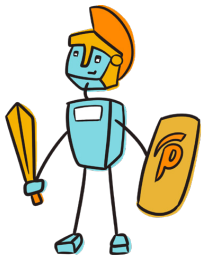
pretorin

AI-NATIVE GOVERNMENT CYBERSECURITY COMPLIANCE

The fastest path to authorization. Period.



Pretorin is an AI-native platform that automates cybersecurity compliance across **FedRAMP, DoD RMF, NIST 800-53, and CMMC** — so agencies and vendors achieve, maintain, and prove authorization faster than ever.

Lowering barriers. Raising the bar.

For many modern government systems, **the time and cost to achieve authorization now exceed the time and cost to build the software itself.** FedRAMP authorizations commonly run 12–18 months; RMF and CMMC add hundreds more controls. The most innovative systems stall in compliance purgatory long after the technical work is done.

12→1 mo	90%	10x	Any stack
Authorization timeline reduction — from waiting to fielding	Cost reduction for compliance package preparation	Force multiplier for your security team	Any software type, any technology stack

THE PROBLEM Compliance has become the wall between built and fielded

Hundreds of controls
NIST 800-53 catalogs hundreds of controls — each needs narratives, policy references, and linked technical evidence.

A multi-framework world
FedRAMP for civilian agencies, RMF and CMMC for DoD. The mappings are real but poorly operationalized, so teams duplicate work.

Documentation drift
Evidence lives in spreadsheets and eMASS exports, disconnected from the codebase. Every change can restart the clock.

Tools that don't fit
Commercial GRC tools track tasks but aren't in your code or CI/CD. Consultants are expensive and rarely faster.

HOW IT WORKS One loop: from system reality to signed authorization

1 · AI Security Agent
Reads the artifacts your engineers already use — code, infrastructure-as-code, configs, CI/CD, and deployment manifests — and builds a live model of how your system really works.

2 · Cross-framework graph
Controls are modeled as a connected graph. One implementation detail — like enforcing TLS or MFA — satisfies many controls across FedRAMP, RMF, and CMMC at once.

3 · AI-drafted, human-approved
Runs in your PRs and pipelines, drafts OSCAL-native artifacts grounded in real evidence, and routes them to a reviewer who accepts, edits, or overrides.

Ingests: source repos · IaC · CI/CD pipelines · runtime logs & metrics · security policies → **Generates:** OSCAL models · System Security Plan (SSP) · Assessment Plan / Report · POA&M

THE DIFFERENCE From ATO as burden to ATO as infrastructure

	TRADITIONAL APPROACH	With Pretorin
Time to authorization	12–24 months, then it restarts	**Continuous — cATO via OSCAL**
Documentation	Manual, written by your engineers	**AI-generated, human-approved**
Cross-framework work	Duplicated for each framework	**Mapped once, reused everywhere**
Cost to maintain	High (consultants + labor)	**~70% lower through automation**
When issues surface	At assessment review	**At commit, in your pipeline**

© 2026 Pretorin, Inc. · Proprietary & confidential

Compliance as infrastructure, not a burden.

pretorin

WHY PRETORIN What makes us different

AI-native, not bolted on

Built from the ground up as an AI system that reads code, IaC, and configuration — **not a legacy GRC tool with an AI feature added**. Every claim is grounded in observable evidence, never hallucinated.

Cross-framework by design

A connected control graph maps requirements across **FedRAMP, DoD RMF, NIST 800-53, and CMMC**, so a single change updates a shared understanding instead of each framework in isolation.

Lifecycle-integrated & continuous

Compliance runs like CI: PRs and deploys are checkpoints that flag affected controls and refresh documentation. It **catches drift early** and keeps artifacts current as your system evolves.

Human-in-the-loop by default

Authorization decisions stay with accountable people. Pretorin automates the mechanical work and **explains every control gap in plain terms**, so lean teams gain real expertise fast.

WHO IT'S FOR Built for the teams compliance leaves behind

STARTUPS & VENDORS

FedRAMP + CMMC at once

Map technical and organizational controls to both frameworks in parallel — build SSPs, evidence, and POA&Ms incrementally instead of a last-minute sprint.

DoD PROGRAM OFFICES

Modernize a legacy system

Reconcile documentation against the running system, surface drift, and keep RMF / NIST 800-53 artifacts true to the current state as you migrate.

SYSTEMS INTEGRATORS

A portfolio of ATOs

Model shared services once and inherit them across systems. Portfolio views reveal coverage, gaps, and the highest-payoff investments.

DEPLOY YOUR WAY Meets the standard it helps you achieve

Managed gov cloud

Runs as a segregated service in government-ready cloud, integrating through tightly scoped access to your repos and pipelines.

Private & air-gapped

Deploy in your own tenant or on-prem, including disconnected networks. The agent and models run inside your boundary — evidence never leaves the enclave.

Audit-ready by design

Encryption in transit and at rest, role- and attribute-based access, and a traceable record of every file examined and every human edit.

FRAMEWORKS SUPPORTED

FedRAMP · DoD RMF · NIST 800-53 · NIST 800-171 · CMMC

AVAILABLE TODAY

Platform · API · MCP · CLI

OUR MISSION

Improve the quality of government software.

Built by a team that has **led AI efforts inside the U.S. Army** and advised federal software programs. The platform, API, MCP, and CLI are live — start automating documentation, control mapping, and continuous monitoring today.

Get started — platform.pretorin.com

CONTACT

Isaac Faber, PhD · CEO & Co-Founder
isaac@pretorin.com

Ruben Cruz · COO & Co-Founder
ruben@pretorin.com

222 S Mill Ave, Suite 800, Tempe, AZ 85281

© 2026 Pretorin, Inc. · Proprietary & confidential