
* Can the organization operate Rev. 5 and 20x simultaneously during transition? The engagement establishes a dual-run operating model intended to minimize duplicated compliance work while preserving required Rev. 5 processes.

For Class C, FedRAMP's current rules require historical KSI metrics that include 30-day summaries, up to one year of summary history where available, and daily metric data up to one

year where available.

That makes early evidence collection particularly important. A technical control can potentially be corrected quickly; months of missing historical evidence cannot be created retroactively.

Six Concrete Transition Deliverables

The diagnostic is structured around tangible outputs that security, engineering, compliance, and executive teams can use to manage the transition:

1. FedRAMP Rev. 5-to-20x Transition Diagnostic Report: A current-state assessment identifying technical, evidence, operational, and certification-readiness gaps.

2. Dated Transition Roadmap: A milestone-driven implementation plan connecting remediation activities, dependencies, historical evidence accumulation, assessment preparation, and FedRAMP deadlines.

3. Evidence Architecture and JSON Schema Gap Analysis: A source-to-evidence-to-KSI-to-SDR architecture showing where security evidence originates, how it can be validated, and how it can populate applicable FedRAMP machine-readable structures.

4. KSI Historical Evidence and Maturity Plan: An evidence-history assessment identifying existing retention, missing telemetry, automation requirements, evidence clocks, and projected readiness dates.

5. Rev. 5 / 20x Dual-Run Operating Model: A transition architecture designed to use common authoritative security evidence for both existing Rev. 5 obligations and emerging 20x assurance requirements wherever practical.

6. Assessor-Ready 20x Proof Package and Quarterly Reporting Model: Representative machine-readable outputs and a recurring reporting structure for measuring KSI maturity, evidence health, schema validity, engineering deficiencies, and transition progress.

Engineering Validation Becomes Part of Compliance Readiness

The diagnostic also examines whether automated security measures can be independently verified and validated.

Under the new FedRAMP model, the Security Decision Record replaces the traditional SSP with a persistently maintained record of security decisions. It includes implementation information as well as verification, validation, independent verification, independent validation, and applicable supporting artifacts.

That changes the nature of preparation.

“A screenshot can show what a system appeared to be doing at a moment in time. Twenty-X pushes the industry toward something substantially more valuable: demonstrating how the security measure works, where its data comes from, whether that data is trustworthy, whether the validation logic is sound, and whether another party can independently verify the result,” Peters said.

Lazarus Alliance therefore evaluates evidence generators, APIs, queries, automation logic, validation methods, failure criteria, historical retention, and ownership alongside traditional compliance documentation.

One Evidence Architecture, Multiple Assurance Outputs

A central design principle of the diagnostic is to avoid creating another standalone compliance repository.

Instead, Lazarus Alliance works with providers to identify authoritative operational security sources and develop an evidence architecture in which the same underlying security information can support multiple assurance requirements.

The intended model is:

Operational Security Systems Authoritative Evidence Verification and Validation Machine-Readable Assurance Data FedRAMP Reporting and Independent Assessment

This approach is intended to reduce repetitive evidence preparation while improving traceability between what engineering systems actually do and what an organization represents to assessors and federal customers.

Preparing Existing Rev. 5 Providers for a Changing FedRAMP Program

FedRAMP has stated that 20x is intended to replace the Rev. 5 process. The program will stop accepting new Rev. 5 Certification applications on June 11, 2027, while the final end date for existing Rev. 5 Certifications has not yet been established. FedRAMP has urged existing providers to begin adopting the new approach to improve their transition position.

The Lazarus Alliance diagnostic is therefore designed not to predict FedRAMP's remaining transition decisions, but to help providers establish capabilities that can be acted on now and adapted as the program evolves.

“Waiting for every transition detail to be finalized does not create historical evidence, build automated validation, establish authoritative data sources, or make engineering systems

machine-readable," Peters said. "Those capabilities take time. The objective is to identify the work that can be responsibly started now and give leadership a dated, evidence-based roadmap for what comes next."

Availability

The Lazarus Alliance FedRAMP Rev. 5-to-20x Transition Diagnostic is available for cloud service providers with existing Rev. 5 environments and organizations evaluating migration to FedRAMP 20x.

The diagnostic can be followed by separately scoped FedRAMP 20x Transition Implementation and, where independence requirements permit, FedRAMP 20x Independent Assessment services.

About Lazarus Alliance

Lazarus Alliance, Inc. provides cybersecurity audit, assessment, risk, privacy, testing, governance, and advisory services to organizations operating in regulated and high-assurance environments. The company supports organizations across major cybersecurity and compliance frameworks and helps clients translate complex security requirements into measurable, defensible assurance.

Lazarus Alliance is Proactive Cybersecurity®.

Michael Peters
Lazarus Alliance, Inc.
+1 8888967580
email us here
Visit us on social media:
LinkedIn
YouTube
X

This press release can be viewed online at: https://www.einpresswire.com/article/943040695

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.