Kaseya® | CHANNEL MASTERED

WHITEPAPER

Compliance as a Service for MSPs

The revenue-generating managed service your customers need—and you can deliver today

Powered by Kaseya Compliance as a Service

Introduction

MSPs have always had two ways to grow profitability: sell more services or reduce costs. For MSPs that have already deepened relationships with existing customers, adding new services to their catalog is the only reliable path forward. Compliance as a Service (CaaS) is the most promising addition most MSPs are not yet making.

Kaseya—a provider you've likely already relied on for RMM, PSA, backup, and security—has built a purpose-designed Compliance as a Service program specifically to help MSPs capture this opportunity. This paper makes the case for why now is the right time to capitalize on compliance services, what the revenue looks like across multiple verticals, and how Kaseya's CaaS framework lets you enter the market regardless of where your team stands today.

The demand is here now

The numbers on the CaaS opportunity tell a striking story. According to the ScalePad 2026 MSP Trends Report, only 36% of MSPs currently offer formal compliance services, meaning nearly two-thirds of the market has yet to enter the space at all. The same research found that compliance-focused MSPs are significantly more likely to project revenue growth exceeding 50% in 2026. [1] The CyberSmart MSP Survey 2026 reinforces this: 61% of MSPs are now expected by their customers to help meet compliance needs, a customer mandate that is growing faster than MSPs are staffing for it. [2]

Customers in regulated industries are feeling the pressure especially acutely. Thomson Reuters' Cost of Compliance research estimates global organizational spending on regulatory compliance at $304 billion in 2025, with average SMB compliance spend climbing roughly 62% since 2020. [3] A 40-person medical practice answers the same HIPAA Security Rule questions as a regional hospital system but cannot hire a compliance officer of its own. They can, and will, hire you.

The regulatory landscape driving compliance demand is not slowing down either. HIPAA enforcement by the HHS Office for Civil Rights imposed more than $144 million in cumulative penalties through 2025, with enforcement activity still climbing, and over 55% of those penalty actions targeted practices with fewer than 50 employees. [3] The EU AI Act is phasing in penalties reaching 7% of global revenue, state privacy laws continue to multiply across the U.S., and meeting Cybersecurity Maturity Model Certification (CMMC) mandates is now a condition of keeping Department of Defense contracts for more than 300,000 companies in the Defense Industrial Base as well.

What makes this moment different from prior regulatory cycles is its scale and simultaneity. Multiple frameworks are tightening at once across healthcare, defense, financial services, legal, and manufacturing. No single vertical is driving the opportunity, all of them are. Fully 63% of organizations surveyed in ISC2's 2025 Cybersecurity Workforce Study report staffing shortages, which means SMBs cannot solve this internally even when they want to. [4] The talent gap and the compliance mandate are converging, and the MSP who shows up with a credible compliance capability is the one who wins the account.

Kaseya's own research reinforces the picture: nearly 70% of MSP customers are already asking for compliance support, yet only about 15% of MSPs currently offer it. Compliance now ranks as the service MSPs say they are most likely to add in the coming year, ahead of everything else on their roadmap. [13]

This is a long-term, MRR-generating engagement, not a one-time project

The most important thing to understand about compliance is what it is not: a project you deliver and close out. Compliance is an ongoing process of assuring adherence to a wide and fluctuating set of rules, regulations, and specifications. Being compliant once doesn't protect a customer when an incident happens six months later. That continuous nature is precisely what makes it such an attractive managed service that's billed monthly, renewed annually, and difficult to unwind once embedded.

Every assessment also surfaces remediation requirements and expansion opportunities beyond the compliance checklist itself: unpatched systems, missing MFA, exposed credentials. Compliance is often the entry point into a customer's full security stack, not a service that sits apart from it. MSPs who treat the first compliance engagement as a door-opener consistently find themselves managing a much broader relationship within 12 to 18 months.

The cost of waiting is measurable

The consequences of non-compliance are no longer hypothetical. The IBM Cost of a Data Breach Report 2026 pegs the average healthcare breach cost at $6.64 million, the highest of any industry for the 13th consecutive year. [5] For SMBs specifically, breach costs in 2026 are running between $120,000 and $1.2 million for typical incidents, and ransomware recovery costs average over $1.5 million. Roughly three in five small businesses closes permanently within six months following a major cyber incident. [6]

MSPs carry real exposure here too, not just their customers. One documented case involved an MSP whose own marketing language—claiming to be a "one-stop shop for all IT needs"—became evidence used against them when a client lost $1.7 million to a phishing scam. [7] Courts and insurance carriers increasingly evaluate whether an MSP followed standard industry practices, and cyber insurers have begun suing MSPs directly to recover what they paid out on customer claims. [8, 9]

These cases are not reasons to avoid compliance work. They are reasons to do it properly and document it thoroughly. An effective, documented compliance program helps businesses significantly reduce fines and penalties under federal sentencing guidelines when something goes wrong, and it provides the MSP a defensible record of due diligence. [10] Kaseya's Compliance Manager GRC is built specifically to produce that documentation continuously, not just at audit time.

The high-stakes opportunity: CMMC and the defense industrial base

CMMC is worth examining in depth because it illustrates both the stakes and the revenue potential in concrete terms. Phase 1 enforcement began in November 2025. The Pentagon temporarily suspended ramp-up of Phase 2 requirements in July 2026, but Phase 1 requirements remain in effect and the pause does not reduce urgency. If anything, it increases it for MSPs who act now. Consider these facts:

- According to independent research, only 8% of defense contractors requiring Level 2 certification had achieved it as of February 2026.
- Industry analysts project C3PAO assessment backlogs of 24 to 30 months by late 2026. [11]
- There are more than 300,000 companies in the Defense Industrial Base, most too small to have any internal path to certification.
- The global CMMC compliance services market is projected to exceed $3.6 billion by 2033 driven entirely by mandatory enforcement.[12]

The DoD's own estimates frame entry-level costs. A Level 1 self-assessment runs approximately $10,000 per year. Level 2 obligations run $45,000 to $130,000 over a three-year cycle. Level 3 certification costs approximately $60,000 per cycle. But those figures cover assessment fees alone. The larger revenue is in what surrounds them:

- **Gap assessments:** $5,000–$35,000
- **Remediation and implementation:** $35,000–$250,000+
- **Virtual CISO support:** $50,000–$300,000 on larger engagements
- **CUI enclave hosting:** $3,000–$4,000+ per month
- **Required security tooling:** $10,000–$50,000 per year

Taken together, a single CMMC customer commonly represents roughly $387,000 in value over three years, including approximately $252,000 in recurring monthly services and $135,000 in one-time project work, plus $200 to $300 per machine per month in ongoing compliance revenue. [13]

> **In 2025, the Department of Justice collected more than $26 million in False Claims Act settlements** from contractors that claimed to have deployed NIST 800-171 controls they had not actually implemented.

The legal and reputational exposure of getting this wrong is real. Kaseya's on-demand session on the final CMMC rule is a practical next step for MSPs preparing to pitch defense-adjacent customers. [14]

36%

of MSPs currently offer formal compliance services [1]

$304 B

spent globally on regulatory compliance in 2025 [3]

8%

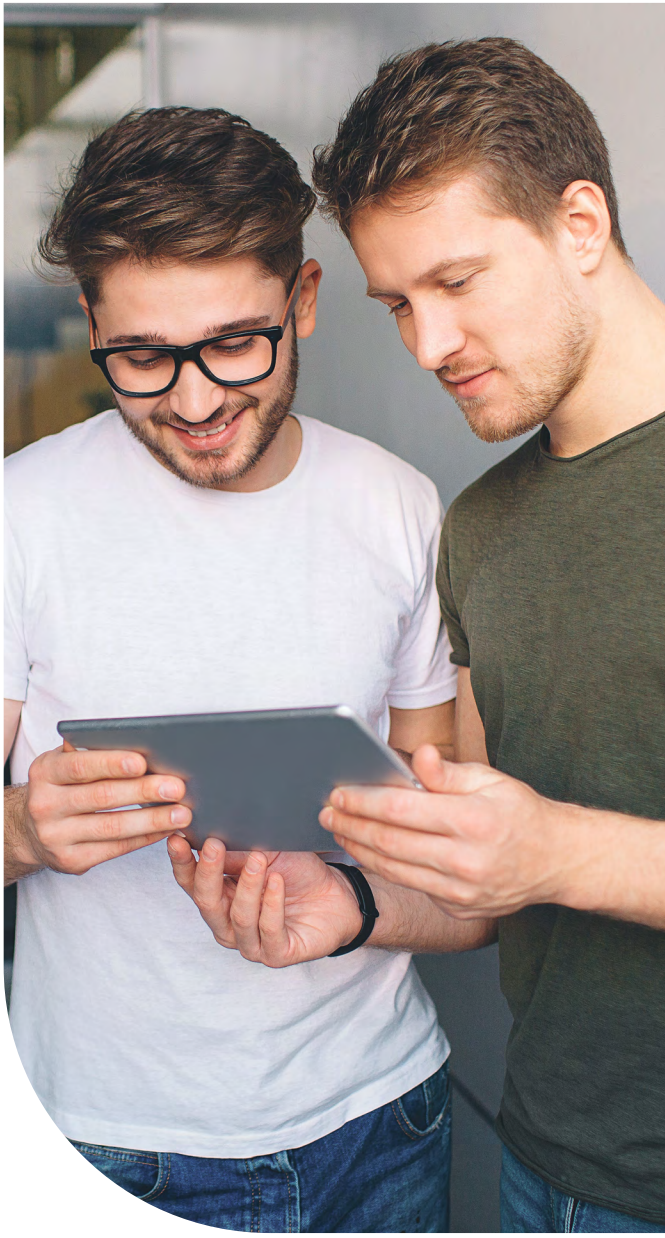
of DIB contractors hold CMMC Level 2 certification [11]

Revenue projections across verticals

CMMC gets the attention, but the compliance opportunity extends well beyond the Defense Industrial Base. Consider a single customer with 45 seats: a base managed services contract is worth roughly $53,000 per year. Add continuous compliance monitoring and that same customer is worth $100,000 to $230,000 per year with no new logo, no new sales cycle required. [13]

Healthcare-focused MSPs command 25–35% pricing premiums over generalist providers, reflecting the HIPAA expertise and liability that comes with those engagements. MSPs who specialize in frameworks like CJIS (criminal justice information) command even higher premiums, as that expertise is rare and the stakes are high. [15] vCISO adoption has also surged: one industry survey found vCISO services skyrocketed 319% in 2025, with 96% of surveyed MSPs reporting moderate to high customer interest. [16] Compliance is the natural on-ramp; the same customer worried about an audit is exactly the customer who needs fractional CISO-level guidance.

The retention and competitive moat



The retention effect ultimately matters as much as the upfront revenue. A customer worried about an audit wants a single point of contact, not three vendors to coordinate. Once you manage a customer's compliance posture, moving away from you becomes a disruptive and expensive process with no clean handoff on continuous monitoring. That stickiness is structural, not just relationship-based.

Offering compliance services to net-new clients also positions you to displace their existing MSP and take the entire account. The MSP who brings compliance capabilities proactively tends to be described in board meetings and referrals as the provider who anticipates problems. The MSP who waits to be asked tends to be managed.

You're the managed service provider. Don't require your customers to manage you.

How Kaseya makes this possible

The most common reason MSPs stay out of the compliance market is not technology. It's the assumption that they need in-house compliance experts before they can begin. Kaseya's Compliance as a Service program was built specifically to remove that barrier. For your customer, Kaseya CaaS replaces a one-time audit with continuous monitoring and automated evidence collection, so documentation is ready whenever a regulator, insurer, or auditor asks for it. For you, it provides the platform, training, and expert support needed to sell and deliver compliance outcomes confidently, and without building a compliance department first.

Kaseya CaaS offers four entry points, designed to meet you wherever you currently stand:

Tooling

Compliance Manager GRC

Scans against CIS Benchmarks, maintains a live risk dashboard, and automates evidence collection auditors ask for.

Expertise

Kaseya professional services

Kaseya's team delivers engagements white-label while you remain the customer's primary contact.

Training

CMCP Ccertification

Build real in-house expertise through Kaseya's Certified MSP Compliance Professional program.

Partners

Trusted compliance partners

Source work to partners like Arrakis Consulting and split revenue—a fast path to earnings while you scale.

These are not four permanent tracks. They are four on-ramps to the same road. MSPs that start by partnering with a Trusted Compliance Partner commonly bring work in-house once they have the customer base and internal confidence to justify it. MSPs that start with tooling often pursue CMCP certification a year in. The framework is designed to grow with your business.

Kaseya Compliance Manager GRC: What it does

Continuous scanning against CIS Benchmarks across your customer environments.

Live risk dashboard so you and your customers always know where gaps exist.

Automated evidence collection that replaces hours of manual documentation before every audit.

Multi-framework support covering CMMC, HIPAA, SOC 2, PCI-DSS, and state privacy frameworks.

Virtual CISO capability on roadmap: automatically aligns each customer's industry to applicable standards and schedules required assessments.

Building your practice: Practical first steps

Kaseya recommends two internal exercises before your first external compliance engagement.

Run the complimentary Kaseya Security Baselining Assessment on an existing customer. Start with a client who already trusts you. The assessment gives your team a real engagement to learn from and produces a finished sample report you can show future customers.

Be your own customer zero. Run SOC 2—the simplest widely-requested framework—on your own MSP business before selling it to clients. It becomes your training exercise and proof of competence, and ensures your first client conversation is not also your first attempt at the work.

On packaging, structure your compliance offering into well-defined tiers before the first sales conversation: a baseline assessment tier, an advanced remediation tier, and a full continuous compliance tier. Pricing and scope should be settled before the customer asks. Ambiguity in scope is the single most common cause of margin erosion on compliance engagements.

Know when the money moves. Compliance spend is not distributed evenly across the year, and the lead time between outreach and closed business is longer than most MSPs expect:

Vertical	Outreach window	Notes
Healthcare / HIPAA	February	Budget approved in June; outreach must start 4 months prior.
Defense / CMMC	Year-round	Urgency driven by contract timelines, not fiscal year. Lead with urgency.
Financial services	Q3 (Sept)	Fiscal year ends Dec 31; compliance budget set in Q4 planning.
Legal / professional	Q2 (Apr)	Mid-year reviews common; spring is the window for new service adoption.
Manufacturing / CUI	Q1 (Jan)	Post-audit season; January conversations capture remediation budget.

Every vertical has a version of this timing. A healthcare prospect you reach in July has already spent their compliance budget. Knowing the calendar changes when and how you prepare, market, and pitch.

Plan for the security work that comes from assessments

Compliance engagements routinely surface remediation requirements and stack expansion opportunities beyond the specific compliance checklist. Determine in advance how you will price and deliver that work so you are never negotiating scope on the fly in the middle of an engagement. Every gap found is a potential project, and every project is a potential tool that requires ongoing management.

As with any new service line, plan to iterate. Very few MSPs get the model right in the first two or three engagements. What matters is starting with the entry point that fits today and adapting as your practice matures. Revisit your pricing, delivery process, and packaging after your first few engagements.

Get started now with Kaseya

Ten businesses are asking for compliance help for every MSP currently able to deliver it. That gap will not stay open indefinitely. Every month spent evaluating is a month competitors spend building sticky, recurring relationships that are structurally difficult to unseat.

Kaseya's complimentary Security Baselining Assessment is the fastest way to find out how much of the CaaS opportunity is already sitting inside your existing customer base. It takes minutes to run and gives you a finished report that serves as both a training tool for your team and a proof-of-competence document for future prospects.

Your next steps with Kaseya CaaS

Step 1: Run the complimentary Kaseya Security Baselining Assessment on one or two existing customers. Visit https://www.kaseya.com/request/demo/ to get started.

Step 2: Explore Kaseya Compliance Manager GRC here and here, and identify which of your current customers are in regulated verticals.

Step 3: Connect with a Kaseya CaaS specialist to discuss whether the Tooling, Expertise, Training, or Partners entry point best fits your practice today.

Step 4: Watch Kaseya's on-demand CMMC session to prepare your team for defense-adjacent customer conversations.

The CaaS market is the largest underserved opportunity in the MSP channel right now. Kaseya has built the platform, the training, and the partner network to help you capture it. The question is how quickly you move.

Sources

1. ScalePad, "2026 MSP Trends Report," March 2026. scalepad.com
2. CyberSmart, "MSP Cybersecurity Survey 2026," June 2026. cybersmart.co.uk
3. Thomson Reuters, Cost of Compliance 2025; HIPAA Journal / HHS OCR enforcement data, as cited in "The Small-Business Compliance Crunch," Nexzen Software, April 2026.
4. CompTIA, "State of the Tech Workforce" / IT industry outlook data, as cited in MSP industry analysis, 2026.
5. IBM, Cost of a Data Breach Report 2026.
6. Total Assure, "Cybercrime Costs in 2026 for SMBs," July 2026. totalassure.com
7. "MSP Sued: Are You Ready?" Semel Consulting, April 2021. semelconsulting.com (reported case)
8. "The Hidden Legal Risks MSPs Ignore Until They Lose a Client or a Lawsuit," TechLawyers.com
9. "Cyber Insurer Sues Policyholders' Cyber Pros," Hunton Andrews Kurth Privacy & Cybersecurity Law Blog.
10. U.S. Sentencing Commission, 2018 Guidelines Manual, Chapter 8.
11. IBSS Corp, "Cybersecurity Compliance Statistics: Federal Contractor Data Hub 2025–2026," May 2026. ibsscorp.com
12. Archive Market Research, "CMMC Consulting Service Market: Trends & 2033 Projections," June 2026.
13. Kaseya, "Compliance as a Service: The MSP Revenue Stream Customers Can't Opt Out Of" (Kaseya Connect 2026); supplementary interview with Kaseya risk management leadership and Carl Carpenter (Arrakis Consulting), July 23, 2026.
14. Kaseya, "CMMC Is Here: What the Final Rule Means for MSPs" (on-demand recording). info.kaseya.com/cmmc
15. Nuronus, "How to Price Compliance Services as an MSP: A 2026 Pricing Guide," August 2026. nuronus.com; HIMSS via Medha Cloud.
16. Cynomi, "The State of the Virtual CISO 2025," July 2025.

Kaseya®

Kaseya is the leading global provider of AI-powered IT management and cybersecurity software. Kaseya delivers a unified technology platform to manage infrastructure, secure endpoints, back up critical data, and streamline operations for more than 40,000 MSP and SMB customers around the globe. To learn more, visit www.kaseya.com.

kaseya.com