Kiteworks | COALFIRE

REPORT

State of CMMC 2.0 Preparedness in the DIB

www.kiteworks.com

This report is published by Kiteworks and co-sponsored by Coalfire. The survey data was collected and processed by Centiment, an independent research firm specializing in market research for the cybersecurity industry. The analysis and recommendations contained in this report represent the collective expertise of both sponsoring organizations in CMMC 2.0 compliance and cybersecurity best practices for the Defense Industrial Base.

Legal Disclaimer

The information provided in this report is for general informational purposes only and should not be construed as professional advice. Kiteworks, Coalfire, and Centiment make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability of the information contained in this report. Any reliance you place on such information is strictly at your own risk. None of the sponsoring or contributing organizations shall be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from loss of data or profits arising out of, or in connection with, the use of this report. Readers should consult with qualified legal counsel and cybersecurity professionals when addressing specific compliance requirements.

About Kiteworks

Kiteworks' mission is to control, monitor, and protect every data interaction between people, machines, and systems across user collaboration, automated workflows, and Enterprise AI—all from one platform. Kiteworks' platform provides customers with a Private Data Network that delivers data governance, compliance, and protection.

The platform unifies, tracks, controls, and secures sensitive content moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all sensitive content communications. Headquartered in Silicon Valley, Kiteworks protects over 100 million end users for over 35,000 global enterprises and government agencies.

About Coalfire

Coalfire, headquartered in Denver, Colorado, is a global services and solutions company specializing in cyber advisory, assessment, and security. The company develops cutting-edge technology platforms that automate defenses against security threats for the world's leading enterprises, cloud providers, and SaaS companies. Coalfire is the foremost provider of FedRAMP compliance assessments and penetration testing services in the United States.

About Centiment

Centiment is a market research firm specializing in data collection and analysis for the cybersecurity and technology sectors. The company delivers actionable insights through customized survey design, targeted respondent recruitment, and sophisticated analytics. Centiment's proprietary research platform ensures exceptional data quality through AI-driven verification and expert human oversight. The company serves Fortune 500 enterprises, technology vendors, and government agencies, providing intelligence for strategic decisions in evolving markets. Headquartered in Denver, Centiment conducts research globally to help organizations understand complex technology landscapes and cybersecurity trends.

Table of Contents

Executive Summary

This report presents findings from a comprehensive survey of **209 organizations** regarding their readiness for the Cybersecurity Maturity Model Certification (CMMC) 2.0 Level 2 compliance. The survey captured insights from respondents across varied organizational sizes and roles within the Defense Industrial Base (DIB), providing a representative picture of current preparation approaches, implementation challenges, and resource allocation strategies.

The data reveals strong correlations between organizational characteristics and compliance readiness. Organizations that conduct thorough gap analyses demonstrate significantly higher rates of structured compliance preparation, with **73%** of these organizations **maintaining fully documented cybersecurity policies** compared to just **28%** of those that have not started gap analyses. Similarly, **77%** of organizations with **completed gap analyses** follow documented encryption standards with verification, versus **42%** of those yet to begin assessment. **Medium-sized organizations** (500-9,999 employees) show the highest engagement with experienced compliance partners at **50%**, compared to **40%** for small organizations and **41%** for large enterprises, suggesting an optimal balance of resources and needs in this segment.

Documentation maturity emerges as a fundamental indicator of security implementation effectiveness. Organizations with fully documented policies implement encryption standards at dramatically higher rates (**83%**) compared to those with partial documentation (**49%**). This documentation gap extends to third-party access controls, where **75%** of fully documented organizations **maintain advanced controls** versus just **56%** for partially documented entities. Perhaps most concerning, organizations with minimal documentation are 30 times more likely to report inconsistent encryption of controlled unclassified information, highlighting a critical vulnerability in supply chain security.

Leadership perspectives reveal meaningful differences in assessment approaches. Cybersecurity leaders express the most critical evaluation of organizational documentation (**54% reporting full documentation**), contrasting sharply with CEO/Founders (**80%**). This disparity suggests potential communication gaps between technical specialists and executive leadership regarding compliance readiness. Budget allocation follows predictable patterns based on organization size, with **62%** of large organizations reporting **approved budgets with dedicated teams**, compared to just **23%** of small organizations, though timeline projections surprisingly show organizations citing budget constraints often targeting more aggressive certification schedules than those facing technical complexity.

The survey identifies a clear progression in compliance challenges as organizations mature. Early-stage challenges focus on technical understanding and basic control implementation, while advanced-stage issues center on scope definition, partner management, and continuous monitoring. Organizations exhibit distinct patterns in resource allocation and third-party engagement based on these challenge perceptions, with **76%** of organizations **working with experienced partners** achieving fully documented policies, compared to **43% handling compliance independently**. These findings provide actionable insights for organizations at all stages of their CMMC 2.0 Level 2 compliance journey, illuminating successful pathways to both certification and meaningful security improvement.

Organizations completing gap analyses are 73% more likely to have fully documented cybersecurity policies.

Organizations with minimal documentation are 30 times more likely to report inconsistent encryption of CUI.

77% of organizations with a completed gap analysis follow verified encryption standards, versus only 42% who haven't begun.

62% of large organizations have dedicated compliance budgets, compared to just 23% of small organizations.

CMMC Level 2 Overview: Purpose, Scope, and Requirements

The Cybersecurity Maturity Model Certification (CMMC) 2.0 Level 2 establishes a critical security framework designed to protect controlled unclassified information (CUI) within the Defense Industrial Base (DIB). CMMC 2.0 represents a significant refinement of the initial CMMC framework, streamlining the model from five levels to three while maintaining rigorous standards for protecting sensitive defense information (Department of Defense [DoD], 2024a). Level 2 specifically aligns with NIST SP 800-171 and encompasses 110 security controls across 14 domains (National Institute of Standards and Technology [NIST], 2020). Organizations seeking CMMC Level 2 certification must implement all 110 required practices and undergo assessment either through self-assessment (for select contracts) or third-party assessment conducted by a Certified Third-Party Assessment Organization (C3PAO).

The framework aims to reduce the substantial annual losses from intellectual property theft and cyber espionage targeting the defense sector. The Department of Defense developed CMMC to address persistent cybersecurity vulnerabilities throughout its supply chain, recognizing that adversaries frequently target smaller contractors as entry points to access sensitive information (Federal Register, 2024). The certification applies to organizations of all sizes within the DIB that handle CUI, from small sub-contractors to large prime contractors.

CMMC operates alongside and complements several related federal cybersecurity regulations and standards. It builds upon NIST SP 800-171, which forms the foundation for Level 2 requirements, and relates to Federal Acquisition Regulation (FAR) clause 52.204-21, which establishes basic safeguarding requirements for federal contractor information systems (Federal Acquisition Regulatory Council, 2022). The framework also connects to the Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, which mandates adequate security for covered defense information (Defense Federal Acquisition Regulatory Supplement, 2025). This regulatory ecosystem creates a comprehensive approach to securing defense information across the supply chain, with CMMC providing the verification mechanism to ensure actual implementation of required security practices.

CMMC Level 2 At a Glance

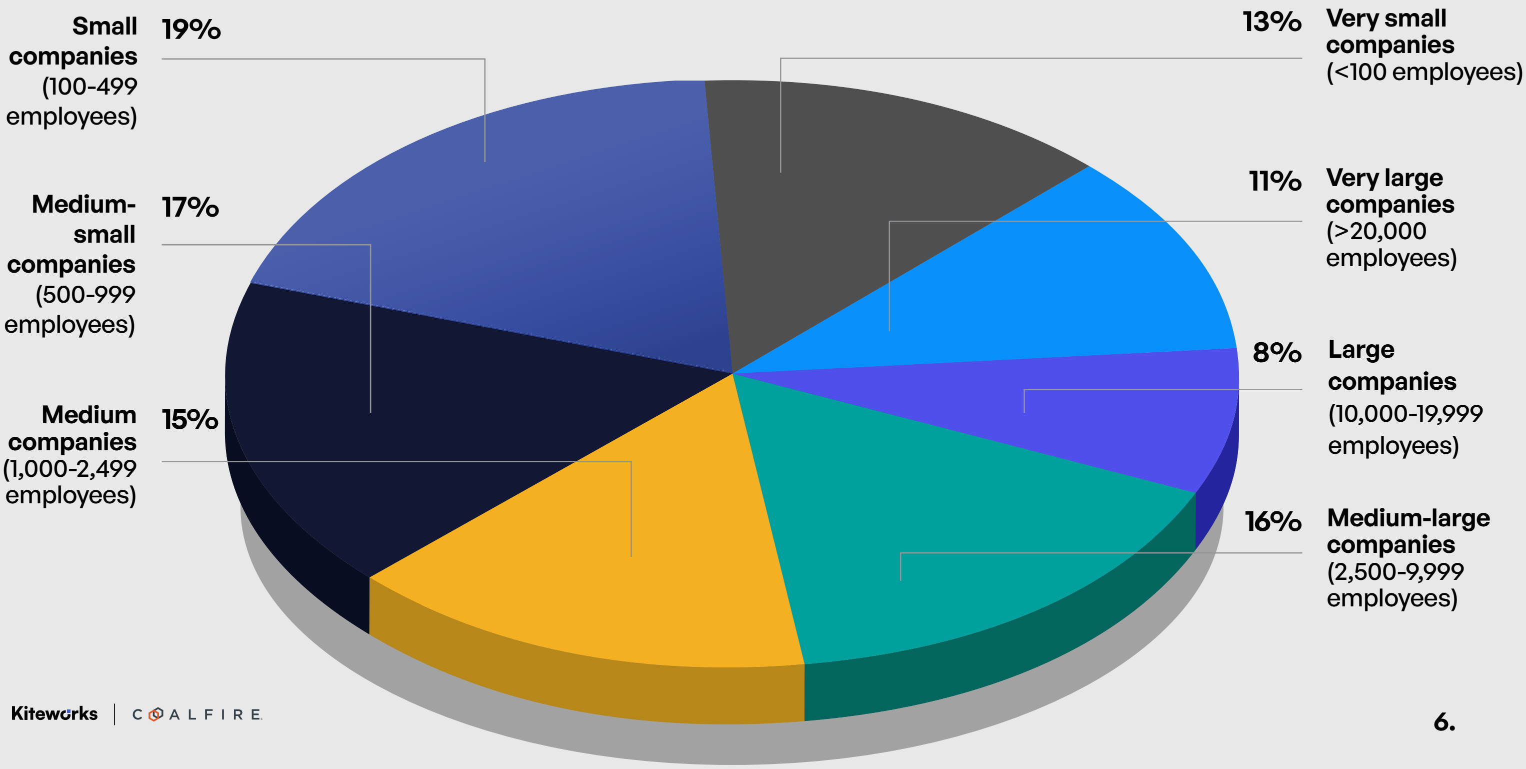
- Directly aligned with **NIST SP 800-171**
- Contains **110 security controls** across 14 domains
- Required for handling **controlled unclassified information (CUI)**
- Certification must be **renewed every three years**

Survey Methodology and Respondent Demographics

The CMMC 2.0 Level 2 readiness survey collected responses from 209 participants representing organizations within the Defense Industrial Base, using 22 targeted questions to assess compliance status, implementation approaches, and challenges. Conducted immediately after the December 2024 publication of the 32 CFR Final Rule, the survey captured organizations' responses to finalized requirements. Respondent organizations spanned all size categories: small organizations with fewer than 500 employees (32%), mid-sized organizations with 500-9,999 employees (48%), and large organizations with 10,000+ employees (20%). The survey included diverse leadership perspectives: CIO/IT Leaders (20%), Cybersecurity Leaders (17%), CEO/Founders (14%), Risk Management Leaders (15%), General Counsel/Legal Leaders (8%), COOs (4%), and CFOs (1%). This distribution enables analysis of how organizational size and leadership roles influence CMMC readiness approaches. Data analysis focused on identifying correlations between organizational characteristics and compliance approaches, examining relationships between gap analysis completion, documentation maturity, and implementation of critical security controls. For clearer pattern identification, responses were grouped into three categories: small (<500 employees), medium (500-9,999 employees), and large organizations (10,000+ employees).

Survey Participation by Company Size

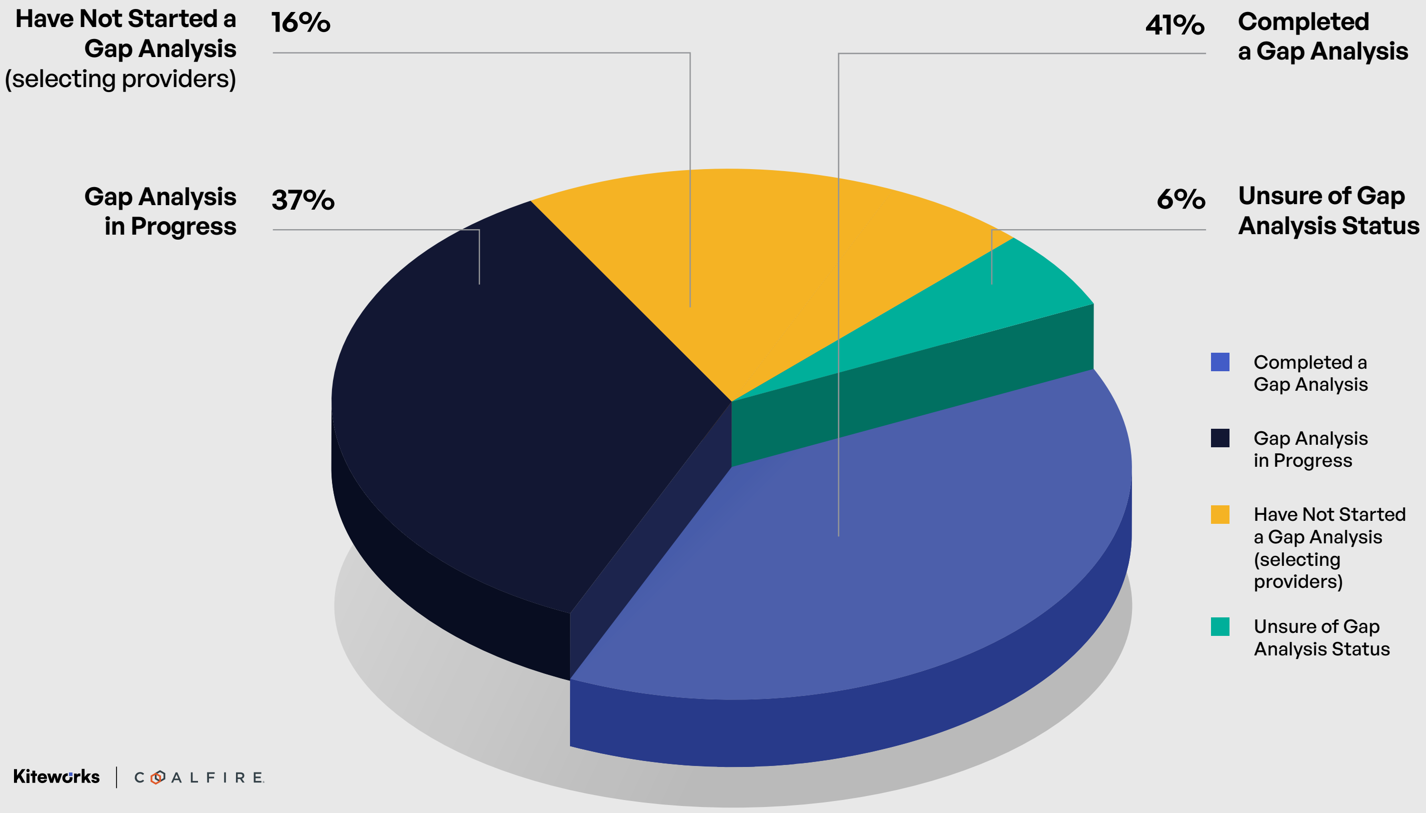
The survey revealed balanced participation across company sizes:



Gap Analysis Completion and Its Impact on CMMC Readiness

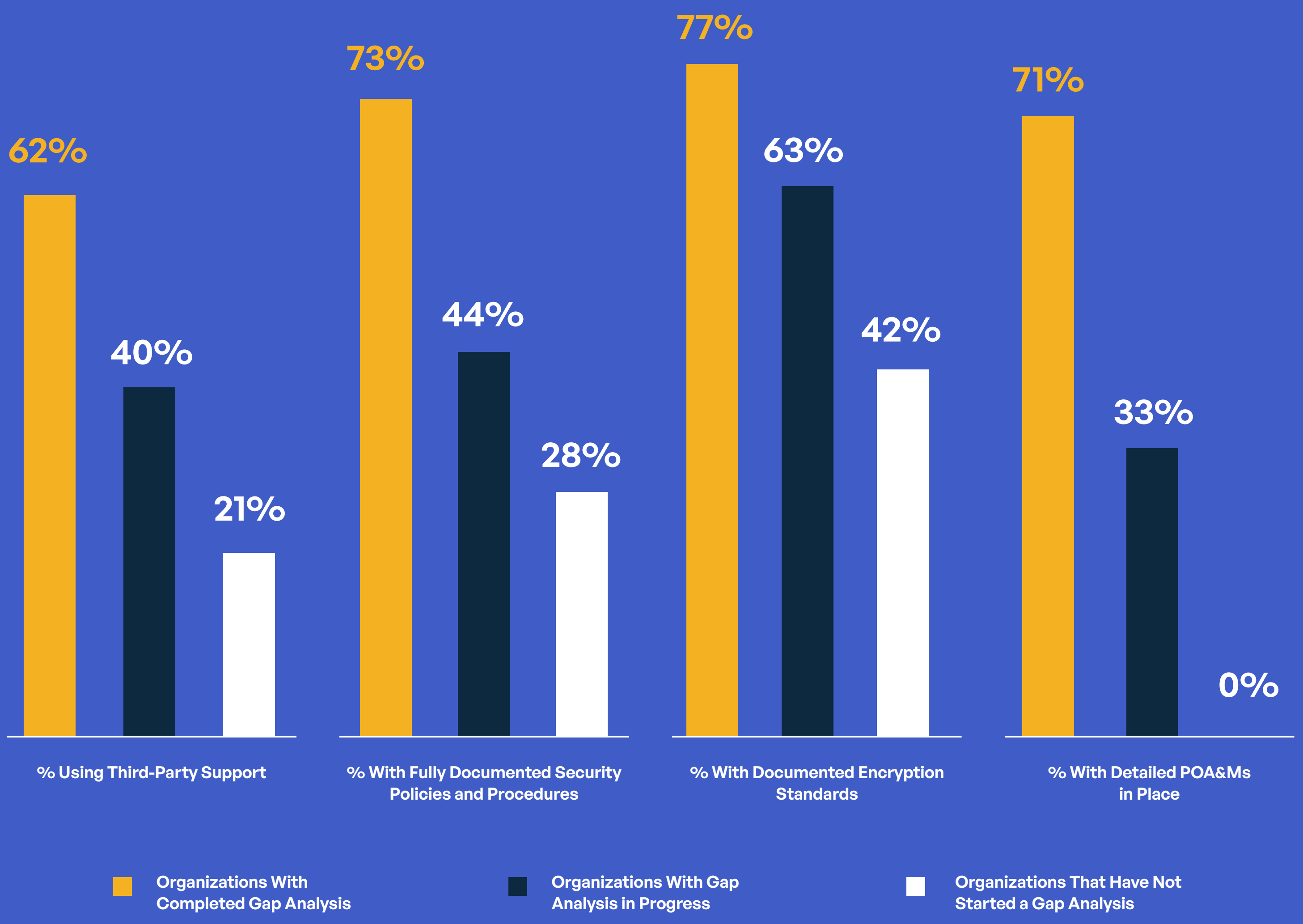
The completion of a formal gap analysis against NIST SP 800-171 requirements represents a fundamental early step in CMMC 2.0 Level 2 preparation, establishing a baseline understanding of organizational security posture. The survey revealed significant variation in gap analysis status across respondent organizations, with important implications for overall compliance readiness. Among surveyed organizations, 41% reported having completed a thorough gap analysis, while 37% indicated their gap analysis was currently in progress. A concerning 16% had not yet started but planned to begin soon, and 6% were unsure of their gap analysis status, suggesting potential communication issues within those organizations or more likely, a lack of planning to begin a gap analysis.

Completed a Gap Analysis



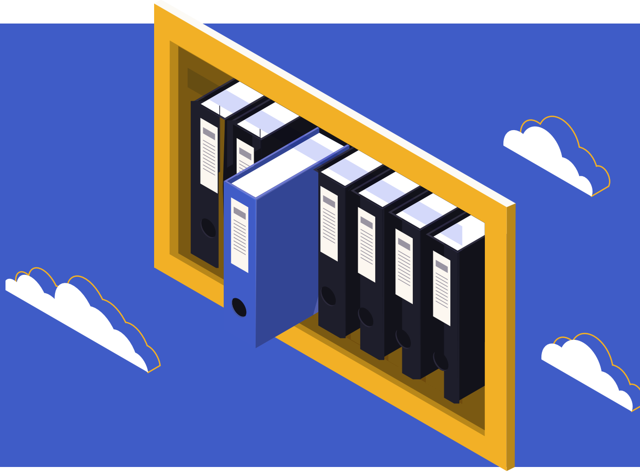
Organizations that completed thorough gap analyses demonstrated markedly different approaches to CMMC compliance compared to those at earlier stages. Most strikingly, organizations with completed gap analyses were significantly more likely to have already engaged experienced external partners, with 62% working with third-party consultants, Registered Provider Organizations (RPOs), or C3PAOs, compared to just 40% of organizations with gap analyses in progress and 21% of those that had not yet started. This pattern suggests that thorough gap analyses help organizations recognize compliance complexities and the value of specialized, external expertise.

Completed Gap Analysis Creates Organizational Security Maturity



The relationship between gap analysis completion and documentation maturity reveals another critical pattern. Organizations with completed gap analyses reported higher rates of fully documented cybersecurity policies and procedures (73%) compared to those with analyses in progress (44%) or not yet started (28%). This correlation highlights how gap analyses drive concrete documentation improvements by identifying specific deficiencies requiring remediation.

Organizational Security Maturity and Gap Analysis



73% With Completed Gap Analysis Have Fully Documented Security Policies and Procedures

44% With Gap Analysis in Progress Have Fully Documented Security Policies and Procedures

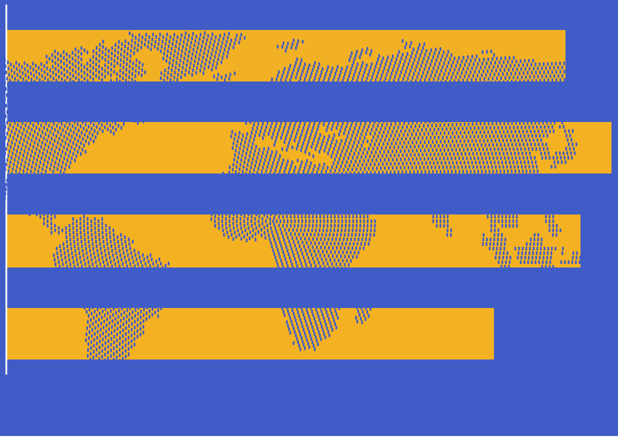
28% That Have Not Started a Gap Analysis Have Fully Documented Security Policies and Procedures

Gap analysis status also correlates strongly with encryption implementation. Among organizations with completed gap analyses, 77% reported following documented encryption standards with verification of implementation. This percentage drops to 63% for organizations with gap analyses in progress and just 42% for organizations that had not yet started. These differences emphasize the role of gap analyses in identifying and driving remediation of specific technical control deficiencies.

Plan of Action and Milestones (POA&M) development shows perhaps the strongest correlation with gap analysis status. Organizations with completed gap analyses were more than twice as likely to have detailed POA&Ms with assigned responsibilities and timelines (71%) compared to those that had not yet started gap analyses (33%). This finding underscores the practical operational value of gap analyses in structuring remediation efforts.

The survey also revealed interesting patterns in the relationship between gap analysis completion and organizational size. Large organizations (10,000+ employees) reported the highest rate of completed gap analyses at 47%, compared to 40% for medium organizations (500-9,999 employees) and 38% for small organizations (<500 employees). However, medium-sized organizations showed the highest percentage of in-progress gap analyses (42%), suggesting active engagement with compliance requirements but potential resource constraints in completing assessments.

Organizations That Have Completed a Gap Analysis



62% work with experienced compliance partners (vs. 21% of those not started)

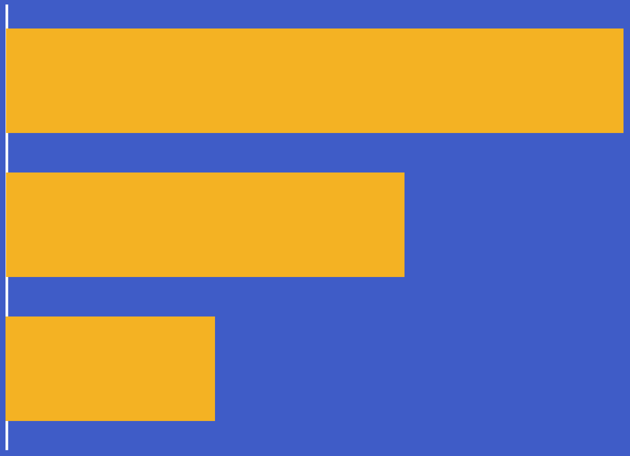
73% have fully documented policies (vs. 28% of those not started)

77% follow verified encryption standards (vs. 42% of those not started)

71% have detailed POA&Ms with assigned responsibilities (vs. 33% of those not started)

The correlation between gap analysis completion and third-party engagement strategies reveals important patterns in how organizations approach compliance assistance. Organizations with completed gap analyses not only engage external partners at higher rates but also show more discernment in partner selection. Among organizations with completed gap analyses that engage external partners, 76% work with experienced partners rather than those still in the selection process. In contrast, organizations with gap analyses in progress show a nearly even split between working with experienced partners (48%) and selecting partners (52%). This pattern suggests that gap analyses help organizations identify specific expertise needs, enabling more targeted partner selection.

Difference Experienced Third Parties Make



62% Organizations With Completed Gap Analysis That Used a Third Party (vs. 76% Used an Experienced Third Party)

40% Organizations With Gap Analysis in Progress That Used a Third Party (vs. 48% Are Using an Experienced Third Party)

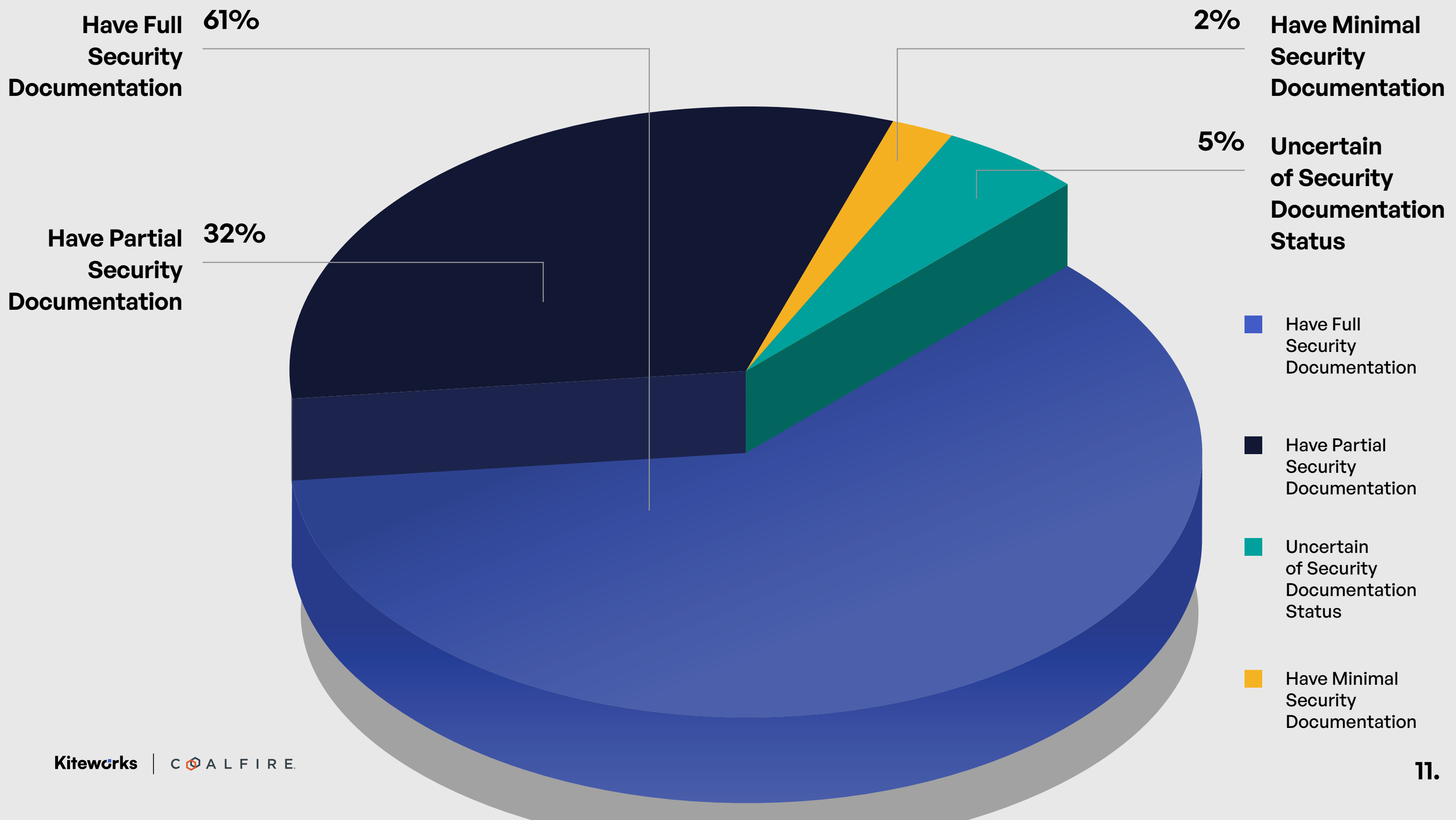
21% Organizations That Have Not Started a Gap Analysis But Have Engaged a Third Party (vs. 52% Have Engaged an Experienced Third Party)

The survey data makes clear that organizations at different stages of gap analysis completion face significantly different CMMC readiness challenges. Organizations that have not completed gap analyses tend to struggle with fundamental questions about requirements applicability and scope, while those with completed analyses focus more on specific technical implementation challenges and resource allocation. This progression underscores the critical role of gap analyses in moving organizations from general awareness to specific, targeted compliance efforts.

Documentation Maturity and Security Control Implementation

The survey results reveal a fundamental relationship between the maturity of an organization's cybersecurity documentation and its effectiveness in implementing specific security controls required for CMMC 2.0 Level 2. Documentation maturity serves as both an indicator of overall cybersecurity governance and a practical foundation for consistent control implementation. Among surveyed organizations, 61% reported fully documented and regularly updated cybersecurity policies and procedures, 32% indicated partial documentation with updates ongoing, 2% reported minimal documentation with plans for significant updates, and 1% were unsure of their documentation status.

Security Documentation



The correlation between documentation maturity and encryption implementation stands out as particularly significant. Among organizations with fully documented policies and procedures, 83% reported following documented encryption standards with verification of implementation. This percentage drops dramatically to 49% for organizations with partially documented policies and 0% for those with minimal documentation. Even more telling, organizations with minimal documentation were 30 times more likely to report inconsistent encryption of CUI (60%) compared to organizations with fully documented policies (2%). These stark differences highlight how comprehensive documentation creates the foundation for consistent, verifiable security control implementation.

60%

of organizations with minimal security documentation are 30x more likely to report inconsistent encryption of CUI.

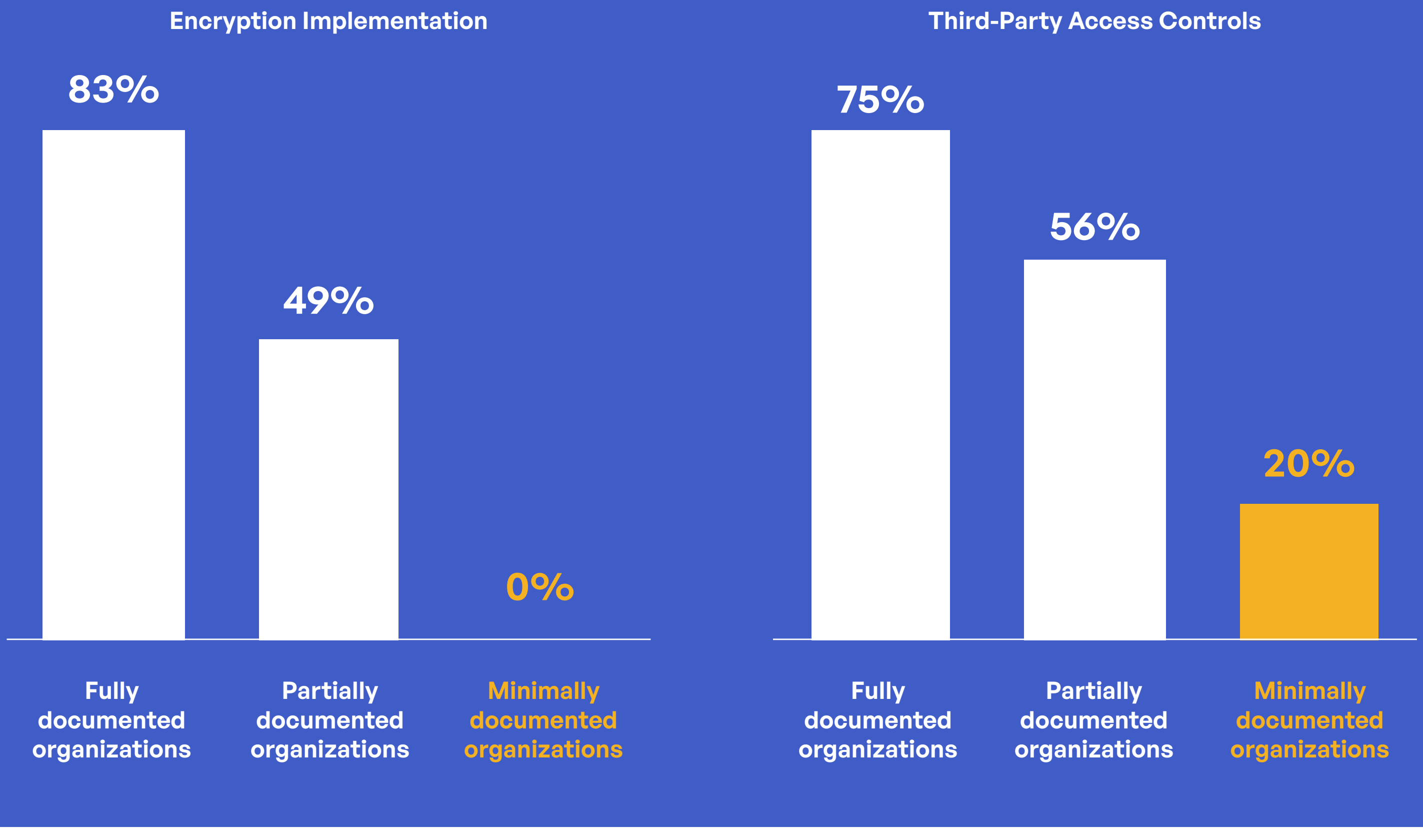
Third-party access controls show similar patterns related to documentation maturity. Of organizations with fully documented policies, 75% reported having advanced controls and systems to ensure third parties can only access authorized CUI. This percentage decreases to 56% for organizations with partially documented policies and just 20% for those with minimal documentation. This pattern demonstrates how mature documentation practices support the implementation of complex technical controls that require clear definitions, processes, and verification mechanisms.

Documentation maturity also correlates strongly with stakeholder involvement in CMMC readiness efforts. Organizations with fully documented policies were more than twice as likely to report highly collaborative approaches with regular cross-functional meetings (56%) compared to those with partially documented policies (26%). This relationship highlights how mature documentation practices both require and facilitate broader organizational engagement, creating a positive feedback loop that enhances overall security governance.

The survey revealed interesting variations in documentation maturity across company sizes. Large organizations (10,000+ employees) reported the highest rate of fully documented policies at 68%, compared to 63% for medium organizations (500-9,999 employees) and 58% for small organizations (<500 employees). However, the percentage of organizations with minimal or uncertain documentation remained consistently low across all size categories (3%-4%), suggesting that basic documentation awareness exists regardless of organizational resources.

The Documentation-Security Implementation Link

The survey reveals dramatic differences in security control implementation based on documentation maturity:



Perceptions of documentation maturity varied notably based on respondent role, revealing important differences in how functional areas assess documentation quality. CEO/Founders reported the highest rate of fully documented policies (80%), while Cybersecurity Leaders reported a significantly lower rate (54%). This disparity suggests potential communication gaps or differences in assessment standards, with technical specialists likely applying more rigorous criteria than executive leadership. COO respondents reported the lowest rate of fully documented policies (33%) and the highest rate of partial documentation (67%), possibly reflecting operational concerns about policy implementation challenges.

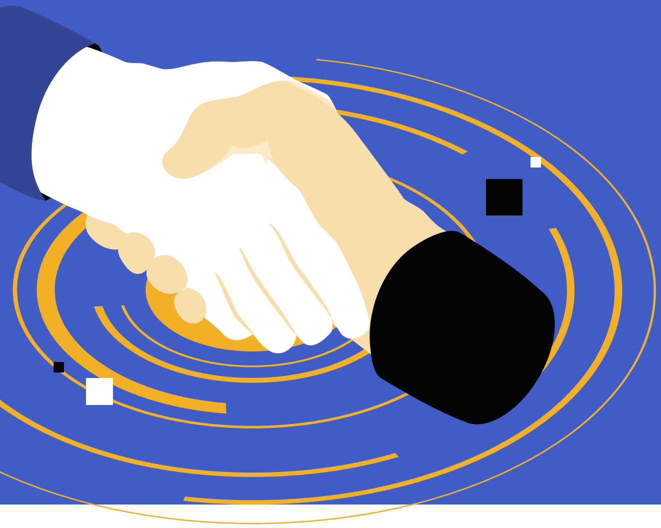
The relationship between documentation maturity and Plan of Action & Milestones (POA&M) development provides another indicator of documentation's role in structured compliance approaches. Organizations with fully documented policies were three times more likely to have detailed POA&Ms with assigned responsibilities and timelines (67%) compared to those with partially documented policies (22%). This pattern suggests that mature documentation practices facilitate the transition from general awareness to specific, actionable compliance planning.

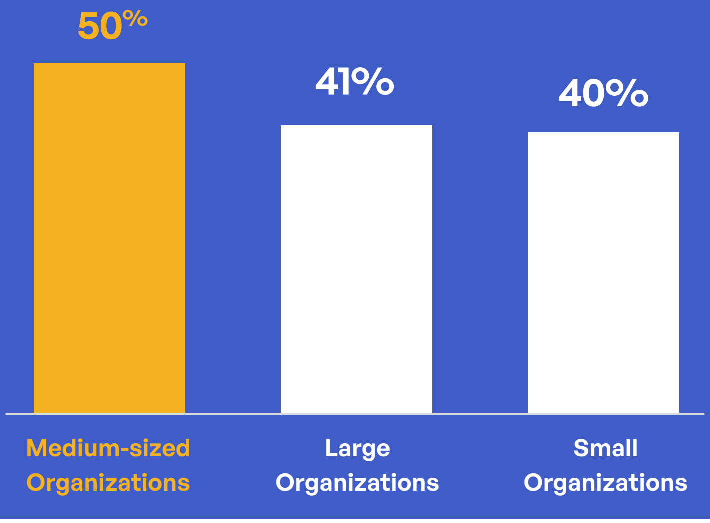
The survey data reveals not just a correlation but a potential causal relationship between documentation maturity and security control implementation. Organizations with fully documented policies demonstrate substantially better performance across all measured security control areas, from access control and encryption to incident response and third-party management. This pattern suggests that comprehensive documentation creates the necessary foundation for effective security implementation by establishing clear requirements, responsibilities, and verification mechanisms.

Third-Party Engagement Patterns and Effectiveness

The relationship between organizational size and third-party engagement reveals important patterns in how different organizations approach external expertise. Medium-sized organizations (500-9,999 employees) showed the highest rate of engagement with experienced partners at 50%, compared to 40% for small organizations (<500 employees) and 41% for large organizations (10,000+ employees). This pattern suggests that medium-sized organizations occupy a particular position where they have sufficient resources to engage external support but may lack the extensive internal expertise found in larger organizations. Small organizations showed the highest rate of handling compliance in-house (22%), equal to large organizations but likely for different reasons—resource constraints for small organizations versus extensive internal capabilities for large ones.

Engagement With Experienced Partners





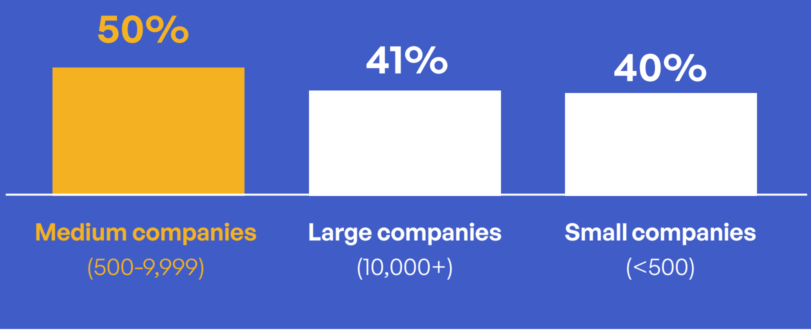
External partner engagement correlates strongly with perceived compliance readiness across multiple dimensions. Organizations working with experienced partners were significantly more likely to report following verified encryption standards (84%) compared to those handling compliance in-house (61%) or those still selecting partners (54%). Similar patterns appeared for third-party access controls, incident response readiness, and compliance budget allocation. These correlations highlight how external expertise can accelerate and enhance compliance preparation across multiple domains.

The relationship between leadership roles and third-party engagement reveals important differences in how functional areas approach compliance assistance. CEO/Founders reported the highest rate of engagement with experienced partners (57%), closely followed by CIO/IT Leaders (57%). In contrast, Cybersecurity Leaders reported the lowest rate of partner engagement (31%) and the highest rate of handling compliance in-house (34%). These differences likely reflect varying assessments of internal capabilities, with specialized cybersecurity leaders more confident in internal resources than generalist executives.

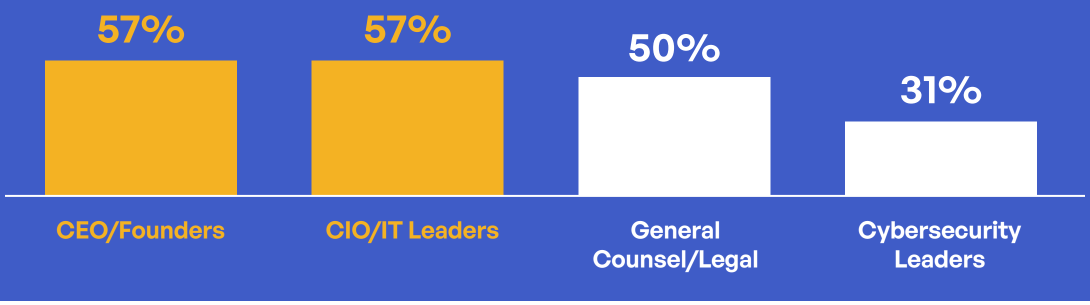
Who Engages External CMMC Experts?

The survey reveals interesting patterns in which organizations work with experienced compliance partners:

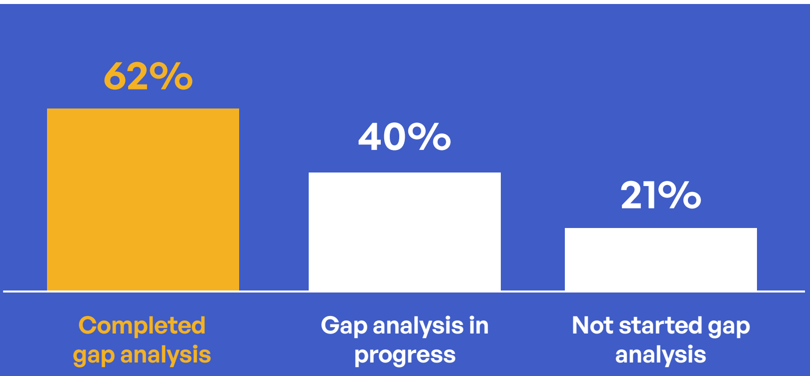
By company size:



By leadership role:



By gap analysis status:



Organizations that engage with experienced CMMC partners are nearly twice as likely to achieve fully documented policies, well-defined assessment scopes, and formal third-party risk management programs—critical success factors that directly impact certification readiness and compliance sustainability.

Organizations engaged with external partners reported different challenges compared to those handling compliance in-house. Partner-engaged organizations more frequently cited budget constraints (38%) and executive buy-in (22%) as primary challenges, while organizations handling compliance in-house more often identified technical complexity (47%) and understanding requirements (34%) as key obstacles. This divergence suggests that external partners effectively address technical and interpretive challenges but may increase resource demands and organizational change requirements.

The timing of partner engagement appears to influence overall compliance approach. Organizations that engaged partners early in their compliance journey (before completing gap analyses) reported higher rates of comprehensive readiness efforts, including formal vendor management programs (68%) and centralized remediation tracking systems (71%). This pattern suggests that early external guidance helps establish more structured, comprehensive compliance approaches from the outset.

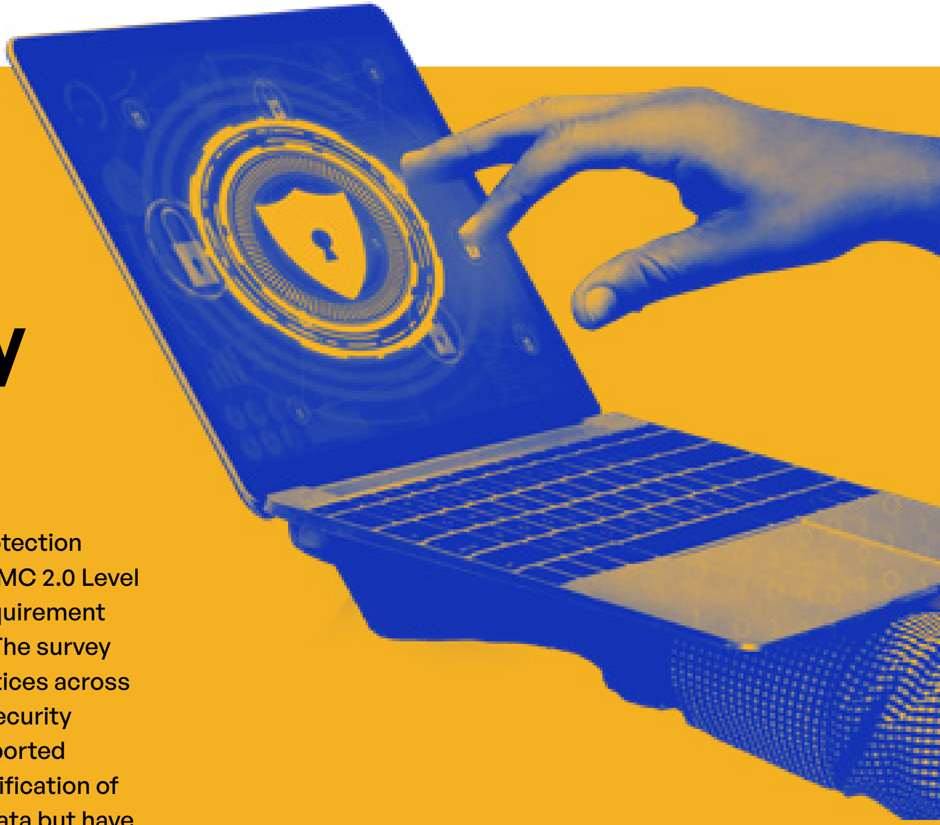
Of those organizations that engage partners early in their compliance journey, nearly

7 out of 10

organizations have formal vendor management programs, and more than 7 out of 10 have remediation systems.

The specific type of third-party engagement shows interesting correlations with organization size and compliance maturity. Small organizations more frequently reported working with general cybersecurity consultants (48%), while medium and large organizations more often engaged specialized RPOs or C3PAOs (57% and 64%, respectively). This difference likely reflects both resource availability and compliance complexity, with larger organizations requiring more specialized expertise focused specifically on CMMC requirements.

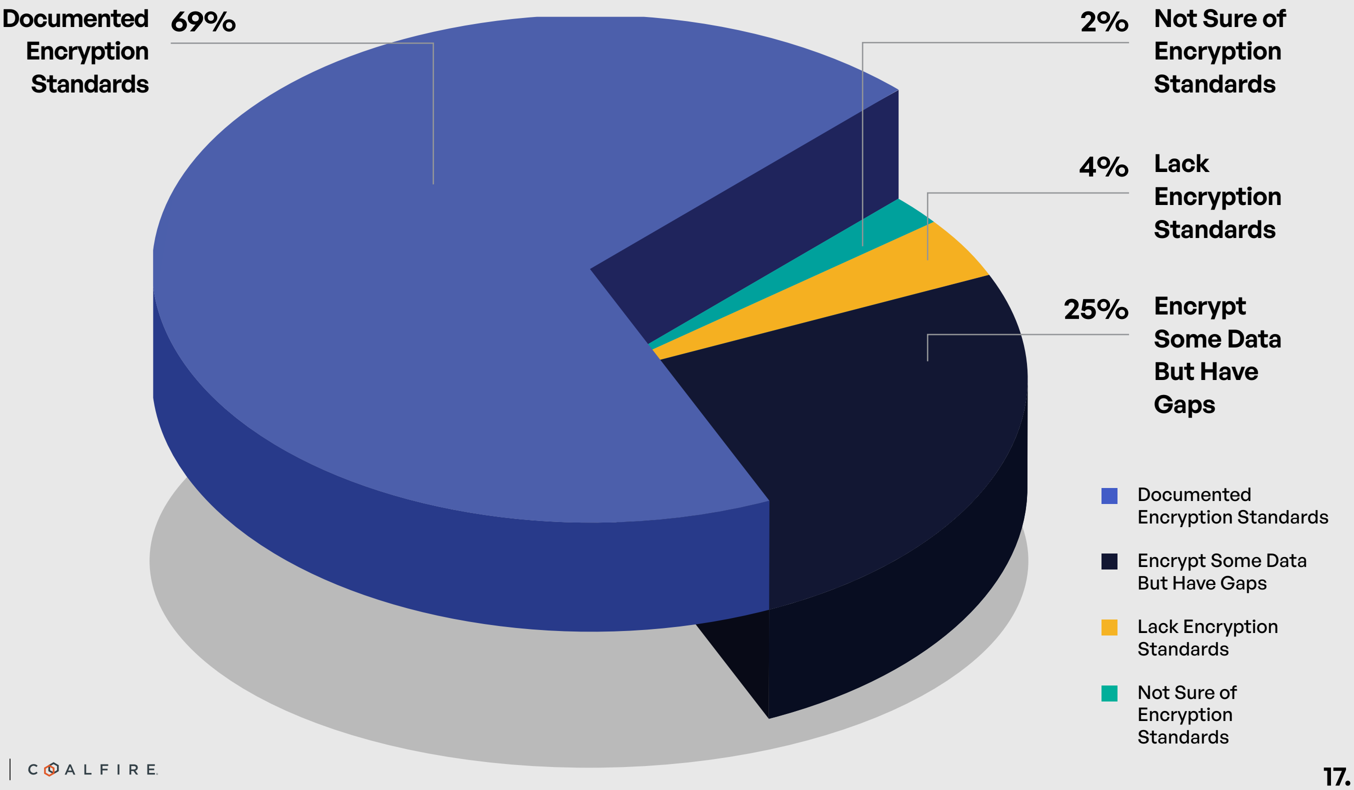
The survey results suggest that external partner engagement yields particular benefits for specific compliance dimensions. Partner-engaged organizations showed especially strong performance in documentation (76% fully documented versus 43% for in-house), scoping definition (63% well-documented versus 27% for in-house), and third-party risk management (72% formal programs versus 39% for in-house). These areas require specialized knowledge and typically benefit from external perspective and experience with similar organizations.



Encryption Practices and Overall Security Posture

The implementation of encryption and other data protection methods for CUI represents a critical element of CMMC 2.0 Level 2 compliance, serving as both a specific technical requirement and an indicator of overall security control maturity. The survey results reveal significant variation in encryption practices across organizations, with important correlations to other security dimensions. Among surveyed organizations, 69% reported following documented encryption standards with verification of implementation, 25% indicated they encrypt some data but have gaps to address, 4% acknowledged not consistently encrypting CUI at rest or in transit, and 2% were unsure of their encryption status.

Encryption Maturity



The correlation between encryption implementation and company size reveals modest but notable differences in approach. Large organizations (10,000+ employees) reported the highest rate of following documented encryption standards at 71%, compared to 69% for medium organizations (500-9,999 employees) and 67% for small organizations (<500 employees). These relatively small differences suggest that encryption implementation may be less resource-dependent than other security controls, with organizations of all sizes recognizing its fundamental importance for protecting sensitive information.

Organizations following documented encryption standards demonstrated significantly stronger performance across all other measured security dimensions. These organizations were more likely to have fully documented security policies (73% versus 29% for those with encryption gaps), detailed POA&Ms (65% versus 23%), advanced third-party access controls (75% versus 49%), and formal vendor management programs (74% versus 28%). This pattern suggests that robust encryption implementation typically exists within a broader context of mature security practices.

Organizations With Documented Encryption Standards

	Fully Documented Security Policies	Detailed POA&Ms	Advanced Third-Party Access Controls	Formal Vendor Management Programs
YES	73%	65%	75%	74%
NO	29%	23%	49%	28%

The relationship between encryption status and third-party engagement strategies reveals important patterns in how organizations address encryption challenges. Organizations still in the process of selecting partners showed the highest rate of encryption gaps (42%), compared to those already working with partners (15%) or handling compliance in-house (25%). This pattern suggests that organizations often recognize encryption gaps early in their compliance journey, driving them to seek external expertise to address these technical challenges.

Encryption implementation showed strong correlation with perception of compliance challenges. Organizations following documented encryption standards most frequently identified budget constraints (34%) and executive buy-in (19%) as primary challenges. In contrast, organizations with encryption gaps or inconsistent implementation more often cited technical complexity (59%) and understanding requirements (41%). This divergence suggests that organizations overcome technical challenges as they mature their encryption practices but then face resource and organizational challenges for broader compliance efforts.

Encryption as a Security Maturity Indicator

Organizations following documented encryption standards demonstrate stronger security across all dimensions:

73% **have fully documented security policies** (vs. 29% with encryption gaps)

65% **have detailed POA&Ms** (vs. 23% with encryption gaps)

75% **have advanced third-party access controls** (vs. 49% with encryption gaps)

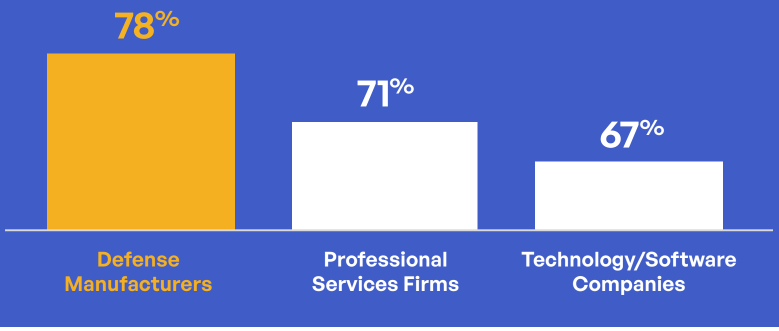
84% **conduct periodic or continuous monitoring** (vs. 57% with encryption gaps)

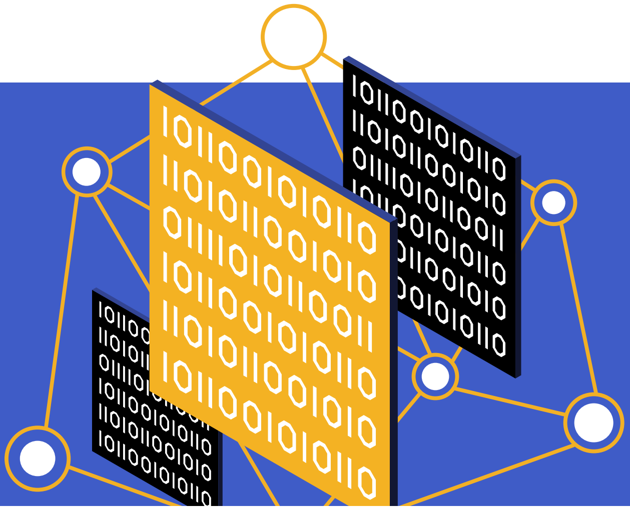
74% **have formal vendor management programs** (vs. 28% with encryption gaps)

The relationship between encryption implementation and security awareness training programs reveals an important connection between technical controls and human factors. Organizations following documented encryption standards reported much higher rates of fully updated and regularly tested security awareness programs (63%) compared to those with encryption gaps (21%). This correlation highlights how organizations with mature technical security controls recognize the importance of complementary human-focused security measures.

Industry sector analysis reveals interesting patterns in encryption implementation. Defense manufacturing organizations reported the highest rate of following documented encryption standards (78%), followed by professional services firms (71%) and technology/software companies (67%). These differences likely reflect variations in experience with handling sensitive information and prior compliance requirements, with defense manufacturers typically having longer experience with DoD information protection requirements.

Industries With Documented Encryption Standards



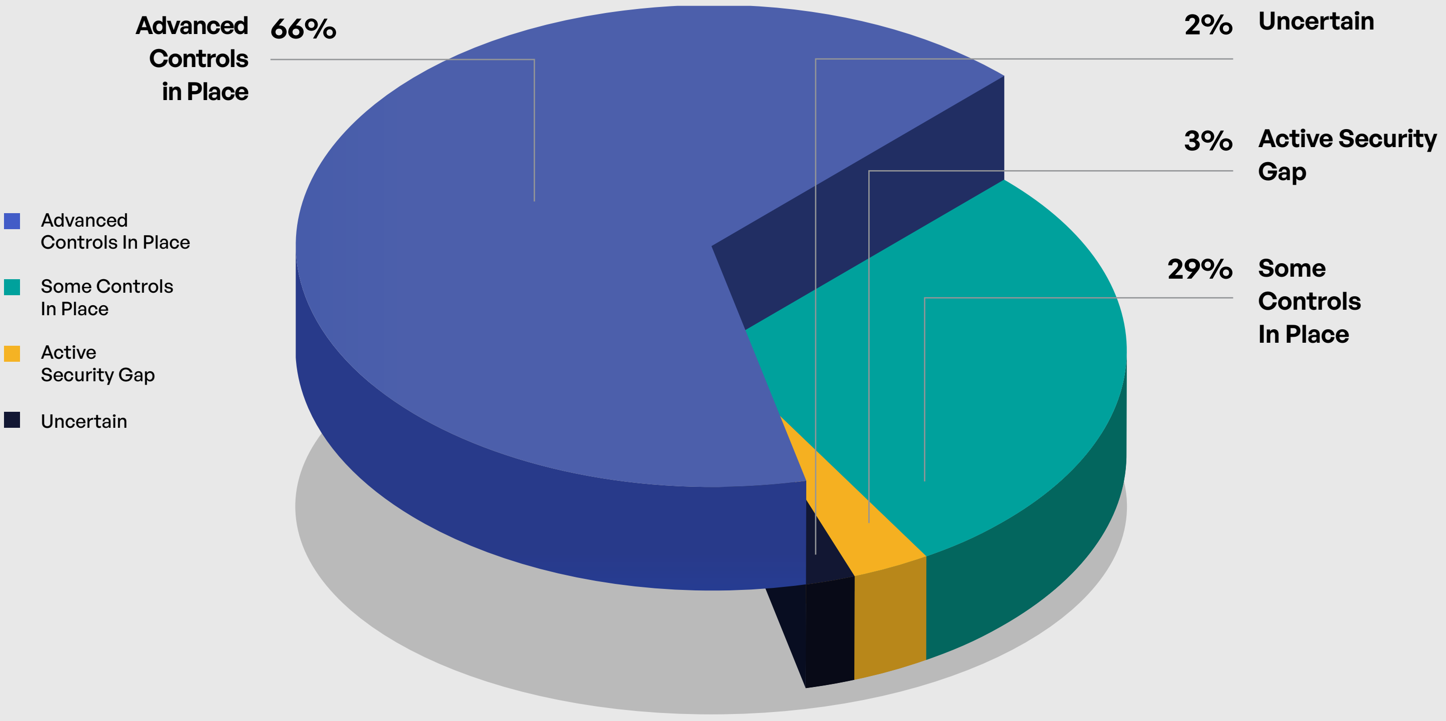


The particular value encryption places within the CMMC framework makes it a critical focus area for compliance efforts. Encryption represents one of the most technically complex control areas within NIST SP 800-171 but also one of the most essential for protecting sensitive information. The survey results suggest that organizations recognize this importance, with even resource-constrained small organizations prioritizing encryption implementation at rates similar to larger organizations with more extensive resources.

Third-Party Access Controls and Supply Chain Security

The implementation of governance tracking and controls for third-party access to CUI represents a critical element of CMMC 2.0 Level 2 compliance, addressing the substantial risks associated with supply chain security. The survey results highlight significant variation in third-party access control maturity across organizations, with important implications for overall security posture. Among surveyed organizations, 66% reported having advanced controls and systems in place for third-party CUI access, 29% indicated they have some controls but lack full visibility and control, 3% acknowledged this as an active gap they are working to address, and 2% were unsure of their control status.

Third-Party Access for CUI



The correlation between third-party access controls and company size reveals important patterns in supply chain security approaches. Large organizations (10,000+ employees) reported the highest rate of advanced controls at 71%, compared to 63% for medium organizations (500-9,999 employees) and 67% for small organizations (<500 employees). This relatively even distribution suggests that organizations across size categories recognize the importance of third-party access controls, though implementation approaches may differ based on resources and supply chain complexity.

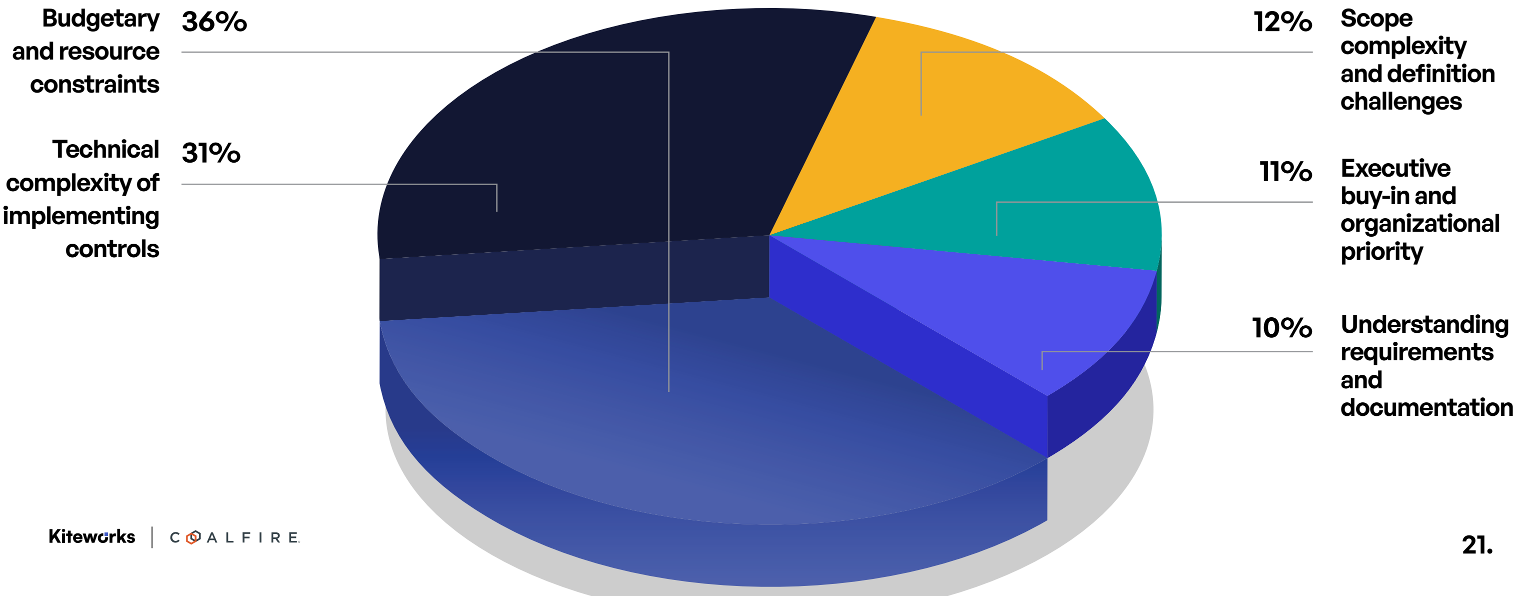
Organizations with advanced third-party access controls demonstrated substantially stronger performance across other security dimensions. These organizations were more likely to have fully documented security policies (78% versus 38% for those with partial controls), follow documented encryption standards (78% versus 51%), and have formal vendor management programs (77% versus 31%). This pattern suggests that robust third-party access controls typically exist within a broader context of mature security governance and technical controls.

Use Advanced Third-Party Access Controls

	Have Fully Documented Security Policies	Follow Documented Encryption Standards	Have Formal Vendor Management Programs
YES	78%	78%	77%
NO	38%	51%	31%

The relationship between third-party access controls and perceived compliance challenges reveals important differences in organizational focus. Organizations with advanced controls most frequently identified budget constraints (37%) and scope complexity (24%) as primary challenges. In contrast, organizations with partial controls or identified gaps more often cited technical complexity (51%) and understanding requirements (38%). This divergence suggests that organizations mature their understanding of both technical and governance requirements as they implement more advanced third-party controls. Interestingly, organizations at different compliance stages report different primary challenges, with less mature organizations focused on technical understanding and more mature organizations concerned with resources and scope definition.

Greatest Perceived CMMC Challenges



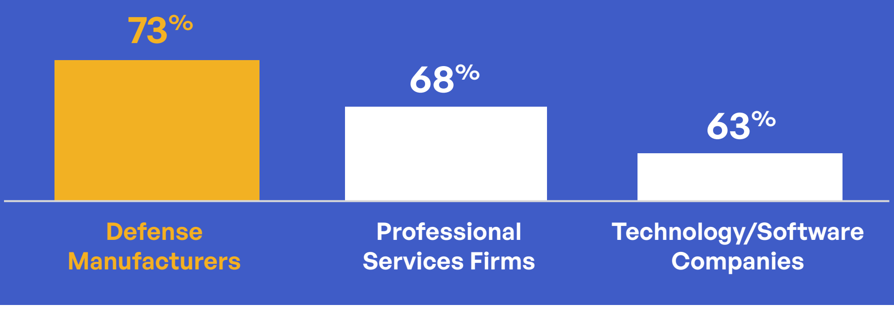
Supply chain complexity shows a strong correlation with third-party access control maturity. Organizations reporting more than 50 suppliers handling CUI were significantly more likely to have advanced controls (79%) compared to those with fewer than 10 suppliers (58%). This pattern suggests that organizations with more complex supply chains recognize the heightened risk and invest accordingly in more sophisticated control mechanisms.

The relationship between third-party access controls and third-party engagement strategies reveals important patterns in how organizations address supply chain security challenges. Organizations working with experienced partners reported the highest rate of advanced controls (76%), compared to those handling compliance in-house (66%) or those still selecting partners (52%). This correlation suggests that external expertise particularly benefits organizations in addressing the complex technical and governance requirements associated with third-party access controls.

Organizations that leverage experienced partners are more likely to have advanced security controls in place (76%) vs. those that handle all compliance in-house (66%).

Industry sector analysis reveals notable differences in third-party access control maturity. Defense manufacturing organizations reported the highest rate of advanced controls (73%), followed by professional services firms (68%) and technology/software companies (63%). These differences likely reflect variations in supply chain complexity and experience with handling sensitive information, with defense manufacturers typically having more established practices for controlling information flow to suppliers and subcontractors.

Industries With Advanced Security Controls



The particular challenges associated with third-party access controls make them a critical focus area for CMMC compliance efforts. These controls require both technical mechanisms and governance processes, spanning organizational boundaries and requiring coordination with external entities (Department of Defense Chief Information Officer [DoD CIO], 2024). The survey results suggest that organizations recognize these challenges, with those at earlier compliance stages identifying third-party controls as a particular area of concern (54% citing it among their top three compliance challenges).

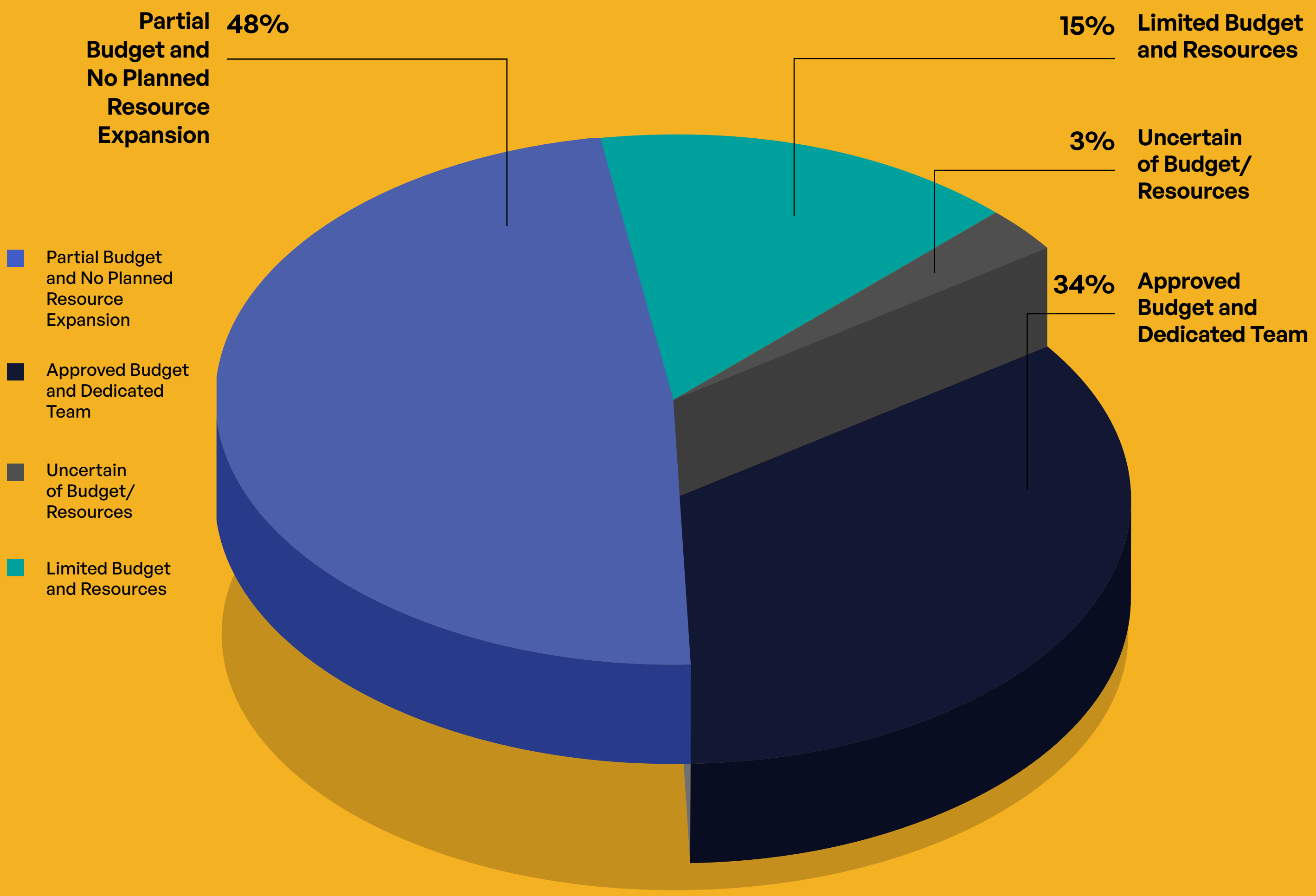
Key Compliance Challenges and Resource Allocation

The survey results highlight the diverse challenges organizations face in pursuing CMMC 2.0 Level 2 compliance, with resource constraints, technical complexity, and organizational factors emerging as key themes. Organizations' identified challenges vary significantly based on size, compliance maturity, and specific role perspective. Among all respondents, 36% identified budgetary and resource constraints as their greatest challenge, followed by technical complexity (31%), scope complexity (12%), executive buy-in (11%), and understanding requirements (10%).

Budgetary and resource constraints are cited most often as the biggest challenge DIB organizations face in addressing CMMC 2.0 compliance (36%).

Budget allocation for CMMC 2.0 compliance shows significant variation across respondent organizations. Among surveyed organizations, 34% reported having an approved budget with a dedicated team, 48% indicated partial budget allocation with plans to expand resources, 15% acknowledged limited or no specific budget allocation, and 3% were unsure of their budget status. The correlation between budget allocation and company size follows expected patterns, with large organizations more likely to have approved budgets (62%) compared to medium (38%) and small organizations (23%).

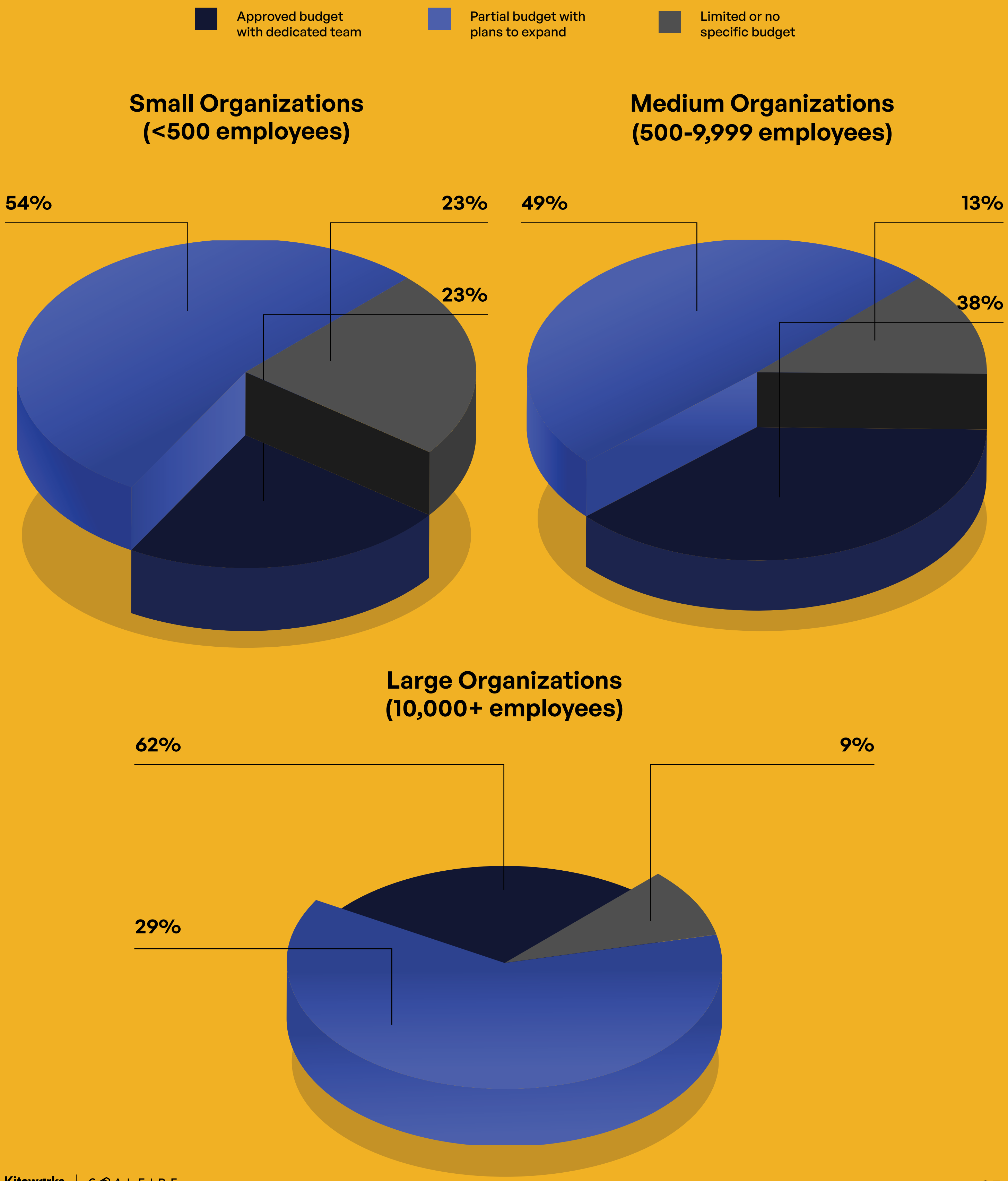
CMMC 2.0 Budget Allocation



Organizations at different compliance maturity stages report markedly different challenge perceptions. Organizations with fully documented policies and advanced security controls most frequently identified budget constraints (38%) and scope complexity (26%) as primary challenges. In contrast, organizations with partial documentation and security gaps more often cited technical complexity (53%) and understanding requirements (27%). This progression suggests that organizations focus initially on understanding and implementing technical requirements before confronting resource allocation and scope definition challenges.

CMMC Budget Allocation by Company Size

The survey reveals significant differences in CMMC budget allocation based on company size:

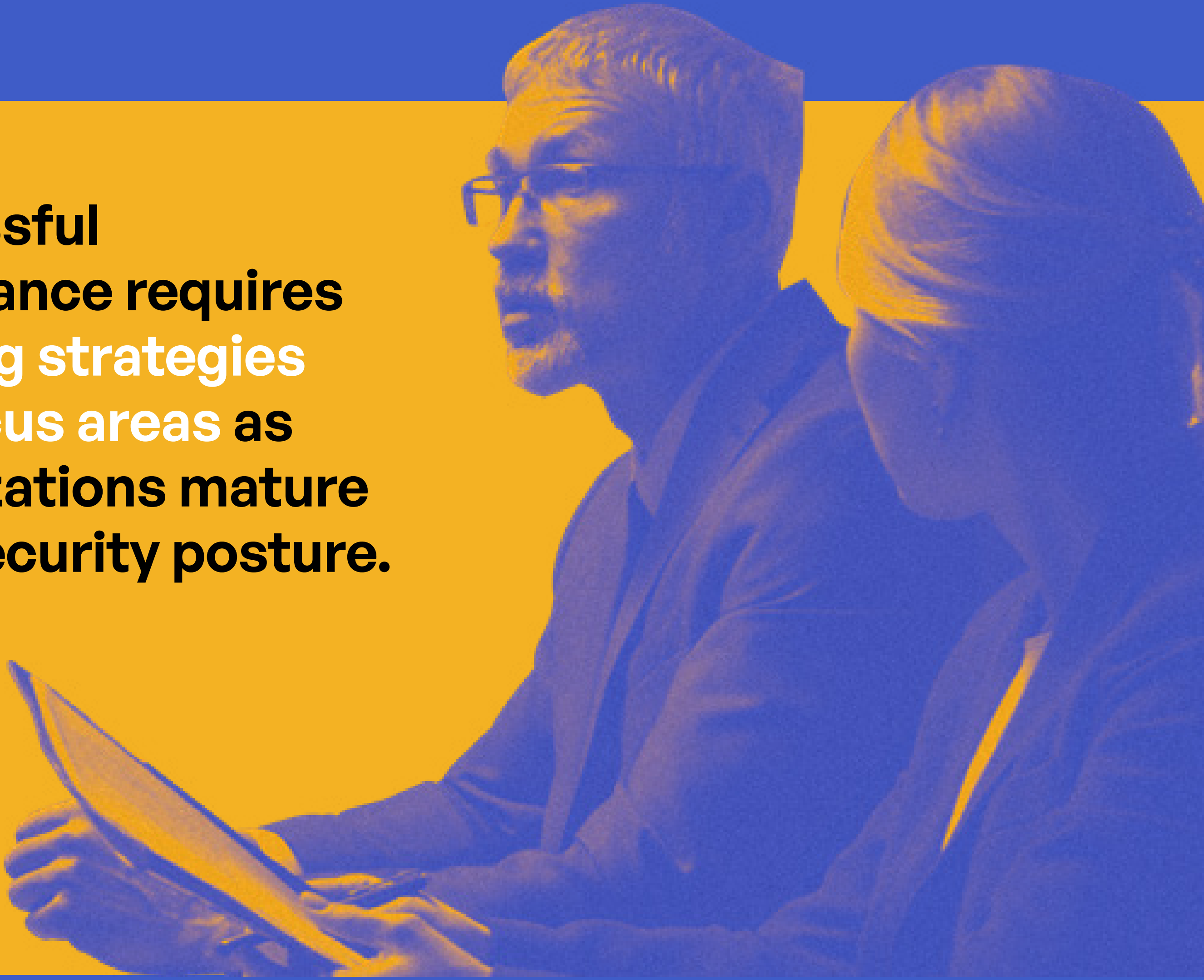


Small Organizations (<500 employees)

Medium Organizations (500-9,999 employees)

Large Organizations (10,000+ employees)

The relationship between challenge perception and compliance timeline reveals important patterns in how organizations approach CMMC preparation. Organizations identifying technical complexity as their primary challenge projected longer compliance timelines, with 67% anticipating certification within 12 to 24 months of the final rule. In contrast, organizations citing budget constraints showed more aggressive timelines, with 41% planning certification within 6 to 12 months. This divergence suggests that technical understanding, rather than resource availability alone, may be the more limiting factor in compliance velocity.



Successful compliance requires evolving strategies and focus areas as organizations mature their security posture.

The survey results highlight the evolution of compliance challenges as organizations progress in their CMMC journey. Early-stage challenges focus on understanding requirements and implementing basic technical controls. Mid-stage challenges center on resource allocation and systematic documentation. Advanced-stage challenges involve scope definition, external partner management, and continuous monitoring. This progression suggests that successful compliance requires evolving strategies and focus areas as organizations mature their security posture.

Key Takeaways and Recommendations

The survey findings reveal clear pathways to successful CMMC Level 2 compliance, with organizations' approaches varying significantly based on size, leadership involvement, and maturity of security practices. Organizations taking structured, systematic approaches consistently achieve better security outcomes across all measured dimensions.

Based on the survey data, following are some of the key actions organizations should prioritize:

Implement advanced governance tracking and controls for CUI access.

Organizations with advanced third-party access controls demonstrate dramatically stronger security posture, with 78% following documented encryption standards versus 51% for those with partial controls. The 66% of organizations already employing advanced controls show 77% higher rates of formal vendor management programs, creating comprehensive visibility throughout their supply chains.

Develop comprehensive security layers for data protection.

Survey data shows that organizations following documented encryption standards (69% of respondents) achieve significantly better security across multiple dimensions. These organizations are three times more likely to have fully documented policies (73% versus 29%) and detailed POA&Ms (65% versus 23%) compared to those with encryption gaps. Prioritize encryption implementation alongside complementary controls for defense-in-depth protection of sensitive information.

Engage specialized third-party expertise for compliance acceleration.

Medium-sized organizations (500-9,999 employees) lead in this approach with 50% working with specialized partners. This engagement correlates with substantially better security outcomes—76% achieve fully documented policies versus 43% for those handling compliance independently. Organizations with completed gap analyses engage external partners at nearly triple the rate (62%) of those yet to begin assessment (21%), recognizing the value of specialized expertise.

Adopt zero-trust data exchange solutions to streamline compliance.

With 29% of organizations reporting partial visibility over third-party CUI access, implementing zero-trust architectures addresses a critical vulnerability. The 76% of organizations working with experienced partners that achieve advanced access controls demonstrate how specialized solutions can overcome this challenge. Defense manufacturers lead in this implementation (73%), leveraging solutions that maintain security while enabling necessary information sharing.

Begin with thorough gap analysis against all 110 NIST SP 800-171 controls.

The 41% of organizations that completed comprehensive assessments are three times more likely to implement strong security controls than those who haven't started. This critical foundation identifies vulnerabilities requiring immediate attention.

As CMMC 2.0 Level 2 implementation continues across the Defense Industrial Base, these survey insights provide valuable guidance for organizations at all readiness stages. The findings clearly indicate that early investment in thorough assessment, comprehensive documentation, and appropriate external expertise significantly enhances an organization's ability to achieve and maintain compliance while improving overall security posture to protect sensitive defense information throughout the supply chain.

March 2025

www.kiteworks.com