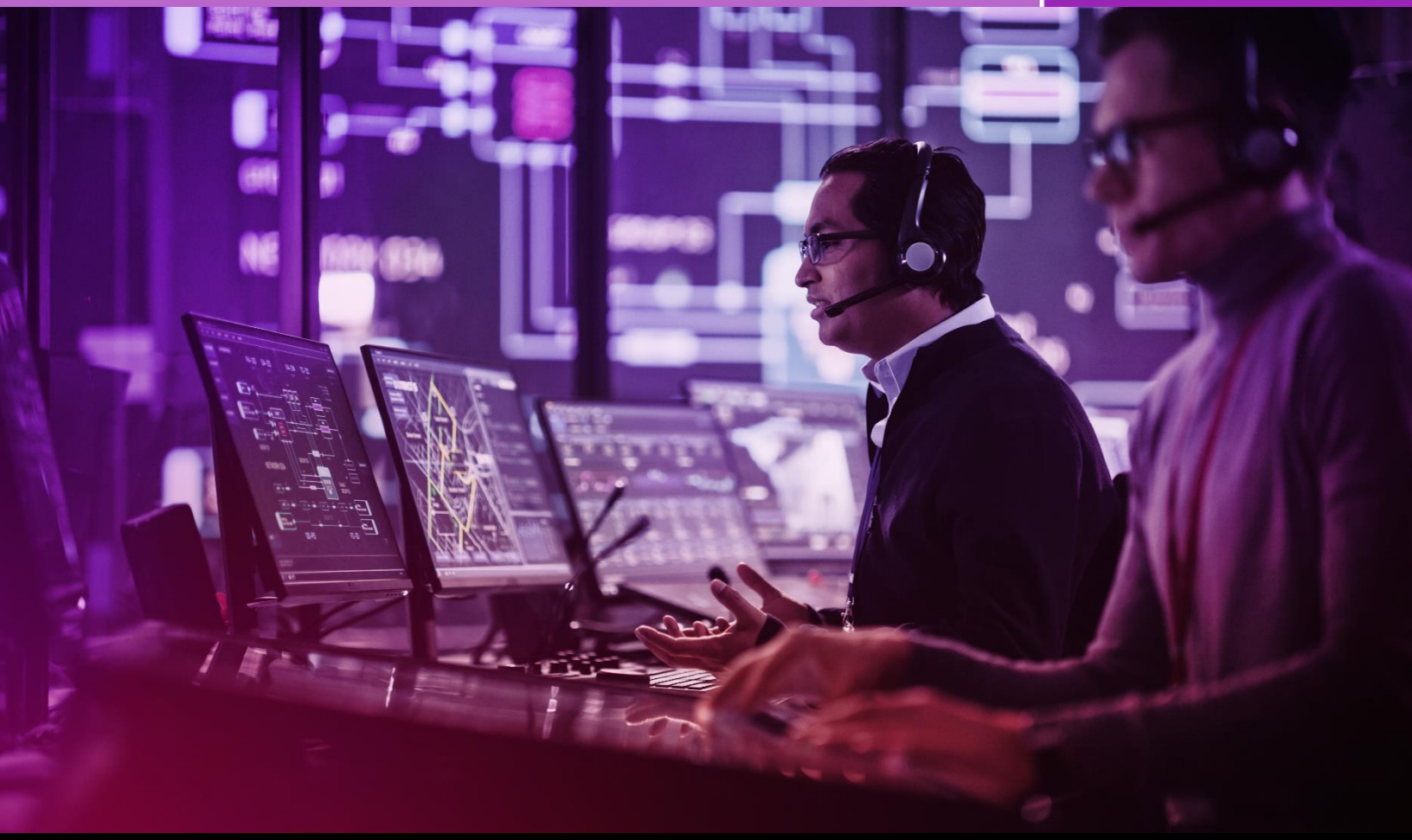
WHITE PAPER



The Power of Proof: Turning CMMC Compliance into Competitive Credibility

KEYSIGHT

Table of Contents

Executive Summary

The Cybersecurity Maturity Model Certification (CMMC) represents the most sweeping transformation of defense cybersecurity standards in decades — and it is no longer optional. By November 2028, every company in the U.S. Defense Industrial Base (DIB) will need certification to compete for Department of Defense (DoD) contracts. Yet, Keysight's commissioned research reveals a stark reality: only 2 percent of organizations are audit-ready, and just 3 percent employ automated validation tools to continuously verify compliance.

This readiness gap has immediate business implications. Companies that delay will forfeit eligibility for new contracts, face rising audit costs, and risk exclusion from the defense supply chain. Keysight's primary research, conducted with SIS International Research, surveyed more than 200 cybersecurity leaders across the DIB and uncovered systemic challenges — talent shortages, outdated infrastructure, and overreliance on self-attested "paper compliance."

Keysight Technologies offers a measurable path forward. With solutions that address 10 of 14 CMMC domains, Keysight enables defense contractors to move from static documentation to evidence-based, continuously validated cybersecurity assurance. Keysight's range of cybersecurity, network visibility, and test solutions helps organizations detect vulnerabilities, verify controls, and demonstrate verifiable compliance.

CMMC readiness is no longer a regulatory checkbox — it is a strategic differentiator. Those who modernize now will not only safeguard their contracts but position themselves as trusted partners in an era when cybersecurity credibility defines competitive advantage.

The Unavoidable Deadline

75% Don't Prioritize CMMC — But 100% Will Need It by November 2028

The U.S. DoD is implementing CMMC, a comprehensive overhaul of cybersecurity standards. This framework marks a fundamental change in how the DoD will evaluate and enforce cybersecurity standards within its supply chain. This change directly impacts over 100,000 companies that comprise the DIB, transforming cybersecurity compliance from a minor contractual requirement into an essential condition for participation. [1]

CMMC Is Mission-Critical, But Over Half of Government Contractors Still Don't Prioritize It

On September 10, 2025, the DoD published the final CMMC Acquisition Rule in the Federal Register, effective November 10, 2025. [2] This initiates a four-phase, three-year rollout of CMMC requirements in DoD solicitations, with requirements appearing immediately after the effective date. [3]

Phase 1 (from November 10, 2025, through November 9, 2026) covers mainly Level 1 (self-assessment) and Level 2 (self-assessment) requirements. Phase 2 (beginning November 10, 2026) begins to require Level 2 certification by a third-party assessment organization (C3PAO) for applicable contracts. Phase 3 (beginning November 10, 2027) increases the requirement for Level 3 (government-led) certification for the most sensitive contracts. By November 10, 2028 (start of Phase 4), compliance becomes mandatory for all applicable DoD contracts, meaning all contracts that involve Controlled Unclassified Information (CUI) must incorporate the applicable CMMC level requirement. [4]

This directive addresses new cyber threats to the defense supply chain. High-profile breaches, such as SolarWinds, reveal systemic vulnerabilities in an interconnected industrial base. As a cybersecurity president and CISO said, participants are only as strong as the weakest link.

Automation is essential for maintaining compliance due to the large amount of data, the complexity of the 110 security controls in NIST SP 800-171 that underpin CMMC Level 2, and the speed required for modern cyber defense, making manual efforts inadequate. [4] This shift emphasizes the CMMC framework's main goal: protecting CUI and Federal Contract Information (FCI), as well as ensuring supply chain integrity in an AI-driven environment. [4]

Get the essential guide for CMMC Compliance.

Just One in Three Defense Contractors Consider CMMC Compliance "Extremely Urgent," Underscoring Uneven Readiness Across the DIB

This new market dynamic rewards proactive organizations. Because achieving compliance typically takes 12 to 18 months, waiting until the final deadline will leave companies behind — unable to compete for CMMC-eligible contracts while prepared competitors move ahead. [6]

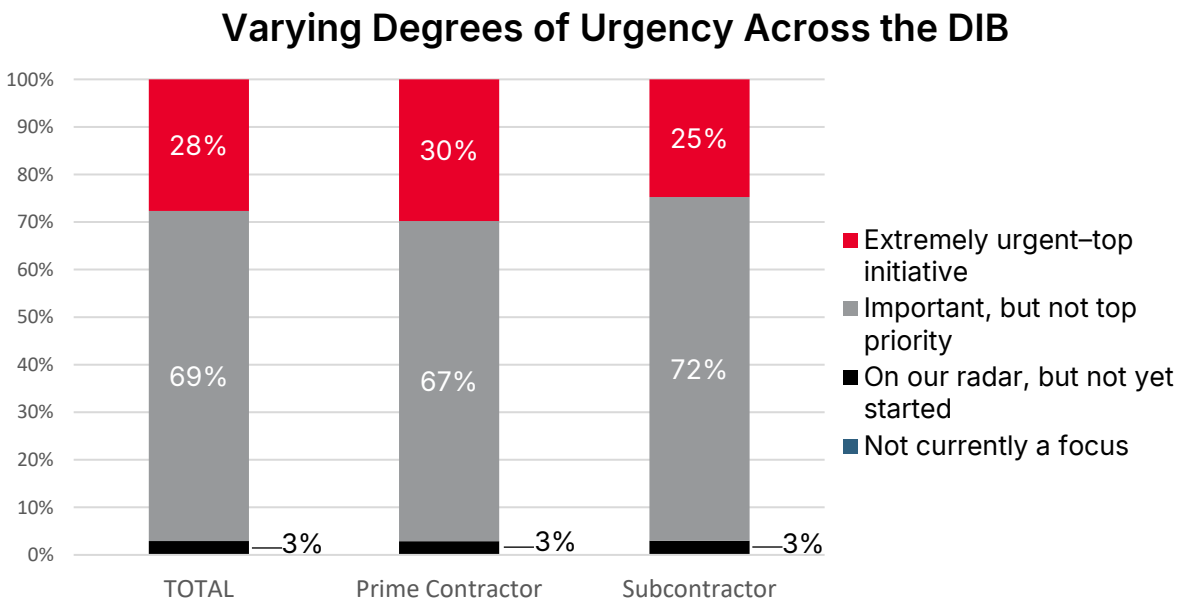


Figure 1. Varying Degrees of Urgency Across the DIB

Why “Good Enough” Security Will Cost You Contracts

98% of Government Contractors Still Aren't Ready

Despite the looming deadlines and clear consequences, most of the DIB remains unprepared for the CMMC mandate. Our research shows a substantial gap between perceived readiness and audit-ready compliance.

When asked about obstacles, respondents cited three major pain points:

- **35%** pointed to the complexity of the requirements
- **30%** cited a lack of internal resources
- **30%** struggled with understanding the requirements and a lack of clear DoD guidance

These challenges reflect deeper systemic issues, including resource constraints, regulatory confusion, and a fundamental misunderstanding of the scope and rigor of CMMC.

Much of this delay stems from a tendency to postpone complex compliance work until enforcement feels imminent. Many organizations, especially those without dedicated compliance teams, view CMMC as a future issue rather than an immediate strategic concern. One CTO summarized:

This reactive approach introduces serious risks. As enforcement expands, companies that take a “wait-and-see” stance may find themselves locked out of contracts or scrambling to achieve compliance under pressure.

Beyond delayed action, confusion about scope and requirements worsens the compliance challenge. One of the most significant barriers is a persistent lack of awareness and clarity. Many organizations, especially small- to mid-sized businesses (SMBs), remain uncertain about which CMMC level applies to them or what the requirements entail. A Director of IT and Enterprise Strategy noted that the messaging can be confusing across similar yet distinct frameworks, such as NIST and CMMC.

> NIST (National Institute of Standards and Technology) establishes the cybersecurity controls that form the foundation of CMMC, including NIST SP 800-171 Rev. 2 and NIST SP 800-172.
>
> While NIST provides voluntary guidelines, CMMC makes those standards mandatory and auditable for DoD contractors.

This nuance has created a false sense of security. As one CISO and certified assessor explained, "Companies assume that because they've done the internal self-assessment and believe they have 110 points, they're compliant. But that's often not the case." In practice, auditors often find that most companies claiming full NIST scores are not accurate. Official audits confirm that DoD contractors routinely overestimate their self-reported cybersecurity scores. Past regulatory uncertainty has compounded the issue. The shift from CMMC 1.0 to 2.0, combined with the phased rollout, has led some to adopt a wait-and-see approach. With the implementation of the final rule imminent, organizations can no longer defer; the time to act is now.

> "Until it happens, and until they get fined... they'd love to sweep it under the rug."

The Price of Misreported Compliance

In one case that resulted in a $4.6 million settlement, a contractor submitted a self-assessment score of 104 out of 110, while an external review calculated the company's actual score to be -142.19

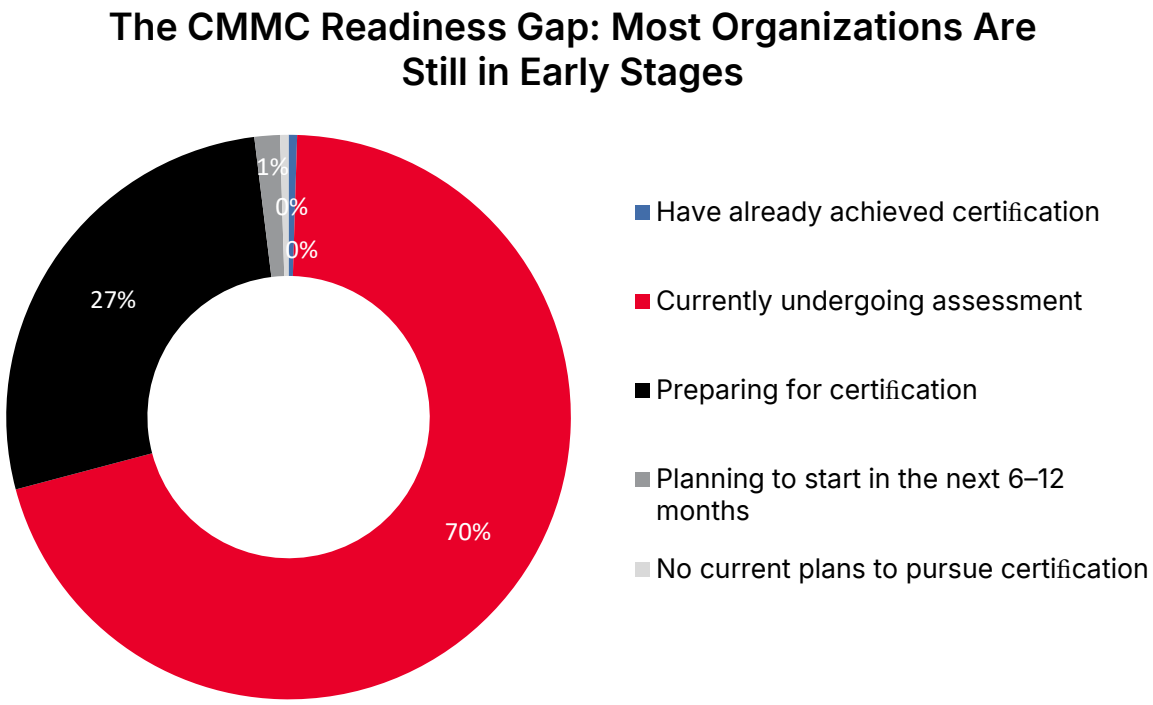


Figure 2. The CMMC Readiness Gap: Most Organizations Are Still in Early Stages

Top CMMC Compliance Barriers

30% Cite Expertise Gaps as Their Biggest Roadblock

DIB contractors face several major operational challenges that create significant barriers to entry. From limited cybersecurity resources to evolving federal requirements and costly validation processes, these challenges represent substantial barriers to entry for many organizations.

- **Cybersecurity Talent Shortage:** The global cybersecurity workforce gap has surged to a record 4.8 million professionals. [7] The United States alone faces more than 500,000 unfilled cybersecurity roles. [8] 30% of respondents cited "internal resources or expertise" as a primary barrier to compliance. This critical talent shortage leaves many SMBs without the in-house expertise needed to interpret and implement the 110 technical controls of CMMC Level 2, forcing them to compete for expensive and scarce external resources.
- **Legacy Infrastructure & Tool Gaps:** Many contractors still rely on outdated IT systems that lack the essential capabilities needed for CMMC compliance. Key controls, such as strong event logging, multi-factor authentication (MFA), and effective vulnerability management, are often absent, leading to costly infrastructure upgrades.
- **MFA and Response Gap:** A November 2023 DoD Inspector General report summarized audits from 2018 to 2023, highlighting failures to enforce multi-factor authentication (MFA) and weak passwords as major cybersecurity issues.[20] A cybersecurity firm's analysis, based on hundreds of contractor assessments, found 73% of clients struggled with correctly implementing MFA and 64% had gaps in incident response. [21]
- **Cost and Resource Constraints:** Achieving compliance is often costly, especially for SMBs. The DoD estimates a Level 2 assessment at $105,000 to $118,000, but this excludes higher costs for remediation, documentation, consulting, and new technology. [9] Total costs can range from $150,000 to over $300,000, making it a prohibitive investment for many small firms lacking funding. [10] As a consultant said, "Limited available capital or budget is preventing organizations from meeting compliance requirements and pursuing certification."

36% of Small Businesses Struggle with Expertise, While CMMC Complexity Stalls 41% of Large Enterprises

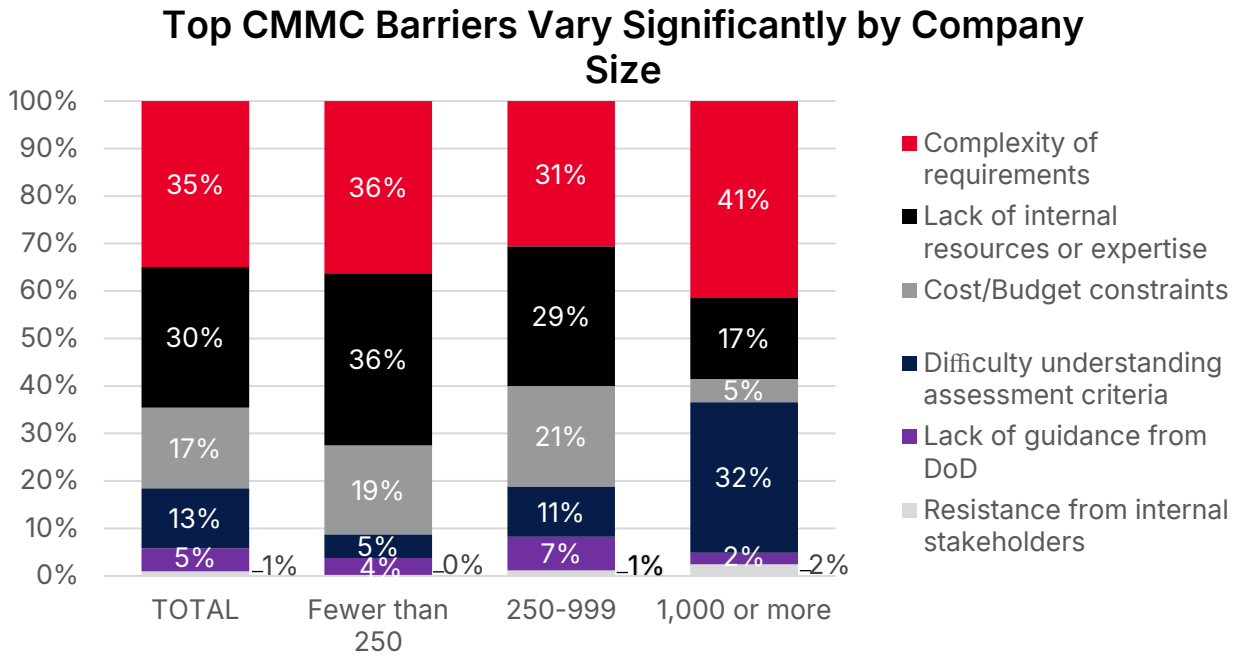


Figure 3. Top CMMC Barriers Vary Significantly by Company Size

These barriers, such as high costs, talent shortages, and technical complexity, are driving market consolidation. Cost and resources are closely connected, impacting small organizations the most, which make up about 70% of the DIB. Many see CMMC as a technical checklist rather than a comprehensive program that includes people, processes, and technology.

Understand the CMMC framework and solutions to help prepare you with confidence.

The High Cost of Inaction: $40M in Recent Settlements

For DIB companies, CMMC has transformed the landscape of risk and competition. Noncompliance now directly threatens revenue and survival, extending beyond fines to include lost contracts, reputational damage, supply chain exclusion, and legal liability under the False Claims Act (FCA).

The Price of "Paper Compliance"

Paper compliance occurs when a company develops policies and procedures to appear compliant but fails to implement them, creating a false sense of security.

The Department of Justice's (DOJ) Civil Cyber-Fraud Initiative has secured multi-million-dollar settlements from contractors accused of falsely claiming cybersecurity compliance, highlighting the serious risks and the government's commitment to accountability. "Paper compliance" without evidence is a risky approach.

Nearly $40M in Settlements Highlight the Cost of Noncompliance — and the List Is Growing

Allegation Summary (Sourced from DOJ Press Releases)	Settlement Amount
Alleged misrepresentations of compliance with DoD cybersecurity clauses (DFARS) related to safeguarding sensitive defense information. [12]	$9,000,000
Alleged failure to meet three required cybersecurity controls for Trusted Internet Connections under GSA contracts. The company received credit for self-disclosure and cooperation. [13]	$4,100,000
Alleged noncompliance with NIST SP 800-171 controls and knowingly submitting an inaccurate (inflated) self-assessment score to the DoD's SPRS system. [14]	$4,600,000
Alleged failure to implement certain NIST SP 800-171 controls and providing an unauthorized foreign third party with access to sensitive defense information. [15]	$1,750,000
DOJ alleged failure to implement required NIST SP 800-171 controls across DoD work, including storing CDI on a development network without required safeguards and lacking an SSP. [22]	$8,400,000
DOJ alleged false certifications of cybersecurity compliance under contracts and failures, such as required vulnerability scanning, reinforcing that non-DIB federal programs are also in scope for cyber FCA actions. [23]	$11,250,000

These cases show a pattern of contractors being penalized for noncompliance and discrepancies between claimed and substantiated compliance. As CMMC formalizes the self-assessment and reporting process, organizations with weak security face legal and financial risks.

From Liability to Verifiability

The immediate consequence of noncompliance is revenue loss. Prime contractors are already actively reducing risks in their supply chains by reviewing subcontractors' security postures and removing noncompliant suppliers from consideration. [20] Some companies are leaving the market, citing certification demands for government contracts as a reason. Those that stay and develop compliance capabilities can gain a competitive edge, with one CEO noting that meeting CMMC standards helps firms win contracts others can't, turning current challenges into long-term advantages.

Beyond satisfying contractual obligations, achieving CMMC compliance enhances both organizational resilience and market competitiveness. It reinforces cybersecurity posture, mitigates breach risks, and demonstrates reliability to customers and partners. By investing in compliance, companies aren’t just meeting requirements — they’re building a durable foundation for growth in a defense ecosystem that prizes security and readiness.

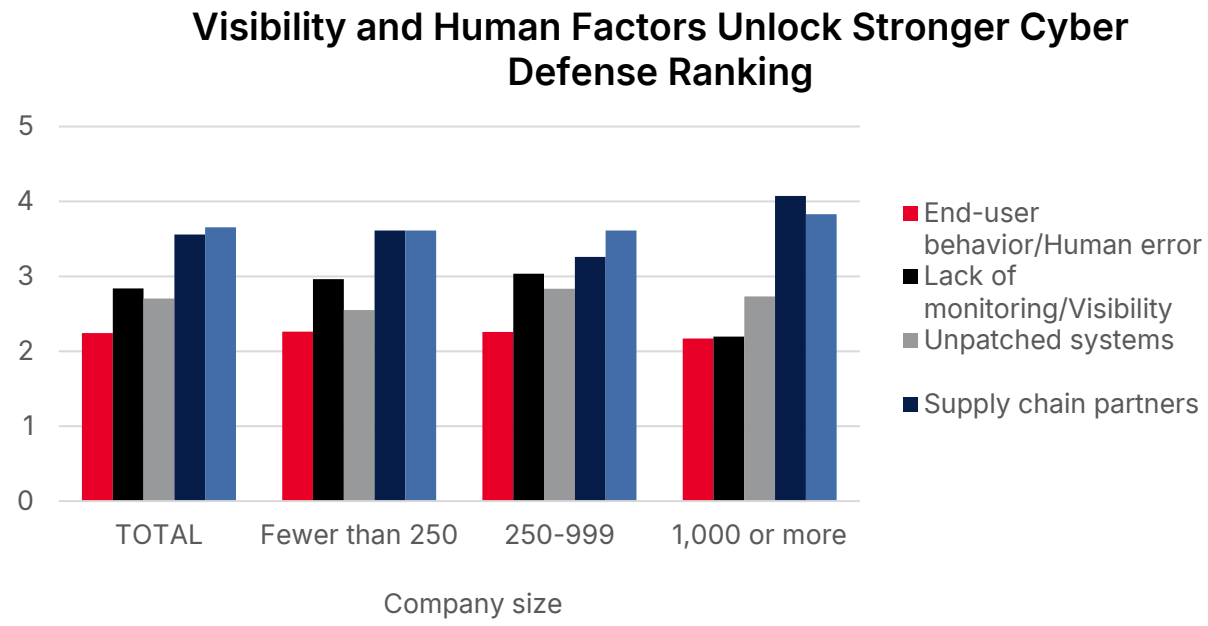


Figure 4. Visibility and Human Factors Unlock Stronger Cyber Defense Ranking 1 (most common) to 5 (least common)

The Path to Certification: A 6-Phase Roadmap

Achieving CMMC certification is a multi-stage process that requires strategic planning, dedicated resources, and a fundamental shift from a reactive to a proactive security posture. Although the process can seem overwhelming, it can be managed effectively with a structured, evidence-based approach. As a CEO who led his company's compliance efforts advises, the first step is to "educate yourself before you hire a third party to do the work for you." A successful CMMC journey progresses through these essential phases, with Keysight's test solutions providing critical support across key points in the process.

Phase 1: Scoping and Self-Assessment

The journey starts with a crucial first step: understanding what needs protection. For many organizations, "the biggest challenge is scoping the project," says a CISO, as they often do not know exactly what CUI they handle or where it is located across their networks. This aligns with the 34% of large companies that report difficulty in understanding assessment criteria and cite insufficient guidance from the DoD. The initial phase involves identifying all systems, assets, people, and data flows that process, store, or transmit CUI, establishing boundaries for the CMMC assessment. A self-assessment against relevant CMMC controls then provides a baseline of the current security posture.

Phase 2: Formal Gap Assessment

A formal gap assessment identifies deficiencies between current security controls and CMMC requirements, utilizing a data-driven approach that offers distinct advantages. While parts of this process are manual, understanding these gaps helps determine where automation can accelerate readiness. For example, organizations can use a tool like Keysight's Threat Simulator to help them meet monitoring requirements to ensure the continued effectiveness of security controls. With the latest automation, Threat Simulator helps continuously test security defenses.

Another automated option is IoT Security Assessment, which provides advanced vulnerability testing. This capability helps identify and reduce cybersecurity risks within IoT ecosystems, strengthening compliance efforts and improving the protection of IoT assets across the DIB.

> To learn how Keysight simplifies risk assessment and compliance, read the Streamline CMMC Risk Assessment & Compliance white paper.

Phase 3: Remediation and Documentation

This phase is often labor-intensive, involving the implementation of new technologies, reconfiguration of systems, and creation of documentation. Activities include deploying security tools, strengthening network configurations, and writing policies directing how each CMMC control is met.

Keysight's Network Taps and Vision Series Network Packet Brokers (NPBs) provide deep visibility and audit trails to monitor and secure network traffic, supporting CMMC domains such as Audit and Accountability (AU) and System and Information Integrity (SI) by ensuring that security tools receive relevant data. TimeKeeper also supports the Audit and Accountability domain by enhancing visibility through precise time synchronization and timestamping, ensuring data integrity and supporting governance.

Phase 4: Validation and Continuous Monitoring

Once controls are implemented, they must be validated and verified. This step ensures compliance is more than paper-based, proving operational readiness. Keysight's Threat Simulator continuously and automatically validates security controls by mimicking real-world attacks, providing audit-ready evidence of effectiveness and mitigation instructions. For zero trust network architectures (ZTNA), Keysight's CyPerf tests that security policies are correctly set to allow the right users access to appropriate resources without excess.

The DIB relies on periodic, manual methods such as single-point-in-time penetration testing, audits, and assessments. It largely lacks insight into the real-time effectiveness of its security controls. Keysight's automated breach-and-attack simulation can directly address this problem. In addition, Vision Orchestrator's intent-based visibility fabric gives organizations centralized control over hundreds of visibility nodes, enabling them to scale and operate visibility solutions across their entire environment.

Of over 200 survey participants, only 3% reported using automated security validation tools to assess their controls, leaving most contractors and subcontractors vulnerable to cybersecurity threats and relying on manual methods such as third-party assessments and internal audits.

Only 3% of DIB Contractors Use Automated Security Validation, while 97% Depend on Manual Audits or External Assessments.

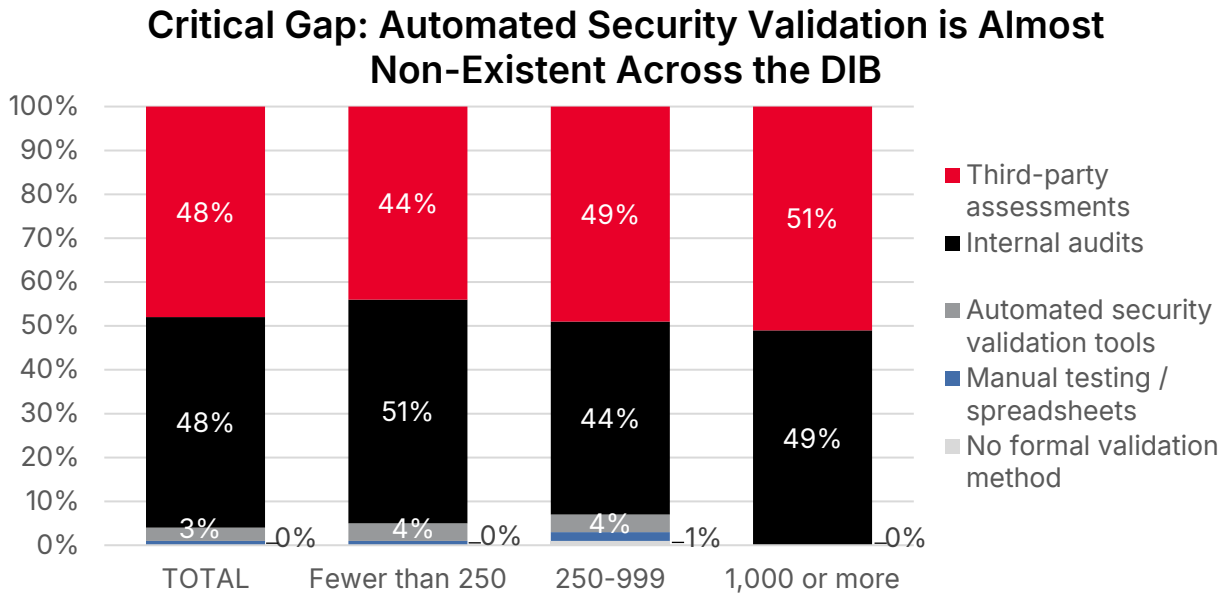


Figure 5. Critical Gap: Automated Security Validation is Almost Non-Existent Across the DIB

Phase 5: Formal Third-Party Assessment

For contractors handling CUI, CMMC certification requires a formal assessment — and passing on the first try is crucial. Due to limited assessor availability, formal CMMC audits already face significant backlogs and long waitlists; one CEO estimated delays of up to five years. Failing an audit can delay reassessment by a year or more, causing organizations to miss critical contract opportunities.

Understanding the specific requirements for each level is essential. CMMC Level 2, based on 110 controls in NIST SP 800-171, may need an annual self-assessment or a triennial assessment by a Certified Third-Party Assessor Organization (C3PAO), depending on the contract. [4] CMMC Level 3 adds controls from NIST SP 800-172 to defend against advanced persistent threats and requires a triennial assessment by the government's Defense Industrial Base Cybersecurity Assessment Center (DIBCAC). [4]

Phase 6: Sustainment and Continuous Improvement

CMMC is an ongoing process, not a one-time event. Certifications remain valid for three years and require annual affirmation to the DoD.[11] This necessitates a program of continuous monitoring, regular training, and ongoing improvement. Keysight's Cyber Training Simulator (KCTS) offers a persistent, live-fire cyber range where security teams can practice incident response, develop procedural memory, and remain prepared for real-world attacks. This hands-on training fulfills CMMC requirements for security training exercises and helps maintain a high level of organizational readiness between formal audits, making compliance a sustainable, operational capability.

Keysight solutions such as Threat Simulator, Vision Series Network Packet Brokers, and Cyber Training Simulator (KCTS) help organizations enhance threat detection, network visibility, workforce training, and breach simulation, helping to identify opportunities for improvement and shape future cybersecurity investments.

For example, as shown in Figure 5, over 83% of survey participants indicated that endpoint detection and response (EDR) remain a top cybersecurity investment priority, highlighting the industry's focus on detection and containment.

Over 50 Percent of Contractors Plan to Invest in Cyber Training and Breach Simulation

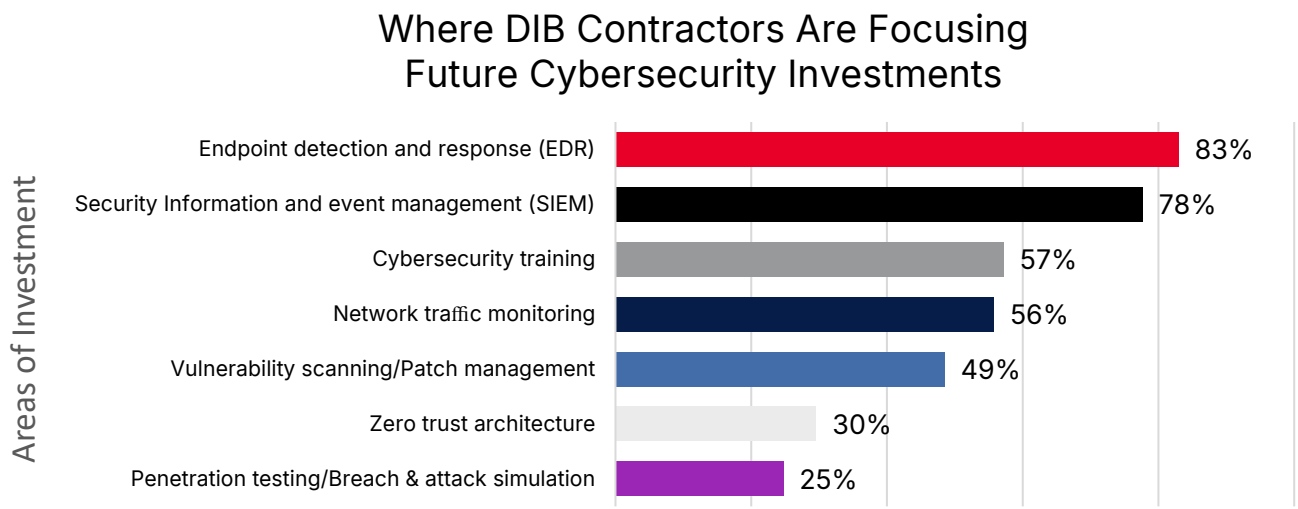


Figure 6. Where DIB Contractors Are Focusing Future Cybersecurity Investments

Use these checklists to navigate the security requirements for Level 1, Level 2, and Level 3 compliance.

Advancing CMMC Readiness Through Trusted Expertise

Keysight is a trusted partner of leading aerospace and defense innovators. Its solutions are embedded in critical design, test, and operational workflows, built on reliable performance, sector expertise, and a commitment to security.

- **Market Leadership:** Keysight maintains the leading position in the test and measurement market, serving the aerospace, defense, and government sectors, with an estimated 23% market share.[21] Its customer base includes all aerospace and defense prime contractors, demonstrating unmatched industry penetration and trust. [22]
- **Deep Sector Experience:** In fiscal year 2024, Keysight reported revenue of $5 billion, with a significant portion driven by the aerospace, defense, and government sectors. [18] This financial achievement reflects a long-term, strategic focus on meeting the specialized needs of the DIB.
- **Comprehensive CMMC Coverage:** Keysight's integrated security solutions provide a platform for achieving and maintaining CMMC readiness. The portfolio enables organizations to test, validate, and strengthen their defenses, helping them meet requirements across 10 of the 14 CMMC domains.[16] From breach-and-attack simulation (Threat Simulator) to network visibility (Vision Series NPBs) and cyber range training (KCTS), Keysight provides the tools to move beyond paper-based compliance to a state of continuous, evidence-based security.

Security Domains

Access Control	Incident Response
Awareness and Training	Risk Assessment
Audit and Accountability	Security Assessment
Configuration Management	System and Communications Protection
Identification and Authentication	System and Information Integrity

Keysight provides the empirical evidence and ongoing validation necessary to transform CMMC from a regulatory challenge into a clear competitive advantage.

Conclusion: Turn CMMC Compliance into Your Competitive Advantage

Join the 2% Who Are Audit-Ready

Market Urgency and Compliance Deadline

CMMC is more than just a new regulation; it is a market-shaping event that is reordering the defense industry. For more than 100,000 companies in the DIB, the era of self-attested, "paper compliance" is now behind us. [1] With CMMC requirements starting to appear in contracts after November 10, 2025, the cost of inaction is a direct threat to contract eligibility and long-term survival. [2]

Why Evidence-Based Compliance Matters

While approximately 30% of respondent organizations remain unprepared — grappling with the talent shortage, outdated systems, and confusion over requirements — a clear path forward exists for those willing to adopt a proactive, evidence-based security approach. [7] The path to CMMC readiness is not about purchasing a single tool or updating a policy document. As experts emphasize, it requires a comprehensive program that integrates people, processes, and technology. True compliance is not claimed; it is demonstrated through ongoing validation, rigorous testing, and clear, empirical evidence that security controls are not only in place but are consistently effective.

Keysight Solutions Strengthen Defenses Across 10 of the 14 CMMC Domains

This is where Keysight offers a unique and essential capability. Unlike vendors offering fragmented point products, Keysight delivers cybersecurity solutions to achieve and maintain CMMC readiness. With solutions including Breach and Attack Simulation (Threat Simulator), Network Visibility (Vision Series NPBs), and Cyber Range Training (KCTS), Keysight helps organizations test, verify, and strengthen their defenses across 10 of the 14 CMMC domains. [20]

This focus on measurable performance enables companies to move beyond the uncertainty of checklists and build a defensible compliance program grounded in objective data. As the DoJ's multi-million-dollar settlements have demonstrated, the only effective defense against noncompliance allegations is verifiable proof. As a trusted, vendor-neutral partner whose solutions are deeply integrated into DIB workflows, Keysight offers more than just technology; it provides the confidence needed to ensure the highest-performing security for your network and applications. [17]

By allowing organizations to verify processes with proven technology, Keysight helps its customers turn the CMMC mandate from a regulatory obligation into a strategic opportunity.

Research Methodology

This white paper relies on independent research by SIS International Research for Keysight Technologies, using a multi-phase, mixed-methods approach. It combines desk research — analyzing the CMMC framework, DIB segmentation, and market mapping — with qualitative and quantitative methods.

Eight qualitative interviews with cybersecurity and compliance experts from small, medium, and large DIB contractors offered insights into their challenges and preparedness. These were supplemented by a survey of 206 decision-makers across different organization sizes and maturity levels.

These findings provide validated, data-driven insights into CMMC awareness, readiness, and barriers, forming the basis of The Power of Proof: Turning CMMC Compliance into Competitive Credibility and reinforcing Keysight's leadership in defense cybersecurity.

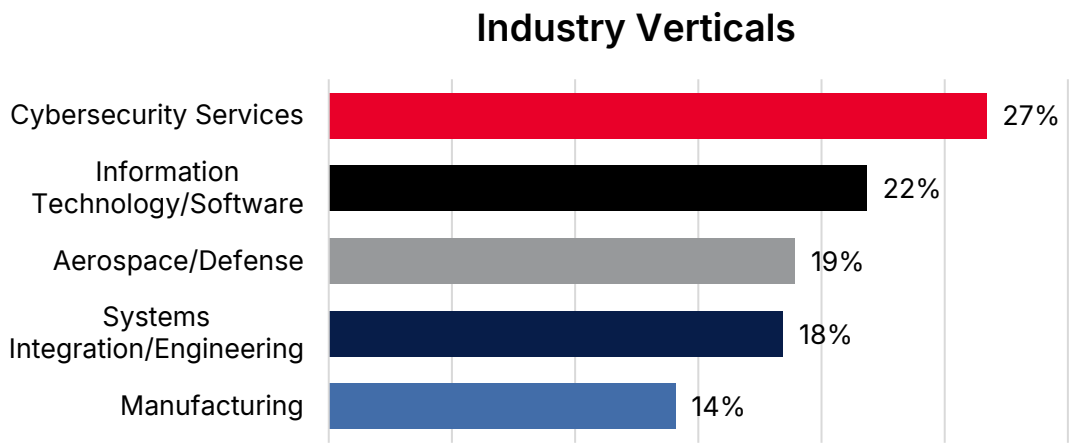


Figure 7. Industry Verticals

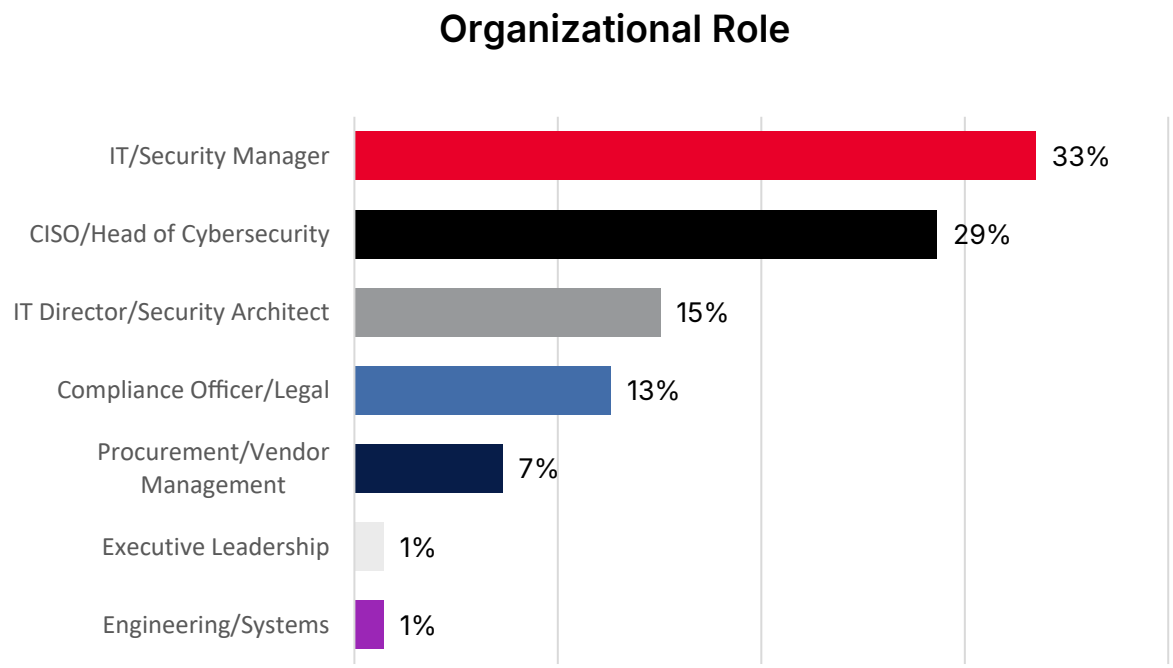


Figure 8. Organizational Role

Appendix: Verified Sources and References

1. Cybersecurity and Infrastructure Security Agency (CISA). (n.d.). Defense Industrial Base Sector. Retrieved October 2025.
2. U.S. Department of Defense. (2025, September 10). Cybersecurity Maturity Model Certification (CMMC) Program. Federal Register.
3. EN Computers. (2025, March). CMMC Compliance Timeline & Deadlines 2025.
4. Thompson Hine LLP. (2025, September 16). DoD Publishes Final CMMC 2.0 Implementation Rule.
5. Davis Wright Tremaine LLP. (2025, September). Defense Department Issues Final Rule to Implement CMMC Cybersecurity Program.
6. Kybersecure. (2025, September 3). How Long Does CMMC 2.0 Implementation Really Take—and Can You Afford to Wait?
7. ISC². (2024). Cybersecurity Workforce Study.
8. CyberSeek. (2025). Cybersecurity Supply/Demand Heat Map. Retrieved October 2025.
9. Secureframe. (n.d.). How Much Does CMMC Certification Cost? Retrieved October 2025.
10. Paramify. (n.d.). How Much Does CMMC Certification Cost in 2025? Retrieved October 2025.
11. U.S. Department of Defense. (n.d.). CMMC 2.0 Levels. DoD CIO. Retrieved October 2025.
12. U.S. Department of Justice, Office of Public Affairs. (2022, July 8). Agrees to Pay $9 Million to Resolve False Claims Act Allegations of Cybersecurity Violations in Federal Government Contracts.
13. U.S. Department of Justice, Office of Public Affairs. (2023, September 5). Cooperating Federal Contractor Resolves Liability for Alleged False Claims Caused by Failure to Fully Implement Cybersecurity Controls.
14. U.S. Department of Justice, Office of Public Affairs. (2025, March 26). Defense Contractor Agrees to Pay $4.6 Million to Settle Cybersecurity Fraud Allegations.
15. McGuireWoods LLP. (2025, August 1). California Defense Contractor and Private Equity Firm Agree to Pay $1.75M to Resolve False Claims Act Liability Relating to Voluntary Self-Disclosure of Cybersecurity Violations. JDSupra.
16. Cybersecurity Maturity Model Certification (CMMC) Program https://www.federalregister.gov/

17. Keysight Technologies. (n.d.). Investor Relations: Why Keysight. Retrieved October 2025.

18. Keysight Technologies, Inc. (2023). Form 10-K for the fiscal year ended October 31, 2023. U.S. Securities and Exchange Commission.

19. Atomus. (2025). DOJ vs Morse: The Cost of Inflated SPRS Scores.

20. Department of Defense Office of Inspector General. (2023, November 30). Special Report: Common Cybersecurity Weaknesses Related to the Protection of DoD Controlled Unclassified Information on Contractor Networks (Report No. DODIG-2024-031).

21. CyberSheath. (n.d.). Top Five Most Difficult Controls to Implement Under NIST 800-171. cybersheath.com.

22. U.S. Department of Justice, Office of Public Affairs. (2025, May 1). Resolve False Claims Act Allegations Relating to Non-Compliance with Cybersecurity Requirements in Federal Contracts.

23. U.S. Department of Justice, Office of Public Affairs. (2025, February 18). Corporation Agrees to Pay Over $11 Million to Resolve False Claims Act Liability for Cybersecurity Violations.