Compliance Acceleration: CMMC, NIST, and FedRAMP Readiness

A structured compliance readiness engagement that identifies control gaps, implements remediation plans, and prepares evidence packages, accelerating the path to certification or authorization.

PRACTICE

Cyber Resilience and Zero Trust

CLIENT PROFILE

Defense contractor or federal agency preparing for CMMC certification, NIST 800-171 assessment, or FedRAMP authorization with gaps in current security controls

Challenge

- Unclear current compliance posture with undocumented security controls
- Significant gap between existing practices and required control frameworks
- Tight certification timelines with limited internal compliance expertise

Approach

- Conduct gap assessment against target framework (CMMC, NIST 800-171, FedRAMP)
- Prioritize remediation activities based on risk and certification timeline
- Implement technical controls and document policies, procedures, and evidence
- Prepare System Security Plan (SSP), POA&M, and assessment-ready evidence packages

Typical Outcomes

- Clear, prioritized remediation roadmap with resource and timeline estimates
- Implemented technical controls closing highest-risk gaps
- Assessment-ready documentation packages reducing certification timeline

Procurement Paths

- GSA MAS for compliance assessment and advisory services
- NASA SEWP V and SEWP VI for security tooling supporting compliance controls
- DoD ESI for covered security products

Compare vehicles and ordering steps on **How to buy**.

Partner Technology Examples

- Tenable
- Elastic Security
- Palo Alto Networks
- Microsoft Azure

Frequently Asked Questions

What is CMMC 2.0 and who needs to comply?

CMMC 2.0 is a DoD framework requiring defense contractors handling Federal Contract Information (FCI) or Controlled Unclassified Information (CUI) to meet specific cybersecurity practices. Level 1 applies to all prime and subcontractors; Level 2 and 3 apply to contractors handling CUI or critical programs.

How does Norseman support CMMC 2.0 readiness?

Norseman provides gap assessments against NIST SP 800-171, remediation roadmaps, System Security Plan (SSP) development, and technical implementation of required controls. Norseman procures required tools through ITES-4H, GSA MAS, and CIO-CS.

What contract vehicles support compliance engagements?

Compliance advisory and implementation services are available via CIO-CS (NITAAC), GSA MAS Professional Services, and ITES-4H. Technology products required for compliance are available across all Norseman

contract vehicles.

This is a representative use case. To request a briefing or a quote, contact Norseman Defense Technologies at 410.579.8600 or sales@norseman.com.