PRESCIENT SECURITY

One Partner for Every Federal Framework

Assessment, validation and testing across federal, defense, state and regulated markets

Every federal framework has its own baseline, evidence expectations and assessor requirements, and the overlap between them is easy to lose when engagements are scattered across vendors. Prescient Security assesses the full federal landscape with one assessment-first methodology, so the evidence you build for one authorization is reusable for the next.

Frameworks we assess

Framework	Who needs it	What Prescient Security delivers
CLOUD AUTHORIZATION		
FedRAMP Rev 5	Cloud providers selling to federal agencies	Readiness, initial and annual assessments against NIST SP 800-53 Rev 5 baselines
FedRAMP 20x	Cloud providers on the streamlined, automation-first path	Cloud providers on the streamlined, automation-first path
GovRAMP	Providers serving state, local and education buyers	Readiness and authorization assessments at each GovRAMP impact level
TX-RAMP	Vendors selling cloud services to Texas state agencies	Level 1 and Level 2 certification assessments
DoD IL4 / IL5	Cloud providers hosting CUI and mission workloads for DoD	Assessment against DoD Cloud Computing SRG overlays on the FedRAMP baseline.
DEFENSE INDUSTRIAL BASE		
CMMC Level 2	Defense contractors and subcontractors handling CUI	Official Level 2 certification as an Authorized C3PAO, plus independent validation
NIST SP 800-171 Rev 2/Rev 3	Cloud providers on the streamlined, automation-first path	Cloud providers on the streamlined, automation-first path
NIST RISK FRAMEWORKS		
NIST CSF 2.0	Organizations building or benchmarking a security program	Gap assessment across all six functions, target profile and tier definition
NIST AI RMF	Organizations developing or deploying AI systems	Assessment across Govern, Map, Measure and Manage, mapped to ISO/IEC 42001
SECTOR AND REGULATORY		
CJIS Security Policy	Agencies and vendors accessing criminal justice information	Assessment against CJIS policy areas with documentation for agency review
ITAR	Organizations handling export-controlled technical data	Assessment of access, storage and transmission controls for ITAR data
FTC Consent Order	Companies under an FTC order requiring independent assessments	Independent assessor reports on the cadence the order requires
IRS Publication 4812	Contractors handling IRS sensitive but unclassified information	Assessment against contractor security and privacy control requirements

How we engage, whatever the framework

Every engagement runs in one of three clearly separated lanes. We never blur adviser and assessor roles for the same customer in the same certification or authorization cycle.

1 Readiness and gap analysis

- Scoped view of in-scope systems, boundaries and data flows
- Structured review of policies, procedures and technical controls
- Prioritized gaps and remediation plan mapped to the target baseline

2 Formal assessment

- Control-by-control evaluation against the framework's assessment procedures
- Evidence-based testing of how controls operate in practice
- Transparent findings with clear rationale and reporting for authorizing officials

3 Continuous validation

- Annual assessments, affirmations and significant change reviews
- Input on using existing tools for ongoing monitoring and evidence collection
- Coordination with COI-safe partners for deeper remediation

Why organizations choose Prescient Security

Authorized C3PAO with federal lineage

Our assessors bring deep experience across NIST, FedRAMP and DoD frameworks, and we conduct official CMMC Level 2 certifications.

Assessment-first, evidence-driven: We start from what you already have

GRC platforms, tickets, logs and existing controls. Then we map it to the baseline instead of rebuilding from scratch.

Clear boundaries, no mixed incentives

Conflict of interest is a design principle. When we assess, we stay independent. When we advise, we stay within limits and route deeper work to partners

One evidence set, many authorizations

NIST SP 800-53, 800-171 and CSF overlap heavily. We map once so FedRAMP, CMMC, GovRAMP and state evidence reinforce each other rather than repeat.

CREST penetration testing and red teaming

FedRAMP requires penetration testing across a defined set of attack vectors, and every authority expects proof that controls hold up under real pressure. Our in-house team delivers both.

1. Penetration testing across all FedRAMP-required attack vectors, scoped to your authorization boundary
2. Adversary-emulation red team exercises that test detection and response, not just configuration
3. Findings written for engineers to fix and for authorizing officials to accept

Ready to start?

Tell us which contracts, customers or regulators you need to satisfy. We will help you sequence the right frameworks and scope one engagement that covers them.