

FedRAMP 20x and the New Economics of Certification

How continuous validation changes cost, effort, and system design.

**Matt Earley**PRESIDENT
38NORTH SECURITY

FedrAMP 20x is often discussed as a faster or simpler path to certification. That misses the more important point.

The real change is economic.

For many cloud providers, the traditional FedRAMP operating model has meant recurring assessment preparation, manual evidence collection, FedRAMP-specific tooling, and, in some environments, duplicated federal and commercial architecture.

FedrAMP 20x changes that model. The final rules shift the program toward continuous validation using current operational information, class-specific automation and historical metrics, machine-readable data, and recurring reporting. That gives cloud providers an opportunity to rethink how they design, operate, and demonstrate security in federal environments.

Strong security, careful architecture, and upfront investment remain essential. In many cases, the upfront work becomes more important. Cloud providers still need to understand their system boundary, apply the Minimum Assessment Scope correctly, identify authoritative data sources, build reliable validation

methods and pipelines, and make sure the information coming from the system is accurate, complete, and reviewable.

For Classes B, C, and D, annual independent assessment also remains. The opportunity is in changing what happens before and between those assessments.

When the operating model is designed well, repeated evidence gathering can be reduced. Commercial tooling may remain part of the architecture where appropriate. Current validation information can already be available when an assessment begins. Significant changes can move through structured notification workflows. Engineering teams can spend less time reconstructing static artifacts and more time improving the system itself.

The business case is not simply “FedRAMP gets cheaper.” It is that the cost structure can change because the operating model changes.

That is the opportunity. This paper outlines where those economic and technical shifts occur and why FedRAMP 20x may change the way cloud providers think about certification, operations, and long-term federal market entry.

— Matt Earley

PRESIDENT, 38NORTH SECURITY

FedRAMP 20x changes the economics of certification.

There are several areas where cloud providers may reduce initial or recurring costs by moving toward FedRAMP 20x.

There can still be sticker shock from the engineering and setup required to support continuous validation. But good scoping, data analysis, system design,

integrations, and automation can create leverage across the lifecycle of the system.

20x changes the economics by changing how systems are scoped, how validation information is produced, how security is demonstrated, how significant changes are communicated, and how much work has to be repeated.

Five shifts drive the difference.

- 
- 01 Leaner Scoping Considerations** P.04
Minimum Assessment Scope and current FedRAMP guidance can keep more commercial tooling in play.
 - 02 A Different Assessment Cost Profile** P.05
Annual independent assessment remains, but continuous validation can reduce the repeated preparation surrounding it.
 - 03 A More Efficient Significant Change Process** P.06
Significant Change Notification creates a more structured way to prepare, communicate, and coordinate change information.
 - 04 Hidden Costs** P.07
The engineering time lost to recurring assessment preparation, response, and evidence reconstruction.
 - 05 Upfront Investment, Long-Term Leverage** P.08
Good system design, telemetry, integrations, and validation methods can reduce repeated effort throughout the lifecycle.

Leaner Scoping Considerations

The first savings opportunity in 20x is understanding what actually needs to be in scope.

The Minimum Assessment Scope, or MAS, gives cloud providers direction for identifying the systems and components that can affect the security of government data and missions.

That matters economically because every unnecessary component brought into the assessed environment can create additional tooling, engineering, validation, maintenance, and reporting work over time.

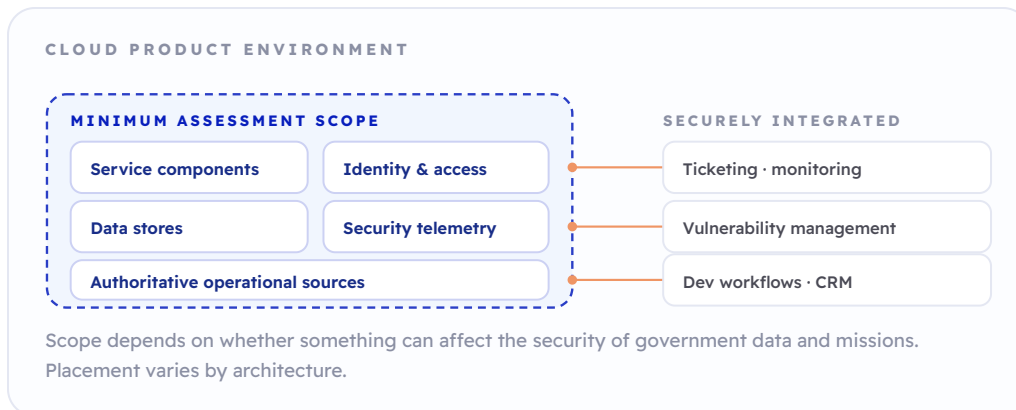
Depending on the architecture, that may include services used for:

- ticketing;
- monitoring;
- vulnerability management;
- development workflows;
- customer relationship management;
- other operational functions.

Better scoping can also give providers more flexibility to retain commercial products and operational tools where they can be securely integrated without unnecessarily expanding the assessed environment.

The goal is not to push as much as possible outside the scope. The goal is to understand what can affect the security of the government data and mission, then design the system accordingly.

For some tools, the difference can be meaningful.



3–5x

FedrAMP-specific versions of some tools may cost more than their commercial counterparts.

THAT CAN REDUCE

- duplicated environments;
- unnecessary FedRAMP-specific tooling;
- resources required to manage parallel systems;
- resources required to maintain multiple versions of the same environment.

BUSINESS IMPACT

Better scoping can reduce duplicated infrastructure, unnecessary tooling costs, and recurring operational overhead.

TECHNICAL IMPACT

Better scoping determines what truly needs to be assessed, what operational information must be maintained, and where commercial technology can remain part of the operating model.

The first savings opportunity in 20x is knowing what does not need to be in scope.

A Different Assessment Cost Profile

The annual assessment remains. The scramble does not have to.

FedRAMP 20x does not eliminate independent assessment.

Providers with Class B, C, or D certifications must complete an independent verification and validation assessment at least annually. For 20x, all KSIs must be included.

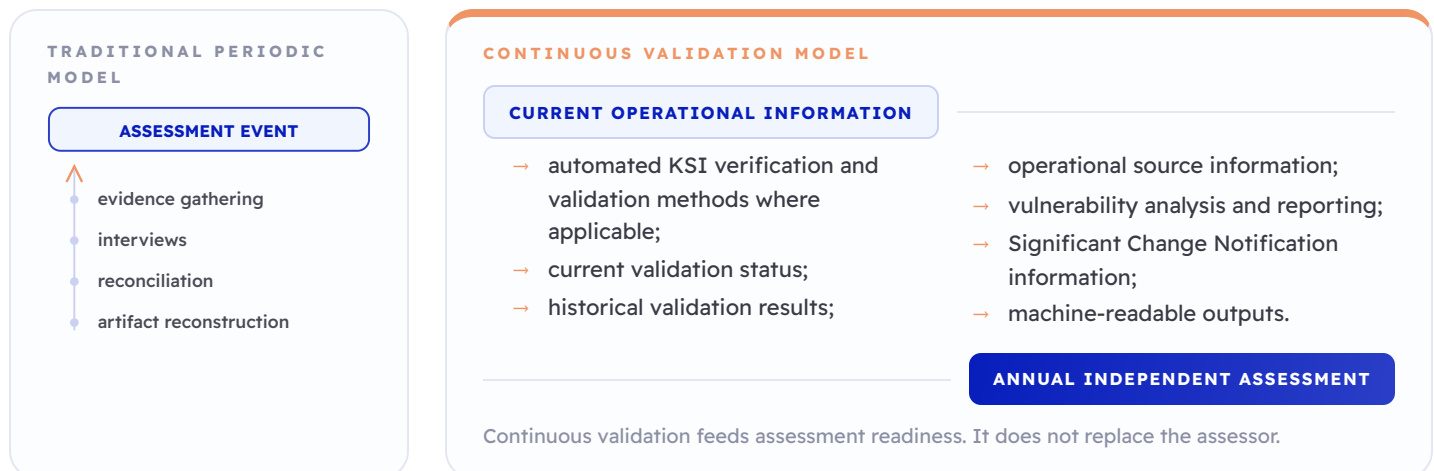
What changes is the information available when that assessment begins.

Under a traditional periodic model, teams may spend weeks or months collecting artifacts, preparing interviews, reconciling documentation, and rebuilding

evidence around an assessment event.

Under continuous validation, teams maintain current verification and validation information as the system operates.

The independent assessor still performs the assessment and applies independent judgment. The economic opportunity comes from reducing the work required to reconstruct the state of the system before the assessment can begin.



\$50K–\$80K

for initial assessment

Current illustrative range for a focused FedRAMP 20x independent assessment, compared with traditional initial assessments that may cost \$150K–\$250K.

Reduced annual assessment-preparation effort

Potential savings from reducing repeated preparation for annual independent assessment. The exact assessment cost will vary considerably by system, class, scope, maturity, assessor, and implementation.

BUSINESS IMPACT

Assessment costs and internal effort can shift away from large evidence-reconstruction events toward maintaining current validation information throughout the year.

TECHNICAL IMPACT

The system must produce accurate, traceable, and reviewable verification and validation information from authoritative operational sources.

Continuous validation does not replace independent assessment. It changes how much has to be reconstructed when assessment time comes.

A More Efficient Significant Change Process

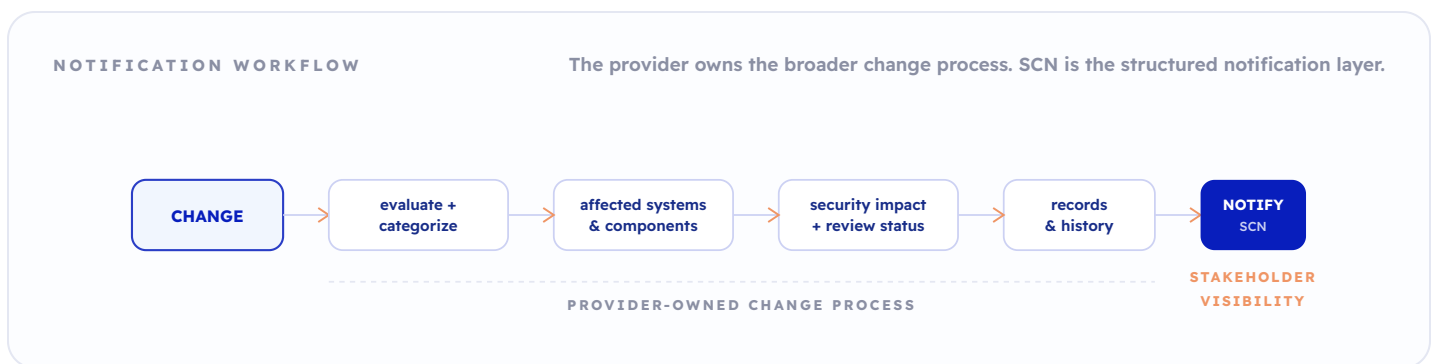
Significant changes become part of a structured notification workflow.

FedRAMP 20x establishes Significant Change Notification, or SCN, as a structured way for providers to communicate significant change information to the stakeholders who need to review it.

Providers still own the broader change process. They must evaluate and categorize changes, maintain appropriate records and history, and make required information available in the required formats.

The opportunity is to make that work part of an established operating model instead of treating every significant change as a new compliance project.

A mature SCN process can bring together change information, affected systems and components, security impact, review status, supporting records, stakeholder visibility, and required notification information.



\$10K–\$40K per change → potentially \$0

The potential reduction to \$0 refers to incremental external review and testing expense, not the total cost of implementing a significant change.

BUSINESS IMPACT

Cloud providers may reduce the cost, delay, and administrative friction associated with preparing and coordinating significant changes.

Potential reduction in incremental external review and testing cost for Significant Change Notification.

Many significant changes may no longer require the same external review and testing expense; exceptions depend on the nature and impact of the change.

TECHNICAL IMPACT

Change activity needs to be visible, governed, traceable, and communicated through a reliable notification process.

20x moves significant change toward a repeatable notification workflow instead of a separate evidence-reconstruction exercise.

Hidden Costs

The sneakiest costs are the weeks of skilled engineering time lost to assessment preparation and response.

Preparing for an initial assessment or annual independent assessment can pull teams away from their regular work for weeks or months.



Those hours have a direct labor cost. They also create opportunity cost. Security and engineering resources pulled into assessment preparation are not spending that time on work that could improve the system.

Weeks to months of team effort can be consumed by assessment preparation and response.

The actual impact depends on the organization's current process, automation maturity, architecture, scope, and the quality of the operational information already available. Continuous validation may reduce this disruption.

BUSINESS IMPACT

Less time can be spent on repeated assessment preparation, evidence chasing, and response.

TECHNICAL IMPACT

Engineering resources can focus more effort on system improvement, automation, vulnerability management, telemetry, and product quality.

An often overlooked cost of periodic assessment is engineering time spent preparing for it.

Upfront Investment, Long-Term Leverage

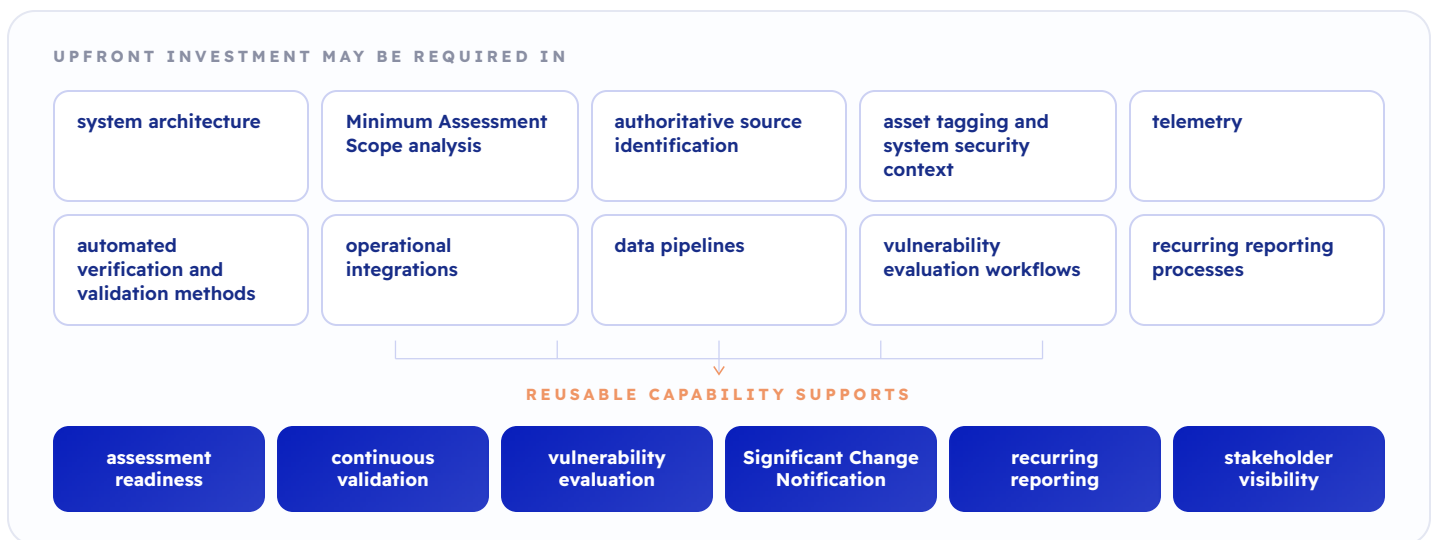
FedRAMP 20x changes where the work happens.

Continuous validation depends on the underlying environment being capable of producing trustworthy operational information.

For organizations with mature cloud environments and good operational data, some of that foundation may already exist. Other organizations may need substantial

engineering work before continuous validation can function effectively.

The investment creates leverage when those capabilities can be used repeatedly instead of rebuilding the same information for each assessment, reporting cycle, or downstream requirement.



THE VALUE CAN COME FROM

- better scoping decisions;
- better tooling decisions;
- stronger operational data;
- repeatable pipelines;
- more automated verification and validation where applicable;
- contextual vulnerability workflows;
- reduced reliance on static artifacts;
- fewer duplicated environments;
- less recurring assessment preparation;
- more efficient significant change coordination.

BUSINESS IMPACT

Upfront engineering can create an operating foundation that reduces repeated work later.

TECHNICAL IMPACT

Teams build the integrations, telemetry, context, and validation methods needed to maintain current information as the system operates.

The upfront investment can be significant. The leverage comes from using that foundation again and again.

Where 20x can change the cost of certification.

3–5x

The price premium for FedRAMP-specific tooling versus standard commercial versions of some of the same tools.

\$50K–\$80K

Current illustrative range for a focused FedRAMP 20x independent assessment, compared with traditional initial assessments that may cost \$150K–\$250K. Actual pricing varies by assessor, scope, system complexity, and implementation.

\$10K–\$40K per change → potentially \$0

Potential reduction in incremental external review and testing cost for Significant Change Notification.

Many significant changes may no longer require the same external review and testing expense; exceptions depend on the nature and impact of the change.

ILLUSTRATIVE COST SHIFT

TRADITIONAL MODEL

More cost concentrated in

- FedRAMP-specific tooling;
- duplicated environments;
- manual evidence collection;
- recurring assessment preparation;
- significant change coordination;
- engineering interruption.

COST STRUCTURE



FEDRAMP 20X

More investment concentrated in

- system design;
- operational data;
- integrations and pipelines;
- telemetry;
- automated verification and validation where applicable;
- ongoing operation.

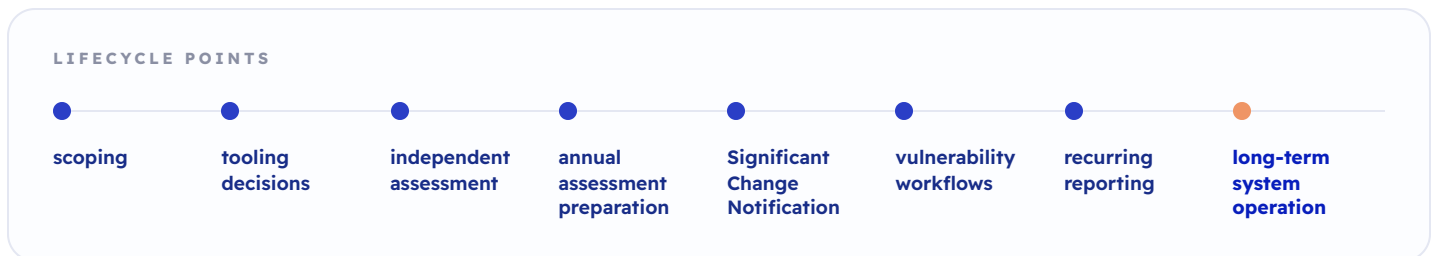
Illustrative market estimates based on 38North practitioner experience and current market quotes as of August 2026. Actual costs and savings vary by assessor, architecture, scope, tooling, system maturity, implementation approach, and engineering requirements. These figures are not guaranteed outcomes or NorthWatch performance claims.

The leverage can compound across the lifecycle.

FedRAMP 20x can change costs at multiple points in the lifecycle.

The biggest opportunity is not limited to direct assessment cost.

It is also found in the hidden costs of duplicated environments, manual evidence collection, recurring preparation, engineering interruptions, and repeated compliance work.



01

The Business Case

Cloud providers that invest early in system design, operational data, integrations, telemetry, and repeatable validation methods may reduce repeated work later.

02

The Operating Model

Instead of rebuilding proof primarily around review events, teams maintain current information showing what is implemented, whether it is working as intended, what changed, and what needs attention.

03

The Payoff

The same operational foundation can support continuous validation, Ongoing Certification Reports, Certification Data Sharing, assessment readiness, vulnerability evaluation, Significant Change Notification, and stakeholder visibility.

20x is not simply “FedRAMP gets cheaper.” It is a fundamentally different operating model for demonstrating and maintaining security.

What 20x means for each stakeholder.

FOR ECONOMIC BUYERS

FedRAMP 20x changes where costs accumulate.

WHERE MONEY MOVES

The opportunity is broader than lower assessment cost.

It includes the potential to reduce **duplicated infrastructure, recurring assessment-preparation cycles, unnecessary FedRAMP-specific tooling, significant change coordination, manual evidence work**, and the amount of highly skilled engineering time consumed by compliance preparation.

Some costs move upstream into architecture, integrations, telemetry, and automation. Those investments can create leverage when the same operational foundation is used repeatedly over the lifecycle of the system.

FOR TECHNICAL BUYERS

FedRAMP 20x rewards good system design.

WHAT CAPABILITY IS REQUIRED

The system must be **scoped correctly, integrated securely, and capable of producing accurate operational information**.

Teams need authoritative sources, appropriate telemetry, reliable pipelines, system security context, and repeatable verification and validation methods.

The earlier those decisions are made, the more downstream work they can support.

FOR EXECUTIVE TEAMS

FedRAMP 20x is more than a compliance update.

WHAT OPERATING MODEL CHANGES

It is a chance to rethink the operating model behind federal certification:

- how the system is built;
- how security is demonstrated;
- how operational information is reused;
- how teams reduce recurring compliance drag over time.
- how vulnerabilities are evaluated;
- how changes are communicated;
- how assessment readiness is maintained;

The economics ultimately follow the operating model.



ABOUT THE AUTHOR

Sam Leestma

VICE PRESIDENT, SOLUTIONS ENGINEERING · 38NORTH SECURITY

Sam Leestma brings deep FedRAMP, cloud security, and federal experience to 38North's work with cloud providers.

Before joining 38North, Sam served as Deputy Program Manager at the FedRAMP PMO, where he worked closely with federal stakeholders, cloud service providers, and assessment partners on the policy, technical, and operational realities of FedRAMP.

At 38North, Sam helps cloud companies understand how FedRAMP 20x changes the operating model behind federal certification, including system design, scoping, operational data, continuous validation, vulnerability workflows, and the economic tradeoffs behind federal market entry.

His work focuses on helping teams build FedRAMP strategies that are technically realistic, commercially viable, and grounded in how cloud systems actually operate.

ABOUT 38NORTH

38North provides compliance advisory and security engineering for regulated cloud environments.

Advisory

defines the path.

Engineering

builds the capabilities
and pipelines.

NorthWatch

operationalizes continuous validation
and makes the results visible,
reviewable, and shareable.

Our team helps cloud companies understand what must change, build what is missing, and operate and demonstrate the result.

Rethink the economics of your FedRAMP path.

To understand how FedRAMP 20x may change the cost, effort, and design of your path, start a conversation with 38North Security.

info@38NorthSecurity.com

