FORTREUM
Powered by KOVR.AI™

EXECUTIVE BRIEF · 2026

THE NEW STANDARD IN COMPLIANCE

The federal compliance industry has reached an inflection point. This brief documents what changed, why the old model no longer works, and what the new standard looks like in practice – from four founders who built the frameworks and the platform that runs under them.

JAMES LEACH
Co-Founder and CEO, Fortreum

MICHAEL CARTER
Co-Founder and President, Fortreum

ANDY BLACK
Co-Founder, KOVR
CSO, Fortreum

SRI IYER
Co-Founder, KOVR
CTO, Fortreum

The Old Standard Is Over

The compliance industry has been running the same play for twenty years. Point-in-time assessments. Annual audits. Evidence collection by hand. It worked — until the market outgrew it.

The threat landscape moved faster than the audit calendar. Regulations multiplied beyond what any team could manually track. Artificial intelligence arrived and changed what operational excellence looks like. And the customers asking for help are now asking for something different: not just a certification, but a risk-informed security and compliance program that reflects how their organization actually operates.

Fortreum was built by the people who helped create the FedRAMP framework itself. KOVR was built by engineers who operated inside the largest cloud infrastructure organizations in the world, watching them spend extraordinary sums and years navigating federal compliance — with individual services still averaging three years to an Authority to Operate. One major SaaS company spent the better part of a decade and millions of dollars just to clear basic federal certifications.

"Point-in-time assessments have been dead for years, even though policy has not shifted yet. The organizations still treating compliance as an annual event are operating behind a standard they believe they have met. We built Fortreum to be the firm that tells them the truth about that — and then fixes it."

JAMES LEACH, CO-FOUNDER, FORTREUM

"We did not theorize the old standard — we lived inside it at scale. We would watch a strong engineering team ship continuously through a modern CI/CD pipeline, then hand their security posture to a compliance process moving at the speed of an annual audit. Two clocks running at completely different speeds on the same system."

ANDY BLACK, CO-FOUNDER, KOVR

The industry spent twenty years optimizing the billable hour instead of eliminating it. That is the problem this brief addresses — and the opportunity the new standard captures.

The Compliance Landscape Broke

Enterprise organizations now navigate dozens of overlapping frameworks simultaneously. The manual model cannot scale.

FedRAMP, CMMC, SOC 2, ISO 27001, HIPAA, PCI, and multiple DoD-specific requirements can all apply to a single organization at once. Each has distinct requirements, credentialing, and timelines. The point-in-time model – point-in-time assessments, siloed teams, annual cycles – cannot keep pace.

AI has introduced a decisive variable. Organizations that adopt AI-native compliance tooling will gain structural advantages in speed, coverage, and cost. Those that do not will fall behind in the next procurement cycle – not gradually, but visibly.

"The average provider today has to meet upwards of 20, 30, in some cases 50 different regulations globally. It is becoming a nightmare to achieve and then ultimately maintain. That is not a problem you solve with more headcount. You solve it by rethinking the model entirely."

MICHAEL CARTER, CO-FOUNDER, FORTREUM

The shift is already in production. In-Q-Tel, the U.S. intelligence community's strategic investment arm, backed KOVR in 2026. The platform operates at Technology Readiness Level 9 in active Air Force and Space Force environments. When the institutions whose entire function is protecting the nation's most sensitive data choose a compliance platform, that is not a pilot program.

FORTREUM IN NUMBERS

Top 5

FEDRAMP3PAO

By authorization volume in the U.S. – one of five firms at this level.
Source: FedRAMP Marketplace, 2026

773%

THREE-YEAR GROWTH

No. 523 on the 2025 Inc. 5000.
Source: Inc. 5000, 2025

25+

YEARS COMBINED EXPERIENCE

Including original FedRAMP PMO personnel.

15+

FRAMEWORKS SUPPORTED

FedRAMP, CMMC, GovRAMP, ISO, SOC, HIPAA, PCI, and more.

Under 97

AUTHORIZED C3PAOS IN MARKET

Serving a DoD requirement of 76,600+ organizations needing CMMC Level 2 certification – fewer than 1 assessor per 780 organizations. Source: Cyber-AB, Jan 2026

Nov 2026

CMMC PHASE 2 DEADLINE

Third-party assessments become mandatory for all Level 2 DoD contracts. Organizations without an authorized C3PAO engagement risk losing contract eligibility. Source: DoD, 2025

AI compliance monitoring market ($B)

Projected growth 2025 to 2030 at 19.4% CAGR. Source: Virtue Market Research, 2025

What The Market Gets Wrong

Three assumptions account for most of the wasted time, budget, and credibility in federal compliance. All three are correctable.

MYTH 01

"Point-in-time assessments are still sufficient."

A compliance report frozen at a single moment tells you how secure an organization was on a day that has already passed. Continuous monitoring requirements are already embedded in FedRAMP and CMMC guidance – the regulators have moved beyond the annual model. Organizations still treating compliance as a once-a-year event are operating behind a standard they believe they have met. The correct model is continuous: evidence synchronized with the live system, posture always visible, and the audit-prep scramble eliminated as a recurring disruption.

MYTH 02

"Achieving one framework means I am close on the others."

SOC 2 does not get you to FedRAMP. FedRAMP and CMMC are not interchangeable. Each requires credentialed personnel specific to that authorization: CMMC Level 2 requires Certified CMMC Assessors; FedRAMP requires an accredited 3PAO. You cannot borrow results across frameworks.

MYTH 03

"AI alone is sufficient – or AI alone is the problem."

Both positions miss the answer. AI is exceptional at reading unstructured evidence, mapping it to controls, and generating audit-ready narrative at speed. What it cannot be is the accountable authority that stands behind a determination a federal Authorizing Official will challenge. A confident wrong answer in a federal package is not a time-saving – it is a liability. The right model is AI doing the volume work at machine speed, with credentialed human judgment validating the output. Anyone selling either extreme is selling risk.

"Customers regularly arrive convinced they are 80% of the way to an authorization they have barely started. The value is understanding where frameworks genuinely overlap – so evidence collected once can satisfy many – and being honest about where they do not."

ANDY BLACK AND **SRI IYER,** CO-FOUNDERS, KOVR

What It Looks Like In Practice

The question has shifted from "are we compliant?" to "how do we know – in real time – and can we prove it?"

THE OLD STANDARD	THE NEW STANDARD
Reactive compliance	Continuous, real-time posture monitoring
Annual audit cycles	Always-on evidence collection and readiness
Manual evidence gathering	Automated artifact collection and framework mapping
Siloed security and compliance	Unified offensive and defensive strategy
Fear-based vendor positioning	Confidence through verified, authoritative assurance
One-size-fits-all frameworks	Framework-agnostic intelligence with public sector depth
80% automation, 20% guesswork	AI-native platform with governance authority

"Automation alone does not create trust – authority does. There are plenty of companies that can take you 80% of the way. But getting to 100%, authoritatively, with the governance guardrails that actually hold water? That is the differentiator. That is the special sauce – the power of AI, plus trust through governance."

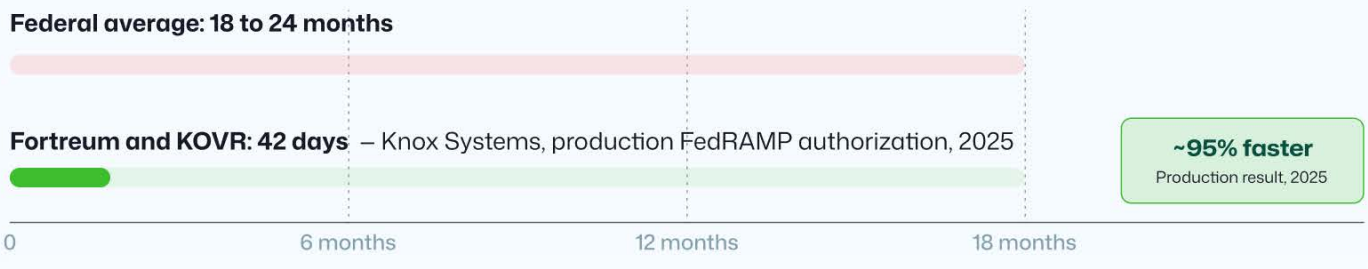
JAMES LEACH, CO-FOUNDER, FORTREUM

"What surprises clients most is what stops being an event. Compliance was always a dreaded annual cliff – a fire drill and a month of disruption. The new standard turns it into a continuous state. Evidence stays synchronized with the live system, readiness is always visible, and audit prep as a distinct painful phase essentially disappears."

ANDY BLACK AND **SRI IYER,** CO-FOUNDERS, KOVR

Authorization timeline: old model vs. integrated approach

Federal process average vs. KOVR-integrated engagements – 2025 production result



Automation And Authority. Not One. Both.

AI gets you to 80%. The last 20% is where authorizations are won or rejected – and only governance authority closes that gap

"AI is great, but it has to be done responsibly. Governance is not keeping up with the pace of AI. How do you know your IT investment actually mitigates risk, and how well does it do it? AI is just another utility to validate that – but you still need the authority behind it that regulators and agencies recognize"

JAMES LEACH, CO-FOUNDER, FORTREUM

KOVR is built on strict retrieval-augmented generation architecture: every output is grounded in evidence retrieved from the customer's own environment. When the platform states that multi-factor authentication is enforced, it is because it retrieved the specific configuration file that proves it. No evidence, no claim. KOVR operates at a sub-0.5% hallucination rate on critical controls.

"We treat trustworthiness as an architecture problem, not a marketing claim. Every AI-derived assessment ships with an explanation of its reasoning, so an Authorizing Official can validate the logic – not just accept the conclusion."

SRI IYER, CO-FOUNDER, KOVR

For the most sensitive environments, KOVR deploys inside the customer's own authorization boundary – on-premises, GovCloud, or fully air-gapped. The compliance engine runs inside the boundary it secures.

Most automation tools reach roughly 80% of what a federal authorization requires. They are fast, scalable, and cost-effective at evidence collection and mapping. The problem is the final 20%.

That last 20% is where an Authorizing Official decides whether to approve or reject your package. It requires a credentialed human assessor to validate AI output, resolve ambiguous control interpretations, and stand behind every determination as a matter of professional accountability.

No automation tool can be both the platform producing the work and the independent authority validating it. Those are fundamentally different roles. Fortreum and KOVR occupy both – together.

Retrieval-Augmented Generation (RAG) Architecture

Every output grounded in retrieved customer evidence. Citation to source artifact for every claim.

Human Review

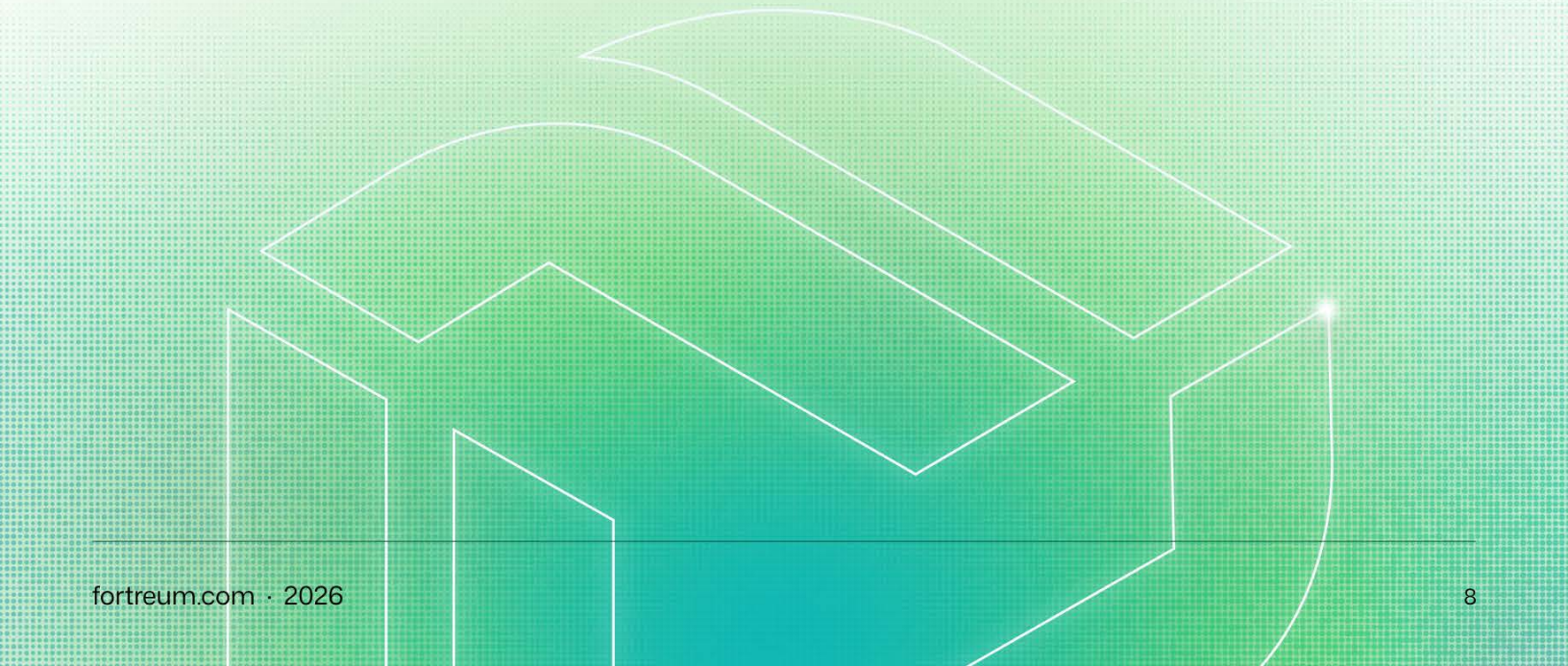
Credentialed assessor validates every AI-drafted determination before it becomes official.

Zero Data Retention

Customer evidence used for context at runtime only. Never trains a foundational model.

Boundary Deployment

Containerized and model-agnostic. Deploys on-premises or air-gapped inside the customer's environment.



Public Sector Is Our Wheelhouse

Fortreum does not compete on breadth. It competes on depth — in the frameworks that unlock government revenue, at the level of difficulty where most firms stop.

WHERE FORTREUM IS ACCREDITED

FedRAMP

Top 5 3PAO by authorization volume. KOVR earned its own FedRAMP Moderate authorization using its own platform.

CMMC

C3PAO authorization held. CCA-certified personnel across all levels. Phase 2 enforcement begins November 2026 — one of the only accredited assessors in a supply-constrained market.

GovRAMP

Accredited GovRAMP 3PAO, providing SLED organizations access to the same depth federal agencies rely on.

ISO / SOC

Accredited certification body. Consolidates multi-framework compliance into a single advisory engagement.

"Some of the larger enterprise customers could have 50, upwards of 100 frameworks. It is untenable given the current model. The proper planning in a three-to-five year view allows us to consolidate these challenges into a unified approach."

MICHAEL CARTER, CO-FOUNDER, FORTREUM

WHERE KOVR IS DEPLOYED

TRL-9

MAXIMUM READINESS LEVEL

Active Air Force and Space Force production — the highest possible deployment classification. Source: KOVR, 2026

1,200+

SYSTEMS AUTOMATING RMF

Active DoD program at scale, in production. Source: KOVR, 2026

In-Q-Tel backed

INTELLIGENCE COMMUNITY VALIDATION

In-Q-Tel, the U.S. intelligence community's strategic investment arm, backed KOVR in 2026. Source: In-Q-Tel, 2026

THE SUPPLY CONSTRAINT

Fewer than 97 authorized C3PAOs exist to serve a DoD requirement of 76,600+ organizations needing CMMC Level 2 certification. To put that in context: fewer than one authorized assessor per 780 organizations that need certification.

Fortreum's C3PAO accreditation is a scarce, regulated credential that new entrants cannot quickly replicate. It is one of the most durable competitive advantages in the federal market today.

"AC-2(1)(a) is not a checkbox to us — it is an atomic unit the engine reasons about. Commodity tools fall apart at parameter-level granularity. That is precisely where KOVR is optimized."

SRI IYER, CO-FOUNDER, KOVR

Built To Complete The Solution For The Customer

Customers want a compliance outcome. Bringing KOVR and Fortreum together is what makes it possible to deliver one.

KOVR needed Fortreum for governance expertise, regulatory credibility, and the human authority that makes AI output defensible. Fortreum needed KOVR to deliver the differentiated technology experience that drives better coverage, depth, speed, and efficiency. Neither half is the complete answer. Together, the result is a better outcome for the customer on every dimension that matters.

"I know the government side of this world well, and it was clear we could not be both the automation engine and the independent authority. Those are different roles. Blurring them would undermine the very trust we were building. That is the moment Fortreum fit."

ANDY BLACK, CO-FOUNDER, KOVR

The integration is not additive – it is multiplicative. Platform output and human validation operate as one continuous workflow from the beginning. Two things that have always been sequential and disconnected – automation and authoritative sign-off – now run together.

PATENTED CAPABILITY

Fortreum and KOVR hold patents in AI-native compliance automation – the only patented capability of its kind in the federal compliance market. This is a credential no competitor can replicate.

THREE WAYS CLIENTS ENGAGE

Assessment Module

KOVR embedded to accelerate testing. Gap assessment in approximately 15 minutes. Real-time readiness indicator. No month-long document collection phases.

Advisory Engagement

Full lifecycle advisory with KOVR as the client platform. SSP generation, POA and M drafting, OSCAL export, and continuous readiness tracking throughout.

Platform License

KOVR deployed inside the customer's own boundary – on-premises, GovCloud, or air-gapped. The compliance engine runs inside the boundary it secures.

Between KOVR's deployments across federal environments and Fortreum's assessment history, the integrated platform draws on one of the largest bodies of anonymized compliance data available – a compounding advantage that grows with every engagement.

Knox Systems. 42 Days.

Customers want a compliance outcome. Bringing KOVR and Fortreum together is what makes it possible to deliver one.

42

DAYS TO FEDRAMP ATO

~95% faster

vs. 18–24 month federal average

Knox Systems needed FedRAMP authorization to access federal agency contracts. KOVR ingested their actual environment — source code, infrastructure, existing documentation — and did the heavy lifting: mapping evidence to controls, drafting implementation narratives, and assembling the System Security Plan. Fortreum's credentialed assessors validated every determination.

A key factor in the speed: KOVR's ability to deploy directly into Knox's existing authorization boundary, eliminating the data transfer delays and environment setup typically required before assessment work can begin. The platform and the authority worked as one program from day one.

Full FedRAMP authorization in 42 days. A production authorization, not a pilot. The same architecture running this result is now deployed at Technology Readiness Level 9 in active Air Force and Space Force environments.

An Exclusive, Natively Integrated Capability

Customers are asking for risk-informed security and compliance programs. Frameworks like FedRAMP require it. Fortreum is the only firm that provides compliance authority and adversarial validation as a single integrated program.

Authorization tells you what your posture should be. Offensive Security Labs tells you whether it actually holds under adversarial conditions. After frameworks are authorized and the monitoring platform is active, Labs answers the question that ultimately matters: does your architecture actually minimize impact when – not if – something is compromised?

AI extends what offensive security can cover: broader scope, faster reconnaissance, more efficient reporting. It does not replace practitioners who understand how adversaries actually think. Labs uses AI as a force multiplier, not a substitute. The combination produces depth that neither achieves alone.

THE COMPLETE ANSWER

The most durable position in public sector combines three things no single competitor currently provides at this depth:

- Compliance authority – authorization earned through credentialed expertise and patented technology
- AI-native continuous monitoring – posture always visible, evidence always current
- Adversarial verification – confirming what is authorized actually holds under pressure
- AI-augmented penetration testing with broader coverage and faster reporting
- Assume-breach risk evaluation – not if, but how well do defenses limit impact
- Adversarial validation of compliance controls against real attack scenarios
- Human-in-the-loop analysis throughout all offensive operations

The Era Of Manual Compliance Is Over

The organizations that act on that now will own the next decade of public sector work. Compliance is becoming a growth engine — but only for those who treat it as a continuous operating model.

CMMC Phase 2 enforcement begins November 2026. Fewer than 97 authorized C3PAOs serve a requirement of 76,600 organizations. FedRAMP 20x is accelerating the CSP authorization pipeline. The supply constraints are structural. Organizations that secure their assessor relationships now will have an advantage that is not recoverable later.

"The future is not AI replacing human expertise — it is AI amplified by human authority. Automation at machine speed, validated by people the regulators trust. That combination is the new standard in compliance. The old one is already gone. The only question left is whether you are building on the new standard or still defending the ruins of the old."

ANDY BLACK AND **SRI IYER,** CO-FOUNDERS, KOVR

The question is: what are you building in its place?

AUTHORS

JAMES LEACH
Co-Founder, Fortreum

MICHAEL CARTER
Co-Founder, Fortreum

ANDY BLACK
Co-Founder, KOVR

SRI IYER
Co-Founder, KOVR