

A STRATEGIC GUIDE FOR GERMAN AND EUROPEAN DEFENSE
COMPANIES AND SUPPLIERS

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC 2.0)



Photo: Getty Images

AUTHORS:
ANDREJ GREINDL, NIKOLAI KÖNIG, MORITZ REINDL

CONTENT

1	EXECUTIVE SUMMARY	03
2	WHY CMMC IS SUDDENLY BECOMING RELEVANT FOR EUROPEAN COMPANIES	04
3	THE TRANSFORMATION OF GLOBAL DEFENSE SUPPLY CHAINS	05
4	WHAT CMMC 2.0 SPECIFICALLY REQUIRES	07
5	IMPACT ON GERMAN AND EUROPEAN SUPPLIERS	09
6	INTERPLAY WITH NIS2, CRA, ISO 27001, TISAX, AND BSI IT-GRUNDSCHUTZ	09
7	HOW COMPANIES CAN ASSESS THEIR READINESS	11
8	RECOMMENDATIONS FOR ACTION FOR THE NEXT 12–24 MONTHS	13
9	CONCLUSION AND STRATEGIC OUTLOOK	14
10	HOW PROTIVITI SUPPORTS YOU	14
11	SOURCES	15
12	ABOUT PROTIVITI	15

LIST OF FIGURES

FIGURE 1	Industries in Germany Most Affected by CMMC	03
FIGURE 2	CMMC 2.0 Rollout Across Four Phases. Illustrative Timeline Based on the DFARS Rule. Inclusion in Individual Solicitations Remains at the Discretion of the Respective DoD Contracting Authority.	04
FIGURE 3	Market Environment 2026: CMMC in the Context of Rising Defense Investments	05
FIGURE 4	CMMC 2.0 Three-Level Model. Level 2 Is the Relevant Tier for the Vast Majority of Suppliers.	06
FIGURE 5	Through Contractual Flow-Down, CMMC Requirements Reach Every Tier of the Supply Chain Processing FCI or CUI, Even Without a Direct DoD Contract.	08
FIGURE 6	Typical CMMC Exposure of German Mid-Sized Companies: Three Practical Examples	08
FIGURE 7	Reusability Heat Map: Where Existing Standards Cover CMMC Requirements (green), Where Adaptation Is Needed (yellow), and where the U.S.-Specific Gap Remains (red).	09
FIGURE 8	Illustrative Distribution of Implementation Effort: Reusable Elements from Existing Standards and the Remaining U.S.-Specific Delta (Experience-Based Estimate).	10
FIGURE 9	A Unified Control Framework for Three Regulatory Requirements (CMMC, NIS2, and CRA)	10
FIGURE 10	The SPRS Score as Evidence of Cybersecurity Maturity in the CMMC Environment	11
FIGURE 11	Assessing CMMC Readiness of Mid-Sized Companies Across Five Core Dimensions	12
FIGURE 12	24-Month Roadmap in Four Waves. “No-Regret First”: Prioritizing Measures That Create Value for NIS2 and Remain Beneficial Regardless of the final CMMC Level.	13

1. EXECUTIVE SUMMARY

The Cybersecurity Maturity Model Certification (CMMC) has developed relevance far beyond the borders of the United States. With the entry into force of the procurement rule in the Defense Federal Acquisition Regulation Supplement (DFARS) on November 10, 2025, CMMC is gradually being incorporated into every new contract of the U.S. Department of Defense (Department of Defense, DoD) – and, via transatlantic supply chains, OEM requirements, and joint ventures, into the order books of European suppliers, many of whom do not currently hold a direct DoD contract.

For German and European companies, this brings about three simultaneous shifts: Cybersecurity is evolving from an IT task into a contractual pre-requisite for market access. The burden of proof is shifting from self-declaration to verifiable certification by accredited third parties; and the time-frame is shrinking, as prime contractors are already passing the requirement down the supply chain through contracts.

Key message: CMMC will affect European companies sooner than many currently assume. Those who conduct a thorough assessment of their current status now and strategically leverage existing ISO 27001, TISAX, or IT-Grundschutz frameworks for

CMMC will secure access to one of the world's largest procurement markets – and turn a regulatory obligation into a robust competitive advantage.

Update (July 2026): On July 13, 2026, the U.S. DoD suspended the rollout of CMMC Phase II and opened a 60-day CMMC Reform Task Force review of the certification model. Phase I self-assessment obligations, NIST SP 800-171 implementation, DFARS 252.204-7012 safeguarding duties, and SPRS reporting remain fully in force. This is best read as a pause of the third-party certification mechanism, not a relaxation of the underlying cybersecurity requirements – the analysis and roadmap below remain valid, and early preparation remains the more cost-effective path. See Sections 2 and 9 for details.

This white paper provides a fact-based overview of the current legal landscape (as of June 2026), translates the CMMC 2.0 requirements into management decisions, compares CMMC in a structured manner with NIS2, CRA, ISO 27001, TISAX, and BSI IT-Grundschutz, and outlines a concrete roadmap for the next 12 to 24 months. The five key take-aways at a glance:

1. The trigger is real and has a specific date. A three-year, four-phase rollout has been underway since November 10, 2025. Once full implemen-

CMMC 2.0 · AFFECTED INDUSTRIES

Seven industries, one requirement

The German sectors most exposed to CMMC – wherever FCI or CUI is processed for a US/DoD program

01

Mechanical Engineering

Mechanical parts, gears, motors and housings for military vehicles and weapons systems.

02

Automotive & Suppliers

Dual-use parts – chassis, wiring harnesses, engines – that also serve military platforms.

03

Electrical Engineering

Sensors, cameras, radio tech, power supplies and circuit boards for defense electronics.

04

Aerospace

Structural parts, avionics and propulsion for aircraft, helicopters, drones and satellites.

05

Semiconductors & Optics

Semiconductor chips, sensors and precision optics, enabling weapons, guidance and surveillance systems.

06

Software & IT Services

Software for military systems and cloud/data services for defense primes.

07

Engineering & Design Services

Design offices developing weapons systems, ammunition and military vehicles.



THE COMMON THREAD

Most are dual-use: civilian parts & know-how that also serve US/DoD programs – pulling FCI/CUI, and CMMC, into scope.

Figure 1 – Industries in Germany Most Affected by CMMC

tation takes effect (originally expected by the end of 2028), no new DoD contracts can be awarded without the appropriate CMMC level.

2. The impact is indirect but widespread. Not only direct DoD contractors but also subcontractors and sub-subcontractors at all levels are affected as soon as they handle FCI or CUI.
3. Proving compliance will become more difficult. CMMC replaces simple self-certification for sensitive data with certification by accredited assessment organizations (C3PAO) or a government-led audit (DIBCAC).
4. Existing compliance is a head start, not a free pass. ISO 27001, TISAX, or IT-Grundschutz cover a certain portion of the organizational requirements, but the remaining gap is specific to the U.S. and complex.
5. Early preparation is more cost-effective than last-minute scrambling. Those who take advantage of the 12- to 24-month lead time can avoid bidding freezes, bottlenecks due to limited audit capacity, and overpriced emergency projects. While the future shape and timeline of CMMC continue to evolve, the underlying cybersecurity risks and security expectations remain unchanged. Organizations that use this period to strengthen their cybersecurity posture, governance processes, and NIST SP 800-171 compliance can gain a significant competitive advantage and be better positioned when certification requirements are ultimately enforced.

2. WHY CMMC IS SUDDENLY BECOMING RELEVANT FOR EUROPEAN COMPANIES

For years, European suppliers were able to treat CMMC as an internal U.S. initiative whose deadlines were bound to be postponed anyway. This interpretation will be obsolete as of the end of 2025. Two sets of regulations now overlap and misinterpreting them is a common mistake in the market.

Two sets of regulations, one program – and the date that matters

The regulations in [32 CFR Part 170](#) (effective December 16, 2024) establish the CMMC program itself: the tiered structure, the evaluation criteria, and the audit ecosystem comprising the accreditation body, C3PAOs, and auditors. [48 CFR/DFARS](#) (published on September 10, 2025, effective November 10, 2025) is the lever that really makes a difference: The regulations introduce two interlocking contract clauses: 252.204-7025 requires proof of a specific CMMC tier already in the solicitation, and 252.204-7021 subsequently makes compliance with that tier a continuing obligation throughout the entire contract term. This makes a valid CMMC tier a contractual prerequisite for award.

CMMC 2.0 · DFARS ROLLOUT

The clock has been ticking since November 2025

Four-phase rollout over three years – the preparation window is open now

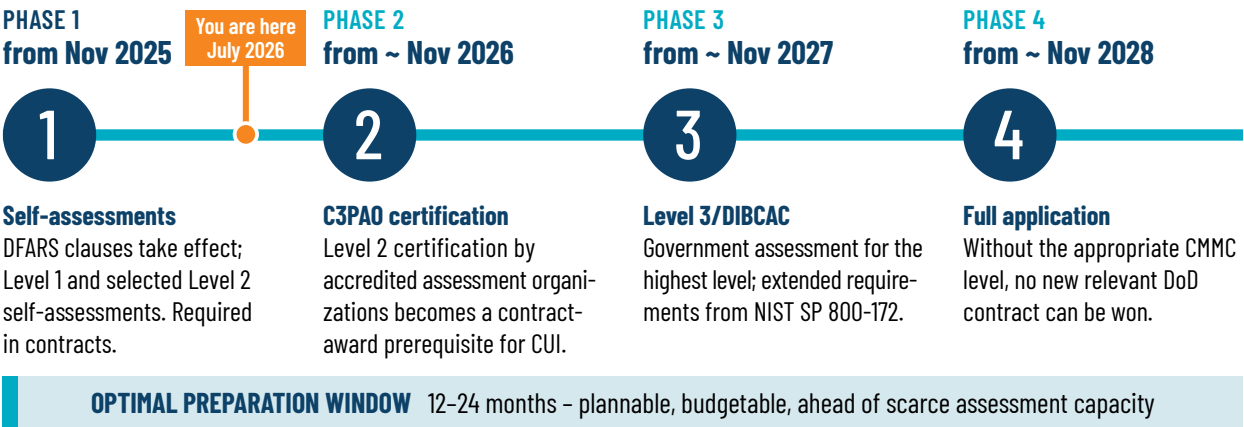


Figure 2 – CMMC 2.0 Rollout Across Four Phases. Illustrative Timeline Based on the DFARS Rule. Inclusion in Individual Solicitations Remains at the Discretion of the Respective DoD Contracting Authority.

The phased rollout – the clock has been ticking since November 2025

The DoD is not implementing the requirement overnight but is phasing it in over four stages. This phased approach is not a reason to wait; rather, it precisely defines the timeframe within which preparation is both possible and efficient: Phase 1 starting in November 2025 (self-assessments), Phase 2 starting around November 2026 (C3PAO certification for Level 2), Phase 3 starting around November 2027 (Level 3/DIBCAC), Phase 4 starting around November 2028 (full implementation in all relevant contracts). On July 13, 2026, the DoD suspended the rollout of Phases 2 through 4 and launched a 60-day CMMC Reform Task Force review, informed by a public Request for Information with industry comments due August 14, 2026; the Task Force's recommendations are expected around mid-September 2026. Phase 1 remains fully in force, and the dates above should for now be read as the original plan rather than a confirmed schedule.

From management's perspective, three questions can no longer be put off:

- **Why should I care about this today?** Because prime contractors pass on the requirement contractually before they themselves are required to be certified. The requirements reach suppliers **before the regulatory deadline**.

- **What risks arise from inaction?** Loss of prequalification with OEM customers, exclusion from bids, bottlenecks due to limited testing capacity, and – in the worst case – **being quietly replaced by an already certified competitor**.

- **What opportunities arise from early preparation?** A certifiable security status becomes a **selling point**: It signals reliability to OEMs, shortens supplier audits, and opens up programs that remain closed to competitors.

3. THE TRANSFORMATION OF GLOBAL DEFENSE SUPPLY CHAINS

CMMC is entering a defense market undergoing historic upheaval. The economic significance of this issue can only be understood against the backdrop of three parallel developments: a growing volume of U.S. procurement, an unprecedented European rearmament drive, and the increasing interdependence of both markets.

The U.S. Market: volume and procurement power

U.S. national defense spending will reach approximately **\$1.04 trillion** in **fiscal** year 2026 comprising about \$893 billion in regular Pentagon funding and

DEFENSE MARKETS · MARKET CONTEXT 2026

CMMC in numbers

A market in historic transformation – on both sides of the Atlantic

USA · PROCUREMENT POWER

1.04 trillion USD

US defense spending FY2026 – the largest single customer worldwide

220,000+

Companies in the Defense Industrial Base

~80,000

of which, per DoD estimates, must meet **Level 2** requirements

EUROPE · REARMAMENT

5 % of GDP

NATO target by 2035 (The Hague, June 2025) – 3.5 % core + 1.5 % resilience

82.69 billion €

German defense budget 2026 (Section 14)

800 billion €

EU ReArm Europe/Readiness 2030 incl. SAFE loan instrument (150 billion €)

Figure 3 – Market Environment 2026: CMMC in the Context of Rising Defense Investments

approximately \$152 billion from an additional budgetary process. A significant portion of these flows into the industrial base in the form of contract volume. The DoD is thus the largest single customer for defense goods worldwide and, through CMMC, defines the entry requirements for this market. The Defense Industrial Base comprises over 220,000 companies. According to DoD estimates, about 80,000 of these must meet Level 2 requirements. The real bottleneck, however, lies not in the requirements themselves, but in the limited testing capacity of the still-nascent C3PAO landscape.

Europe is ramping up its defense capabilities – and creating new supply chains

At the same time, the European market is changing faster than at any time since the Cold War:

- **NATO – The Hague 2025:** In June 2025, member states committed to spending 5% of GDP on defense and defense-related resilience by 2035 (3.5% for core military spending + 1.5% for defense-related spending).
- **Germany:** The 2026 federal budget totals €524.5 billion, of which €82.69 billion is allocated to the defense budget. A 2025 amendment to the Basic Law exempts defense spending exceeding 1% of GDP from the debt brake.

- **EU – ReArm Europe/Readiness 2030:** The package presented in March 2025 is intended to mobilize up to €800 billion. The SAFE loan facility (€150 billion) promotes joint procurement under a “Spend European” principle (max. 35% of component value from outside the EU/EEA/Ukraine).

“Spend European” – and why it does not undermine CMMC

At first glance, the “Spend European” principle appears to be a shift away from U.S. supply chains. In reality, however, transatlantic interdependence remains high: Key platforms such as the F-35, Patriot, and HIMARS remain U.S. systems that incorporate European components, and European programs utilize U.S. technology. Anyone who wants to supply both markets will need to comply with both sets of regulations in the future – **CMMC for the U.S. side, and NIS2 and CRA for the EU side.**

From “trusted supplier” to certified supplier

The real structural change is cultural: trust is becoming verifiable. Whereas OEMs used to rely on long-standing business relationships and self-reported information from their suppliers, the new regime requires verifiable evidence. For European small and medium-sized enterprises, this sends a

CMMC 2.0 · LEVEL MODEL

Three levels – the data question decides

It is not company size that determines the level, but the data processed

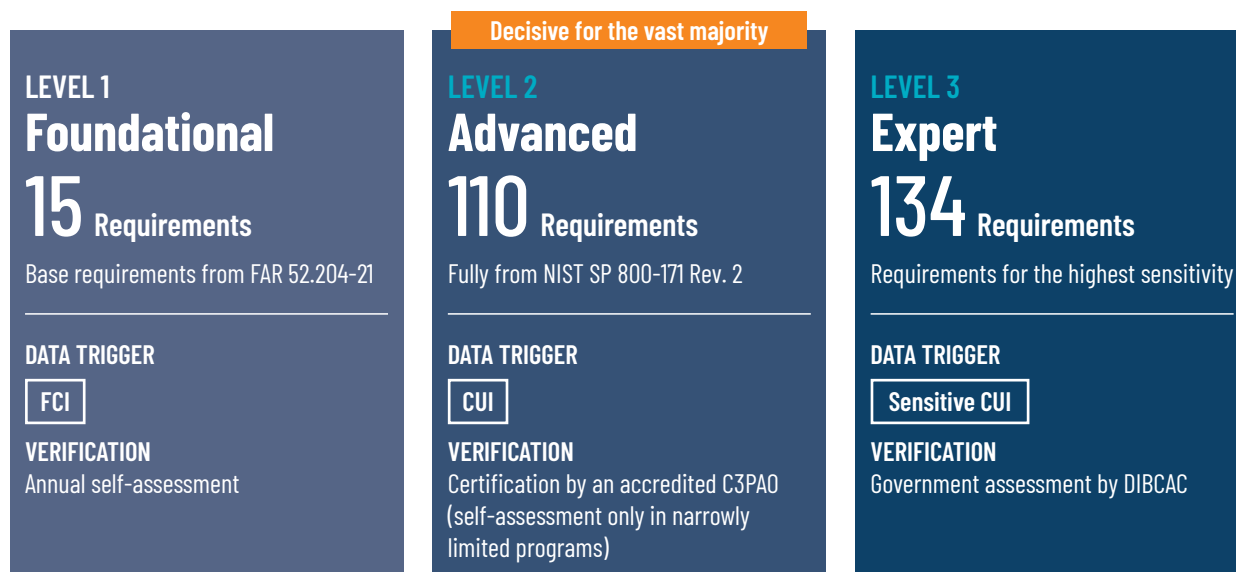


Figure 4 – CMMC 2.0 Three-Level Model. Level 2 Is the Relevant Tier for the Vast Majority of Suppliers.

twofold message: the barrier to entry is rising, but those who clear it will measurably set themselves apart from the competition.

4. WHAT CMMC 2.0 SPECIFICALLY REQUIRES

CMMC 2.0 has streamlined the original five-tier model from 2019 down to three tiers. The logic is simple: the more sensitive the data being processed, the stricter the requirements and the more independent the verification must be.

FCI and CUI – the all-important data question

Which CMMC level a company needs does not depend on its size, but on the data it processes on behalf of the client. Federal Contract Information (FCI) refers to non-public contract information, while Controlled Unclassified Information (CUI) refers to information worthy of protection but not classified, such as technical drawings, specifications, or manufacturing data. The classification is determined by the contracting authority or prime contractor; therefore, the first practical task for every supplier is to identify where FCI or CUI is actually located within its systems.

An overview of the three levels

Level 1 (Foundational) requires 15 basic requirements from the standard contract clause for U.S. federal contractors (FAR 52.204-21) and an annual self-assessment. Level 2 (Advanced) comprises 110 requirements from NIST SP 800-171 Rev. 2 and is typically certified by a C3PAO. Level 3 (Expert) comprises the Level 2 requirements supplemented by a subset of advanced requirements from NIST SP 800-172 and is audited by the government agency DIBCAC.

Three common misconceptions persist and should be clarified in advance:

- “Level 2 always allows for self-assessment.” False – Self-assessment is permitted only for very limited programs; for CUI, C3PAO certification is the norm.
- “NIST 800-171 Rev. 3 is now in effect.” False – CMMC remains bound by Rev. 2; although Rev. 3 is final, it is not yet authoritative due to a DoD Class Deviation.

- “A POA&M is sufficient in the long term.” Incorrect – it only allows for conditional certification; open items must be resolved within 180 days. Critical requirements are not eligible for POA&M.

The 14 control areas of Level 2

Level 2 is based entirely on the 14 control areas of NIST SP 800-171 Rev. 2: Access Control (AC), Awareness & Training (AT), Audit & Accountability (AU), Configuration Management (CM), Identification & Authentication (IA), Incident Response (IR), Maintenance (MA), Media Protection (MP), Personnel Security (PS), Physical Protection (PE), Risk Assessment (RA), Security Assessment (CA), System & Communications Protection (SC), and System & Information Integrity (SI). Crucial for management: These areas are not purely technical. Personnel Security and Awareness & Training, for example, require organizational measures, processes, and training.

The five technical focus areas requiring the most effort

- **Multi-factor authentication (MFA)** for all access to CUI systems – often requiring retrofitting in legacy ERP and CAD environments.
- **Network segmentation** to separate CUI-processing systems from production and office networks – often the most invasive measure.
- **Encryption using FIPS-validated methods** for CUI during transmission and storage; not all existing encryption methods meet FIPS requirements.
- **Logging & monitoring (SIEM)** with centralized, analyzable storage – not yet centralized at many medium-sized companies.
- **Vulnerability management & penetration testing** with established scanning, patching, and testing routines and traceable deadlines.

The special case of the cloud, which is often overlooked

Anyone processing CUI in Microsoft 365, Azure, AWS, or Google Cloud must use a FedRAMP Moderate-equivalent environment – in practice, the government “GovCloud”/“GCC High” variants. Changing the tenant environment is complex, time-consuming, and should be planned well in advance. Retrospective migrations are among the most expensive CMMC surprises. The equivalent of FedRAMP in Germany is the BSI C5 standard. Both are recognized as security standards for cloud providers designed to protect sensitive data.

CMMC 2.0 · CONTRACTUAL FLOW-DOWN

CMMC reaches every tier of the supply chain

Even without a direct DoD contract – as soon as FCI or CUI is processed



Figure 5 – Through Contractual Flow-Down, CMMC Requirements Reach Every Tier of the Supply Chain Processing FCI or CUI, Even Without a Direct DoD Contract.

CMMC 2.0 · IN PRACTICE

Three typical scenarios

How the requirement reaches German mid-sized companies – and how they respond

CASE A

The sensor manufacturer

SME · ~80 employees · ISO 27001 in place

TRIGGER

Supplies an EU integrator with a US prime. The prime classifies the specification and tolerance data as CUI and requires Level 2 within 18 months.

RISK

The integrator has already evaluated a certified alternative supplier and reserves the right to switch on short notice.

SOLUTION

CUI scoping into a separated enclave; MFA, centralized logging, FIPS crypto; reuse of ~65% of the ISO controls.

BENEFIT

Certification readiness as a sales argument and secured program participation, plus solid evidence for customers.

CASE B

The systems integrator

Large enterprise · de facto prime role

TRIGGER

Integrates a system for a NATO country with US components and re-export to a US unit. Must meet Level 2/3 itself and manage the supply chain.

RISK

A single non-compliant subcontractor system and significantly delays the ongoing NATO solicitation.

SOLUTION

Company-wide CUI data-flow mapping; supplier compliance program with a contract clause; C3PAO readiness over 24–30 months.

BENEFIT

Robust supply-chain governance as a differentiator in NATO solicitations and a clear competitive advantage in award procedures.

CASE C

The embedded-software provider

Boutique · ~40 employees

TRIGGER

Licenses embedded software to a US integrator for a defense program; parts of development and maintenance are performed offshore.

RISK

If the source code is CUI, Level 2 applies – including external developers and build/repository infrastructure. The offshore access points are critical.

SOLUTION

Securing the development chain (DevSecOps, access segregation, code signing); if needed, relocating CUI-relevant work into a controlled enclave.

BENEFIT

Access to security-critical US software programs that favor certified providers, ideal for long-term customer retention.

Figure 6 – Typical CMMC Exposure of German Mid-Sized Companies: Three Practical Examples

5. IMPACT ON GERMAN AND EUROPEAN SUPPLIERS

The key question is rarely “Do we have to comply with CMMC?” but rather “How will this requirement affect us and when?” Even without a direct DoD contract, CMMC can become contractually binding.

Five ways CMMC can affect a European company

- **OEM/Prime Flow-down:** A U.S. prime contractor contractually passes on CMMC obligations to all suppliers with access to CUI – regardless of their location.
- **International Joint Ventures:** In transatlantic consortia, the requirement applies to all partners who handle shared CUI.
- **NATO/FMS Programs:** Procurements through U.S. systems (Foreign Military Sales) bring U.S. requirements into the European supply chain.
- **M&A transactions:** A U.S. buyer or a target subject to certification makes CMMC readiness a component of due diligence and purchase price determination.

- **Future RFP:** Direct qualification for DoD contracts in niche areas where Europe leads in technology – sensor technology, optics, propulsion systems, and cyber hardware.

Three typical real-world scenarios

The following scenarios are anonymized, illustrative examples of typical situations in German SMEs – they depict patterns, not specific client cases:

6. INTERPLAY WITH NIS2, CRA, ISO 27001, TISAX, AND BSI IT-GRUNDSCHUTZ

The good news for European companies: CMMC isn’t being developed in a vacuum. Those who have already invested in European and international security standards start with a solid foundation. The bad news: Not a single one of these standards fully covers CMMC – the remaining gap is specific and must be documented.

CMMC 2.0 · FRAMEWORK COMPARISON

Where existing standards cover CMMC

Two topic areas remain red across all standards – the CMMC-specific delta

Standard ↑ / Area →	Selected example areas					Covered by no EU standard on its own	
	Governance & Risk	Access & Cryptography	Incident Response	Supply chain	Secure Development	CUI handling	Verification & third-party audit
NIS2 EU Directive	High	Partial	High	High	Partial	Gap	Gap
CRA EU Regulation (products)	Partial	Partial	Partial	High	High	Gap	Gap
ISO 27001 International, certifiable	High	High	High	Partial	Partial	Gap	Gap
TISAX Automotive/VDA ISA	High	High	High	High	Partial	Gap	Gap
BSI IT-Grundschutz German methodology	High	High	High	Partial	Partial	Gap	Gap

■ High – largely covered
 ■ Partial – adaptation needed
 ■ Gap – CMMC-specific

Figure 7 – Reusability Heat Map: Where Existing Standards Cover CMMC Requirements (green), Where Adaptation Is Needed (yellow), and where the U.S.–Specific Gap Remains (red).

CMMC 2.0 · IMPLEMENTATION EFFORT

Two-thirds are already built

The decisive additional effort is the CMMC-specific delta

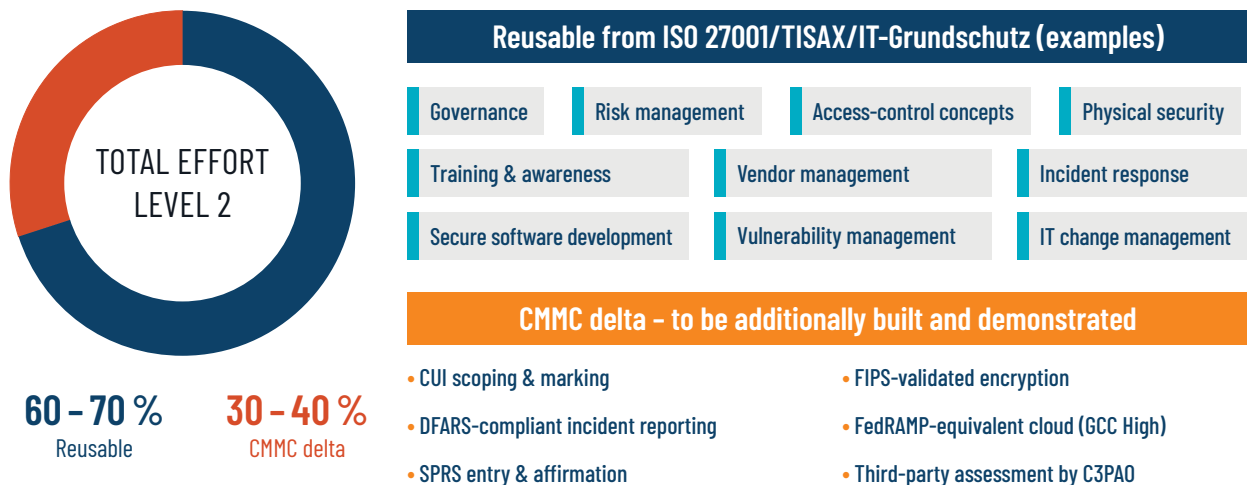


Figure 8 – Illustrative Distribution of Implementation Effort: Reusable Elements from Existing Standards and the Remaining U.S.-Specific Delta (Experience-Based Estimate).

COMBINED COMPLIANCE · STRATEGIC LEVER

Three obligations, one foundation

CMMC, NIS2, and CRA on a shared control framework

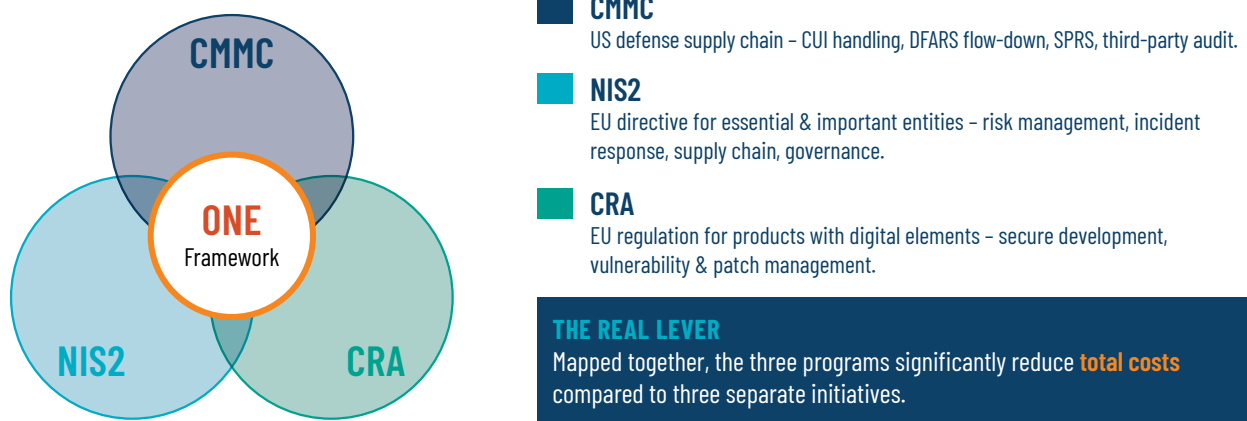


Figure 9 – A Unified Control Framework for Three Regulatory Requirements (CMMC, NIS2, and CRA)

The framework comparison at a glance

The heat map highlights the key pattern: Across all standards – the columns “CUI Handling” and “Verification (SPRS and Third-Party Audit)” are colored red. This is precisely where the U.S.-specific gap lies, one that no single European investment can bridge on its own:

- **NIS2** (EU Directive, mandatory for essential/critical facilities): high overlap in risk management, incident response, supply chain security, and governance. Gaps: CUI handling, DFARS flow-down, SPRS, FIPS cryptography, third-party auditing.

- **CRA** (EU Regulation on Products with Digital Elements): Overlap in secure development as well as vulnerability and patch management. Gap: Product- rather than organization-focused – no CUI/ISMS scope.
- **ISO 27001** (international, voluntary/certifiable): High coverage of process controls – ISMS, risk, access, cryptography, incident response. Gap: U.S.-specific requirements such as CUI marking, FIPS cryptography, SPRS affirmation, log retention, and FedRAMP-equivalent cloud.

- **TISAX** (Automotive, VDA ISA): Provides an ISMS foundation, supplier assurance, and prototype protection. Gap: Defense/CUI-specific requirements and U.S. regulations.
- **BSI IT-Grundschutz** (German methodology): provides a catalog of controls and a risk methodology closely aligned with ISO. Gap: identical to ISO – U.S.-specific requirements are missing.

The management perspective: what can be reused?

As a rule of thumb, approximately 60–70 % of the requirements from ISO 27001, TISAX, or IT-Grundschutz can be reused – governance, risk management, access policies, training, incident response processes, and physical security. The additional effort is the CMMC delta: CUI scoping and marking, FIPS-validated encryption, DFARS-compliant incident reporting, FedRAMP-equivalent cloud, SPRS registration with annual affirmation, and the third-party audit itself. The percentage is based on experience, not a certified mapping rate.

Combined Compliance Thesis: Companies that map NIS2, CRA, and CMMC in parallel to a common control framework significantly reduce the total cost of compliance compared to three separate programs. This integration – not individual certification – is the true strategic lever.

7. HOW COMPANIES CAN ASSESS THEIR READINESS

Before making any investment, companies must assess their current status. This answers two questions: What level do we really need – and how far are we from it?

The SPRS score – the currency of verification

For Level 2, companies assess their implementation of the 110 requirements and enter the result as a numerical value into the Supplier Performance Risk System (SPRS). The scale starts at 110 points; for each unmet requirement, 5, 3, or 1 point is deducted – depending on its weight – and the score can drop as low as –203. The SPRS score is thus the first cyber maturity metric visible to clients; a low score or a missing score is already a disqualification criterion in prequalification processes today.

» The SPRS score is the first customer-visible measure of cybersecurity maturity. A low or missing score can already disqualify a company today. «

CMMC 2.0 - VERIFICATION

The SPRS score – the currency of verification

The first cyber-maturity metric that customers can view

STARTING VALUE LEVEL 2

110

Points at full implementation

The 110 requirements from NIST SP 800-171 Rev. 2 are scored. The result is posted to the Supplier Performance Risk System.

Value range of the SPRS score



For each open requirement, points are deducted (depending on weight). The value can drop as low as –203.

-5

Critical requirement
highest weight

-3

Important requirement
medium weight

-1

Supporting requirement
low weight

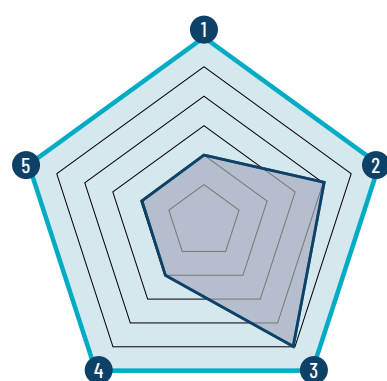
ALREADY RELEVANT TODAY A low or missing score is already a disqualifying criterion in pre-qualifications.

Figure 10 – The SPRS Score as Evidence of Cybersecurity Maturity in the CMMC Environment

CMMC 2.0 • READINESS MODEL

Five dimensions for assessing your position

Typical maturity level in mid-sized companies versus the CMMC target profile



Target profile (CMMC Level 2)
Typical current state, mid-sized companies

1	Data & scope Do we know where FCI/CUI resides and who accesses it?	low
2	Technical controls MFA, segmentation, FIPS crypto, SIEM – gaps particularly in crypto and logging.	medium
3	Processes & governance IT/InfoSec processes and structures established – especially at ISO/TISAX-certified companies	medium-high
4	Supply chain Are subcontractors and cloud providers CMMC-capable? Often the biggest blind spot.	low
5	Ability to provide evidence Is audit-proof documentation in place? Are the SPRS entry and the affirmation handled?	low

Figure 11 – Assessing CMMC Readiness of Mid-Sized Companies Across Five Core Dimensions

Five-dimensional readiness model

- **Data & Scope:** Do we know where FCI/CUI data is located and who has access to it? Maturity levels are generally low among small and medium-sized businesses – and are rarely assessed systematically.
- **Technical Controls:** Are MFA, segmentation, FIPS encryption, and SIEM in place? Maturity level is moderate – gaps exist primarily in encryption and logging.
- **Processes & Governance:** Are incident response, patching, and supplier processes documented and followed? Maturity level: medium to high, particularly among ISO/TISAX-certified companies.
- **Supply chain:** Are subcontractors and cloud providers CMMC-compliant? Maturity level is low – the biggest blind spot.

- **Auditability:** Are audit-proof processes, controls, and documentation in place, and are the SPRS entry and affirmation properly managed? Low maturity level – documentation is often incomplete.

Ten-point readiness check for management

1. We know which of our customers are DoD end users (directly or indirectly).
2. We have reviewed contractual CMMC/DFARS clauses in existing and new contracts.
3. We have identified FCI/CUI in our systems and documented their data flow.
4. We know the required CMMC level (1, 2, or 3) for each customer relationship.
5. We have determined a current SPRS score based on NIST 800-171 Rev. 2.
6. MFA, network segmentation, and FIPS encryption have been implemented for CUI systems.
7. We operate centralized logging and monitoring with defined retention policies.
8. Our CUI-relevant cloud is FedRAMP-equivalent (e.g., GCC High).
9. Our subcontractors with CUI/FCI access are contractually bound.
10. A person responsible for the annual affirmation has been designated.

» If the answer to any of these questions is 'No', the next logical step is a structured readiness or gap assessment before investing in individual remediation measures. «

8. RECOMMENDATIONS FOR ACTION FOR THE NEXT 12-24 MONTHS

The following roadmap translates the requirements into an economically justifiable sequence. The guiding principle is “No-Regret First”: Measures that add value regardless of the final CMMC level and also for NIS2 are prioritized. The July 2026 suspension of Phase 2 reinforces rather than undercuts this principle: DoD officials and industry advisors are urging contractors to keep executing self-assessment and NIST 800-171 measures throughout the review period, since these retain their value regardless of how the certification model ultimately evolves.

Roadmap in four phases

- **Wave 1 – Clarity (Months 0–3):** Contract and customer analysis, CUI/FCI scoping, target level per customer, initial SPRS assessment, business case.
- **Wave 2 – Foundation (Months 3–9):** “No-Regret” measures – MFA, logging/SIEM, segmentation plan, FIPS cryptography, awareness; mapping of existing controls (e.g., from ISO 27001 or TISAX).

- **Wave 3 – Depth & Supply Chain (Months 9–18):** Remaining controls, cloud migration (GCC High), supplier compliance program, evidence management, internal preliminary review.
- **Wave 4 – Verification (Months 18–24):** C3PAO readiness assessment, remediation of findings, formal assessment, SPRS entry, and affirmation.

The five most important “no-regret” measures

1. Conduct CUI/FCI scoping → without a scope, there can be no reliable estimate of costs and effort.
2. Roll out MFA across the board for sensitive access points → high security benefits, low relative costs.
3. Establish centralized logging/monitoring → required for both CMMC and NIS2.
4. Contractually bind suppliers with CUI access → address the biggest blind spot first.
5. Map existing ISO/TISAX/IT-Grundschutz controls to NIST 800-171 → Avoid duplication of effort.

Assess the effort realistically

The effort and costs of Level 2 certification vary greatly depending on scope, IT maturity, and supply chain complexity – reliable estimates range from **the mid-five- to high-six-figure euro amounts over two to three years**. What matters most is not

CMMC 2.0 · ACTION ROADMAP

24 months in four waves

“No-regret first” – measures that also add value for NIS2 are prioritized

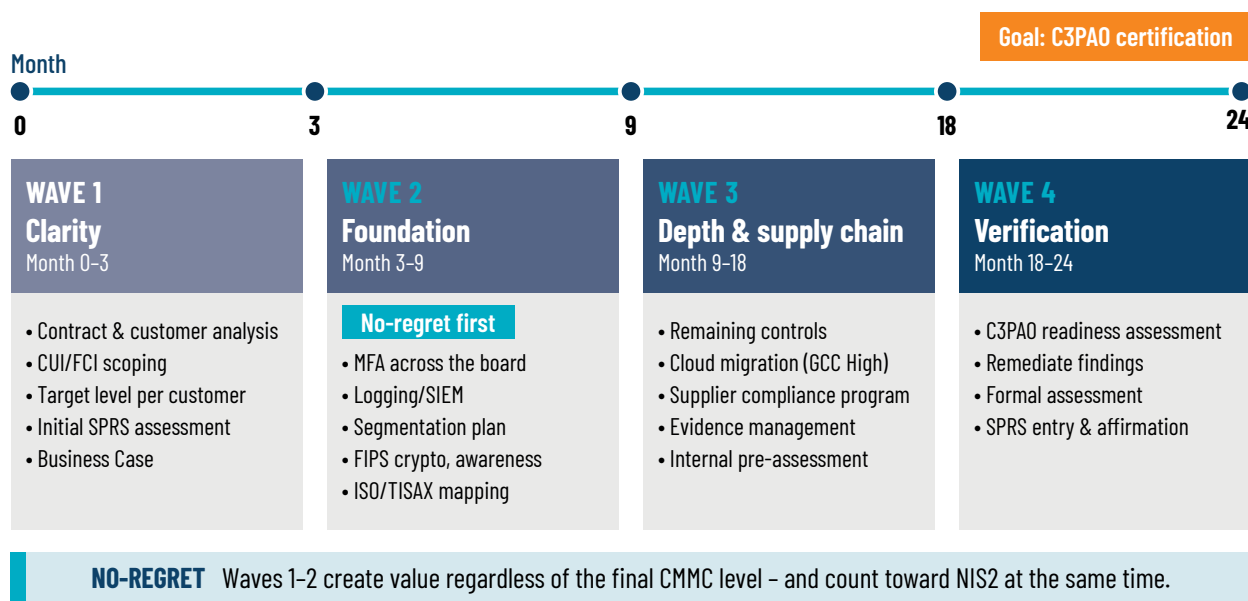


Figure 12 – 24-Month Roadmap in Four Waves. “No-Regret First”: Prioritizing Measures That Create Value for NIS2 and Remain Beneficial Regardless of the final CMMC Level.

so much the absolute figure as the timing. Preparation with a 12- to 24-month lead time can be planned and budgeted for, whereas an emergency project under the pressure of a tender deadline cannot – and also faces limited, and therefore expensive, audit capacity.

The five most expensive surprises – and how to avoid them

- **Cloud migration to a FedRAMP-equivalent environment:** CUI in standard Microsoft 365/Azure/AWS is not sufficient; government-grade variants such as GCC High are required → Decide and plan early.
- **FIPS-validated encryption:** Existing encryption often does not meet FIPS requirements; individual legacy systems must be replaced → Review your cryptographic infrastructure early on.
- **Offshore and external development access:** Unregulated third-party access to CUI can block certification → Isolate access or move it to an enclave.
- **Bottleneck in C3PAO audit capacity:** The number of accredited auditors is limited; under the pressure of competitive bidding, deadlines become tight and costly. Time readiness accordingly.
- **The subcontractor cascade:** A single non-compliant subcontractor with access to CUI jeopardizes the entire certification → Map the supply chain early and incorporate it into contracts.

9. CONCLUSION AND STRATEGIC OUTLOOK

CMMC is not a temporary U.S. regulatory issue, but rather an expression of lasting structural change: In a world of increasing geopolitical tensions, **proven cyber resilience** is becoming **a prerequisite for participation in defense supply chains** – on both sides of the Atlantic.

This presents German and European companies with a clear strategic choice. They can treat CMMC as an external burden and adopt a reactive, wait-and-see approach – at the risk of losing programs and customers – Or they recognize the standard for what it is intended to be: a seal of quality for reliability that sets them apart in a growing market and can be efficiently integrated with existing investments in NIS2, CRA, or best-practice standards (ISO 27001, TISAX, or IT-Grundschutz).

To summarize the key point once again: CMMC will affect European companies sooner than many assume. The DFARS regulation is in effect, demand is trickling down through the supply chain, and audit capacity is scarce. Those who assess their current status now and strategically expand their existing ISMS will secure **market access** and turn a requirement into a **competitive advantage**.

Here are four developments to watch in 2026/2027:

- **CMMC Reform Task Force (near-term):** The DoD suspended the Phase 2 rollout on July 13, 2026, and is reviewing the certification model, assessment methodology, and the burden on small and mid-sized suppliers. Recommendations are expected around mid-September 2026, following a public comment period open through August 14, 2026. The outcome will shape how and when C3PAO certification returns, not whether NIST 800-171-based protections apply.
- **NIST 800-171 Rev. 3:** A future incorporation into CMMC would change certain requirements – architectures should be designed to be adaptable.
- **European counter-movement:** With “Buy European” and a possible EU counterpart for verifiable supply chain cybersecurity, parallel compliance requirements could emerge – an integrated framework pays off twice over.
- **Supply chain consolidation:** Certification is becoming an M&A factor – mature providers are becoming more attractive targets and partners.

10. HOW PROTIVITI SUPPORTS YOU

Protiviti supports industrial and technology companies throughout the entire CMMC lifecycle – from the initial assessment to maintaining certification. The approach combines in-depth regulatory expertise with industry implementation experience and the strategic reuse of existing compliance investments:

- **Readiness & Gap Assessment** against NIST 800-171 Rev. 2, including SPRS scoring and a prioritized action roadmap.
- **CUI Scoping & Architecture** – Identification of FCI/CUI, enclave design, and cloud strategy (FedRAMP-equivalent).
- **Combined compliance programs** for the integrated implementation of CMMC, NIS2, CRA, ISO 27001, and TISAX on a common control framework.

- **Cybersecurity Governance** – Establishment of policies, roles, incident response, and vendor management.
- **M&A due diligence** to assess the CMMC maturity of targets as a value and risk factor in transactions.
- **Managed services** for monitoring, evidence maintenance, and annual affirmation.

11. SOURCES (SELECTION)

- U.S. Department of Defense – CMMC Program Resources; DFARS regulation, effective November 10, 2025 (clauses 252.204-7021 and 252.204-7025)
- NIST SP 800-171 Rev. 2/Rev. 3 and NIST SP 800-172; DoD Class Deviation 2023-00006.
- U.S. Defense Budget for FY2026 (NDAA and Reconciliation); publicly reported total amount of approximately 1.04 trillion USD.
- NATO – The Hague Summit, June 2025 (5% GDP target by 2035).
- Federal Budget 2026/Section 14; 2025 amendment to the Basic Law regarding the debt brake.
- European Commission – ReArm Europe/Readiness 2030 (March 2025) and SAFE Regulation (May 2025).
- U.S. Department of Defense – CIO memorandum and press statement, July 13, 2026, suspending CMMC Phase II implementation and establishing the CMMC Reform Task Force; associated Request for Information, “Reforming CMMC and Reducing Compliance Burden for the Defense Industrial Base” (comment period through August 14, 2026). Protiviti US – “CMMC Phase II Suspension: Facts vs. Fiction” (July 2026).

12. ABOUT PROTIVITI

Protiviti (www.protiviti.com) is a global consulting firm that helps companies transform and protect themselves. Through a network of more than 90 offices in over 25 countries, Protiviti and its independent member firms deliver in-depth expertise in technology, artificial intelligence, data, operations, finance, legal, compliance, risk, and internal audit.

In the context of CMMC, Protiviti supports suppliers to the defense and aerospace industries, as well as mid-sized manufacturing companies, throughout the entire lifecycle – from regulatory assessment to the design of controls and architecture, through to internal audit and audit readiness.

This white paper was prepared in July 2026 and reflects the status of CMMC 2.0 as set forth in the 32 CFR program rule (effective December 2024) and the 48 CFR/DFARS procurement rule (effective November 10, 2025). This revision additionally reflects the DoD’s July 13, 2026 suspension of the CMMC Phase II rollout and the resulting 60-day program review; the review’s outcome was not yet known at the time of this revision and should be verified against current DoD guidance. It is not a substitute for legal or certification advice in specific cases.

CONTACTS



ANDREJ GREINDL

Managing Director

+49 172 698 30 53

andrej.greindl@protiviti.com



NIKOLAI KÖNIG

Director

+49 172 698 3047

nikolai.koenig@protiviti.com

www.protiviti.de



© Protiviti GmbH