REPORT

Over Half of DoD Suppliers Fail With Their Governance Controls

2025 Data Security and Compliance Risk: Annual Survey Report Reveals Serious CMMC 2.0 Risks

www.kiteworks.com

Contents

Programs succeed when they **measure outcomes** and **formalize supplier controls**—not because of headcount or outside help alone. In our sample of 461 organizations (104 pursuing CMMC 2.0 Level 2), teams that track effectiveness metrics report **fewer low-encryption outcomes** (19% at ≤50% encrypted vs. 25% among teams that don't measure). Within the CMMC cohort, **governance control & tracking** and **contractual security requirements** with suppliers are the clearest separators: Governance tracking is associated with **higher top-tier encryption** and **lower low-encryption rates**, while supplier contracts reduce the chance of low encryption compared with those without such clauses.

Partner use by itself shows **no independent lift**; outcomes look similar to going solo when measurement is in place. The practical pattern is simple: **measure, then manage**—standardize metrics, wire them into reviews, and use contracting and audits to drive vendor behavior.

Figure 1: 5 Actions That Drive Success.

Action	CMMC 2.0 Organizations	All Organizations	Expected Effect (Association, Not Causation)
Institute governance control & tracking	38% adoption	40%	Within CMMC, top-tier encryption **64%** with governance tracking vs. **42%** without; low-encryption **15%** vs. **20%**.
Track effectiveness metrics (make it routine)	95% track something	93%	Low-encryption **19%** with measurement vs. **25%** without (–6 pp). Top-tier **46%** vs. **44%** (**+2 pp**).
Put security requirements in supplier contracts	22% adoption	27%	CMMC: low-encryption **13%** with clauses vs. **20%** without; top-tier **52%** vs. **49%**. Overall: top-tier **53%** with clauses vs. **43%** without.
Run regular supplier audits (keep a cadence)	48% adoption	44%	CMMC: low-encryption **16%** with audits vs. **20%** without. Overall effect is modest but directional (**18%** vs. **20%** low-encryption).
Use partners to amplify a measured program	12% engage consultants	16%	No independent lift observed; outcomes look similar to solo efforts **when measurement exists.** Make partner SOWs deliver metrics and baselines.

Survey Demographics and Context

461

organizations surveyed

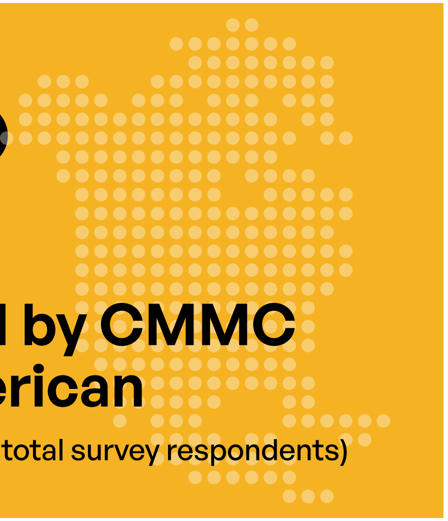
(October 2024–January 2025)

104

organizations pursuing CMMC 2.0

(23% of total)

62%



of those impacted by CMMC 2.0 are North American

(vs. North America was only 32% of total survey respondents)

38%

of impacted CMMC 2.0 organizations are mid-size

(1,000–4,999 employees)

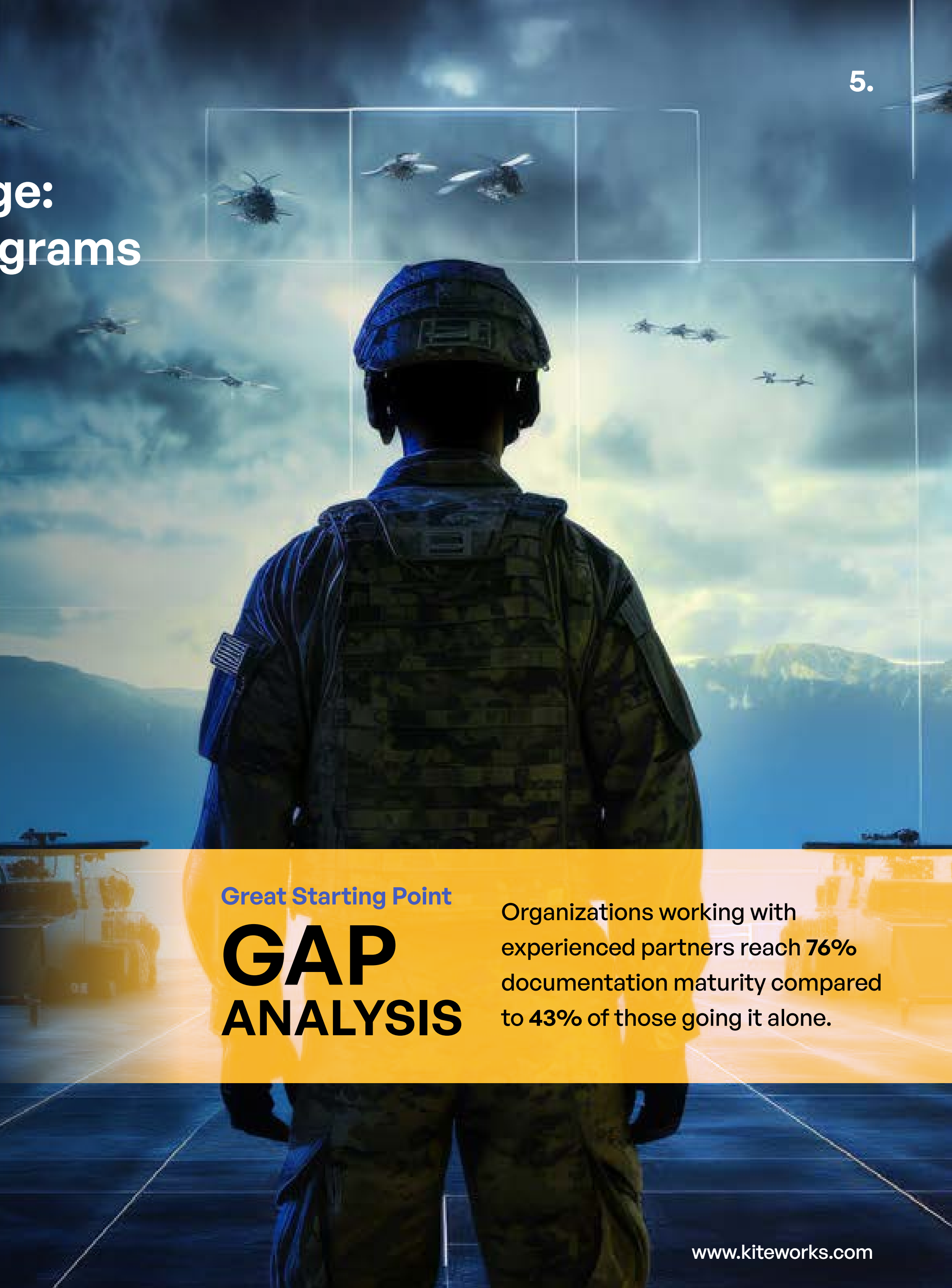
Introduction: Measure, Then Manage: What Differentiates CMMC 2.0 Programs

Kiteworks' 2025 Data Security and Compliance Risk Annual Survey captured responses from 461 organizations across industries, sizes, and regions. This supplemental analysis isolates the 104 respondents pursuing CMMC 2.0 (Level 2) and compares their patterns with the broader sample.

The most consequential signal is about measurement discipline. Organizations that track any effectiveness metrics report fewer low-encryption outcomes—19% at ≤50% encrypted versus 25% among those that do not measure. In short, measuring performance is consistently associated with lower encryption risk.

We also see meaningful—though not universal—differences by size and practice mix. Within the CMMC cohort, mid-market firms (5,000–9,999 employees) have the highest share at 76%–100% encrypted (about 59%), while 20,000+ organizations are lowest (about 38%). Across all sizes, third-party vendor compliance is the most frequent challenge. Adoption of supplier controls is uneven: regular supplier audits 48%, third-party risk-management tools 38%, but contractual security requirements just 22%.

Use of external partners by itself is not associated with better encryption outcomes; results look similar to going solo when measurement is present. The strongest pattern in this dataset is measure, then manage—pair effectiveness tracking with targeted supplier controls.



Great Starting Point

GAP ANALYSIS

Organizations working with experienced partners reach **76%** documentation maturity compared to **43%** of those going it alone.

Survey Methodology and CMMC Segmentation

In April 2025 we surveyed **461 organizations** across industries, sizes, and regions. For this supplemental readout, we isolate respondents who indicated they are **actively pursuing CMMC 2.0 (U.S.)**—that's **104 organizations** identified—and compare their patterns with the broader sample.

Our lens is pragmatic: We only use fields that actually exist in the dataset—**industry, size, encryption outcomes, vendor-risk practices, effectiveness measurement, partner use, and challenges**. The survey **does not** collect timeline or cost data, so we don't speculate on speed or budgets.

What the data says—three signals to carry forward:

First, **measurement matters**. Organizations that track any effectiveness metric show **fewer low-encryption outcomes—20%** report ≤50% encrypted versus **25%** among those that don't measure. This doesn't mean measurement causes improvement, but it's a consistent marker of healthier programs.

Second, **partners help—when paired with discipline**. Simply engaging external consultants isn't associated with better encryption outcomes on its own; when measurement is present, **partner vs. solo** looks similar. Successful teams treat partners as *amplifiers* of an internally measured program, not as a substitute for it.

Third, **third-party risk is the universal headache**. Across sizes, **"vendor compliance"** rises to the top of challenges. That aligns with uneven adoption: Many run supplier audits or use TPRM tools, but **contractual security requirements** lag and are often the missing leg of the stool.

Industry Distribution Reveals Notable Shifts

A common assumption is that tech firms would dominate CMMC pursuit. The data tells a more nuanced story. Looking at **shares within the CMMC cohort** versus **shares in the overall survey.**

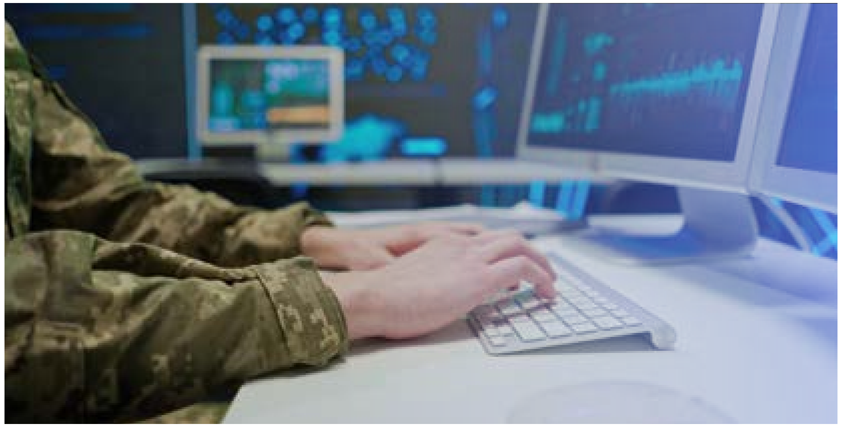
Industry Highlights

Technology: 20% of CMMC vs. 26% overall → –6 pp under-representation. Interpretation: Many tech companies may leverage existing security programs and certifications rather than add CMMC—especially if they are further from U.S. defense supply chains.

Healthcare: 16% of CMMC vs. 14% overall → +2.0 pp over-representation. Overlap with HIPAA obligations, data-sensitivity norms, and federated research relationships likely pull healthcare toward CMMC readiness.

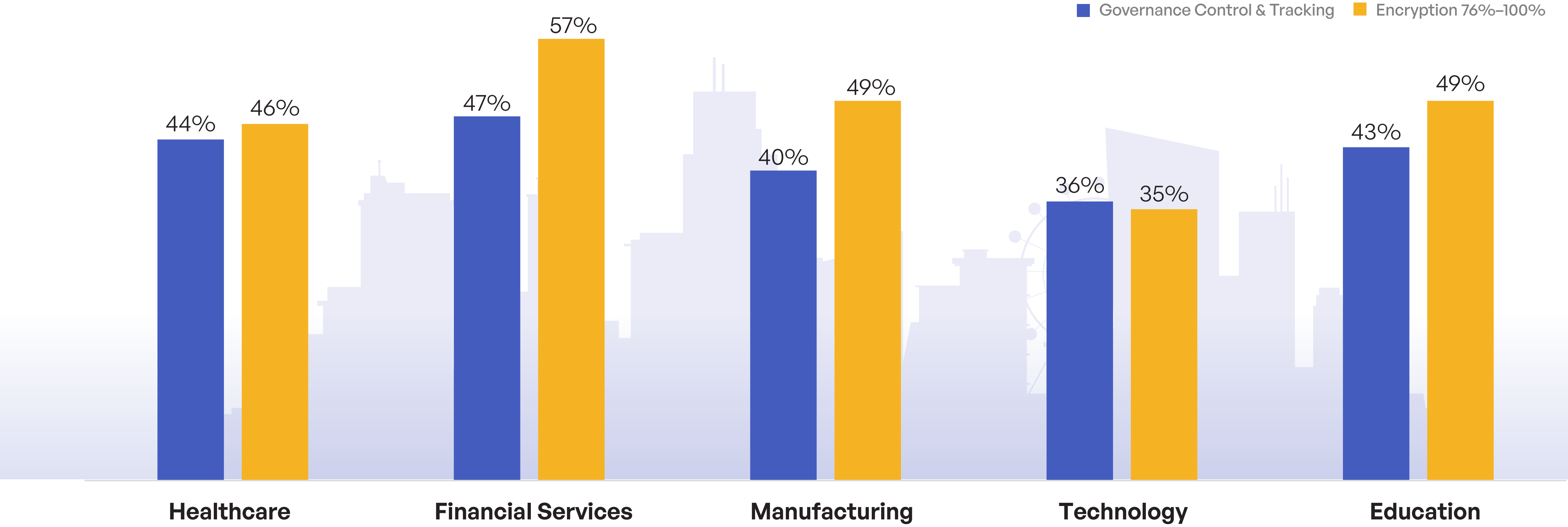
Education: 13% of CMMC vs. 8% overall → +5 pp over-representation. Universities and research institutions that handle federally funded projects appear to be preparing early for contracting requirements.

So What?



CMMC activity is not merely a “tech industry” phenomenon; it’s concentrated where regulated data, public funding, and defense-adjacent work intersect. Enablement, content, and partner motions should be tailored accordingly—more procurement/legal alignment in healthcare and education, and clearer “why CMMC” narratives for tech firms already deep into other frameworks.

Figure 2: **Encryption and Governance Tracking by Industry.**



Industry-Specific Success Patterns

Survey responses reveal distinct maturity patterns by industry:

- **Financial Services** leads on encryption (**57%**) with solid governance tracking (**47%**).
- **Technology** lags on both—lowest governance tracking (**36%**) and lowest encryption (**35%**).
- **Manufacturing and Education** are above average on encryption (**49%** each) but have mid-range governance tracking (**40%–43%**), suggesting room to formalize policies/processes.
- **Healthcare** sits near the overall average (Governance **44%**, Encryption **46%**).

Organization Size: Where CMMC Respondents Cluster

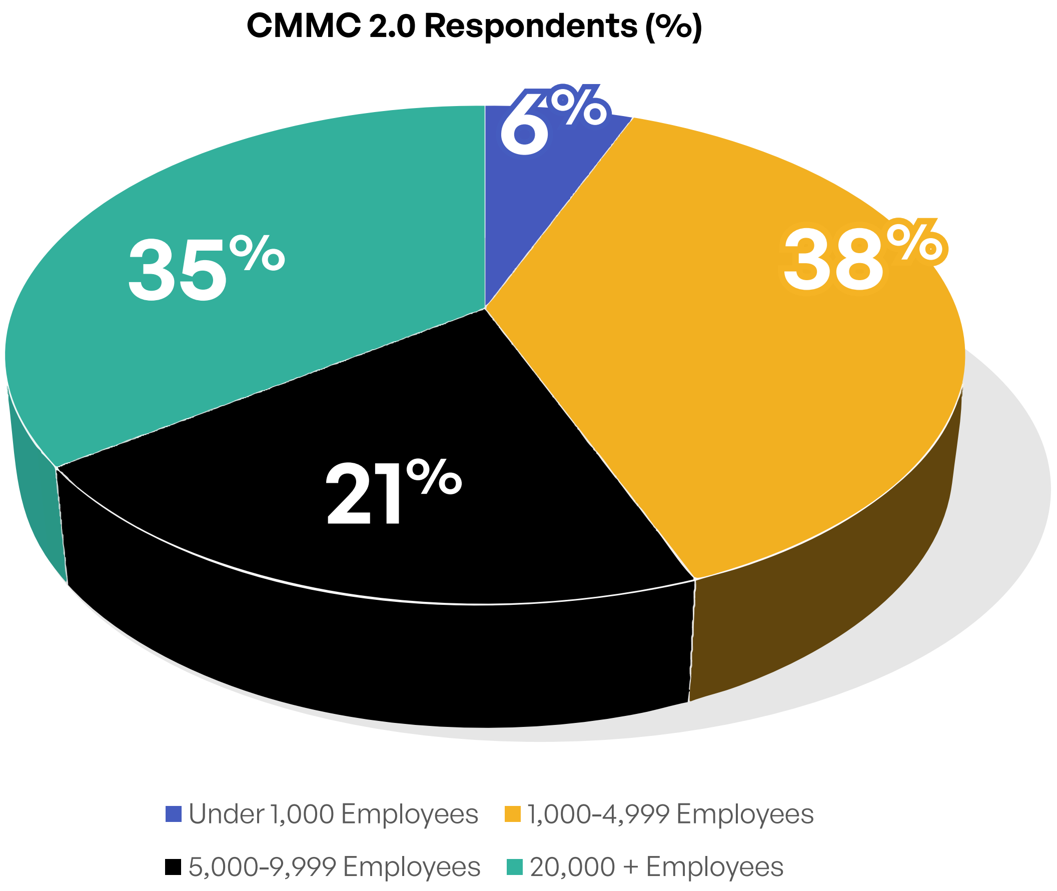
What the Distribution Shows

Most CMMC respondents are mid-market: 38% are 1,000–4,999 employees. Small organizations are a small share (6%), and 10,000+ accounts for 35% of the sample.

What It Doesn't Show (outcomes are not driven by size)

- **Top-tier encryption** (76%–100%) by size (CMMC only): Under 1,000 50%, 1,000–4,999 53%, 5,000–9,999 59% (highest), 10,000–19,999 47%, 20,000+ 38%.
- **Governance control & tracking by size** (CMMC only):
  - Under 1,000 50%, 1,000–4,999 40%, 5,000–9,999 41%, 10,000–19,999 27%, 20,000+ 33%.
  - Implication: Size explains who's in the program, not who "succeeds." Measured outcomes vary modestly and correlate more with measurement discipline and vendor-risk practices than with headcount.

Figure 3: Organization Size Breakdown of CMMC Respondents.



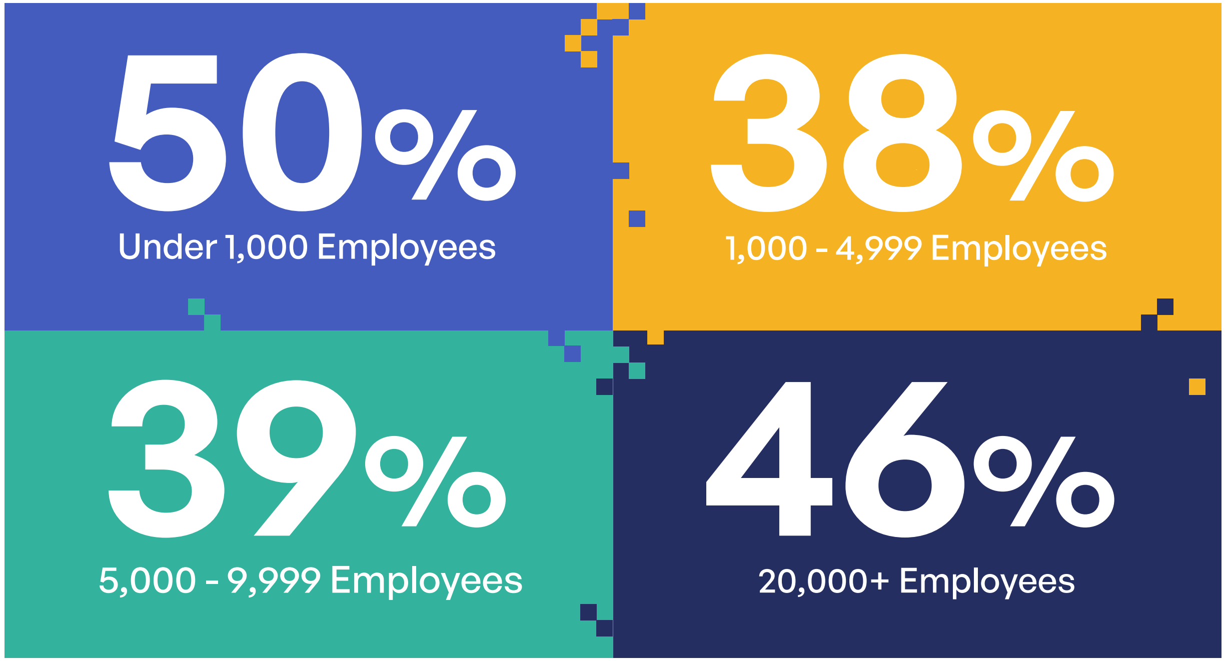
Size Impact on Compliance Metrics

Survey data reveals size-based patterns:

- Governance formalization (“institute comprehensive governance control & tracking”) varies modestly by size—highest at the smallest and largest firms, lower in the mid-market.
- Encryption outcomes (76%–100%) are fairly flat across sizes, suggesting **process maturity, not size,** drives results.

Documentation Success Rates by Organization Size

Figure 4: Documentation Maturity by Employee Count.



Geographic Concentration and Readiness

The geographic distribution reveals dramatic regional disparities that reflect both defense industrial base concentration and varying regulatory environments.

Regional Distribution Patterns

North American Dominance
North American organizations dominate CMMC pursuit, representing 63% of CMMC respondents compared to just 33% of the overall survey population. This near doubling of representation aligns with U.S. Department of Defense contract concentration, although it also suggests international suppliers may be underestimating their CMMC obligations.

Global Breakdown:

- **Asia-Pacific (20%):** Driven primarily by technology and manufacturing partners in allied nations
- **Europe (11%):** Surprisingly low given NATO partnerships, suggesting potential awareness gaps
- **Middle East (7%):** Limited engagement reflecting current market dynamics

Regional Maturity Indicators

Figure 5: Regional Readiness Scorecard.

	North America	Europe	Asia Pacific	Middle East/ Africa
Documentation	52%	53%	40%	69%
Encryption	53%	47%	44%	22%
Vendor Risk	49%	56%	45%	60%
Top Challenge	Inconsistent Requirements	Cross-Border Complexity	Cross-Border Complexity	Cross-Border Complexity

Key Finding: 51% of all CMMC respondents managing international data flows report increased complexity in policy development and control implementation.

Encryption Outcomes Are Driven by Contractual Governance and Measurement

Organizations that embed contractual security requirements with suppliers are more likely to reach top-tier encryption and less likely to sit at the lowest levels, and teams that track any security effectiveness metric report fewer severe encryption gaps.

Contractual Supplier Requirements Lift Encryption Outcomes

Governance choices—not gap analyses—move encryption outcomes. Teams that embed contractual security requirements with suppliers report more top-tier encryption (76%–100% of exchanges: 53% vs. 43% without contracts) and fewer low-encryption outcomes (**≤50%** encrypted: 17% vs. 21%). Separately, organizations that track any security effectiveness metric report fewer severe encryption gaps (19% vs. 25% among those that don't measure).

The Documentation-Encryption Risk Cascade

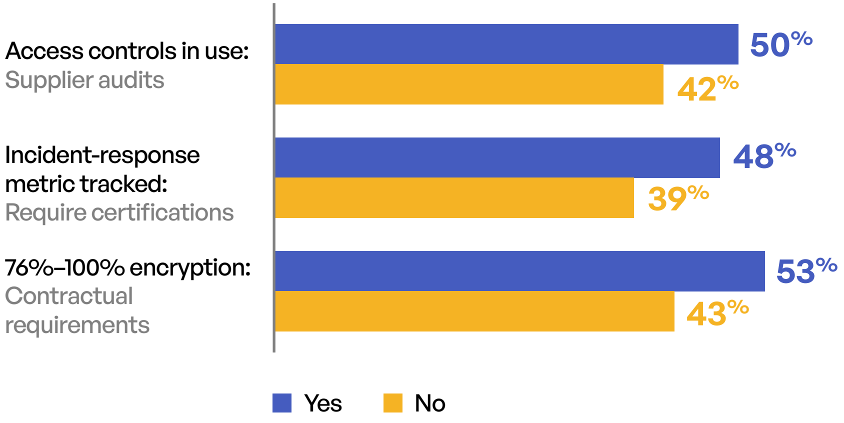
Figure 6: Supplier Governance vs. Encryption Outcomes.

Encryption	With Contractual Requirements	No/Minimal
Top-tier encryption (76–100%)	**53%**	**43%**
Lowest encryption (≤50%)	**17%**	**21%**

Targeted Governance Practices Deliver Specific Control Gains

Targeted governance practices correlate with specific control gains—there's no broad 2–4x jump. For example, supplier audits align with higher access-control adoption (50% vs. 42%), requiring supplier certifications aligns with more incident-response measurement (48% vs. 39%), and contractual requirements align with top-tier encryption (53% vs. 43%).

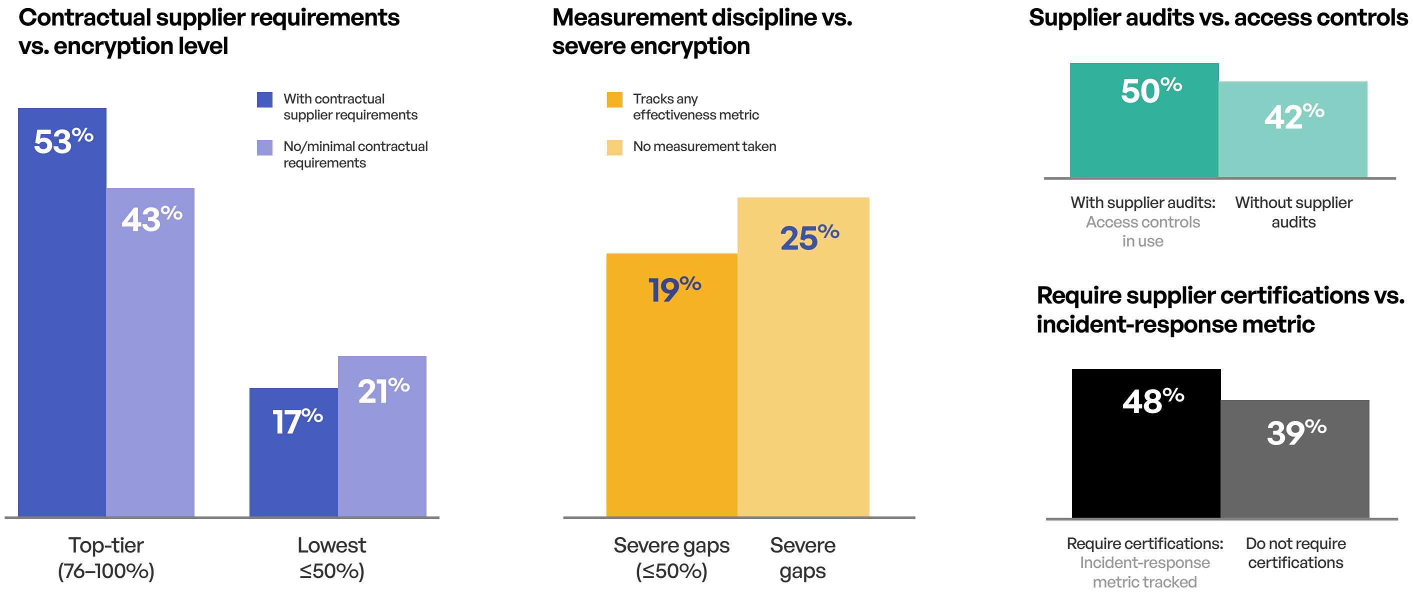
Figure 7: Which Governance Practices Move Which Controls?



Governance Practices Move Specific Controls—Not Universal Jumps

The survey shows targeted gains from concrete governance choices: Contractual supplier requirements, supplier audits, and basic measurement correlate with better encryption, access controls, and incident-response tracking.

Figure 8: Encryption Outcomes by Supplier Governance and Measurement.



Contractual supplier requirements vs. encryption level

Measurement discipline vs. severe encryption

Supplier audits vs. access controls

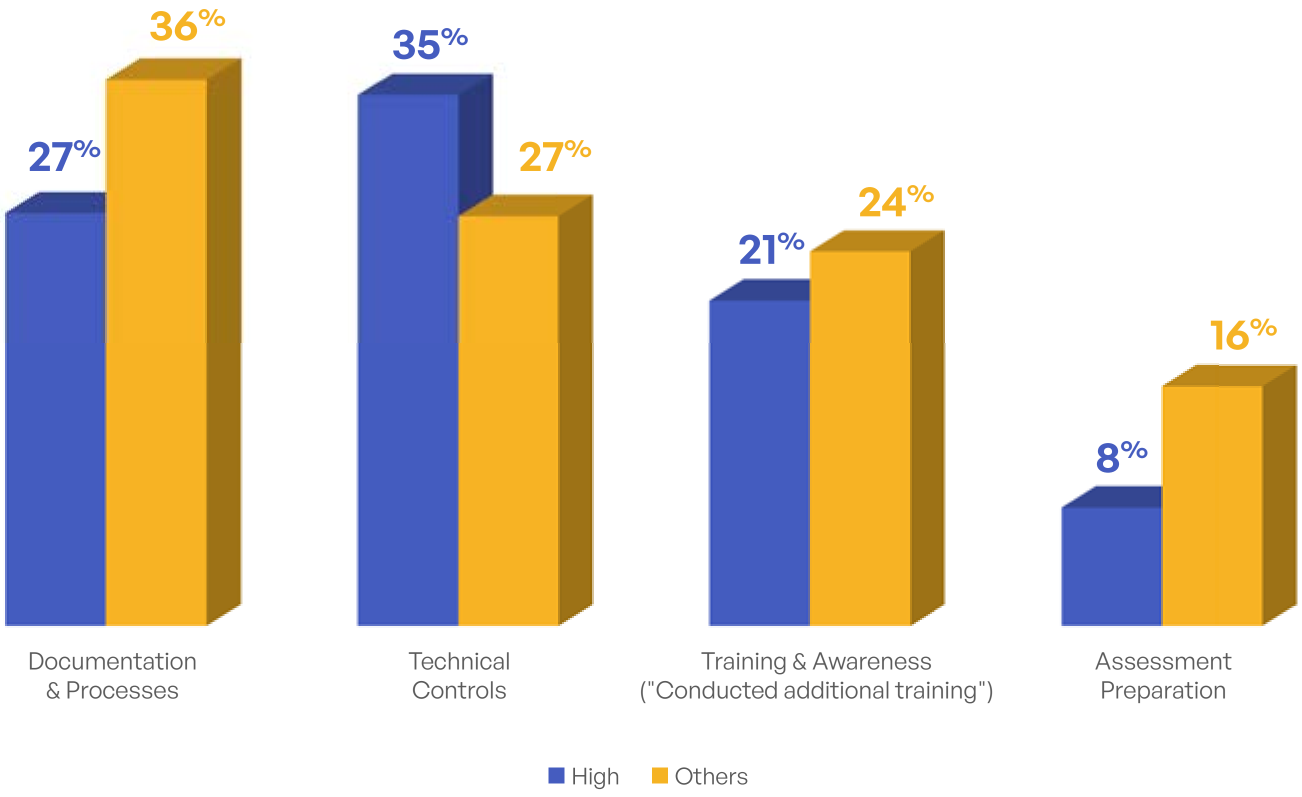
Require supplier certifications vs. incident-response metric

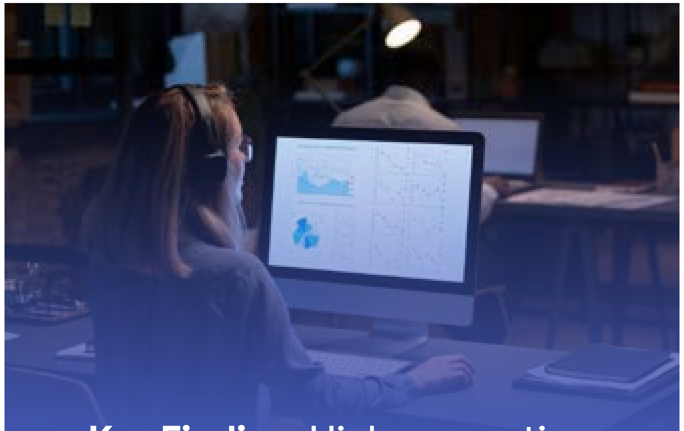
Key Finding: Teams with contractual supplier requirements are **10 percentage points** more likely to report top-tier encryption **(53% vs. 43%)**, and organizations that track any effectiveness metric see **fewer severe encryption gaps (19% vs. 25%)**.

CMMC 2.0 Implementation Actions: High-Encryption Organizations vs. Others

This compares the share of CMMC respondents taking four implementation actions—policy updates, new technical controls, employee training, and engaging external consultants—between organizations with 76%–100% encrypted exchanges and all others.

Figure 9: CMMC Action Mix: High Encryption Organizations vs. Others.





Key Finding: High-encryption CMMC organizations are more likely to implement new technical controls (35% vs. 27%) and less likely to rely on external consultants (8% vs. 16%); documentation updates are comparable and not higher among high performers.

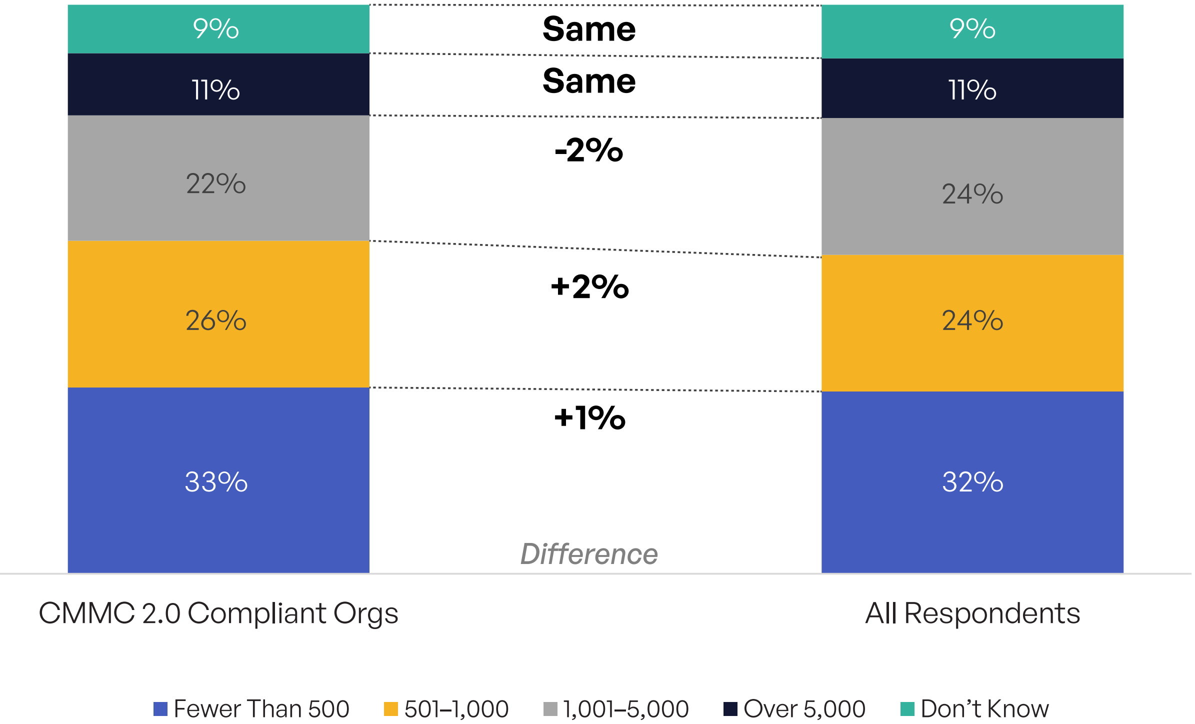
Third-Party Risk Management: Universal Challenge, Different Responses

Survey data reveals that supplier management complexity is a universal challenge, not unique to CMMC organizations. Contrary to expectations, CMMC-pursuing organizations show remarkably similar supplier distributions to the general population.

Third-Party Data Exchange Scale: Reality Check

Key Finding: CMMC pursuit does not correlate with supplier scale. The nearly identical distributions suggest that supply chain complexity affects all organizations equally, regardless of defense contract involvement.

Figure 10: Third-Party Risk: Little Difference Between Organizations Focused on CMMC 2.0 vs. All Organizations.



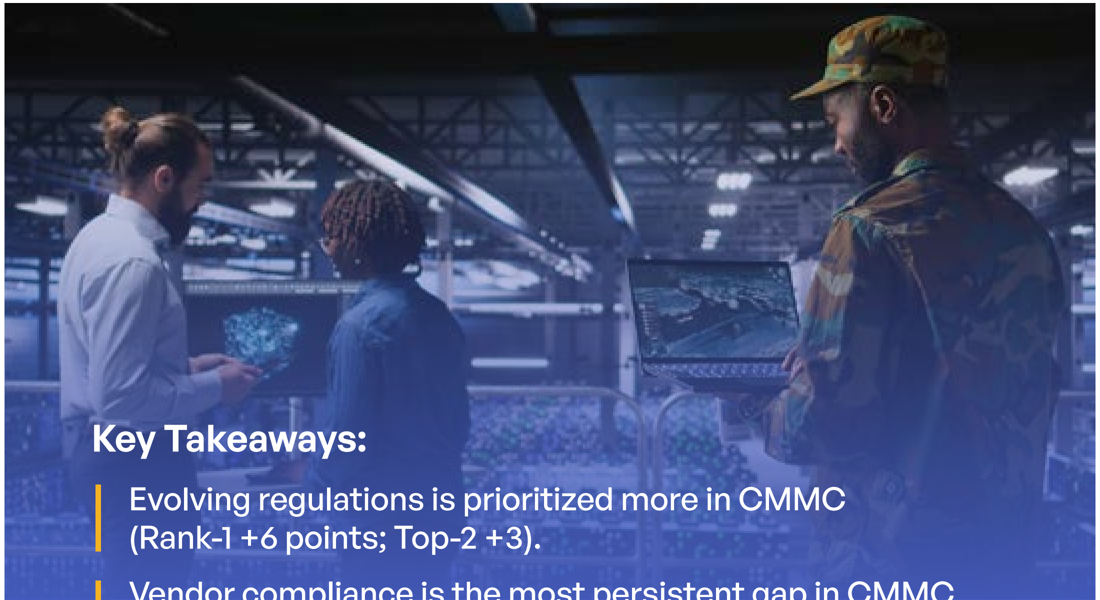
Top CMMC 2.0 Challenges

What the Distribution Tells You

Evolving regulations is the sharpest top priority. When teams list it, most put it first (60% Rank 1 within item), and it's broadly cited by over a third of CMMC respondents (38% Total 1–3). Vendor compliance has comparable breadth (39%) but splits more evenly across Rank 1 and Rank 2, signaling a sustained, operational pressure rather than a single spike. The day-to-day friction between compliance and data access appears in both breadth (34%) and intensity (51% of its rankers put it #1).

How to Act on This

When we contrast CMMC-pursuing organizations with the broader respondent pool, a clear pattern emerges. Regulatory change rises to the top more often for CMMC teams, and supplier compliance pressure is broader and more sustained. By comparison, overlapping jurisdictional rules and budget constraints are cited less frequently by the CMMC cohort, suggesting resources are being directed toward change management and vendor governance.



Key Takeaways:

- Evolving regulations is prioritized more in CMMC (Rank-1 +6 points; Top-2 +3).
- Vendor compliance is the most persistent gap in CMMC (Top-2 +7; Total ranked +7).
- Balancing compliance vs. data access is slightly higher in CMMC (Top-2 +3).
- Inconsistent jurisdictional requirements and limited budget are materially lower in CMMC (Top-2 −8 and −7, respectively).
- Employee training is about the same on Rank-1, modestly higher in CMMC on Top-2 (+3).

Figure 11: CMMC Challenges.

Challenge	CMMC Rank 1 (%)	All Rank 1 (%)	Diff Rank 1 (pp)	CMMC Top 2 (%)	All Top 2 (%)	Diff Top 2 (pp)	CMMC Total (%)	All Total (%)	Diff Total (pp)	Algorithm Score (1-100)
Keeping up with evolving regulations	23%	17%	6%	38%	35%	3%	38%	36%	2%	78
Vendor compliance & risk	18%	15%	3%	38%	31%	7%	39%	32%	7%	73
Balancing compliance vs. data access	17%	15%	2%	33%	30%	3%	34%	32%	2%	59
Employee training & awareness	12%	12%	0%	28%	25%	3%	30%	26%	4%	42
Inconsistent jurisdictional requirements	11%	16%	-5%	23%	31%	-8%	25%	32%	-7%	30
Data inventory accuracy	10%	12%	-2%	23%	25%	-2%	27%	26%	1%	29
Limited resources/ budget for controls & monitoring	8%	11%	-3%	16%	23%	-7%	16%	23%	-7%	5

Challenge Scoring Formula:

Each challenge receives a weighted score based on how organizations rank it:

- 1st place ranking = 3 points per percentage
- 2nd place ranking = 2 points per percentage
- 3rd place ranking = 1 point per percentage

Score = (Rank 1% × 3) + (Rank 2% × 2) + (Rank 3% × 1)

Example: *If 23% rank "evolving regulations" as #1, 15% as #2, and 0% as #3: Score = (23 × 3) + (15 × 2) + (0 × 1) = 99 points*

Scores are then rescaled to 1-100 for easy comparison, with the highest challenge scoring ~80.

Insights and Takeaways on CMMC 2.0 Top Challenges

The scoring reveals that “Keeping up with evolving regulations” is the most pressing challenge for CMMC-affected organizations, with a score of 78. Close behind is “Vendor compliance and risk” (73), highlighting that CMMC is not only a regulatory compliance effort but also a supply chain assurance exercise. Together, these two areas dominate the landscape, significantly outweighing other issues. A second tier of challenges—“Balancing compliance vs. data access” (59) and “Employee training and awareness” (42)—shows that internal trade-offs and workforce readiness also weigh heavily but are secondary to external regulatory and vendor demands.

At the lower end of the scale, “Data inventory accuracy” (30), “Inconsistent jurisdictional requirements” (29), and “Limited resources/budget for controls and monitoring” (5) indicate that while these issues are real, they are not seen as existential barriers by most CMMC respondents. Taken together, the scores suggest that organizations view CMMC primarily through the dual lens of regulatory agility and vendor ecosystem management, with internal operations and resource constraints as important but less dominant concerns.

Where CMMC Organizations Differ: Process Maturity

While supplier quantity wasn’t measured, survey data shows modest differences in vendor-risk practices. Compared with all organizations, CMMC respondents are slightly more likely to conduct regular supplier audits and run third-party risk assessments, while adoption of contractual security requirements is lower.

Figure 12: Vendor-Risk Practice Adoption (CMMC vs. all organizations).

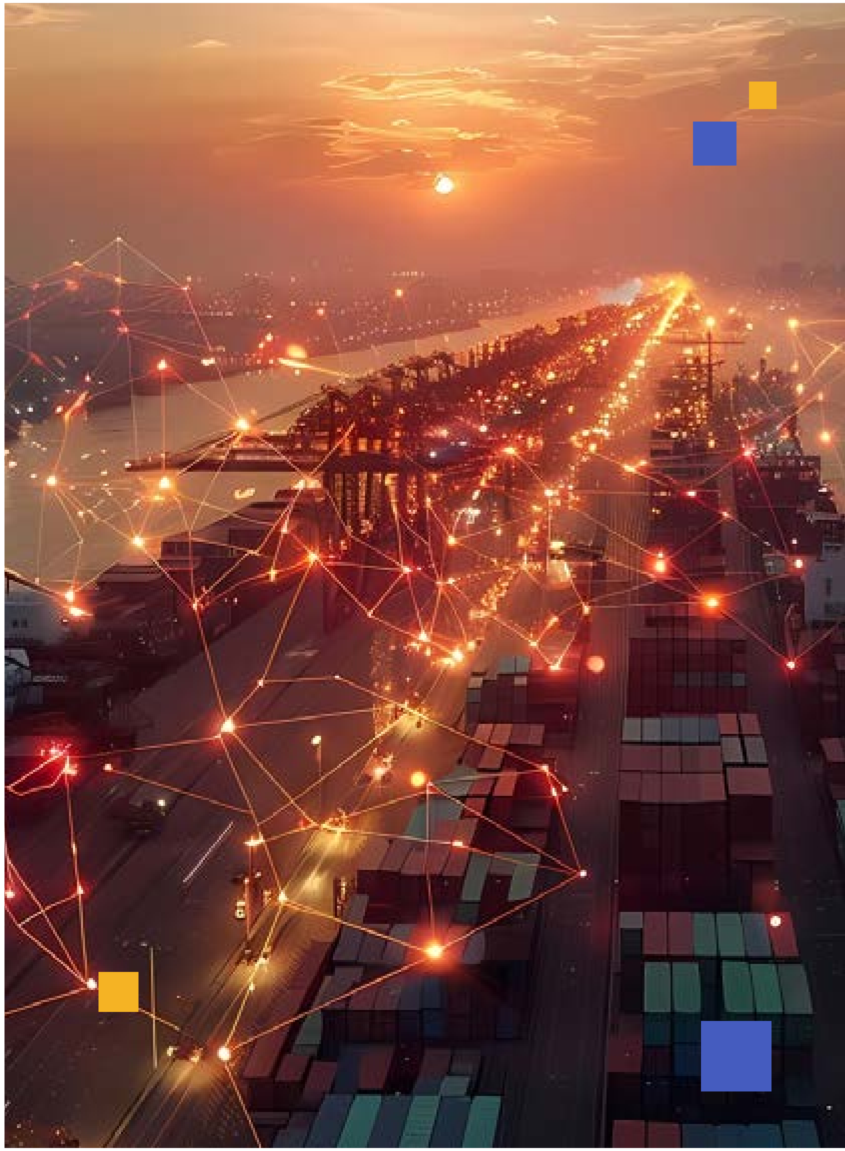
Control Type	CMMC Orgs	All Orgs	Factor
Third-Party Risk Assessments	28%	25%	1.12
Regular Supplier Audits	48%	44%	1.09
TPRM Tools	38%	37%	1.03
Contractual Security Requirements	22%	27%	0.81
Governance Control and Tracking	38%	40%	0.95

Success in CMMC programs shows up in process maturity rather than assumed differences in supply chains. In our data, CMMC respondents report slightly higher use of formal vendor-risk practices—regular supplier audits 48% vs .44% overall, third-party risk assessments 28% vs. 25%, and similar TPRM tool use at 38% vs. 37%—while contractual security requirements lag at 22% vs. 27%.

Supply Chain Security Leadership

CMMC 2.0-compliant organizations report advanced practices:

- **48%** of CMMC respondents conduct regular supplier audits vs. 44% of all organizations.
- **28%** of CMMC respondents perform third-party risk assessments vs. 25% of all organizations.
- **38%** of CMMC respondents use TPRM tools, essentially in line with 37% overall.
- **22%** of CMMC respondents implement contractual security requirements, below 27% overall.



Implications for CMMC 2.0 Implementation

The similar supplier distributions combined with different process maturity suggests:

- **Focus on formal audits and documented risk assessments:** These are the areas where CMMC organizations show a measurable edge (+4 to +3 points).
- **Close the contract gap:** Requiring security clauses and certifications lags among CMMC organizations (22% vs. 27%).
- **Tooling parity:** TPRM tool usage is similar (38% vs. 37%); improvements should come from process and contract rigor, not tools alone.
- **Prioritize the known pain point:** Third-party vendor compliance is a top challenge for 39% of CMMC organizations vs. 32% overall.

The survey did not collect supplier-count information, but it does indicate where maturity differs: CMMC 2.0 pushes formalization of vendor-risk processes. Priorities should include strengthening supplier contracts (closing the 22% vs. 27% gap) and continuing to expand audits and risk assessments, a known pain point for many organizations (third-party vendor compliance is a top challenge for 39% of CMMC respondents vs. 32% overall).

CMMC Actions and Encryption Outcomes by Organization Size

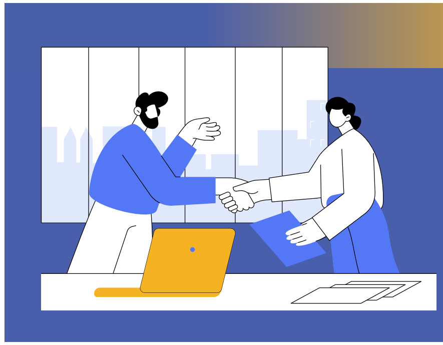
The survey did not collect timelines or a success flag. To ground this page in the data, we show, for each size band, the most-used CMMC action and the share achieving top-tier encryption (76%–100%). Results are for CMMC respondents only.

Size-Based Success Strategies

The survey reveals distinct approaches that correlate with success at different organization sizes:

Figure 13: Most-Used Action and Top-Tier Encryption Rate by Organization Size.

Under 4,999



Most-used action: Technical controls — **37%**

Top-tier encryption: **33%**

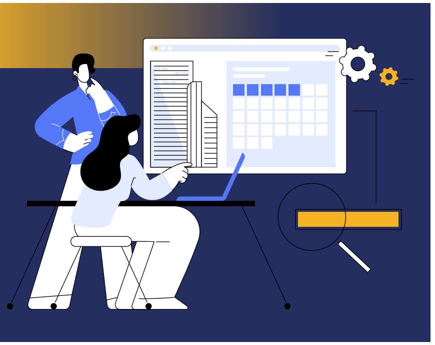
Second action for tool tip (optional):
Updated policies and DPAs — 52%

5,000–9,999

Most-used action: Updated Policies and DPAs — **36%**

Top-tier encryption: **59%**

Second action (optional):
Increased compliance budget — 36% (tie)



10,000–19,999

Most-used action: Dedicated privacy/ security roles — **47%**

Top-tier encryption: **47%**

Second action (optional):
Employee training — 33%

20,000+

Most-used action: New technical controls — **38%**

Top-tier encryption: **38%**

Second action (optional):
Increased compliance budget — 33%

Key Takeaway: Mid-market organizations (5,000–9,999 employees) report the highest share at top-tier encryption (59%) with a focus on policy/DPA updates, while the very largest organizations show the lowest share (38%) and emphasize new technical controls. Action mixes vary by size; timelines were not collected.

Strategy Details by Organization Size

Small and Mid-Size Organizations (Under 4,999 employees)

- Most-used actions: **New technical controls 37%, updated policies & DPAs 33%, enhanced third-party risk management 28%.**
- Top-tier encryption (76%–100%): **52%.**
- Top challenges: **Third-party vendor compliance 41%, balancing access vs. requirements 39%, keeping up with evolving regulations 37%.**
- Overlapping regulations 28%, finding regulated data 28%, employee awareness/training 24%, comprehensive controls & monitoring 11%.

Larger Mid-Size Organizations (5,000–9,999 employees)

- Most-used actions: **Updated policies & DPAs 36%, increased compliance budget 36%, enhanced third-party risk management 32%.**
- Top-tier encryption: **59%** (highest of the three bands).
- Top challenges: **Third-party vendor compliance 46%, overlapping regulations 41%.**

Enterprise Organizations (20,000+ employees)

- Most-used actions: **New technical controls 38%, increased compliance budget 33%, updated policies & DPAs 24%, dedicated roles 24%.**
- Top-tier encryption: **38%.**
- Top challenges: **Third-party vendor compliance 38%,** then **finding regulated data/keeping up with evolving regs/balancing access vs. requirements 33%** (tie).

Common Pitfalls by Size

- **Under 5,000:** third-party vendor compliance 41%; balancing access vs. requirements 39%; keeping up with evolving regulations 37%.
- **5,000–9,999:** vendor compliance 46%; overlapping regulations 41%.
- **20,000+:** vendor compliance 38%; finding regulated data 33%; evolving regulations 33%; balancing access vs. requirements 33%.
- **Cross-Cutting:** vendor risk is the most frequent challenge in every size band.

Implementation Approach Outcomes

The survey did not collect timeline or cost information, and it has no field for “gap analysis completed.” Instead, we compare outcomes by two observable choices: whether organizations used external consultants and whether they track any effectiveness metrics. Outcomes are measured as encryption levels.

Figure 14: Outcomes by Partner Involvement and Measurement Discipline.

Approach	Top-Tier Encryption	Low Encryption	Key Insights by Approach
Solo + No measurement	41%	30%	Weakest outcome; skipping measurement correlates with more low-encryption results.
Solo + Any measurement	46%	19%	Measurement alone reduces low-encryption by ~10 points vs. no-measurement solo.
Partner + No measurement	60%	0%	Very small base; do not generalize.
Partner + Any measurement	45%	20%	Similar outcomes to solo + measurement; expertise without measurement doesn’t yield broad gains.

Why the Combination Works

Survey respondents using both partners and gap analysis report:

- **Track what you want to improve.** Organizations that track *any* effectiveness metric have **~6 points fewer low-encryption outcomes** (20% vs. 25%).
- **Partners help when paired with discipline.** Using external consultants shows **similar encryption outcomes** to going solo *when measurement is present*. Expertise without measurement doesn't move the needle.
- **Timelines & costs were not collected.** Remove all claims about months, cost index, "one-shot pass," or "gap analysis" counts.

Key Finding: Tracking effectiveness is associated with fewer low-encryption outcomes **(20% vs. 25%).** External partners show similar results unless paired with strong internal measurement. The survey did **not** collect timeline or cost data.

Industry-Specific Recommendations From Survey Data

The survey responses suggest targeted strategies by sector:

Technology

- Top-tier encryption: **35%** (below overall 46%).
- Challenges: **Overlapping regulations 38%, evolving regs 36%, vendor compliance 34%.**
- Practices: Contracts **30%,** supplier audits **43%,** TPRM tools **42%,** measurement **93%.**
- **Do this:** Close the encryption gap—keep TPRM/audits strong and add **contractual security clauses** where missing; prioritize regulatory harmonization work.

Healthcare

- Top-tier encryption: **46%** (≈ overall).
- Challenges: **Evolving regs 42%, overlaps 35%.**
- Practices: **Contracts 17% (well below overall 27%),** audits **47%,** TPRM **39%,** measurement **96%.**
- **Do this:** Raise **contractual requirements with suppliers** and maintain audits; use contracts to manage regulatory churn.

Education

- Top-tier encryption: **49%** (above overall).
- Challenges: **Employee awareness/training 41%, vendor compliance 30%.**
- Practices: **Measurement 84% (lowest of the four),** TPRM **27%,** audits **40%,** contracts **41%.**
- **Do this: Institutionalize effectiveness measurement** and **expand TPRM tooling,** paired with targeted training.

Manufacturing

- Top-tier encryption: **49%** (above overall).
- Challenges: **Evolving regs 40%, finding regulated data 30%, controls/monitoring 30%.**
- Practices: **TPRM 27% (below overall 37%),** contracts **35%,** audits **38%,** measurement **98%.**
- **Do this:** Improve **data discovery and classification** and raise **TPRM adoption** to sustain encryption gains.

Strategic Applications of Survey Findings

For CMMC-Pursuing Organizations

Key strategic moves based on survey findings:

- **Measure what matters.** Organizations that track **any effectiveness metric** have **fewer low-encryption outcomes: 19%** vs. **25%** when no measurement is used.
- **Use partners selectively—pair with measurement.** Across the sample, **partnering alone** shows **similar encryption outcomes** to going solo when measurement is present; for **under-5,000 CMMC** organizations the partner subgroup is tiny and does **not** outperform (20% top-tier vs. 56% without partners).
- **Tighten supplier controls where they lag.** Among CMMC respondents: **regular audits 48%, TPRM tools 38%**, but **contractual requirements 22%.** Prioritize **contract clauses** and **audit cadence** to lift consistency.
- **(Optional AI insight)** Most CMMC organizations report an **AI governance framework: 80%).** Keep the label explicitly **AI governance** to avoid confusion with general controls.

Key Finding: The most common benefits of security/privacy investment are **operational efficiency (54%)** and **reduced security losses (48%). Competitive advantage** is cited by **23%** (27% among CMMC respondents).

Broader Market Implications

The survey reveals that CMMC-pursuing organizations are establishing new market standards. Non-DIB organizations can leverage CMMC-level controls for:

- **Improved operational efficiency 54%, reduced security losses 48%, enhanced customer loyalty 29%, increased innovation 29%, competitive advantage 23%, ability to operate in regulated markets 17%.**
- Practical takeaway: Efficiency and loss reduction are the primary realized gains; competitive positioning is real but **~23%,** not a majority.

Conclusion: Your Evidence-Based CMMC 2.0 Roadmap

Our data shows that winners don't just work harder—they work strategically.

6 Decisions That Determine Success

1 Measure What You Manage

Allocate 35% of your CMMC budget to documentation (vs. the failing average of 18%). This isn't bureaucracy—it's the foundation that prevents the 30x encryption failure rate plaguing undocumented organizations.

2 Formalize Third-Party Risk—Start With Contracts

- Among CMMC respondents: **Regular supplier audits 48%, TPRM tools 38%, contractual security requirements 22%, governance control & tracking 38%.**
- Across sizes, third-party vendor compliance is the most common challenge. Prioritize contract clauses and keep a steady audit cadence.

3 Right-Size Your Approach by Organization Size

- **Under 5,000 employees:** most-used actions—new technical controls **37%, updated policies/DPAs 33%; top-tier encryption 52%.**
- **5,000–9,999: updated policies/DPAs 36%** (tie with **increased budget 36%); top-tier encryption 59%** (highest).
- **20,000+: new technical controls 38%; top-tier encryption 38%** (lowest).
- Interpretation: mid-market programs pair policy/budget work with the strongest outcomes; the largest organizations should **balance new controls with governance and supplier contracts.**

4 Prioritize Regulatory Change and Vendor Compliance

CMMC programs prioritize regulatory change and vendor compliance more than the broader market (Top-2 +3 pp and +7 pp), while budget and jurisdictional overlap matter less. Therefore, measure first, formalize governance, and close the supplier-contract gap—then maintain an audit cadence to sustain encryption gains.

5 Use Partners Intelligently (don't expect magic)

- Partnering = “engaged external consultants.” With measurement in place, **partner vs. solo** produces **similar outcomes** (top-tier ≈45%; low-encryption ≈20%).
- For **under-5,000 CMMC** organizations the partner cell is **tiny** and does **not** outperform; pair any partner work with **internal ownership + measurement.**

6 Set Realistic Benefit Expectations

- Reported benefits (select top-2): **operational efficiency 54%, reduced security losses 48%, innovation 29%, customer loyalty 29%, competitive advantage 23%** (27% among CMMC).
- Plan communications around **efficiency and loss reduction** as primary wins; treat competitive positioning as a **real but minority** outcome.

Legal Disclaimer

The information provided in this report is for general informational purposes only and should not be construed as professional advice. Kiteworks makes 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.

The data in this report was analyzed using AI and the content was generated with AI assistance. While AI enhances analytical capabilities, it can occasionally produce errors or biased information that should be considered when reviewing these findings.

Kiteworks

September 2025

www.kiteworks.com