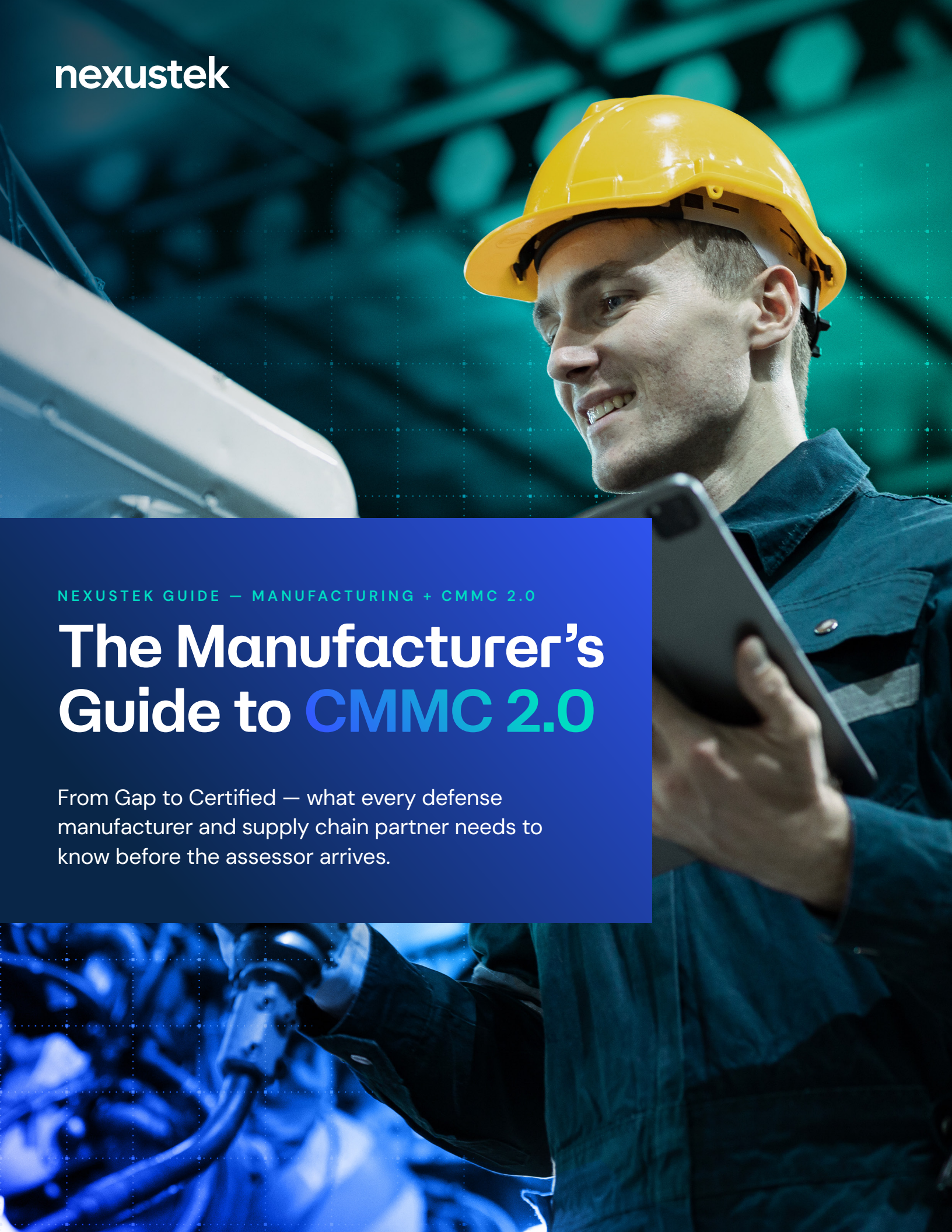
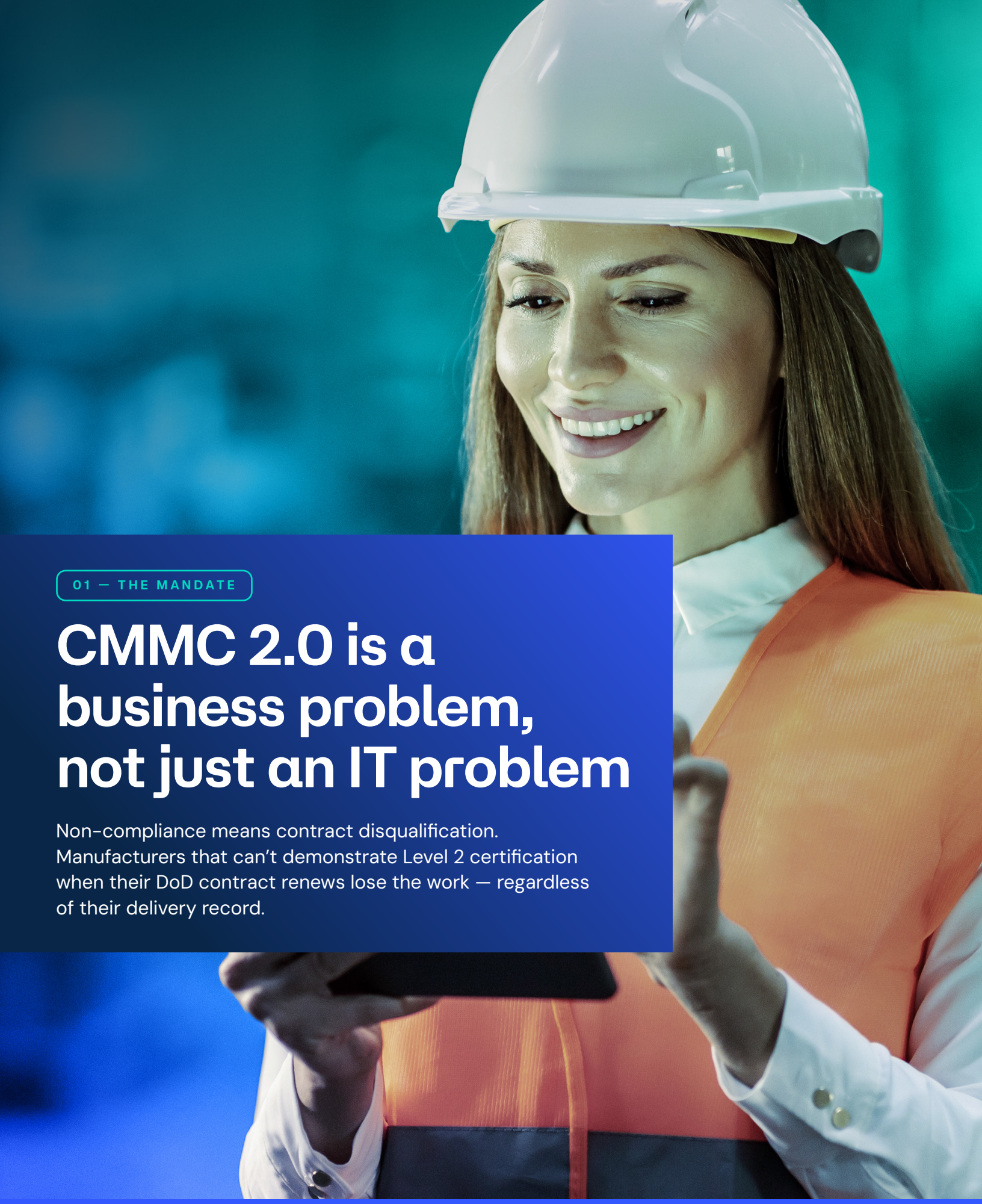
nexustek



NEXUSTEK GUIDE — MANUFACTURING + CMMC 2.0

The Manufacturer's Guide to CMMC 2.0

From Gap to Certified — what every defense manufacturer and supply chain partner needs to know before the assessor arrives.



01 — THE MANDATE

CMMC 2.0 is a business problem, not just an IT problem

Non-compliance means contract disqualification. Manufacturers that can't demonstrate Level 2 certification when their DoD contract renews lose the work — regardless of their delivery record.

Why this guide exists

The DoD's CMMC 2.0 framework is now in effect. For manufacturers in the defense industrial base, Level 2 certification is no longer optional — it is a contract requirement tied directly to the ability to receive, perform on, and renew DoD work.

Most manufacturers are not ready. The gap between current IT posture and the 110 controls required is significant. Lean IT teams, aging infrastructure, shop-floor endpoints with no security controls, and tools deployed without governance frameworks are the norm across mid-market manufacturing — and every one is a compliance gap assessors will flag.

80,000
contractors need Level 2.
Only 270 hold a final certificate.

1%
feel fully prepared for CMMC audits

89%
have suffered losses from a cyber incident

1%
of defense contractors feel fully prepared for CMMC audits

CYBERSHEATH, 2025

89%
have already suffered financial or business losses from a cyber incident

CYBERSHEATH, 2025

270
hold a final CMMC certificate out of 80,000 contractors required

CYBERSHEATH, SEPT 2025

The three levels — and where you land

CMMC 2.0 uses three levels tied to the type of federal information you handle. Understanding which level applies to your contract profile is the first step in any compliance engagement.

LEVEL 1 — FOUNDATIONAL

17 Practices

Applies to Federal Contract Information (FCI) only

Basic safeguarding practices

Annual self-assessment — no third-party audit

LEVEL 2 — ADVANCED

110 Practices

Applies to Controlled Unclassified Information (CUI)

14 domains aligned to NIST SP 800-171

Triennial C3PAO audit for critical programs

Most mid-market manufacturers require Level 2.

LEVEL 3 — EXPERT

NIST 800-172

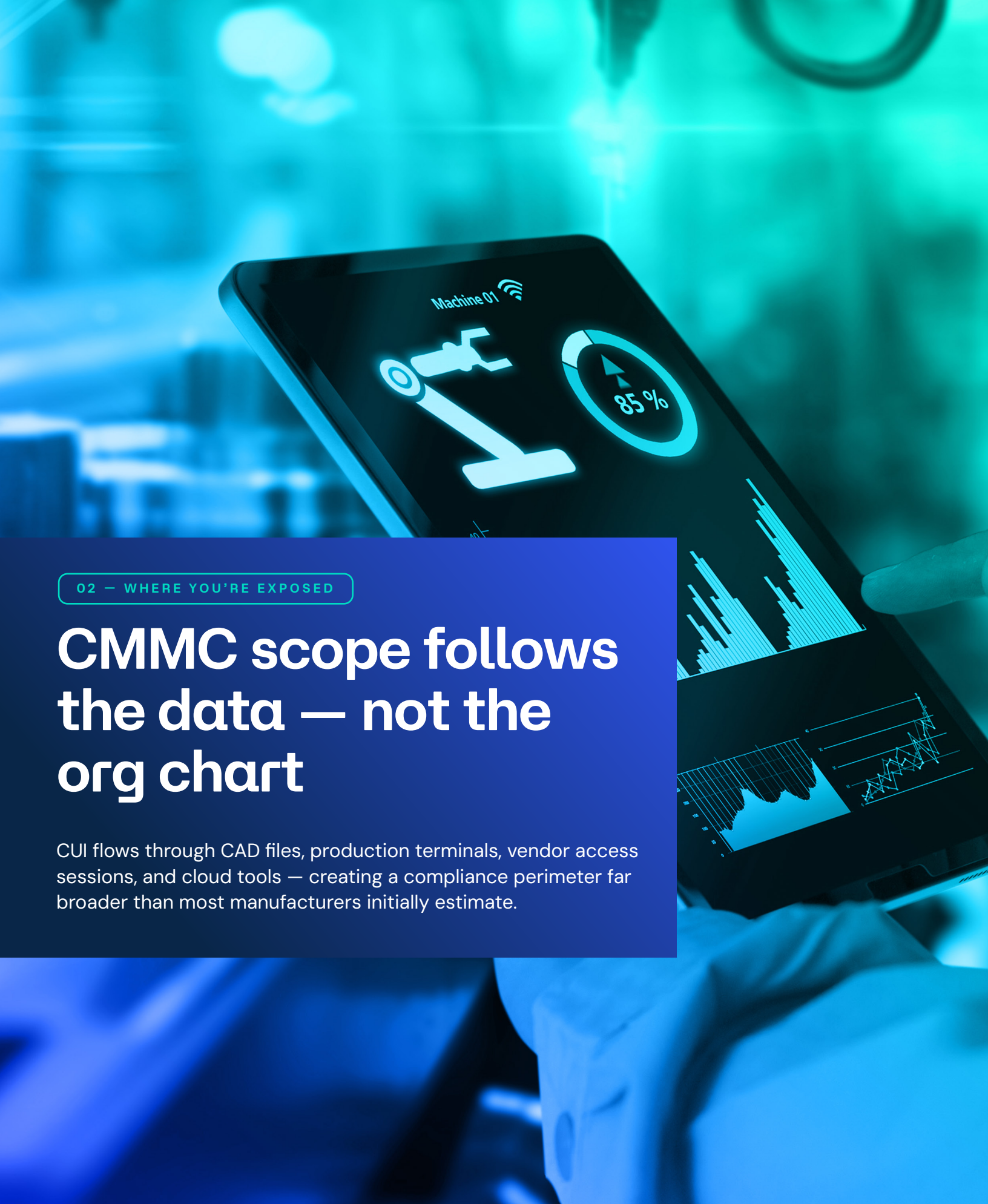
Select high-priority DoD programs

Enhanced controls beyond NIST 800-171

Government-led assessment by DCMA

ON C3PAOS

A Certified Third-Party Assessment Organization is the only body authorized to conduct a formal Level 2 certification assessment. NexusTek is not a C3PAO — we prepare manufacturers to pass the C3PAO assessment. The two roles are distinct and complementary.



02 — WHERE YOU'RE EXPOSED

CMMC scope follows the data — not the org chart

CUI flows through CAD files, production terminals, vendor access sessions, and cloud tools — creating a compliance perimeter far broader than most manufacturers initially estimate.

The four highest-risk exposure areas

Every system, endpoint, or vendor connection that touches CUI is in scope. Getting the scope definition right before beginning remediation prevents the most expensive surprises.

01	**CAD, PLM, and engineering environments** Drawings, BOMs, technical data packages, and revision-controlled files are the primary home for CUI in manufacturing. Access control, audit trails, and defined data boundaries are required on every system that stores or accesses them.	CRITICAL
02	**Shop-floor and production endpoints** Operator terminals displaying build instructions, test procedures, and inspection data are in CMMC scope whenever CUI reaches them. VDI and session isolation are the primary architectural responses — they keep the endpoint out of scope while meeting production workflow requirements.	CRITICAL
03	**Vendor and integrator remote access** CNC maintenance, MES integration, and OEM access paths are among the most frequently cited gaps in Level 2 assessments. Unmanaged vendor access bypasses virtually every perimeter control a manufacturer has in place.	HIGH
04	**Cloud and file sharing for engineering workflows** Cloud services storing, processing, or transmitting CUI must be FedRAMP Moderate authorized or equivalent. Most commercial file-sync and document management tools do not meet this standard — and most manufacturers are using them for engineering collaboration.	REGULATORY

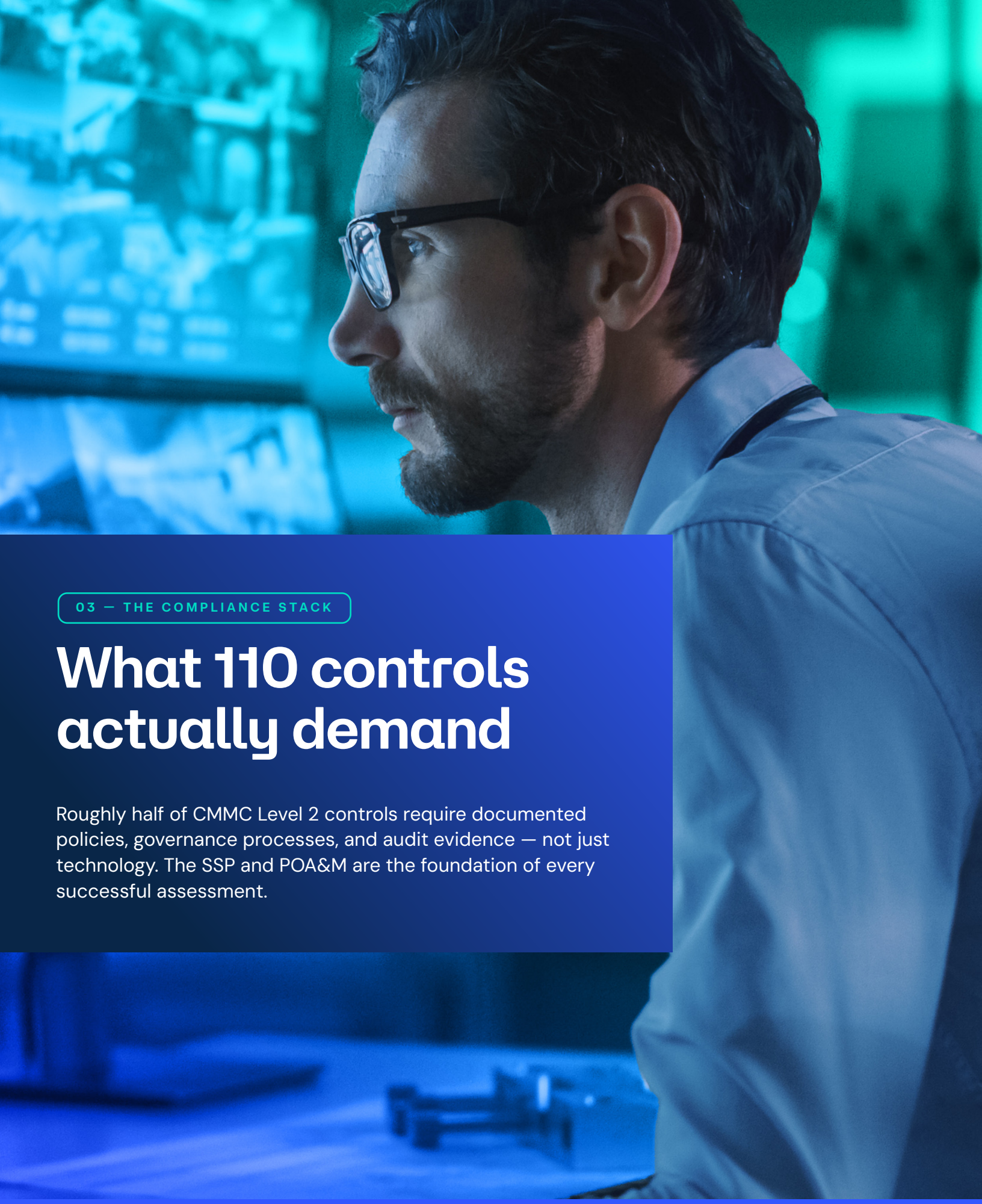
The 6 compliance challenges unique to manufacturing

CMMC was written against a standard corporate IT environment. Manufacturing is not that. These six challenges explain why mid-market manufacturers need external expert support — not just tools.

01	**Lean or absent internal IT** CMMC Level 2 requires 110 controls spanning access management, incident response, audit logging, system hardening, and more. Most manufacturers have one or two generalist IT staff — or none. One person cannot design, implement, and sustain that scope while also running a help desk.
02	**Aging infrastructure** End-of-life servers, switches, and firewalls that cannot be patched are an active compliance liability. Systems that cannot be patched cannot meet CMMC configuration management requirements — assessors flag EOL infrastructure immediately.
03	**IT/OT convergence** As manufacturers connect production equipment, PLCs, and SCADA systems to corporate networks, CUI can reach the production floor through paths never designed for auditability. CMMC does not exempt OT environments when CUI flows through them.
04	**Multi-site fragmentation** Multiple facilities create fragmented IT environments where security policies are applied inconsistently. Remote sites often operate without adequate monitoring — creating blind spots assessors will flag during evidence review.
05	**Supply chain exposure** Drawings and technical packages move to machining shops, PCB fabricators, assembly partners, and test houses. CMMC requirements flow down to subcontractors based on the information they handle — regardless of their size or contract tier.
06	**No formal cybersecurity program** The most common reason manufacturers fail CMMC assessments is not the absence of security tools — it is the absence of the SSP, POA&M, documented policies, and incident response procedures that assessors require as evidence. Tools without governance fail audits.

PROOF POINT

89% of defense contractors have already suffered financial, reputational, or operational losses from a cyber incident. Most had security tools in place. The gap is governance — not technology.



03 — THE COMPLIANCE STACK

What 110 controls actually demand

Roughly half of CMMC Level 2 controls require documented policies, governance processes, and audit evidence — not just technology. The SSP and POA&M are the foundation of every successful assessment.

HOW TO DEFINE YOUR CUI ENCLAVE — AND REDUCE COST

Not every system needs to meet Level 2 requirements — only those that store, process, or transmit CUI. A well-defined CUI enclave can significantly reduce the number of systems in scope, the complexity of remediation, and the total cost of compliance.

> A defined CUI enclave covering only the systems that touch controlled data can **reduce compliance scope and cost substantially**. Getting the scope definition right before remediation begins is one of the highest-leverage decisions in any CMMC engagement.

A systematic data flow analysis identifies where CUI enters, moves, rests, and who accesses it — most manufacturers significantly over- or underestimate scope on the first pass.

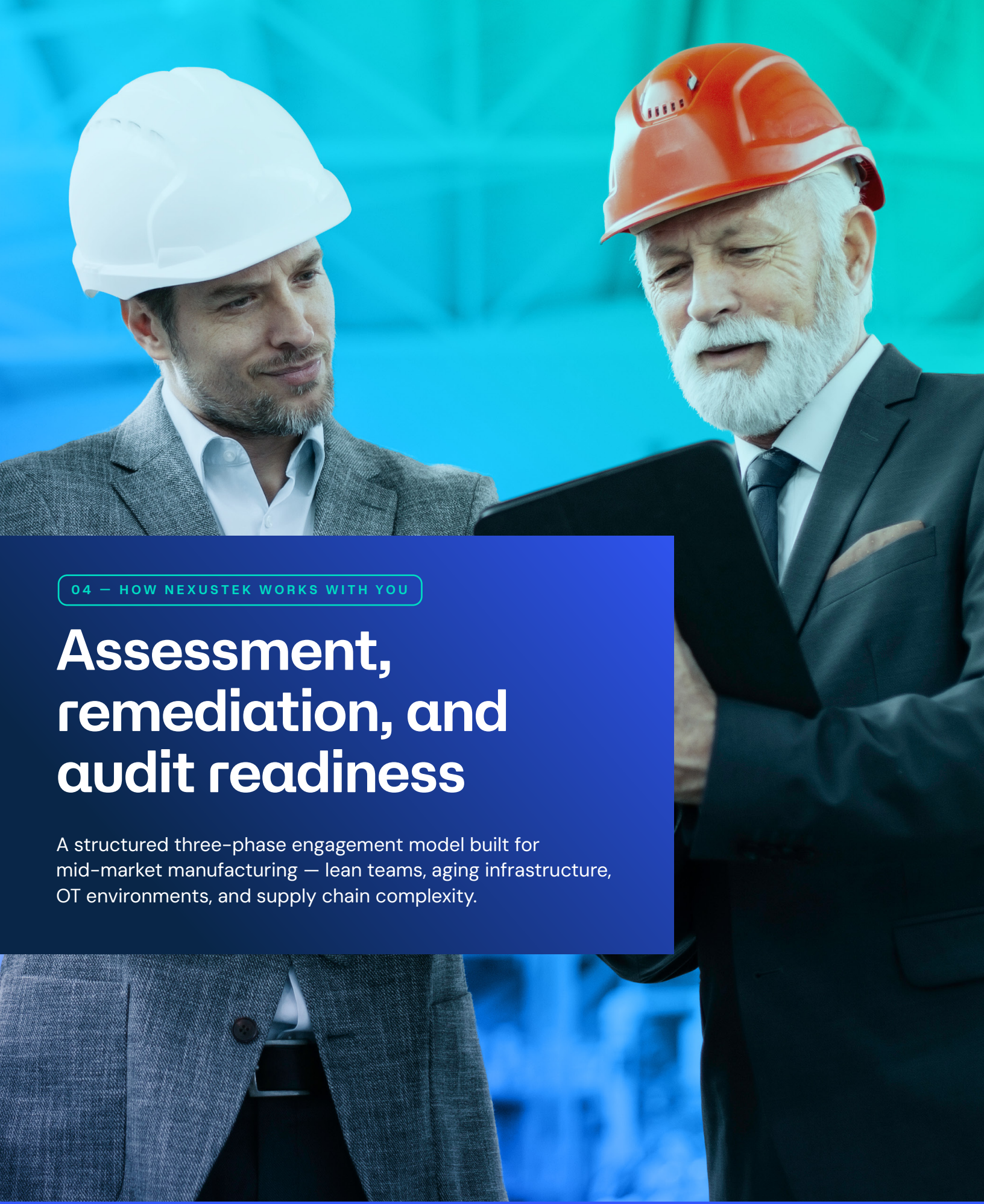
VDI and session isolation remove high-risk shop-floor endpoints from full Level 2 scope by displaying CUI through a controlled session rather than storing it locally.

Subcontractors receiving technical data packages from primes carry CUI obligations regardless of whether the data is labeled — and the systems handling it are in scope.

The four highest-risk exposure areas

SERVICE	CMMC DOMAIN(S)	WHAT IT DELIVERS
CMMC 2.0 Compliance Services ALL DOMAINS	All 14 Domains	Gap assessment, remediation, SSP/POA&M documentation, C3PAO audit preparation. The core engagement.
vCISO Services GOVERNANCE	Risk Assessment; All Domains	Owns the SSP and POA&M. Builds the formal program structure assessors require. Sustains compliance between cycles.
MDR + 24/7 SOC CYBERSECURITY	Incident Response; Audit + Accountability	Continuous monitoring with documented incident response. Satisfies both operational and evidentiary audit requirements.
IAM + MFA CLOUD	Access Control; Identification + Authentication	Least-privilege access to CUI systems. Mandatory for all accounts at Level 2. Produces the access logs assessors review.
EDR CYBERSECURITY	System + Comms. Protection; Incident Response	Endpoint protection for CUI-touching systems including production floor PCs and engineering workstations.
AI Email Security CYBERSECURITY	System + Communications Protection	Filters and monitors email — the primary channel for engineering drawings moving to suppliers.
Managed IT / Co-Managed IT IT OPS	Configuration Management; All Domains	Patching, monitoring, help desk, and lifecycle management. The proactive posture CMMC requires.

The SSP and POA&M are the most critical compliance documents. The System Security Plan describes how each of the 110 controls is implemented. The Plan of Action and Milestones documents how gaps are being remediated. Without these, there is nothing for a C3PAO assessor to evaluate — regardless of what technology you have deployed.



04 — HOW NEXUSTEK WORKS WITH YOU

Assessment, remediation, and audit readiness

A structured three-phase engagement model built for mid-market manufacturing — lean teams, aging infrastructure, OT environments, and supply chain complexity.

The engagement model

Each phase builds on the previous one, creating a documented, defensible compliance posture that holds up under C3PAO scrutiny — not as a one-time sprint, but as a sustainable managed program.

PHASE 01 — READINESS

CMMC Readiness Assessment

Gap analysis across all 110 NIST SP 800-171 controls

SPRS score baseline established

CUI scoping — IT, OT, cloud, and vendor environments

Prioritized remediation roadmap delivered

PHASE 02 — REMEDIATION

Implementation + Documentation

Technical control deployment: EDR, IAM, MFA, MDR, email security

SSP and POA&M built to C3PAO evidentiary standards

Policy development and employee security training

PHASE 03 — CERTIFICATION

Audit Readiness Support

C3PAO pre-assessment preparation and walkthrough

Evidence package assembly and validation

Ongoing vCISO governance between cycles

SUSTAINING COMPLIANCE

CMMC Level 2 certification is not a one-time event. Annual self-assessment, SSP maintenance, POA&M management, and mandatory incident reporting are ongoing obligations. Manufacturers who treat compliance as a project — rather than a managed program — consistently fail their second assessment cycle.

CLIENT RESULTS

PROVEN IN MANUFACTURING ENVIRONMENTS

NexusTek has delivered managed IT and cybersecurity outcomes for manufacturers with distributed operations, lean IT teams, and complex infrastructure environments.

WHAT THESE ENGAGEMENTS ILLUSTRATE

- Structured assessment-first approach before any remediation begins
- Infrastructure modernization and security program build in parallel
- Ongoing managed support that sustains the posture after go-live
- The same capabilities that underpin a CMMC 2.0 readiness engagement

INDUSTRIAL TANK MANUFACTURER

- 100+ employee U.S. manufacturer, multi-state operations, strained MSP relationship, and outdated infrastructure
- NexusTek delivered: clean MSP transition, M365 deployment, endpoint and email security, disaster recovery, and new warehouse infrastructure
- Moved from reactive to proactive IT management. Replaced EOL servers, switches, and firewalls across multiple locations
- Established 24/7 help desk and proactive monitoring — the operational foundation a CMMC program requires

CONSUMER GOODS MANUFACTURER

- 350+ employees, two data breaches — security tools deployed but no formal program, policies, or employee training
- NexusTek delivered: vCISO-led NIST CSF assessment, gap analysis across people, process, and technology, formal cybersecurity program, MFA, access controls, and employee training
- Identified and remediated core vulnerabilities. Formalized policies and procedures. Reduced overall risk exposure
- Established ongoing security governance — the vCISO-led model that directly maps to CMMC compliance sustainment

WHY NEXUSTEK

FULL COMPLIANCE STACK — ONE PARTNER

EDR, IAM, MFA, MDR, email security, and vCISO under one accountable partner. No vendor coordination. No gaps.

BUILT AHEAD OF THE MANDATE

NexusTek built its CMMC 2.0 readiness practice in 2025, before the January 2026 DoD rollout. Manufacturers get a team that has already done this at scale.

20+ YEARS NIST AND CYBERSECURITY DELIVERY

NIST 800-53 and SOC2 heritage. CMMC Level 2 is an extension of an established delivery model — not a capability built for a deadline.

30 yr
IT services experience including NIST 800-53 and SOC2

1,200+
Active clients across the US

98%
Client satisfaction rating

CRN MSP500
10 consecutive years recognized

Start with a CMMC Readiness Assessment

In 30 minutes, NexusTek maps your environment against all 110 NIST SP 800-171 controls, establishes your SPRS score baseline, and delivers a prioritized remediation roadmap — before your prime contractor or DoD assessor asks for it.

NexusTek is not a C3PAO. We prepare manufacturers to pass the assessment.

VISIT NEXUSTEK.COM TO SCHEDULE AN ASSESSMENT

Protect Your Contracts. Achieve CMMC 2.0.
nexustek.com · (877) 470-0401 · info@nexustek.com

nexustek