

EINE STRATEGISCHE ORIENTIERUNGSHILFE FÜR DEUTSCHE UND
EUROPÄISCHE VERTEIDIGUNGSUNTERNEHMEN UND -ZULIEFERER

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC 2.0)



Foto: Getty Images

AUTOREN:
ANDREJ GREINDL, NIKOLAI KÖNIG, MORITZ REINDL

INHALT

1	EXECUTIVE SUMMARY	03
2	WARUM CMMC FÜR EUROPÄISCHE UNTERNEHMEN PLÖTZLICH RELEVANT WIRD	04
3	DIE TRANSFORMATION DER GLOBALEN VERTEIDIGUNGSLieferketten	05
4	WAS CMMC 2.0 KONKRET FORDERT	06
5	AUSWIRKUNGEN AUF DEUTSCHE UND EUROPÄISCHE ZULIEFERER	07
6	ZUSAMMENSPIEL MIT NIS2, CRA, ISO 27001, TISAX UND BSI IT-GRUNDSCHUTZ	09
7	WIE UNTERNEHMEN IHRE READINESS BEWERTEN KÖNNEN	11
8	HANDLUNGSEMPFEHLUNGEN FÜR DIE NÄCHSTEN 12-24 MONATE	12
9	FAZIT UND STRATEGISCHER AUSBLICK	14
10	WIE PROTIVITI UNTERSTÜTZT	14
11	QUELLEN	14
12	ÜBER PROTIVITI	15

BILDERVERZEICHNIS

ABBILDUNG 1	Von CMMC maßgeblich betroffene Branchen in Deutschland	03
ABBILDUNG 2	CMMC-2.0-Rollout in vier Phasen. Richtwerte auf Basis der DFARS-Regel; die Aufnahme in einzelne Ausschreibungen liegt im Ermessen der jeweiligen DoD-Beschaffungsstelle.	04
ABBILDUNG 3	Marktumfeld 2026: CMMC im Kontext wachsender Verteidigungsinvestitionen	05
ABBILDUNG 4	CMMC-2.0-Stufenmodell. Level 2 ist für die große Mehrheit der Zulieferer die maßgebliche Stufe.	06
ABBILDUNG 5	Über den vertraglichen Flow-down erreicht die CMMC-Pflicht jede Stufe der Lieferkette, die FCI oder CUI verarbeitet – auch ohne direkten DoD-Vertrag.	08
ABBILDUNG 6	Typische CMMC-Betroffenheit deutscher Mittelständler: Drei Praxisbeispiele	08
ABBILDUNG 7	Wiederverwendungs-Heatmap: Wo bestehende Standards CMMC-Anforderungen abdecken (grün), wo Anpassung nötig ist (gelb) und wo die spezifisch US-amerikanische Lücke bleibt (rot).	09
ABBILDUNG 8	Grobe Aufteilung des Implementierungsaufwands: ein wiederverwendbarer Anteil aus vorhandenen Standards und ein US-spezifisches Delta (erfahrungsbasierte Schätzung).	10
ABBILDUNG 9	Ein Kontroll-Framework für drei regulatorische Anforderungen (CMMC, NIS2 und CRA)	10
ABBILDUNG 10	Der SPRS-Score als Nachweis der Cyber-Reife im CMMC-Umfeld	11
ABBILDUNG 11	Standortbestimmung der CMMC-Reife mittelständischer Unternehmen entlang fünf zentraler Dimensionen	12
ABBILDUNG 12	24-Monats-Roadmap in vier Wellen. „No-Regret zuerst“: Maßnahmen mit Wert auch für NIS2 und unabhängig von der finalen CMMC-Stufe werden vorgezogen.	13

1. EXECUTIVE SUMMARY

Die Cybersecurity Maturity Model Certification (CMMC) hat längst eine Relevanz über die Grenzen der USA hinaus entwickelt. Mit Inkrafttreten der Beschaffungsregel des Defense Federal Acquisition Regulation Supplement (DFARS) am 10. November 2025 wandert CMMC schrittweise in jeden neuen Vertrag des US-Verteidigungsministeriums (Department of Defense, DoD) – und über transatlantische Lieferketten, OEM-Anforderungen und Joint Ventures auch in die Auftragsbücher europäischer Zulieferer, die heute oft noch keinen direkten DoD-Vertrag halten.

Für deutsche und europäische Unternehmen verschieben sich damit drei Dinge zugleich: Cyber-sicherheit wird von einer IT-Aufgabe zu einer vertraglichen Marktzugangsvoraussetzung. Der Nachweis verlagert sich von der Selbstauskunft zur prüfbareren Zertifizierung durch akkreditierte Dritte; und der Zeithorizont schrumpft, weil Prime Contractors die Anforderung bereits heute vertraglich nach unten weiterreichen.

Kernbotschaft: CMMC betrifft europäische Unternehmen früher, als viele heute annehmen. Wer jetzt eine fundierte Standortbestimmung vornimmt und vorhandene ISO-27001-, TISAX- oder IT-Grundschutz-Strukturen gezielt für CMMC nutzbar

macht, sichert sich den Zugang zu einem der größten Beschaffungsmärkte der Welt – und macht aus einer regulatorischen Pflicht einen belastbaren Wettbewerbsvorteil.

Dieses Whitepaper liefert eine faktenbasierte Einordnung der aktuellen Rechtslage (Stand Juni 2026), übersetzt die CMMC-2.0-Anforderungen in Managemententscheidungen, vergleicht CMMC strukturiert mit NIS2, CRA, ISO 27001, TISAX und BSI IT-Grundschutz und skizziert einen konkreten Fahrplan für die nächsten 12 bis 24 Monate. Die fünf Kernaussagen auf einen Blick:

1. Der Auslöser ist real und datiert. Seit dem 10. November 2025 läuft ein dreijähriger, vierphasiger Rollout. Ab der vollständigen Anwendung (voraussichtlich Ende 2028) ist ohne passende CMMC-Stufe kein neuer DoD-Auftrag mehr zu gewinnen.
2. Die Betroffenheit ist indirekt, aber breit. Nicht nur direkte DoD-Vertragspartner, sondern Sub- und Sub-Sub-Lieferanten auf allen Stufen sind betroffen, sobald sie FCI oder CUI verarbeiten.
3. Der Nachweis wird härter. CMMC ersetzt die reine Selbstattestierung für sensible Daten durch eine Zertifizierung über akkreditierte Prüforga-nisationen (C3PAO) bzw. eine Regierungsprüfung (DIBCAC).

CMMC 2.0 · BETROFFENE INDUSTRIEN

Sieben Industrien, eine Anforderung

Die deutschen Sektoren, die am stärksten von CMMC betroffen sind

01

Maschinenbau

Mechanische Teile, Motoren und Gehäuse für Militärfahrzeuge und Waffensysteme.

02

Automobil & Zulieferer

Dual-Use-Teile – Fahrgestell, Kabelbäume, Motoren – die auch militärischen Plattformen dienen.

03

Elektrotechnik

Sensoren, Kameras, Funktechnik, Stromversorgungen und Leiterplatten für Verteidigungselektronik.

04

Luft- und Raumfahrt

Strukturelle Teile, Avionik und Antrieb für Flugzeuge, Hubschrauber, Drohnen und Satelliten.

05

Halbleiter & Optik

Halbleiterchips, Sensoren und Präzisionsoptik, die Waffen, Leit- und Überwachungssysteme ermöglichen.

06

IT-Dienstleistungen

Software für militärische Systeme und Cloud-/Datendienste für Verteidigungsprimen.

07

Ingenieurdienstleistungen

Designbüros, die Waffensysteme, Munition und militärische Fahrzeuge entwickeln.



DER ROTE FADEN

Dual-Use: zivile Teile und Know-how fließen in US/DoD-Programme – damit greifen FCI/CUI und CMMC.

Abbildung 1 – Von CMMC maßgeblich betroffene Branchen in Deutschland

4. Vorhandene Compliance ist ein Vorsprung, kein Freifahrtschein. ISO 27001, TISAX oder IT-Grundschutz decken einen gewissen Teil der organisatorischen Anforderungen ab – die verbleibende Lücke ist jedoch spezifisch US-amerikanisch und komplex.
5. Frühe Vorbereitung ist günstiger als später Aktionismus. Wer den 12- bis 24-Monats-Vorlauf nutzt, vermeidet Ausschreibungssperren, Engpässe bei knappen Prüfkapazitäten und überbeuerte Notfallprojekte.

2. WARUM CMMC FÜR EUROPÄISCHE UNTERNEHMEN PLÖTZLICH RELEVANT WIRD

Über Jahre konnten europäische Zulieferer CMMC als US-internes Vorhaben behandeln, dessen Termine sich ohnehin verschieben. Diese Leseart ist seit Ende 2025 überholt. Zwei Regelwerke greifen jetzt ineinander und ihre Fehlinterpretation ist ein häufig auftretender Fehler im Markt.

Zwei Regelwerke, ein Programm – und das Datum, das zählt

Das Regelwerk **32 CFR Part 170** (wirksam seit 16. Dezember 2024) etabliert das CMMC-Programm selbst: die Stufenlogik, die Bewertungsmaßstäbe und das Prüf-Ökosystem aus Akkreditierungsstelle, C3PAOs und Prüfern. **48 CFR/DFARS** (veröffentlicht am 10. September 2025, wirksam am 10.

November 2025) ist der Hebel, der wirklich wirkt: Das Regelwerk bringt zwei Vertragsklauseln ins Spiel, die ineinandergreifen: 252.204-7025 verlangt schon in der Ausschreibung den Nachweis einer bestimmten CMMC-Stufe, und 252.204-7021 macht deren Einhaltung anschließend zur dauerhaften Pflicht während der gesamten Vertragslaufzeit. Damit wird eine gültige CMMC-Stufe zur vertraglichen Vergabevoraussetzung.

Der phasenweise Rollout – die Uhr läuft seit November 2025

Das DoD führt die Anforderung nicht über Nacht ein, sondern staffelt sie über vier Phasen. Diese Staffelung ist kein Grund zum Abwarten, sondern definiert genau das Zeitfenster, in dem eine Vorbereitung möglich und effizient ist: Phase 1 ab November 2025 (Selbstbewertungen), Phase 2 ab ca. November 2026 (C3PAO-Zertifizierung für Level 2), Phase 3 ab ca. November 2027 (Level 3/DIBCAC), Phase 4 ab ca. November 2028 (vollständige Anwendung in allen einschlägigen Verträgen).

Aus Sicht der Geschäftsführung lassen sich drei Fragen nicht länger vertagen:

- **Warum sollte mich das heute interessieren?** Weil Prime Contractors die Anforderung vertraglich durchreichen, bevor sie selbst zertifiziert sein müssen. Die Anforderungen erreichen Zulieferer vor dem regulatorischen Stichtag.
- **Welche Risiken entstehen bei Untätigkeit?** Verlust der Präqualifikation bei OEM-Kunden, Ausschluss aus Ausschreibungen, Engpässe bei knappen

CMMC 2.0 · DFARS-ROLLOUT

Die Uhr läuft seit November 2025

Vierphasiger Rollout über drei Jahre – das Vorbereitungsfenster ist jetzt offen



OPTIMALES VORBEREITUNGSFENSTER 12-24 Monate – planbar, budgetierbar, vor knappen Prüfkapazitäten

Abbildung 2 – CMMC-2.0-Rollout in vier Phasen. Richtwerte auf Basis der DFARS-Regel; die Aufnahme in einzelne Ausschreibungen liegt im Ermessen der jeweiligen DoD-Beschaffungsstelle.

Prüfkapazitäten und – im schlimmsten Fall – **der stille Austausch gegen einen bereits zertifizierten Wettbewerber.**

- **Welche Chance entsteht bei einer frühzeitigen Vorbereitung?** Ein zertifizierungsfähiger Sicherheitsstatus wird zum **Vertriebsargument**: Er signalisiert OEMs Verlässlichkeit, verkürzt Lieferanten-Audits und öffnet Programme, die Wettbewerbern verschlossen bleiben.

3. DIE TRANSFORMATION DER GLOBALEN VERTEIDIGUNGS-LIEFERKETTEN

CMMC trifft auf einen Verteidigungsmarkt im historischen Umbruch. Die wirtschaftliche Relevanz des Themas erschließt sich nur vor dem Hintergrund dreier paralleler Entwicklungen: eines wachsenden US-Beschaffungsvolumens, einer beispiellosen europäischen Aufrüstung und einer zunehmenden Verzahnung beider Märkte.

Der US-Markt: Volumen und Beschaffungsmacht

Die nationalen US-Verteidigungsausgaben erreichen im Haushaltsjahr 2026 rund **1,04 Billionen US-Dollar** – zusammengesetzt aus etwa 893 Mrd. USD regulärer Pentagon-Mittel und rund 152 Mrd. USD

aus einem zusätzlichen Haushaltsverfahren. Ein erheblicher Teil davon fließt als Auftragsvolumen in die industrielle Basis. Das DoD ist damit der größte Einzelkunde für Verteidigungsgüter weltweit – und definiert mit CMMC die Eintrittskarte zu diesem Markt. Die Defense Industrial Base umfasst über 220.000 Unternehmen. Rund 80.000 davon müssen nach DoD-Schätzung die Anforderungen der Stufe 2 erfüllen. Der eigentliche Engpass liegt jedoch nicht bei den Anforderungen, sondern bei den knappen Prüfkapazitäten der noch jungen C3PAO-Landschaft.

Europa rüstet auf – und schafft neue Lieferketten

Parallel verändert sich der europäische Markt schneller als je seit dem Kalten Krieg:

- **NATO – Den Haag 2025:** Die Mitgliedstaaten haben sich im Juni 2025 verpflichtet, bis 2035 5 % des BIP für Verteidigung und verteidigungsnahe Resilienz aufzuwenden (3,5 % militärischer Kern + 1,5 % verteidigungsnahe).
- **Deutschland:** Der Bundeshaushalt 2026 umfasst 524,5 Mrd. €, davon 82,69 Mrd. € für den Verteidigungsetat. Eine Grundgesetzänderung 2025 nimmt Verteidigungsausgaben oberhalb von 1 % des BIP von der Schuldenbremse aus.
- **EU – ReArm Europe/Readiness 2030:** Das im März 2025 vorgestellte Paket soll bis zu 800 Mrd. € mobilisieren. Das Darlehensinstrument SAFE

VERTEIDIGUNGSMÄRKTE · MARKTKONTEXT 2026

CMMC in Zahlen

Ein Markt im historischen Umbruch – auf beiden Seiten des Atlantiks

USA · BESCHAFFUNGSMACHT

1,04 Bio. USD

US-Verteidigungsausgaben FY2026 – größter Einzelkunde weltweit

220.000+

Unternehmen in der Defense Industrial Base

~80.000

davon müssen nach DoD-Schätzung die Anforderungen der **Stufe 2** erfüllen

EUROPA · AUFRÜSTUNG

5 % des BIP

NATO-Ziel bis 2035 (Den Haag, Juni 2025) – 3,5 % Kern + 1,5 % Resilienz

82,69 Mrd. €

deutscher Verteidigungsetat 2026 (Einzelplan 14)

800 Mrd. €

EU ReArm Europe/Readiness 2030 inkl. SAFE-Darlehensinstrument (150 Mrd. €)

Abbildung 3 – Marktumfeld 2026: CMMC im Kontext wachsender Verteidigungsinvestitionen

(150 Mrd. €) fördert gemeinsame Beschaffung unter einem „spend European“-Prinzip (max. 35 % Komponentenwert von außerhalb EU/EWR/Ukraine).

„Spend European“ – und warum es CMMC nicht entwertet

Das „spend European“-Prinzip wirkt auf den ersten Blick wie eine Abkehr von US-Lieferketten. Tatsächlich bleibt die transatlantische Verflechtung jedoch hoch: Schlüsselplattformen wie F-35, Patriot oder HIMARS bleiben US-Systeme, in die europäische Komponenten einfließen und europäische Programme nutzen US-Technologie. Wer für beide Welten liefern will, braucht künftig beide Compliance-Welten – **CMMC für die US-Seite, NIS2 und CRA für die EU-Seite.**

Vom „Trusted Supplier“ zum zertifizierten Supplier

Die eigentliche strukturelle Veränderung ist kulturell, Vertrauen wird verifizierbar. Wo OEMs ihre Zulieferer früher über langjährige Geschäftsbeziehungen und Eigenauskünfte einbanden, verlangt das neue Regime einen prüfbaren Nachweis. Für europäische Mittelständler bedeutet das eine doppelte Botschaft: die Eintrittshürde steigt, aber wer sie nimmt, differenziert sich messbar vom Wettbewerb.

4. WAS CMMC 2.0 KONKRET FORDERT

CMMC 2.0 hat das ursprüngliche Fünf-Stufen-Modell von 2019 auf drei Stufen verschlankt. Die Logik ist einfach: Je sensibler die verarbeiteten Daten, desto strenger die Anforderungen und desto unabhängiger der Nachweis.

FCI und CUI – die alles entscheidende Datenfrage

Welche CMMC-Stufe ein Unternehmen benötigt, hängt nicht von seiner Größe ab, sondern von den Daten, die es im Auftrag verarbeitet. Federal Contract Information (FCI) sind nicht-öffentliche Vertragsinformationen, Controlled Unclassified Information (CUI) sind schützenswerte, aber nicht klassifizierte Informationen wie technische Zeichnungen, Spezifikationen oder Fertigungsdaten. Die Klassifizierung legt der Auftraggeber bzw. Prime Contractor fest – die erste praktische Aufgabe jedes Zulieferers ist daher, zu identifizieren, wo in seinen Systemen FCI oder CUI tatsächlich liegt.

Die drei Stufen im Überblick

Level 1 (Foundational) verlangt 15 Basisanforderungen aus der Standard-Vertragsklausel für

CMMC 2.0 - STUFENMODELL

Drei Stufen – die Datenfrage entscheidet

Nicht die Unternehmensgröße bestimmt die Stufe, sondern die verarbeiteten Daten

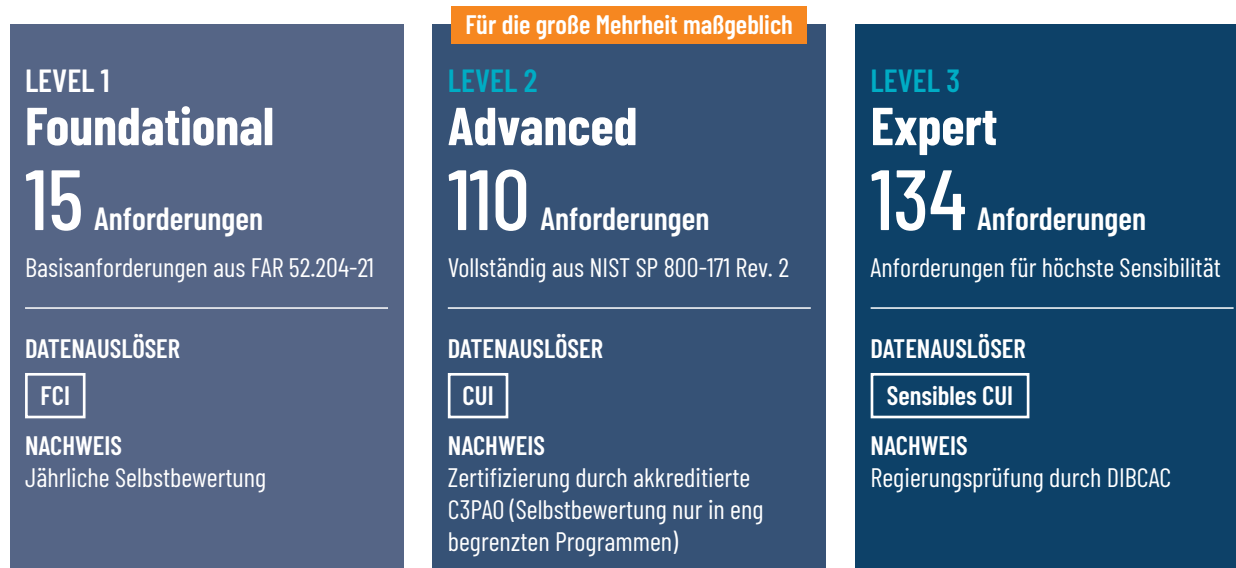


Abbildung 4 – CMMC-2.0-Stufenmodell. Level 2 ist für die große Mehrheit der Zulieferer die maßgebliche Stufe.

US-Bundesauftragnehmer (FAR 52.204-21) und eine jährliche Selbstbewertung. Level 2 (Advanced) umfasst die 110 Anforderungen aus NIST SP 800-171 Rev. 2 und wird im Regelfall durch eine C3PAO zertifiziert. Level 3 (Expert) umfasst die Anforderungen von Level 2 ergänzt um eine Teilmenge erweiterter Anforderungen aus NIST SP 800-172 und wird durch die Regierungsstelle DIBCAC geprüft.

Drei häufige Irrtümer halten sich hartnäckig und sollten vorab ausgeräumt werden:

- „Level 2 erlaubt immer eine Selbstbewertung.“ Falsch – Eine Selbstbewertung ist nur für eng begrenzte Programme zulässig – der Regelfall für CUI ist die C3PAO-Zertifizierung.
- „NIST 800-171 Rev. 3 gilt jetzt.“ Falsch – CMMC ist weiterhin an Rev. 2 gebunden; Rev. 3 ist zwar final, aber per DoD-Class-Deviation noch nicht maßgeblich.
- „Ein POA&M reicht dauerhaft.“ Falsch – er erlaubt nur eine bedingte Zertifizierung, offene Punkte sind binnen 180 Tagen zu schließen. Kritische Anforderungen sind nicht POA&M-fähig.

Die 14 Kontrollbereiche des Level 2

Level 2 stützt sich vollständig auf die 14 Kontrollbereiche der 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) und System & Information Integrity (SI). Entscheidend für das Management: Diese Bereiche sind nicht rein technisch – Personnel Security und Awareness & Training etwa verlangen organisatorische Maßnahmen, Prozesse und Schulung.

Die fünf technischen Schwerpunkte mit dem größten Aufwand

- **Multi-Faktor-Authentifizierung (MFA)** für alle Zugänge zu CUI-Systemen – häufig nachzurüsten bei Legacy-ERP- und CAD-Umgebungen.
- **Netzwerksegmentierung** zur Trennung der CUI-verarbeitenden Systeme von Produktions- und Büronetzen – oft die invasivste Maßnahme.
- **Verschlüsselung mit FIPS-validierten Verfahren** für CUI bei Übertragung und Speicherung; nicht jede vorhandene Verschlüsselung erfüllt die FIPS-Anforderung.

- **Protokollierung & Monitoring (SIEM)** mit zentraler, auswertbarer Aufbewahrung – bei vielen Mittelständlern bisher nicht zentralisiert.
- **Schwachstellenmanagement & Penetrationstests** mit etablierten Scan-, Patch- und Test-Routinen und nachvollziehbaren Fristen.

Der Cloud-Sonderfall, der oft übersehen wird

Wer CUI in Microsoft 365, Azure, AWS oder Google Cloud verarbeitet, muss eine FedRAMP-Moderate-äquivalente Umgebung nutzen – in der Praxis die staatlichen „GovCloud“-/„GCC High“-Varianten. Ein Wechsel der Tenant-Umgebung ist aufwendig, langwierig und sollte früh geplant werden. Nachträgliche Migrationen gehören zu den teuersten CMMC-Überraschungen. Das Äquivalent zu FedRAMP stellt in Deutschland der BSI-C5-Standard dar. Beides sind anerkannte Sicherheitsstandards für Cloud-Anbieter, um sensible Daten zu schützen.

5. AUSWIRKUNGEN AUF DEUTSCHE UND EUROPÄISCHE ZULIEFERER

Die zentrale Frage lautet selten „Müssen wir CMMC erfüllen?“, sondern „Über welchen Pfad erreicht uns die Anforderung – und wann?“. Auch ohne direkten DoD-Vertrag kann CMMC vertraglich bindend werden.

Fünf Wege, über die CMMC ein europäisches Unternehmen erreicht

- **OEM-/Prime-Flow-down:** Ein US-Generalunternehmer gibt CMMC-Pflichten vertraglich an alle Zulieferer mit CUI-Zugang weiter – unabhängig vom Sitz.
- **Internationale Joint Ventures:** In transatlantischen Konsortien gilt die Anforderung für alle Partner, die gemeinsame CUI verarbeiten.
- **NATO-/FMS-Programme:** Beschaffungen über US-Systeme (Foreign Military Sales) ziehen US-Anforderungen in die europäische Zulieferkette.
- **M&A-Transaktionen:** Ein US-Käufer oder ein zertifizierungspflichtiges Target macht CMMC-Reife zum Bestandteil der Due Diligence und Kaufpreisfindung.
- **Künftige Ausschreibungen:** Direkte Qualifikation für DoD-Aufträge in Nischen mit europäischer Technologieführerschaft – Sensorik, Optik, Antriebe, Cyber-Hardware.

CMMC 2.0 · VERTRAGLICHER FLOW-DOWN

CMMC erreicht jede Stufe der Lieferkette

Auch ohne direkten DoD-Vertrag – sobald FCI oder CUI verarbeitet werden



Abbildung 5 – Über den vertraglichen Flow-down erreicht die CMMC-Pflicht jede Stufe der Lieferkette, die FCI oder CUI verarbeitet – auch ohne direkten DoD-Vertrag.

CMMC 2.0 · RAHMENWERK-VERGLEICH

Drei typische Konstellationen

Wie die Anforderung deutsche Mittelständler erreicht – und wie sie reagieren

FALL A Der Sensorhersteller KMU · ~80 Mitarbeiter · ISO 27001 vorhanden	FALL B Der Systemintegrator Großunternehmen · faktische Prime-Rolle	FALL C Der Embedded-Software-Anbieter Boutique · ~40 Mitarbeitende
AUSLÖSER Liefert an einen EU-Integrator mit US-Prime. Der Prime klassifiziert die Spezifikations- und Toleranzdaten als CUI und fordert Level 2 binnen 18 Monaten. RISIKO Der Integrator hat bereits einen zertifizierten Alternativlieferanten evaluiert und behält sich einen kurzfristigen Wechsel vor. LÖSUNGSWEG CUI-Scoping auf eine separierte Enklave; MFA, zentrales Logging, FIPS-Krypto; Wiederverwendung ~65 % der ISO-Kontrollen. NUTZEN Zertifizierungsfähigkeit als Vertriebsargument und gesicherte Programmteilnahme sowie ein belastbarer Nachweis gegenüber Auftraggebern.	AUSLÖSER Integriert ein System für ein NATO-Land mit US-Komponenten und Re-Export an eine US-Teilkraft. Muss selbst Level 2/3 erfüllen und die Lieferkette steuern. RISIKO Ein einziger nicht-konformer Sub-Lieferant gefährdet die Zertifizierung des gesamten Systemverbunds und verzögert die laufende NATO-Ausschreibung erheblich. LÖSUNGSWEG Unternehmensweites CUI-Datenfluss-Mapping; Lieferanten-Compliance-Programm mit Vertragsklausel; C3PAO-Readiness über 24-30 Monate. NUTZEN Belastbare Supply-Chain-Governance als Differenzierung in NATO-Ausschreibungen und ein klarer Wettbewerbsvorteil bei Vergabeverfahren.	AUSLÖSER Lizenziert Embedded-Software an einen US-Integrator für ein Verteidigungsprogramm; Teile der Entwicklung und Wartung erfolgen offshore. RISIKO Ist der Quellcode CUI, greift Level 2 – inkl. externer Entwickler und Build-/Repository-Infrastruktur. Kritisch sind die Offshore-Zugänge. LÖSUNGSWEG Absicherung der Entwicklungskette (DevSecOps, Zugriffstrennung, Code-Signing); ggf. Verlagerung CUI-relevanter Arbeit in eine kontrollierte Enklave. NUTZEN Zugang zu sicherheitskritischen US-Softwareprogrammen, die zertifizierte Anbieter bevorzugen, ideal für langfristige Kundenbindung.

Abbildung 6 – Typische CMMC-Betroffenheit deutscher Mittelständler: Drei Praxisbeispiele

Drei typische Konstellationen aus der Praxis

Die folgenden Konstellationen sind anonymisierte, illustrative Beispiele typischer Ausgangslagen im deutschen Mittelstand – sie bilden Muster ab, keine konkreten Mandate:

6. ZUSAMMENSPIEL MIT NIS2, CRA, ISO 27001, TISAX UND BSI IT-GRUNDSCHUTZ

Die gute Nachricht für europäische Unternehmen: CMMC entsteht nicht im luftleeren Raum. Wer bereits in europäische und internationale Sicherheitsstandards investiert hat, startet mit einem belastbaren Fundament. Die schlechte Nachricht: Kein einziger dieser Standards deckt CMMC vollständig ab – die verbleibende Lücke ist spezifisch und nachweispflichtig.

Der Rahmenwerk-Vergleich auf einen Blick

Die Heatmap zeigt das Muster, auf das es ankommt: Über alle Standards hinweg sind die Spalten „CUI-Handling“ und „Nachweis (SPRS und Drittprüfung)“ rot. Genau hier liegt das US-spezifische Delta, das keine europäische Investition allein schließt:

- **NIS2** (EU-Richtlinie, Pflicht für wesentliche/wichtige Einrichtungen): hohe Überschneidung bei Risikomanagement, Incident Response, Lieferkettensicherheit und Governance. Lücke: CUI-Handhabung, DFARS-Flow-down, SPRS, FIPS-Krypto, Drittprüfung.
- **CRA** (EU-Verordnung für Produkte mit digitalen Elementen): Überschneidung bei Secure Development sowie Schwachstellen- und Patch-Management. Lücke: Produkt- statt Organisationsfokus – kein CUI-/ISMS-Scope.
- **ISO 27001** (international, freiwillig/zertifizierbar): hohe Deckung der Prozesskontrollen – ISMS, Risiko, Zugriff, Krypto, Incident Response. Lücke: US-Spezifika wie CUI-Markierung, FIPS-Krypto, SPRS-Affirmation, Log-Retention, FedRAMP-äquivalente Cloud.
- **TISAX** (Automotive, VDA ISA): liefert ISMS-Basis, Lieferanten-Assurance und Prototypenschutz. Lücke: Defense-/CUI-Spezifika und US-Regulatorik.
- **BSI IT-Grundschatz** (deutsche Methodik): liefert Kontrollkatalog und Risikomethodik mit hoher ISO-Nähe. Lücke: identisch zu ISO – die US-Spezifika fehlen.

CMMC 2.0 · RAHMENWERK-VERGLEICH

Wo bestehende Standards CMMC abdecken

Zwei Themenbereiche bleiben über alle Standards hinweg rot – das CMMC-spezifische Delta

Standard ↑ / Bereich →	Ausgewählte Beispiel-Bereiche					Von keinem EU-Standard allein abgedeckt	
	Governance & Risiko	Zugriff & Krypto	Incident Response	Lieferkette	Secure Development	CUI-Handling	Nachweis & Drittprüfung
NIS2 EU-Richtlinie	Hoch	Teilweise	Hoch	Hoch	Teilweise	Lücke	Lücke
CRA EU-Verordnung (Produkte)	Teilweise	Teilweise	Teilweise	Hoch	Hoch	Lücke	Lücke
ISO 27001 International, zertifizierbar	Hoch	Hoch	Hoch	Teilweise	Teilweise	Lücke	Lücke
TISAX Automotive/VDA ISA	Hoch	Hoch	Hoch	Hoch	Teilweise	Lücke	Lücke
BSI IT-Grundschatz Deutsche Methodik	Hoch	Hoch	Hoch	Teilweise	Teilweise	Lücke	Lücke

■ Hoch – weitgehend abgedeckt
 ■ Teilweise – Anpassung nötig
 ■ Lücke – CMMC-spezifisch

Abbildung 7 – Wiederverwendungs-Heatmap: Wo bestehende Standards CMMC-Anforderungen abdecken (grün), wo Anpassung nötig ist (gelb) und wo die spezifisch US-amerikanische Lücke bleibt (rot).

CMMC 2.0 · IMPLEMENTIERUNGS-AUFWAND

Zwei Drittel sind schon gebaut

Der entscheidende Mehraufwand ist das CMMC-spezifische Delta



60 – 70 %
Wiederverwendbar

30 – 40 %
CMMC-Delta

Wiederverwendbar aus ISO 27001/TISAX/IT-Grundschutz (Beispiele)

Governance

Risikomanagement

Zugriffskonzepte

Physische Sicherheit

Schulung & Awareness

Dienstleistermanagement

Incident-Response

Sichere Softwareentwicklung

Schwachstellenmanagement

IT Change Management

CMMC-Delta – zusätzlich aufzubauen und nachzuweisen

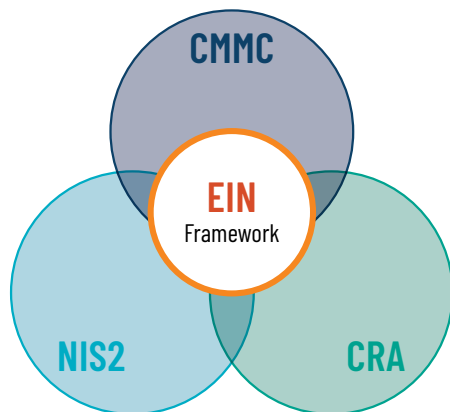
- CUI-Scoping & -Markierung
- DFARS-konforme Vorfalldmeldung
- SPRS-Eintrag & Affirmation
- FIPS-validierte Verschlüsselung
- FedRAMP-äquivalente Cloud (GCC High)
- Drittprüfung durch C3PAO

Abbildung 8 – Grobe Aufteilung des Implementierungsaufwands: ein wiederverwendbarer Anteil aus vorhandenen Standards und ein US-spezifisches Delta (erfahrungsbasierte Schätzung).

COMBINED COMPLIANCE · STRATEGISCHER HEBEL

Drei Pflichten, ein Fundament

CMMC, NIS2 und CRA auf einem gemeinsamen Kontroll-Framework



CMMC

US-Verteidigungslieferkette – CUI-Handling, DFARS-Flow-down, SPRS, Drittprüfung

NIS2

EU-Richtlinie für wesentliche & wichtige Einrichtungen – Risikomanagement, Incident Response, Lieferkette, Governance

CRA

EU-Verordnung für Produkte mit digitalen Elementen – Secure Development, Schwachstellen- & Patch-Management

DER EIGENTLICHE HEBEL

Gemeinsam abgebildet senken die drei Programme die **Gesamtkosten** deutlich gegenüber drei getrennten Initiativen.

Abbildung 9 – Ein Kontroll-Framework für drei regulatorische Anforderungen (CMMC, NIS2 und CRA)

Die Managementsicht: Was lässt sich wiederverwenden?

Als Faustregel sind rund 60–70 % der Anforderungen aus ISO 27001, TISAX oder IT-Grundschutz wiederverwendbar – Governance, Risikomanagement, Zugriffskonzepte, Schulung, Incident-Response-Prozesse und physische Sicherheit. Der zusätzliche

Aufwand ist das CMMC-Delta: CUI-Scoping und -Markierung, FIPS-validierte Verschlüsselung, DFARS-konforme Vorfalldmeldung, FedRAMP-äquivalente Cloud, SPRS-Eintrag mit jährlicher Affirmation sowie die Drittprüfung selbst. Die Prozentangabe ist eine Erfahrungsgröße, keine zertifizierte Mapping-Quote.

Combined-Compliance-These: Unternehmen, die NIS2, CRA und CMMC parallel auf ein gemeinsames Kontroll-Framework abbilden, senken die Gesamtkosten der Compliance deutlich gegenüber drei getrennten Programmen. Diese Integration – nicht die einzelne Zertifizierung – ist der eigentliche strategische Hebel.

7. WIE UNTERNEHMEN IHRE READINESS BEWERTEN KÖNNEN

Vor jeder Investition steht die Standortbestimmung. Sie beantwortet zwei Fragen: Welche Stufe brauchen wir wirklich – und wie weit sind wir von ihr entfernt?

Der SPRS-Score – die Währung des Nachweises

Für Level 2 bewerten Unternehmen ihre Umsetzung der 110 Anforderungen und stellen das Ergebnis als Zahlenwert in das Supplier Performance Risk System (SPRS) ein. Die Skala beginnt bei 110 Punkten, je offener Anforderung werden – je nach Gewicht – 5, 3 oder 1 Punkt abgezogen, der Wert kann bis auf –203 fallen.

Fünf-Dimensionen-Readiness-Modell

- **Daten & Scope:** Wissen wir, wo FCI/CUI liegt und wer darauf zugreift? Reifegrad im Mittelstand meist niedrig – selten systematisch erhoben.
- **Technische Kontrollen:** Sind MFA, Segmentierung, FIPS-Krypto und SIEM vorhanden? Reifegrad mittel – Lücken vor allem bei Krypto und Logging.
- **Prozesse & Governance:** Sind IR-, Patch- und Lieferantenprozesse dokumentiert und gelebt? Reifegrad mittel bis hoch insbesondere bei ISO-/TISAX-zertifizierten Unternehmen.
- **Lieferkette:** Sind Sub-Lieferanten und Cloud-Provider CMMC-fähig? Reifegrad niedrig – der größte Blindspot.
- **Nachweisfähigkeit:** Sind revisionssichere Prozesse, Kontrollen und Dokumentation vorhanden und der SPRS-Eintrag und die Affirmation geregelt? Reifegrad niedrig – Dokumentation oft lückenhaft.

» Ein niedriger oder fehlender Wert ist heute schon ein Ausschlusskriterium bei Präqualifikationen. «

CMMC 2.0 · NACHWEIS

Der SPRS-Score – die Währung des Nachweises

Die erste, von Auftraggebern einsehbare Kennzahl der Cyber-Reife

STARTWERT LEVEL 2

110

Punkte bei voller Umsetzung

Bewertet werden die 110 Anforderungen aus NIST SP 800-171 Rev. 2. Das Ergebnis wird ins Supplier Performance Risk System eingestellt.

Wertebereich des SPRS-Scores



Je offener Anforderung werden (je nach Gewicht) Punkte abgezogen. Der Wert kann bis auf –203 fallen.

-5

Kritische Anforderung
höchstes Gewicht

-3

Wichtige Anforderung
mittleres Gewicht

-1

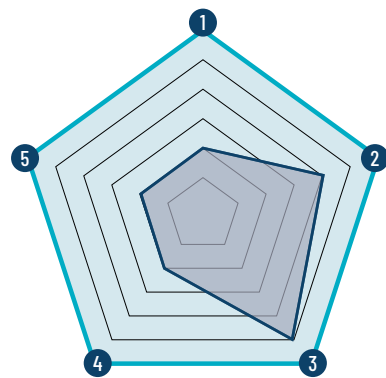
Ergänzende Anforderung
geringes Gewicht

SCHON HEUTE RELEVANT Ein niedriger oder fehlender Score ist bereits jetzt ein Ausschlusskriterium bei Präqualifikationen.

Abbildung 10 – Der SPRS-Score als Nachweis der Cyber-Reife im CMMC-Umfeld

Fünf Dimensionen der Standortbestimmung

Typischer Reifegrad im Mittelstand gegenüber dem CMMC-Zielprofil



■ Zielprofil (CMMC-Level 2)

■ Typischer Ist-Zustand Mittelstand

1	Daten & Scope Wissen wir, wo FCI/CUI liegt und wer darauf zugreift?	niedrig
2	Technische Kontrollen MFA, Segmentierung, FIPS-Krypto, SIEM – Lücken insbesondere bei Krypto und Logging	mittel
3	Prozesse & Governance IT-/InfoSec-Prozesse und -Strukturen etabliert – vor allem bei ISO-/TISAX-zertifizierten Unternehmen	mittel-hoch
4	Lieferkette Sind Sub-Lieferanten und Cloud-Provider CMMC-fähig? Häufig der größte Blindspot	niedrig
5	Nachweisfähigkeit Ist eine revisionssichere Dokumentation vorhanden? Ist der SPRS-Eintrag und die Bestätigung (Affirmation) geregelt?	niedrig

Abbildung 11 – Standortbestimmung der CMMC-Reife mittelständischer Unternehmen entlang fünf zentraler Dimensionen

Zehn-Punkte-Readiness-Check für die Geschäftsführung

1. Wir wissen, welche unserer Kunden DoD-End-abnehmer sind (direkt oder indirekt).
2. Wir haben vertragliche CMMC-/DFARS-Klauseln in Bestands- und Neuverträgen geprüft.
3. Wir haben FCI/CUI in unseren Systemen identifiziert und ihren Datenfluss dokumentiert.
4. Wir kennen die benötigte CMMC-Stufe (1, 2 oder 3) je Kundenbeziehung.
5. Wir haben einen aktuellen SPRS-Score auf Basis von NIST 800-171 Rev. 2 ermittelt.
6. MFA, Netzwerksegmentierung und FIPS-Verschlüsselung sind für CUI-Systeme umgesetzt.
7. Wir betreiben zentrales Logging/Monitoring mit definierter Aufbewahrung.

8. Unsere CUI-relevante Cloud ist FedRAMP-äquivalent (z. B. GCC High).
9. Unsere Sub-Lieferanten mit CUI/FCI-Zugang sind vertraglich eingebunden.
10. Ein Verantwortlicher für die jährliche Affirmation ist benannt.

8. HANDLUNGSEMPFEHLUNGEN FÜR DIE NÄCHSTEN 12-24 MONATE

Die folgende Roadmap übersetzt die Anforderungen in eine wirtschaftlich vertretbare Reihenfolge. Leitprinzip ist „No-Regret zuerst“: Maßnahmen, die unabhängig von der finalen CMMC-Stufe und auch für NIS2 Wert stiften, werden vorgezogen.

Roadmap in vier Wellen

- **Welle 1 – Klarheit (Monat 0-3):** Vertrags- und Kundenanalyse, CUI/FCI-Scoping, Ziel-Stufe je Kunde, SPRS-Erstbewertung, Business Case.
- **Welle 2 – Fundament (Monat 3-9):** No-Regret-Maßnahmen – MFA, Logging/SIEM, Segmentierungsplan, FIPS-Krypto, Awareness; Mapping vorhandener Kontrollen (z. B. aus ISO 27001 oder TISAX).

» Wenn einer dieser Punkte mit Nein beantwortet wird, ist der nächste sinnvolle Schritt die Durchführung eines strukturierten Readiness- bzw. Gap-Assessments, bevor Budget in Einzelmaßnahmen fließt. «

- **Welle 3 – Tiefe & Lieferkette (Monat 9–18):** Restkontrollen, Cloud-Migration (GCC High), Lieferanten-Compliance-Programm, Evidenz-Management, interne Vorprüfung.
- **Welle 4 – Nachweis (Monat 18–24):** C3PAO-Readiness-Assessment, Behebung der Findings, formales Assessment, SPRS-Eintrag und Affirmation.

Die fünf wichtigsten No-Regret-Maßnahmen

1. CUI-/FCI-Scoping durchführen → ohne Scope keine belastbare Kosten- und Aufwandsschätzung.
2. MFA flächendeckend für sensible Zugänge ausrollen → hoher Sicherheitsnutzen, niedrige relative Kosten.
3. Zentrales Logging/Monitoring etablieren → Pflicht für CMMC und NIS2 zugleich.
4. Lieferanten mit CUI-Zugang vertraglich verpflichten → der größte Blindspot zuerst.
5. Bestehende ISO-/TISAX-/IT-Grundschutz-Kontrollen auf NIST 800-171 mappen → Vermeidung von Doppelarbeit.

Aufwand realistisch einordnen

Der Aufwand und die Kosten einer Level-2-Zertifizierung variieren stark mit Scope, IT-Reife und Lieferkettenkomplexität – seriöse Schätzungen reichen von **mittleren fünf- bis hohen sechsstelligen Eurobeträgen über zwei bis drei Jahre**. Entscheidend ist weniger die absolute Zahl als der Zeitpunkt. Eine Vorbereitung im 12- bis 24-Monats-Vorlauf ist planbar und budgetierbar, ein Notfallprojekt unter Ausschreibungsdruck ist es nicht – und trifft zudem auf knappe, dann teure Prüfkapazitäten.

Die fünf teuersten Überraschungen – und wie man sie vermeidet

- **Cloud-Migration auf FedRAMP-äquivalente Umgebung:** CUI in Standard-Microsoft-365/Azure/AWS reicht nicht, nötig sind staatliche Varianten wie GCC High → Früh entscheiden und planen.
- **FIPS-validierte Verschlüsselung:** Vorhandene Verschlüsselung erfüllt die FIPS-Anforderung oft nicht, einzelne Altsysteme müssen ersetzt werden → Krypto-Bestand früh prüfen.

CMMC 2.0 · HANDLUNGS-ROADMAP

24 Monate in vier Wellen

„No-Regret zuerst“ – Maßnahmen mit Wert auch für NIS2 werden vorgezogen

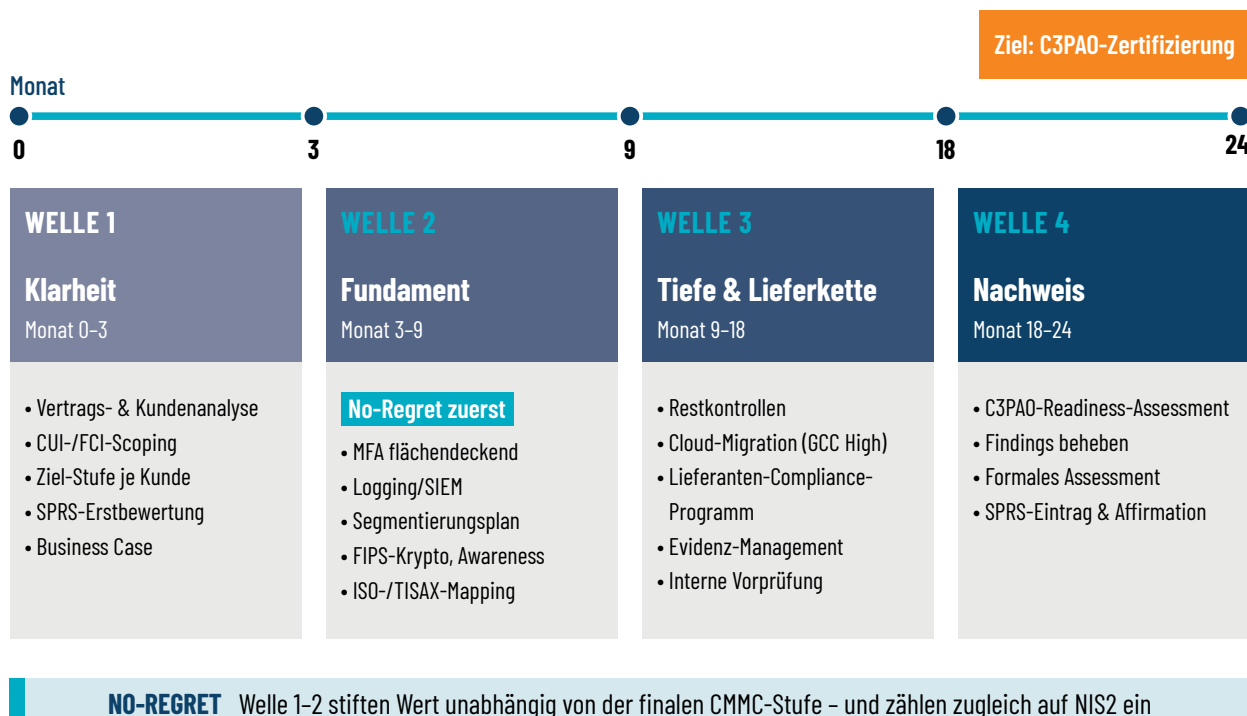


Abbildung 12 – 24-Monats-Roadmap in vier Wellen. „No-Regret zuerst“: Maßnahmen mit Wert auch für NIS2 und unabhängig von der finalen CMMC-Stufe werden vorgezogen.

- **Offshore- und externe Entwicklungszugänge:** Ungeregelte Drittzugriffe auf CUI können die Zertifizierung blockieren → Zugriffe trennen oder in eine Enklave verlagern.
- **Engpass bei C3PAO-Prüfkapazitäten:** Die Zahl akkreditierter Prüfer ist begrenzt, unter Ausschreibungsdruck werden Termine knapp und teuer. Readiness entsprechend timen.
- **Die Sub-Lieferanten-Kaskade:** Ein einziger nicht-konformer Sub-Lieferant mit CUI-Zugang gefährdet die gesamte Zertifizierung → Lieferkette früh kartieren und vertraglich einbinden.

9. FAZIT UND STRATEGISCHER AUSBLICK

CMMC ist kein vorübergehendes US-Regulierungsthema, sondern Ausdruck eines dauerhaften Strukturwandels: In einer Welt zunehmender geopolitischer Spannungen wird **nachgewiesene Cyber-Resilienz zur Grundvoraussetzung für die Teilnahme an Verteidigungslieferketten** – auf beiden Seiten des Atlantiks.

Für deutsche und europäische Unternehmen ergibt sich daraus eine klare strategische Wahl. Sie können CMMC als externe Belastung behandeln und reaktiv abwarten – mit dem Risiko, Programme und Kunden zu verlieren – oder sie erkennen den Standard als das, was er sein soll: ein Qualitätssiegel für Verlässlichkeit, das in einem wachsenden Markt differenziert und sich mit bestehenden Investitionen in NIS2, CRA oder Best Practice Standards (ISO 27001, TISAX oder IT-Grundschutz) effizient verbinden lässt.

Der rote Faden noch einmal auf den Punkt: CMMC betrifft europäische Unternehmen früher, als viele annehmen. Die DFARS-Regel ist in Kraft, die Nachfrage wandert durch die Lieferkette, und die Prüfkapazitäten sind knapp. Wer jetzt eine Standortbestimmung vornimmt und sein bestehendes ISMS gezielt erweitert, sichert sich **Marktzugang** und macht aus einer Pflicht einen **Vorsprung**.

Drei Entwicklungen sollten Sie 2026/2027 beobachten:

- **NIST 800-171 Rev. 3:** Eine künftige Übernahme in CMMC würde einzelne Anforderungen verändern – Architekturen sollten anpassungsfähig ausgelegt werden.

- **Europäische Gegenbewegung:** Mit „spend European“ und einem möglichen EU-Pendant zu prüfbarer Lieferketten-Cybersicherheit könnten parallele Nachweispflichten entstehen – ein integriertes Framework zahlt sich doppelt aus.
- **Konsolidierung der Lieferketten:** Zertifizierung wird zum M&A-Faktor – reife Anbieter werden zu attraktiveren Targets und Partnern.

10. WIE PROTIVITI UNTERSTÜTZT

Protiviti begleitet Industrie- und Technologieunternehmen entlang des gesamten CMMC-Lebenszyklus – von der ersten Standortbestimmung bis zur Aufrechterhaltung der Zertifizierung. Der Ansatz verbindet regulatorische Tiefe mit industrieller Umsetzungserfahrung und der bewussten Wiederverwendung bestehender Compliance-Investitionen:

- **Readiness- & Gap-Assessment** gegen NIST 800-171 Rev. 2 inkl. SPRS-Scoring und priorisierter Maßnahmen-Roadmap.
- **CUI-Scoping & Architektur** – Identifikation von FCI/CUI, Enklaven-Design und Cloud-Strategie (FedRAMP-äquivalent).
- **Combined-Compliance-Programme** zur integrierten Umsetzung von CMMC, NIS2, CRA, ISO 27001 und TISAX auf einem gemeinsamen Kontroll-Framework.
- **Cybersecurity Governance** – Aufbau von Richtlinien, Rollen, Incident-Response- und Lieferanten-Steuerung.
- **M&A Due Diligence** zur Bewertung der CMMC-Reife von Targets als Wert- und Risikofaktor in Transaktionen.
- **Managed Services** für Monitoring, Evidenz-Pflege und die jährliche Affirmation.

11. QUELLEN (AUSWAHL)

- U.S. Department of Defense – CMMC Program Resources; DFARS-Regel, wirksam 10. November 2025 (Klauseln 252.204-7021 und 252.204-7025)
- NIST SP 800-171 Rev. 2/Rev. 3 sowie NIST SP 800-172; DoD Class Deviation 2023-O0006
- US-Verteidigungshaushalt FY2026 (NDAA und Reconciliation); öffentlich berichtete Gesamthöhe rund 1,04 Bio. USD
- NATO – Den Haag Gipfel, Juni 2025 (5-%-BIP-Ziel bis 2035)

- Bundeshaushalt 2026/Einzelplan 14; Grundgesetz-änderung 2025 zur Schuldenbremse
- Europäische Kommission – ReArm Europe/Readiness 2030 (März 2025) und SAFE-Verordnung (Mai 2025).

12. ÜBER PROTIVITI

Protiviti (www.protiviti.com) ist ein global tätiges Beratungsunternehmen, das Unternehmen hilft, sich zu transformieren und zu schützen. Über ein Netzwerk von mehr als 90 Büros in über 25 Ländern liefern Protiviti und seine unabhängigen Mitgliedsfirmen tiefgehende Expertise in den Bereichen Technologie, künstliche Intelligenz, Daten, Operations, Finanzen, Recht, Compliance, Risiko und interne Revision.

Im Kontext von CMMC unterstützt Protiviti Zulieferer der Verteidigungs- und Luftfahrtindustrie sowie mittelständische Fertigungsunternehmen entlang des gesamten Lebenszyklus – von der regulatorischen Standortbestimmung über das Design von Kontrollen und Architektur bis zu interner Revision und Prüfungsbereitschaft.

Dieses Whitepaper wurde im Juli 2026 erstellt und gibt den Stand von CMMC 2.0 gemäß der 32-CFR-Programmregel (wirksam Dezember 2024) und der 48-CFR-/DFARS-Beschaffungsregel (wirksam 10. November 2025) wieder. Es ersetzt keine Rechts- oder Zertifizierungsberatung im Einzelfall.

www.protiviti.de



© Protiviti GmbH

KONTAKTE



ANDREJ GREINDL

Managing Director

+49 172 698 30 53

andrej.greindl@protiviti.com



NIKOLAI KÖNIG

Director

+49 172 698 3047

nikolai.koenig@protiviti.com

WEITERER AUTOR



MORITZ REINDL

Consultant

+49 151 7242 47 67

moritz.reindl@protiviti.com