Datasheet

CMMC Proof Compliance Accelerator

Level 2 Certified

Let's take the complexity out of compliance.

We'll help you choose the right starting point and support you through the path to certification.

About nysernet

We are nysernet—a nonprofit organization serving those who serve others, across New York State and beyond. For four decades, we have partnered with our members to solve common challenges, build secure foundations, and spark new connections. As a trusted conduit to power those who serve the community, we believe the future is in our hands—yours and ours. Through a vibrant community designed by you, for you, and with you, we will pave new pathways to progress, together. We saved you a seat.

www.nysernet.org

membership@nysernet.org

nysernet

Navigating CMMC requirements can be daunting—especially for organizations with limited compliance experience or internal resources. From interpreting controls to documenting evidence, the process can quickly become time-consuming and error-prone, putting contracts and timelines at risk.

The CMMC Proof Compliance Acceleration System simplifies the entire process. Built by CMMC-certified experts, this turnkey solution walks you through scoping, gap identification, remediation, and documentation—step by step. You'll receive practical tools, policy templates, expert guidance, and a clear path forward to compliance.

Benefits

- **Accelerate Certification**
  Fast-track your path to CMMC Level 2 with a clear, guided approach that simplifies complex requirements.
- **Win More Contracts**
  Unlock access to government contracts requiring Controlled Unclassified Information (CUI) handling by demonstrating verified compliance.
- **Reduce Risk & Liability**
  Avoid costly fines, penalties, and reputational damage by ensuring you're always audit-ready and compliant.
- **Stand Out From the Competition**
  Position your organization as a trusted, cyber-resilient partner with a proven commitment to security.
- **Gain Peace of Mind**
  Eliminate uncertainty and stress with expert-backed support throughout your CMMC journey.

Key Features

- Strategic plan tailored to FAR 52.204-21 and DFARS 252.204-7012 obligations
- CMMC Level 2 Rev. 2 Gap Assessment completed in just six weeks
- SPRS score calculation to benchmark and track compliance progress
- Development of a customized System Security Plan (SSP) and IT procedures
- Hands-on support to remediate deficiencies for assessment readiness
- Accelerated path to CMMC Level 2 certification in as little as 3–6 months
- Comprehensive documentation to demonstrate commitment to cybersecurity
- Increased eligibility for contracts involving Controlled Unclassified Information (CUI)

Datasheet

Your Path to CMMC Certification—Simplified

No matter where you are in your compliance journey, our system offers a clear, expert-guided path to CMMC success. Each phase is designed to meet you where you are—whether you're just getting started or ready for certification—allowing you to pick and choose based on your institution's needs.

Phase 1: Pre-Assessment

Designed for organizations at the beginning of their CMMC preparation who need to establish a clear picture of their environment. This phase supports teams in identifying and categorizing federal unclassified information (FCI) and controlled unclassified information (CUI), building IT network and data flow diagrams, and inventorying all assets. It's especially valuable for those defining assessment scopes and exploring ways to limit the boundaries of compliance. If you're unsure what needs to be protected—or want to streamline your effort—Phase 1 lays the essential groundwork.

Phase 2: Assessment

For organizations ready to evaluate where they stand in relation to CMMC requirements. This phase includes completing an IT risk assessment and conducting both Level 1 and Level 2 CMMC assessments to measure current compliance. It's ideal for institutions that have defined their environment and are now seeking to identify security gaps, validate existing controls, and understand what remains to be addressed before certification. Phase 2 provides the diagnostic insights needed to move confidently into remediation.

Phase 3: Remediation

For organizations that have completed their assessments and are ready to act on the findings. It focuses on assigning responsibility for remediation tasks, tracking their progress, and confirming that all Plan of Action and Milestones (POA&M) items are fully resolved. It's ideal for teams that want to ensure every identified gap is not only addressed, but also functioning as intended—paving the way for a successful certification outcome.

Phase 4: Documentation

For teams preparing the formal documentation required for certification. It focuses on updating the System Security Plan (SSP) and refining policies and procedures to reflect the current state of compliance. Ideal for organizations that have completed remediation, this step ensures that documentation accurately supports all implemented controls and aligns with the expectations of assessors.

Phase 5: Certification

For organizations ready to validate their compliance and pursue official certification. It includes gathering and uploading evidence for each assessment objective, conducting a mock Level 2 assessment to ensure readiness, and selecting an authorized C3PAO for the formal review. It's best suited for teams that want to go into their certification assessment fully prepared, with confidence that their controls, documentation, and practices will stand up to scrutiny.

Ready for expert support every step of the way?

Contact us at **membership@nysernet.org** to determine where to start.

nysernet

www.nysernet.org