Propulsion

The 2026 SMB cybersecurity & compliance benchmark report

What 100+ business leaders admitted about flying blind on risk

Contents

Introduction:

What SMBs don't know about *their compliance*

Most small business leaders believe they're compliant. That belief—more than any gap in their tools, any shortage of staff, or any regulatory change they missed—is what this report is really about.

Late in 2025, Propulsion conducted 102 in-depth, one-on-one interviews with business leaders at U.S. companies ranging from 6 to 1,500 employees. These weren't checkbox surveys. With an average session running nearly 26 minutes, they were genuine conversations. Numbers capture what's happening, but the verbatim responses throughout this report capture *why*: how leaders reason about compliance, where their confidence (or lack thereof) comes from, and the hesitations a checkbox question would never surface. Participants were directors, C-suite executives, and owners: the very people responsible for keeping their businesses protected, trusted, and out of trouble.

What they told us is both reassuring and alarming… sometimes in the same sentence.

The reassuring part:

SMB leaders are not disengaged. They know compliance matters. They've designated someone to own it, put processes in place to manage it, and in many cases invested in tools to support it. On a 7-point scale, they rated their confidence in their compliance obligations at an average of 5.4. They rated their tools' effectiveness at 5.6. By those measures, most believe they're in reasonable shape.

The alarming part:

Much of that confidence rests on an assumption that the partner, the tool, or the internal owner they've relied upon is actually doing what they think. Many haven't verified it. Many can't. And the regulatory environment those assumptions are running against is the most complex, fragmented, and fast-moving it's ever been.

Key findings at a glance

38% of SMB leaders aren't sure which regulations apply to their business

40% are managing compliance primarily through spreadsheets

26% have concentrated their entire compliance function in a single overextended employee

64% cite limited internal resources as their #1 compliance challenge—ahead of cost, complexity, or any other factor

14% say the confidence they feel is largely secondhand: borrowed from an MSP, legal counsel, or outside vendor whose work they've never independently verified

4.6 out of 7 SMB leaders' average concern about audits and fines, where 7 means *not concerned at all*. That's dangerously close to comfortable in a regulatory environment that's increasingly targeting businesses of every size.

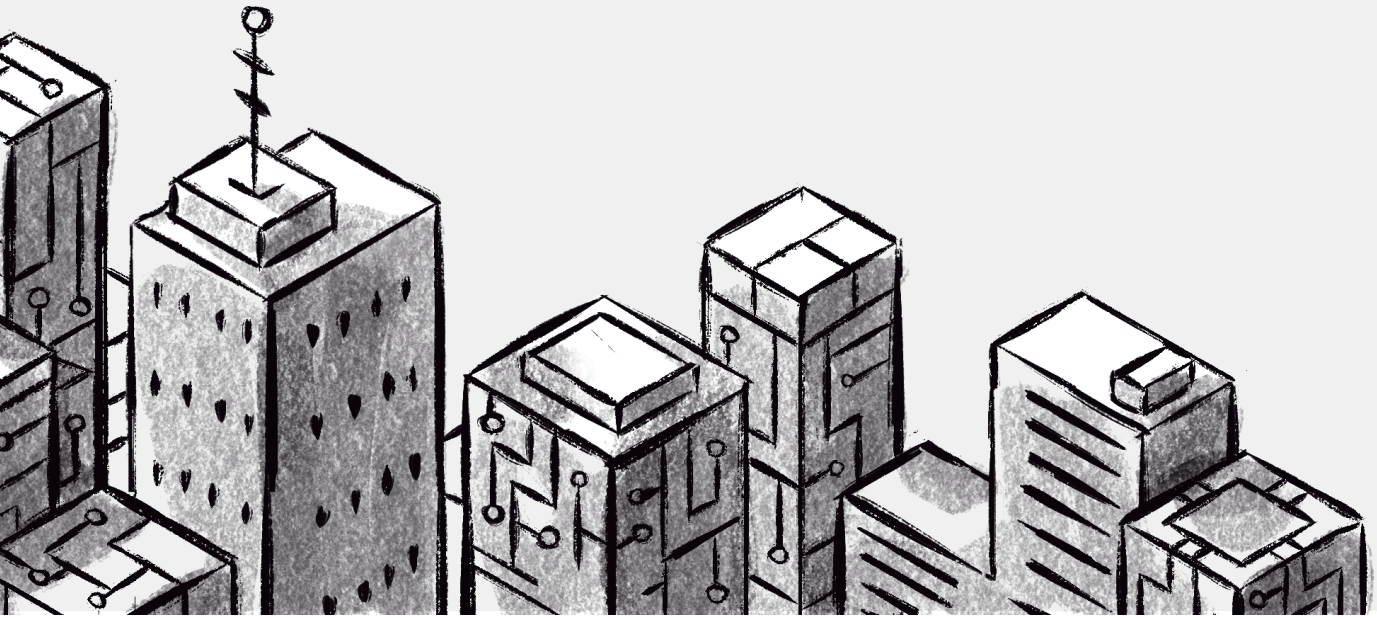
These numbers describe organizations doing their best with limited time, limited budget, and a compliance landscape that was never designed with their size in mind… but applies to them regardless.

Why this matters *right now*

Regulatory exposure is no longer proportional to company size. HIPAA, PCI-DSS, CCPA, CMMC, GDPR (frameworks that SMBs often assume apply primarily to large enterprises) apply based on what a business *does* and whose *data* it handles, not how many people it employs. Others, like SOC 2, are increasingly being pushed down the supply chain by larger customers and partners as a condition of doing business. Meanwhile, the landscape keeps expanding: new state privacy laws, AI regulations, and updated framework requirements are adding obligations faster than most SMBs can track them. The assumption that small businesses fly under the regulatory radar is increasingly difficult to defend.

At the same time, the "someone else handles it" approach—delegating compliance to an MSP, a legal counsel, or a single internal IT person—is becoming more consequential. Outsourcing expertise is well-founded when it comes with visibility, accountability, and proactive communication. But every major framework assumes a shared responsibility model: there are controls only the customer can own, decisions only the customer can make, and evidence only the customer can produce. When those boundaries aren't made explicit upfront, organizations are left with a gap between what they assume is covered and what actually is… and most won't discover it until something external forces the question.

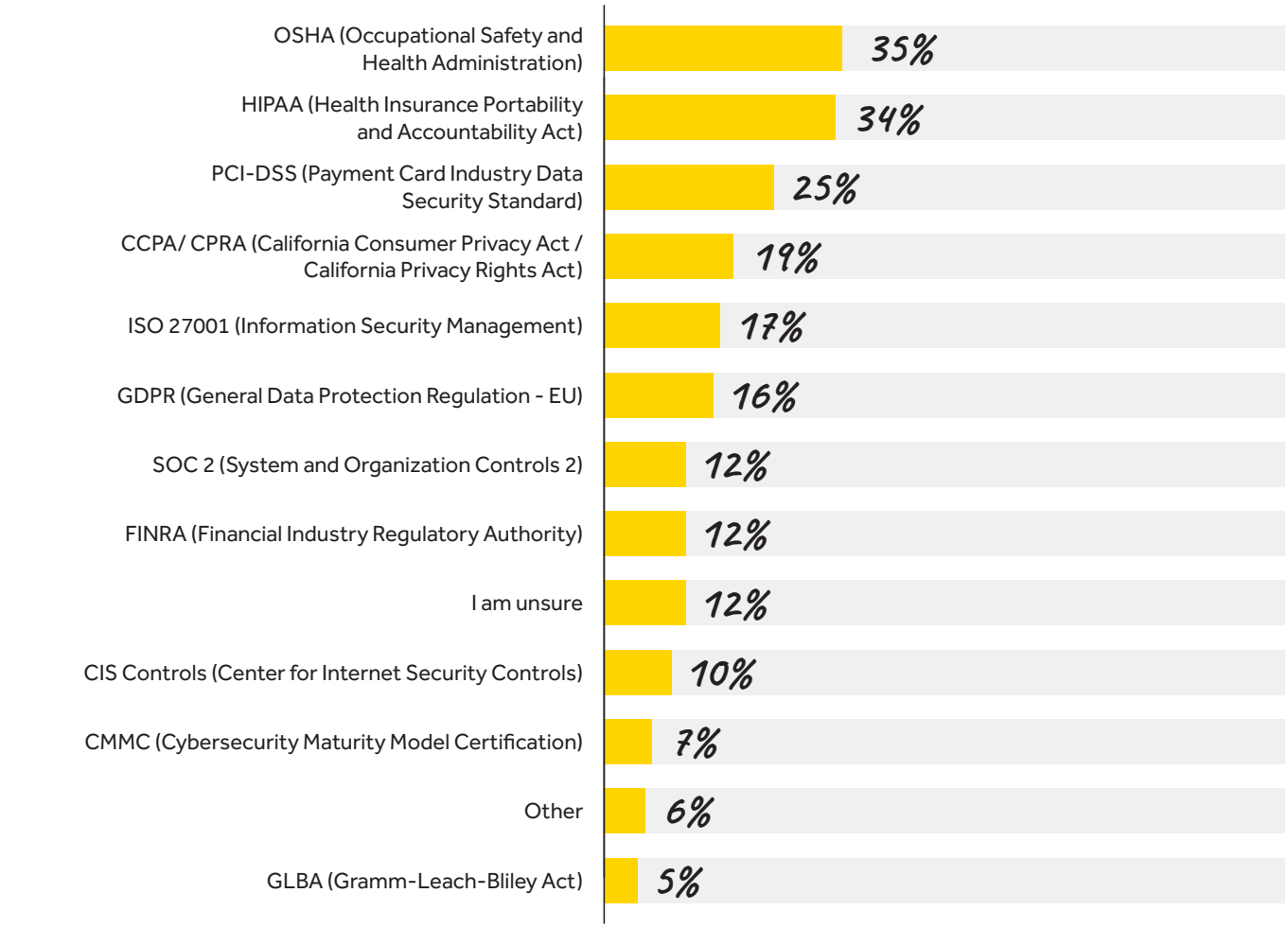
This report provides an accurate picture of where most SMBs currently stand. The distance between where organizations *think* they are and where they *actually* are is where the real risk lives; and closing it requires the right expertise, the right tools, and a partner with a genuine stake in the outcome.



Compliance knowledge *& awareness*

No universal standard, and widespread uncertainty about what applies

Which regulations or standards do you believe apply to your business today?



There *is* no single compliance standard for small businesses in the US. Depending on what a company does, who its customers are, where they're located, how it processes payments, and what data it generates or has access to, it may fall under the jurisdiction of HIPAA, PCI-DSS, GDPR, CCPA, OSHA, GLBA, SOC 2, CMMC, or some combination of all of them.

OSHA topped the list at 35%, followed closely by HIPAA (34%) and PCI-DSS (25%). Privacy regulations—GDPR, CCPA/CPRA—were cited by 16-19% of respondents. More specialized frameworks like CMMC, NIST CSF, and SOX registered in single digits. No single standard dominates, and no single framework applies universally. The scatter in those responses accurately reflects how fragmented the regulatory environment is.

Narrow experience, broad exposure

Asked why they identified the standards they did, respondents split almost evenly. Roughly half (51%) credited hands-on experience and structured training: years in their industry, annual courses, legal reviews, and established compliance routines. The other half (49%) cited uncertainty driven by the sheer volume and complexity of the rules themselves.

That split is telling. In almost every industry, confident and uncertain respondents sit side by side, often describing the same regulations. The confidence that *does* exist tends to be narrowly scoped: tied to one framework a leader has lived with for years, or one tool a vendor manages on their behalf. For many, it's less mastery than familiarity.

> **"I understand enough to have a conversation, but whenever I do have a conversation, I always pull up the information in front of me so that I'm aware of the rules and standards set in place."**
>
> - CIO, Healthcare, 6-20 FTEs

12% of respondents said they weren't sure which regulations applied to their business at *all*. (That number captures only the explicit "I'm not sure" responses. When hedged answers are included—"I think," "I rely on others," "it's constantly changing"—the share of leaders who can't confidently identify their obligations rises to 38%.)

Even deep experience has limits

Leaders who know the frameworks well still find themselves tripped up by shifting thresholds, enforcement gray areas, and evolving guidance. HIPAA, despite being one of the most mature frameworks, still produces edge cases that leave experienced leaders uncertain.

> **"I think I have a pretty good understanding of HIPAA after working in healthcare for over 12 years, but it's constantly changing and evolving, and there's a bunch of small nuanced things that I'm sure I'm not aware of. There's so much information that it's sometimes hard to navigate."**
>
> - CFO, Healthcare, 51-100 FTEs

Newer mandates like CMMC have left some respondents without a clear path forward at all.

> **"The CMMC requirements are extremely unclear and very challenging for me. And I don't actually have much support in that area in the company."**
>
> - Director, Manufacturing, 6-20 FTEs

When complexity wins, leaders delegate

For nearly one in four respondents (23%), the practical response to regulatory complexity is to hand it off—to legal counsel, outside IT vendors, managed service providers, or, in some cases, an internal compliance team or officer. That's a reasonable calculation. Running a business doesn't leave room for a parallel career in regulatory interpretation, and for many leaders, delegation is the only mechanism that lets compliance get done at all.

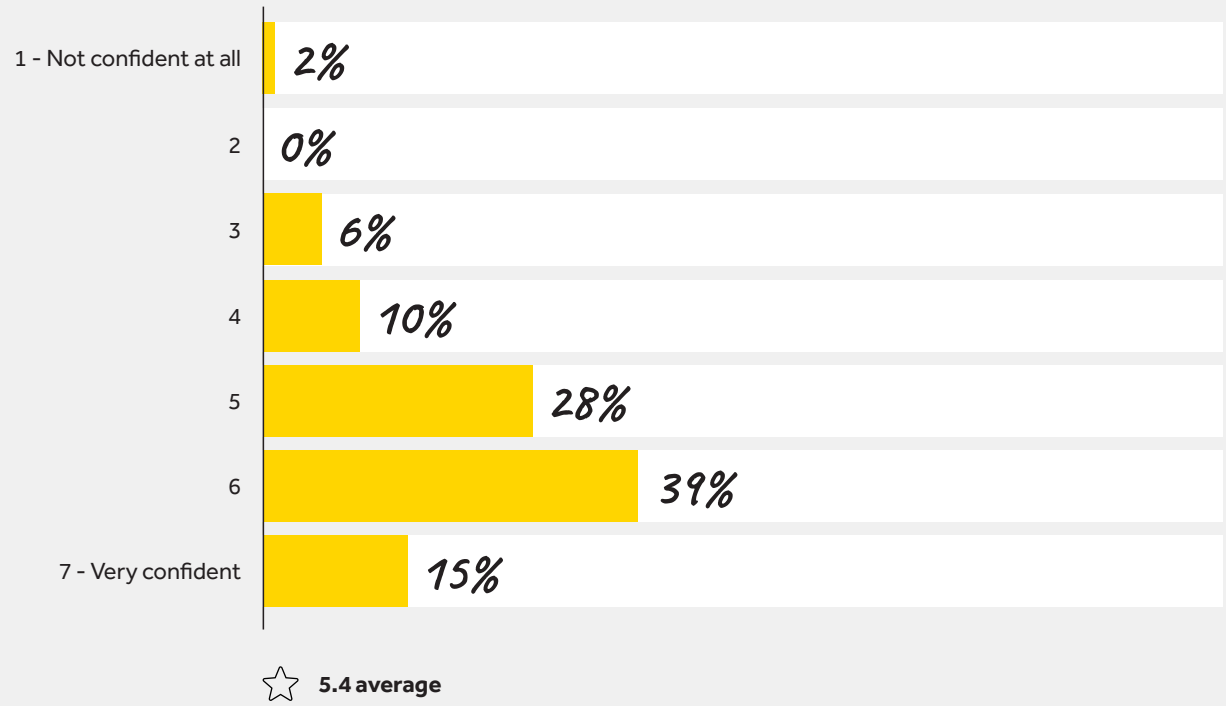
> **"I rely on outside vendors or our IT person to update us and tell us what needs to be done."**
>
> - Director, Non-profit, 51-100 FTEs

The leaders who delegate aren't disengaged. Most understand that compliance matters and that the stakes of getting it wrong are real. What they lack, consistently, is a clear line of sight into what "doing enough" actually looks like for a business their size.

> **"I kind of understand PCI-DSS but leave it up to my credit card company to handle. Should I be doing more?"**
>
> - Owner, Retail/E-commerce, 6-20 FTEs

Most SMB confidence stops at "probably fine"

On a scale of 1 to 7, how confident are you in your overall understanding of your company's compliance obligations?



On a 7-point confidence scale, leaders rated their understanding of their company's compliance obligations at an average of 5.4. That's a passing grade, on the face of it.

But the distribution tells a more complicated story. Only 15% of leaders gave themselves a 7. Nearly 40% gave a 6, and 28% gave a 5. Add those latter numbers together and roughly two-thirds of respondents landed in "probably fine" territory: comfortable, unverified, and exposed.

The ceiling nobody can reach

Across every category—experienced leaders, well-resourced teams, deeply regulated industries—almost no one claimed complete confidence. The reasons cluster around the same core problem: the landscape moves faster than any individual can track.

> **“Obligations are generally clear, but there’s always something that I don’t know, so I couldn't give it a 7.”**
>
> - Owner, Construction, 6-20 FTEs

Regulatory changes were cited by 20% of respondents as the primary reason for their score. Their baseline knowledge feels solid, but what they can’t shake is the anxiety that tomorrow’s rules might make today’s practices obsolete. For leaders operating across multiple states or internationally, that anxiety compounds with each new jurisdiction.

> **“The rules and regulations are constantly changing, and they're different from state to state. It’s really hard to stay up to date with the new laws and all the changes, so I rated it a 5.”**
>
> - Owner, Retail/E-commerce, 6-20 FTEs

The pace of change is one obstacle. The language of the regulations is another.

> **“What contributes to my uncertainty is the fact that [the regulations] are written in such legalese, and because they seem like a moving target.”**
>
> - CMO, Professional Services, 6-20 FTEs

Even respondents with years of direct compliance experience (finance professionals who've spent careers in regulated industries, compliance officers who run audits) stopped short of a 7.

> **“I scored myself a 4 because there seems to be a lot of continuing education around it. Things are continually changing, and I’m wondering if that information is trickling down to me and my department so I can manage the function on my end and contribute to our crisis management response team.”**
>
> - CMO, Healthcare, 51–100 FTEs

Confidence borrowed from others

For 14% of respondents, the confidence they *do* feel is largely secondhand: drawn from an MSP, legal counsel, compliance officer, or business partner. They rate themselves as capable because someone they rely on holds the knowledge they don't.

Relying on outside expertise is a sound strategy. An engaged partner makes it a durable one: proactively reporting to leadership so the organization develops its own line of sight into its compliance posture, rather than inheriting someone else's confidence on trust. The liability enters when the engagement runs passively in both directions: the client doesn't ask, and the partner doesn't tell. Leaders in that position are confident in something that has never caused them to question it.

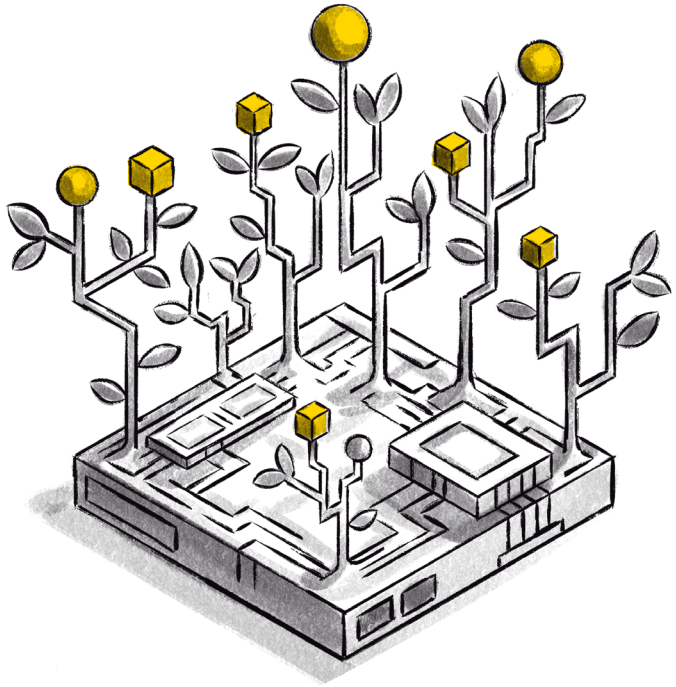
That arrangement works until it doesn't.

> **"Sometimes there's a gray area where things aren't 100% clear, especially if you're being audited. Auditors' interpretations of the requirements differ. You just sort of need to give it your best shot."**
>
> - IT Manager, Healthcare, 1001-1500 FTEs

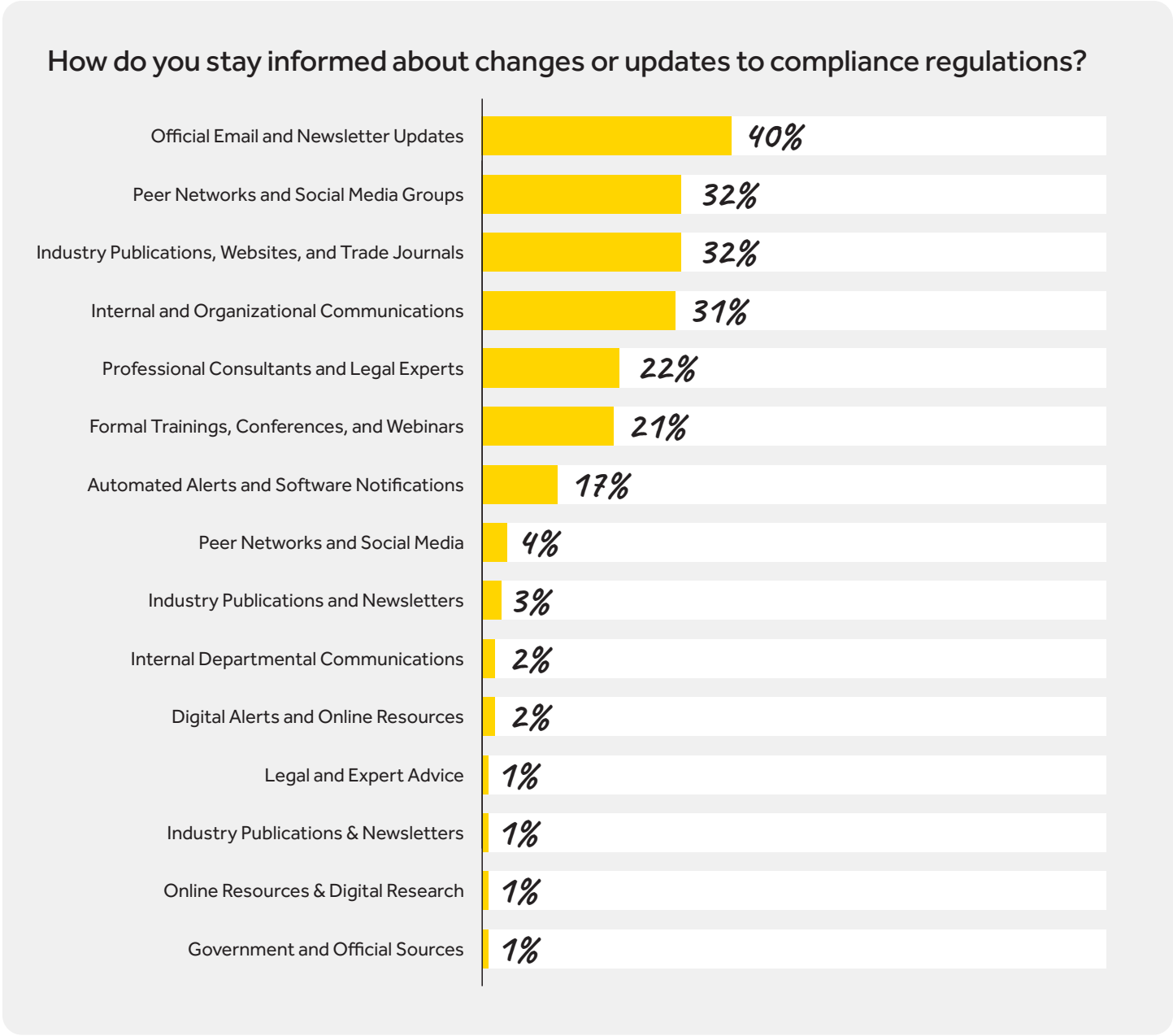
What a 5.4 really signals

The average confidence score reflects a recognizable posture: leaders who know enough to know they don't know everything. That's a more honest position than overconfidence—and a more dangerous one than it appears.

Businesses operating at a 5 or 6 out of 7 are making daily decisions about data handling, vendor contracts, employee records, and payment processing on the assumption that they're *probably compliant*. The exposure accumulates in the space between *probably* and *actually*.



Staying current is a patchwork job with no single reliable source



Staying current as regulations evolve is a job unto itself; and for most SMB leaders, there's no reliable method for doing it. Respondents named more than a dozen distinct sources: agency newsletters, peer networks, legal counsel, trade journals, internal communications, and automated software alerts. Notably, 15% reported using AI tools like ChatGPT and Claude to interpret new regulations and generate quick summaries: an emerging practice that's already prompting some organizations to put formal AI-use policies in place.

The top seven alone span every corner of the information landscape, with no single source cited by more than 40% of respondents. Every leader is conducting their own search, through their own mix of channels, with no guarantee they're finding everything they need.

Waiting to be told

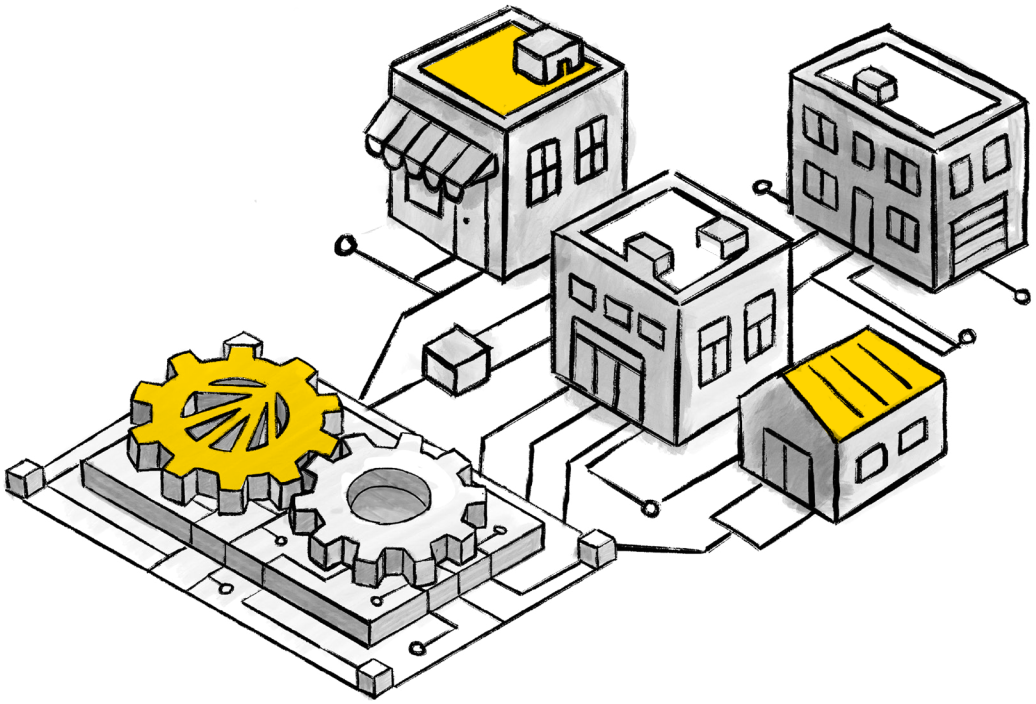
Beneath the variety of sources, a consistent preference runs through the responses: most leaders would rather *receive* compliance updates than go looking for them. Newsletters dominate the list in part because they require nothing of the reader.

That preference is understandable. SMB leaders are running businesses, not compliance departments. But passive monitoring has a structural weakness: it only surfaces what the source decides to send. Updates that fall between newsletters, regulations that no vendor covers, changes that don't make the trade press—all these slip through.

> **"I find newsletters to be the most helpful and reliable because they come to me without me having to do anything, whereas conferences or other things actually require me to go out and find the information."**
>
> - CFO, Non-profit, 51-100 FTEs

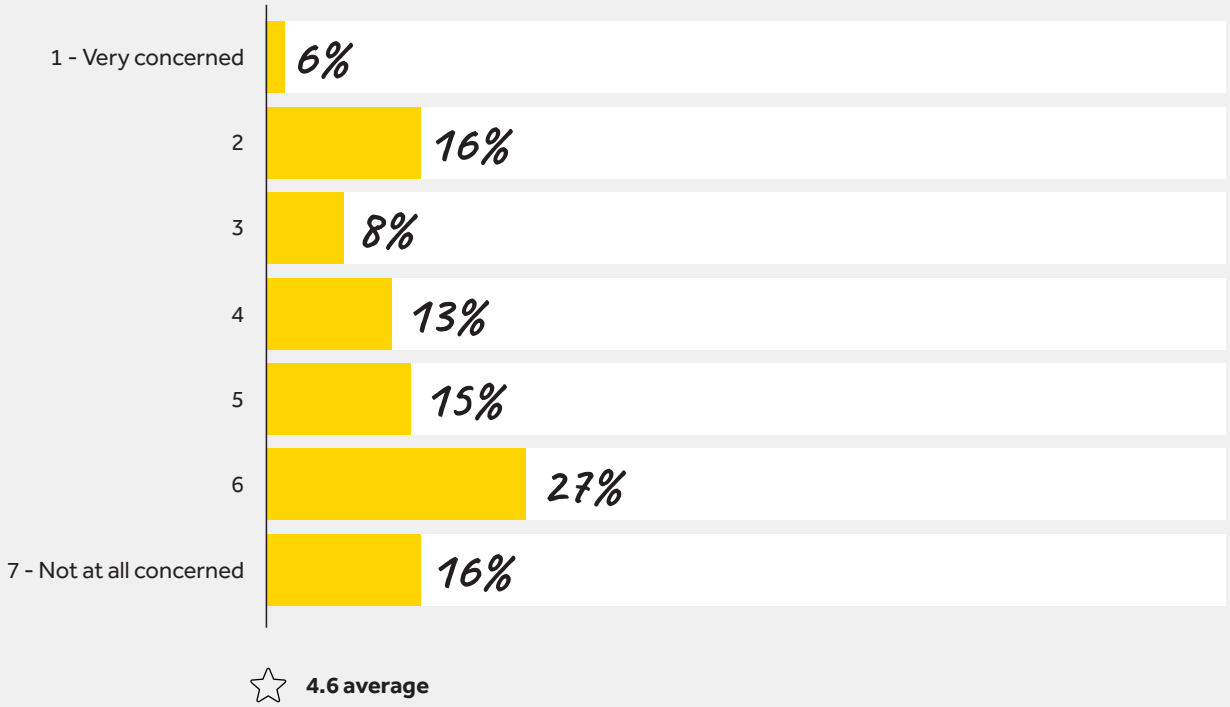
> **"HIPAA I kind of rely on the government to tell me what I need to do. PCI-DSS I hope the credit card company will alert me on changes."**
>
> - Owner, Retail/E-commerce, 6-20 FTEs

"Hope" isn't a compliance strategy. But for a significant share of SMB leaders, it's the closest thing to one they have.



Many SMBs have underestimated the audit risk

How concerned are you about the risk of being audited or fined for non-compliance?



On a 7-point scale measuring concern about audits and fines (1 meant “very concerned” and 7 meant “not at all concerned”), SMB leaders averaged a 4.6. On its face, that reads like measured confidence: leaders are aware of the risk but aren’t losing sleep over it. Read against everything else in this data, that number deserves a closer look.

The small-fish logic

A notable share of respondents expressed low concern for a different reason: they simply don't think they're worth targeting. The assumption that regulators have bigger fish to fry runs across company sizes, and it's one of the more persistent misconceptions in this data.

Even leaders at mid-sized firms express the same logic: that regulators have bigger targets to pursue, more revenue to recover elsewhere, and less reason to look their way.

> **"We're such a small company that it doesn't really matter. We're not gonna be targeted unless we do something really, really bad."**
>
> - General Counsel, Legal Services, 6-20 FTEs

> **"I think they would probably audit the larger companies first, because there's more revenue to be had. They probably wouldn't spend as much time on smaller fish like us."**
>
> - CMO, Financial Services, 1,001-1,500 FTEs

If that reasoning persists at a thousand-person company, it's almost certainly more entrenched at twenty. And it's increasingly at odds with reality. Regulatory enforcement has expanded its focus on SMBs—particularly in healthcare, financial services, and data privacy—precisely because small businesses often lack the controls that larger organizations have in place. A small target isn't an invisible one.

Frameworks with teeth

The small-fish logic collapses fastest in frameworks built around concrete penalties. CMMC, the Department of War's (formerly the DoD's) cybersecurity certification, applies to roughly 230,000 small businesses in the defense supply chain—about 4% of all U.S. small employers—and carries treble damages, contract termination, and personal liability for executives who misrepresent their compliance.

7% of survey respondents flagged it as applicable to their business; just 2% reported actively following it. The latter number is the more revealing one. Even when SMBs *know* CMMC applies to them, most aren't yet doing the work; and within the defense industrial base specifically, most SMBs subject to CMMC don't yet realize they are. Requirements flow down from prime contractors to subcontractors at every tier, and many SMBs hold the kind of data that triggers the requirement without recognizing it.

CMMC:

the framework most SMBs don’t know applies to them

Small businesses make up

73%

of the U.S. defense industrial base.

~230k

of them are now subject to CMMC, and most don’t know they are

The Cybersecurity Maturity Model Certification (CMMC) is the mechanism the U.S. Department of Defense (renamed the Department of War in September 2025) uses to assess and enforce cybersecurity standards across the defense supply chain. The standards aren't new: contractors handling federal contract information (FCI) or controlled unclassified information (CUI) have been required to meet NIST SP 800-171 since 2017, with self-attested compliance scores filed in the federal SPRS system. Until CMMC, that all relied on the honor system.

You may already be in scope

CMMC requirements flow down from prime contractors to subcontractors at every tier. A small business doesn't have to call itself a "defense contractor" to be subject to it. It only has to handle the relevant data somewhere in its work for a federal customer, even several layers removed. Machine shops, software firms, and specialty manufacturers are all affected when their work touches federally controlled data.

Many SMBs first encounter CMMC through a prime contractor's deadline: a security questionnaire, a contract clause, or a notice giving them 60 days to demonstrate Level 2 readiness or be cut from the supply chain.

The cost of getting it wrong

CMMC is enforceable through the False Claims Act, the federal law that penalizes contractors who misrepresent their compliance with government requirements. Penalties include treble damages, contract termination, and potential personal liability for executives who attest falsely. Individual cases have cost contractors more than $11 million, and false attestations can carry criminal penalties of up to 20 years in prison. No breach is required to trigger enforcement; an inaccurate self-reported security score is enough. Beyond the legal exposure, non-compliant contractors lose the ability to bid on new DoD/DoW work entirely.

Why CMMC isn’t just an IT project

CMMC is an operations problem that pulls in nearly every function of the business. HR rewrites how it conducts background checks and role-specific training. Sales changes how bid proposals are received and routed. Operations adds physical safeguards like locked rooms and visitor logs. Finance documents where federal data flows through systems. Most of the engagement goes to documenting and proving that controls operate as defined, across the entire organization, with audit-grade evidence collected over months.

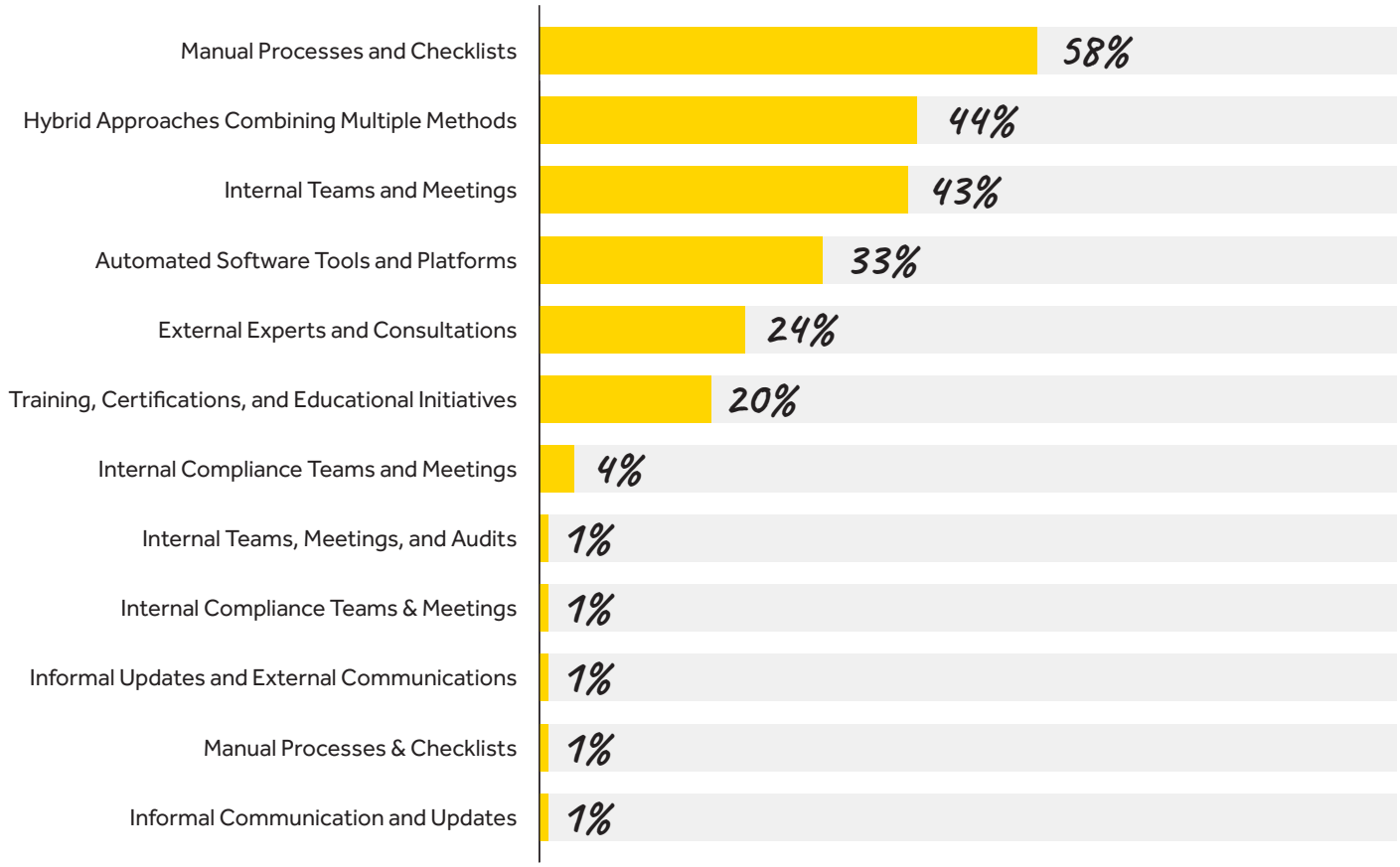
How to know if this might apply to you

Three signals suggest CMMC may apply: any of your customers do work for the federal government, even indirectly; your contracts reference DFARS, FAR, ITAR, or EAR clauses; or you've been asked to complete a security questionnaire or demonstrate cybersecurity posture as a condition of bidding. If any of these are true, you may already be in scope.

Current compliance *practices & support*

Most SMB compliance programs run on intention, not infrastructure

How is your organization currently meeting its compliance requirements?



For most SMB leaders, the answer to "how do we manage compliance day to day?" is a spreadsheet. Or a binder. Or a calendar reminder. Or, in some cases, memory. 58% of respondents described manual processes: paper checklists, shared spreadsheets, calendar reminders, and periodic self-audits conducted by whomever happens to have bandwidth. 43% rely on internal teams and recurring meetings. Only one-third (33%) described using automated software tools, and just a quarter (24%) engage external experts as a regular part of their compliance process.

Spreadsheets and good intentions

Leaders are building the best systems they can with what they have.

> **“Now we have a lot of spreadsheets and reminders in terms of steps needed. Due dates and start and end dates to anything we need to renew or maintain compliance.”**
>
> - CFO, Healthcare, 51-100 FTEs

> **“It’s just a pen to paper audit, usually done by myself as CEO or somebody else in the C-suite.”**
>
> - CEO, Non-profit, 51-100 FTEs

C-suite executives—the people responsible for strategy, growth, and organizational health—are conducting manual compliance audits *themselves* because there’s no one else to do it and no system to do it for them. That’s both a compliance risk and a significant drain on the leadership time that should be going elsewhere.

> **“Manual checks and audits mostly, but it would be nice to utilize a service that tracks it all for me so I don’t have to think or worry about it.”**
>
> - Director, Non-profit, 301-500 FTEs

The automation minority

A third of respondents have moved at least partially toward automated compliance tools: platforms that centralize control tracking, automate evidence collection, and flag issues in real time. But 33% is still a minority. And even within that group, automation tends to cover one framework or one function. A company using Secureframe for SOC 2 may still be managing HIPAA through a shared Google Doc. The tools are islands, not a system.

> **“We use Jira for issue tracking, Slack for communication, and our compliance management platform is Secureframe.”**
>
> - Director, Software, 201-300 FTEs

When no one calls

For some leaders, compliance isn't delegated to a person or managed by a system. It's entirely reactive, triggered only when an outside party flags something.

> **"If ADP calls and tells us we need to do something for HR compliance, we do what they tell us. If Bank of America tells us we need to do something on the financial side, we usually do it. For anything else, the approach is to ask Google: how do we do it, what should we do, what shouldn't we do"**
>
> - Director, Manufacturing, 6-20 FTEs

This is compliance as a waiting game. The problem? Not every violation calls ahead.

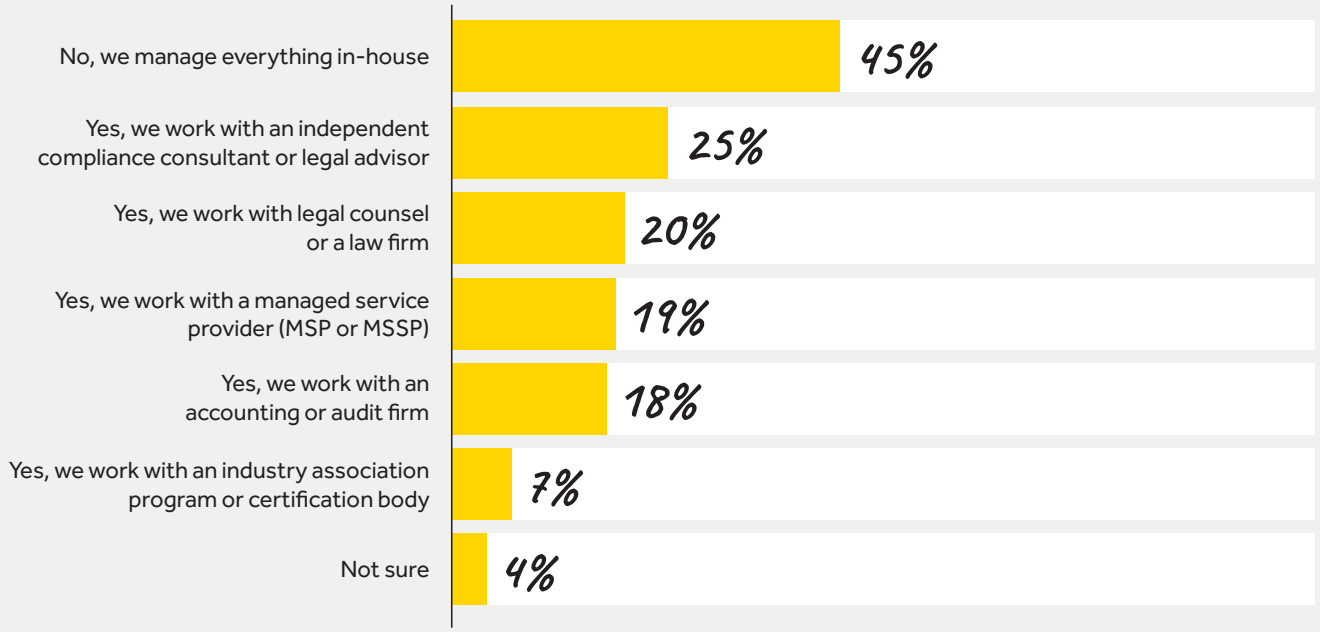
When the call comes from a customer

Another form of external pressure is reshaping the SMB compliance landscape, and Propulsion is seeing it accelerate across its customer base. Major customers and prime contractors are increasingly mandating entire frameworks as a condition of doing business. A Phoenix-based subcontractor for the major wireless carriers received a 60-day ultimatum to remediate the gaps in its security posture or lose the contract. A small business pitched to a larger partner discovered it needed SOC 2 certification, and had no idea what SOC 2 was.

This dynamic is increasingly the forcing function behind SMB compliance work. Larger organizations, having become more disciplined about their own supply-chain risk, are pushing requirements downstream. For their smaller suppliers, the choice is binary: get compliant on someone else's timeline, or get replaced. Compliance stops being a slow-burn obligation and becomes an existential one, often before the SMB has the systems, expertise, or budget to absorb the work.

Outside help is underused, misdirected, and poorly understood

Do you work with any external partners or consultants to support your compliance efforts?



45% go it alone because of cost

Nearly half of respondents manage compliance entirely in-house. For most, the decision comes down to one thing.

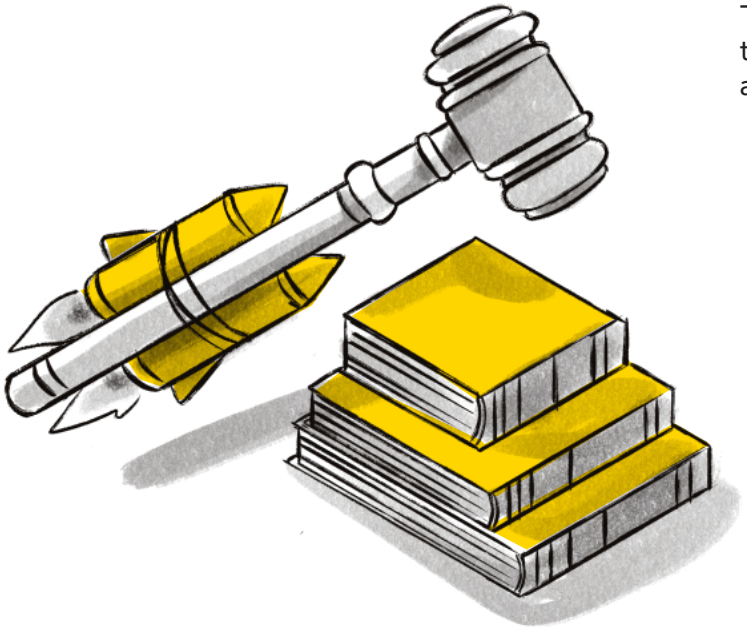
> **"I just feel like spending a lot of money for third party or external partners and consultants could be very costly, so we've pretty much just worked together internally."**
>
> - IT Manager, Other, 301-500 FTEs

The leaders who stay in-house have made a financial calculation, not a confidence one. For many, the status quo persists because the alternative feels out of reach.

Consultants and lawyers first, MSPs a distant third

Of those who *do* engage external partners, independent consultants and legal counsel are the most common choices (25% and 20% respectively). MSPs trail at just 19%, despite being the category best positioned to provide ongoing, integrated compliance support.

The relationships that exist tend to be long-standing: leaders describe partnerships of five, seven, ten, even thirty years. That continuity reflects trust, but it also raises a question about scope. A legal counsel retained for thirty years to review documentation is not the same as a partner actively monitoring the compliance landscape on a client's behalf.



> **"Working with an MSP has been very beneficial. At one point all of our IT operations were in-house, and we found that we had missed some spots in terms of cybersecurity and compliance because, with budgetary constraints, we just didn't have enough people."**
>
> - Head of IT, Education, 51-100 FTEs

That's the argument for outside support—lived, not theoretical. Yet only 19% of respondents work with an MSP.

The quality problem

Having an external partner and knowing what that partner does are two different things. For a meaningful share of respondents, the *relationship* exists but the *visibility* doesn't; and the arrangement is structured in a way that makes that problem hard to detect.

> **"I'm really not sure of our MSP's exact services. I just assume they're keeping track of these different updates as related to different legal aspects of complying with technology."**
>
> - Director, Non-profit, 51-100 FTEs

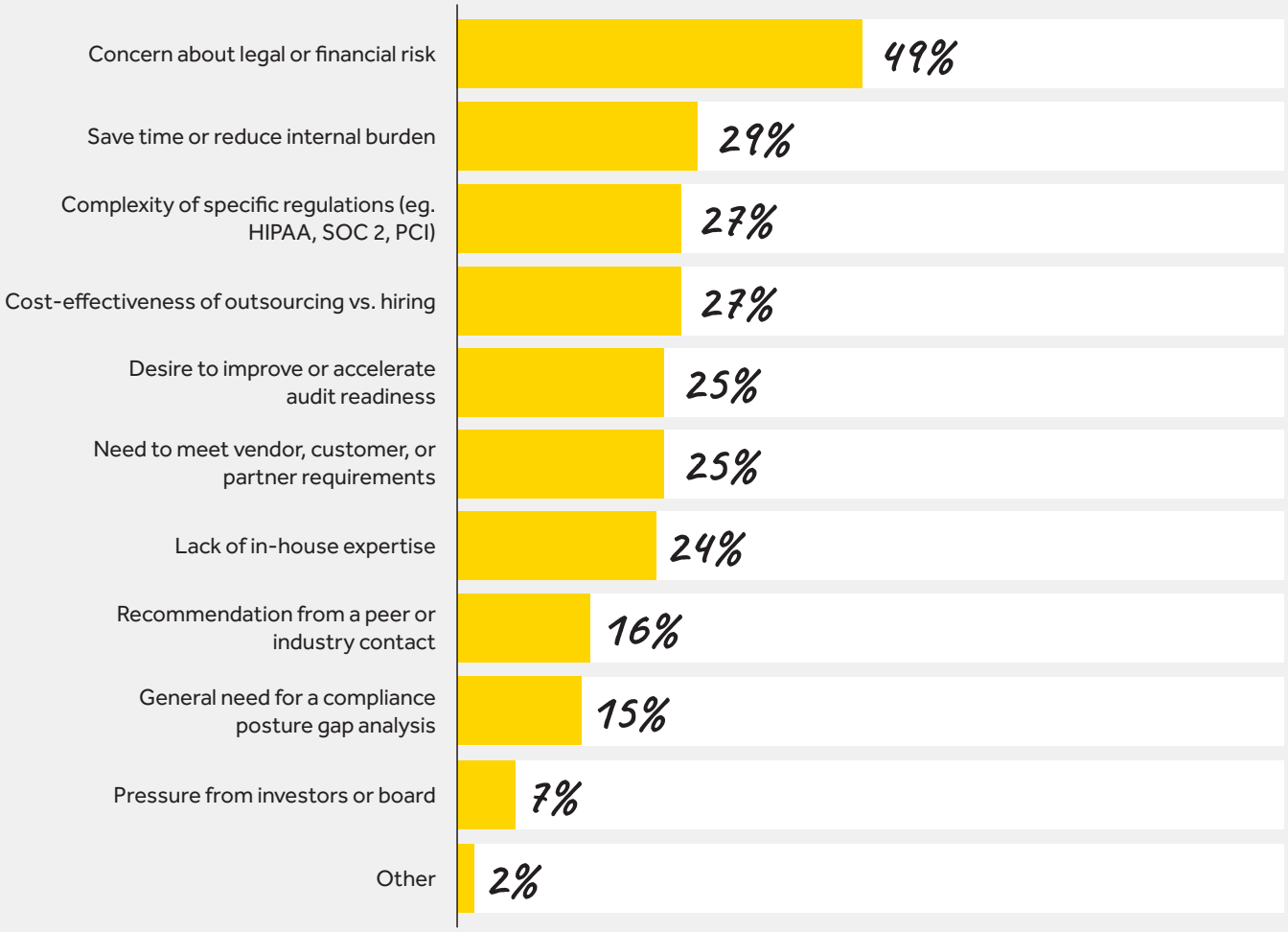
> **"Our legal counsel tries to interpret GDPR and California regulations for us, but I'll be honest, I'm not sure there's any particular expert on it. And since we don't know anyone who's been through an audit, and our legal counsel doesn't either, we don't have a lot of knowledge around whether the advice is sound, or if there's a benchmark there for us to determine whether our legal counsel is providing us with good advice."**
>
> - Director, Professional Services, 6-20 FTEs

> **"We do work with an independent consultant. They oversee financials, compliance with banking, sales tax, and auditing of the accounts. But I do feel that it's just a very small company, and who really even knows whether we are actually getting the best advice. I actually have no clue."**
>
> - Director, Manufacturing, 6-20 FTEs

The same absence of expertise that made outside help necessary is also what makes the relationship difficult to evaluate. A transactional partner fills that void without resolving it: they handle the work, the client stays uninformed, and the relationship persists because there's no internal capacity to question it.

Fear drives compliance investment more than strategy does

What motivated you to seek (or not seek) outside help for compliance?



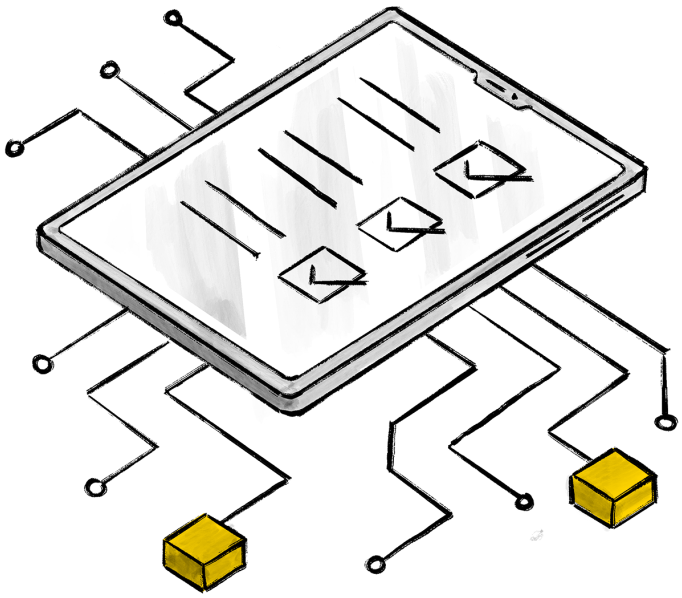
Concern about legal or financial risk was the top motivator for seeking outside compliance help. Forty-nine percent of leaders cited this as a motivation—more than time savings (29%), regulatory complexity (27%), cost-effectiveness (27%), or audit readiness (25%).

> **“I have to be totally transparent: the fear of legal and financial risk would probably be the biggest motivator.”**
>
> - Owner, Real Estate, 6-20 FTEs

For some leaders, the fear is abstract: a general awareness that the consequences of getting it wrong are serious. For others, it’s grounded in something specific: a regulation they don’t fully understand, an audit they’re not prepared for, or a fine they’ve heard about secondhand.

And for a growing share of SMBs, the fear is more immediate still. Major customers and prime contractors are increasingly making compliance a condition of doing business; a failed security questionnaire or a missed certification deadline can mean losing the contract. The financial risk in those cases is a customer relationship walking out the door.

> **“I’m no fool. Before we started the company, I spoke with former colleagues who had done this kind of thing. They all said if you’re running a consulting firm, compliance is your number two concern. Everybody knows that legal liability can sink any company. I was more interested in how to avoid it rather than how to overcome it.”**
>
> - Owner, Technology Consulting, 6-20 FTEs



The cost paradox

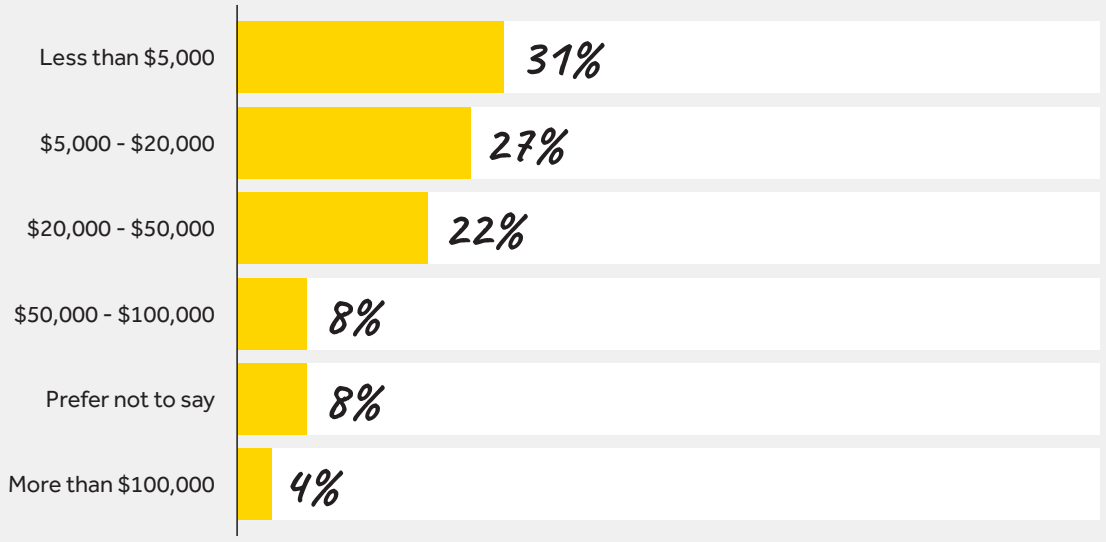
Cost-effectiveness ranked among the top drivers for SMBs that seek outside compliance help, cited by 27% of those who've made the move. The leaders who stay in-house cite cost as the primary reason they *haven't*. Both groups are making the same calculation. The difference is what they're comparing against.

> **"We're considered a small to mid-sized firm, so I can't afford to hire the technical expertise we need. Because of what we do, we tend to be an outsized target of opportunity for nation-state actors. We wanted to get the best of the best and pay for it in a reasonable way."**
>
> - Head of IT, Professional Services, 201-300 FTEs

The reframe from "Can we afford this?" to "What does it cost us *not* to have it?" is what separates the two groups. The leaders still managing compliance internally are comparing the price of outside help against zero. The ones who've brought in an MSP or outside partner are comparing it against the cost of a full-time hire they don't need, gaps they can't see, and an audit they're not ready for.

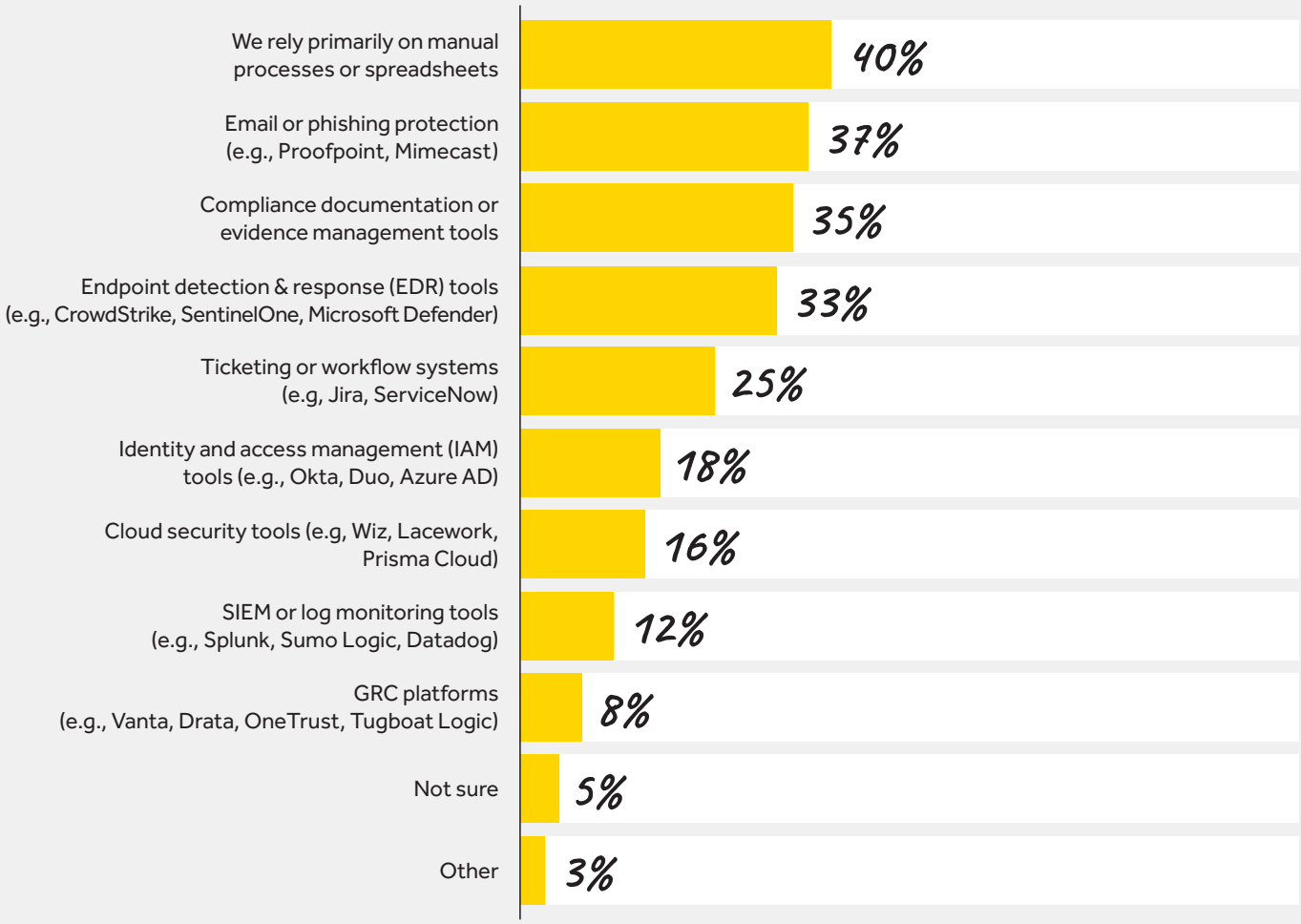
Nearly a third of SMBs (31%) spend less than $5,000 a year on compliance-related services, tools, or personnel. Another 27% spend between $5,000 and $20,000. Combined, 58% are investing at a level that amounts, in most cases, to a part-time consultant or a single software subscription—enough to feel like something is being done, but not enough to match the exposure those organizations are actually carrying.

Roughly how much does your company spend per year on compliance-related services, tools, or personnel?



SMBs have invested in defense; documentation and proof are an afterthought

What tools or technologies are you currently using to help manage your compliance program?



Only 8% of SMBs use a dedicated compliance platform

The most common tools in SMBs' compliance arsenals are built for defense, not documentation. Email and phishing protection leads the list at 37%, followed by compliance documentation and evidence management tools (35%) and endpoint detection and response (EDR) tools (33%). Purpose-built compliance platforms—GRC tools like Vanta, Drata, or OneTrust—are the least common tool in the stack: just 8% of respondents use them.

Security tools protect against threats. Compliance programs demonstrate, document, and prove that an organization meets its obligations. That distinction matters, and one respondent named it precisely:

> **"All of them—EDR, SIEM—are ancillary. Really only Secureframe is the one that puts it all into one space. Most of compliance isn't about what you're doing. It's about what you say you're doing."**
>
> - Head of IT, Software, 21-50 FTEs

A company with best-in-class endpoint protection and no audit trail may be well-defended, but it's also poorly prepared: those tools may satisfy individual compliance controls, but they don't produce the evidence an auditor needs to *confirm* compliance.

Self-aware, and stuck anyway

Four in ten respondents (40%) rely primarily on spreadsheets or manual processes—and many acknowledged, unprompted, that they know it won't last.

> **"I'm somewhat satisfied with using manual spreadsheets for managing compliance. They allow us to tailor our approach to our specific needs. But I also recognize that these can be time-consuming, prone to errors, and may not scale well as our organization grows."**
>
> - Owner, Other, 6-20 FTEs

> **"Thus far, manual processes have worked well-ish for us. However, as we're starting to have a couple of much larger projects, we may have to look again at our approach."**
>
> - CMO, Professional Services, 21-50 FTEs

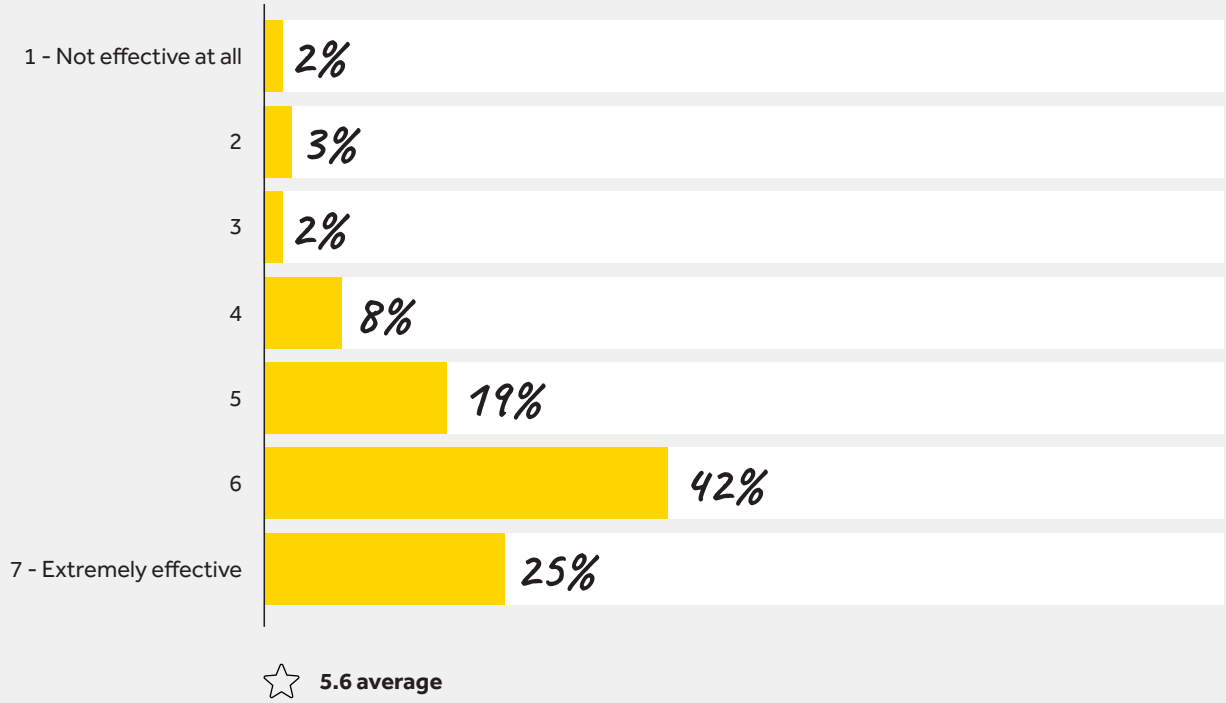
The self-awareness is consistent, and so is the status quo. Leaders acknowledge the ceiling on their current approach. And for those who *have* moved to dedicated compliance tools, the tools themselves can introduce new problems. Integration is a persistent one.

> **"Our compliance documentation and evidence management tools do not integrate with our other systems at all. Our personnel files don't have certifications in them; we have to scan the physical paper, upload it as a PDF, and save it as an attachment to the employee file. It doesn't work very well at all."**
>
> - Chief Compliance Officer, Legal Services, 51-100 FTEs

Scale, a new client requirement, or a first serious audit can expose what "well-ish" was covering for. And a compliance tool that doesn't connect to the rest of the stack can create its own version of the same problem.

High effectiveness scores measuring the wrong thing

How effective are those tools at helping you meet compliance requirements?



A passing grade for a test nobody took

Most SMBs measure compliance tool effectiveness the same way: if nothing has gone wrong, the tools are working. Asked to rate their tools on a 7-point scale, leaders gave an average of 5.6, with nearly two-thirds (67%) giving a 6 or 7. But that score isn't measuring what it appears to.

The most common reason for a high rating, cited by 47% of respondents, was ease of use: tools that work in the background, don't require much input, and stay out of the way. Set against a tooling landscape dominated by manual processes, spreadsheets, and security tools not built for compliance, that's a reasonable thing to value. It's also a definition of effectiveness that requires no audit, no incident, and no independent verification to maintain.

> **"I find it effective as I have not yet been audited. Although it is not a perfect system."**
>
> - Owner, Financial Services, 6-20 FTEs

That's the clearest articulation in the data of how many SMBs are defining effectiveness: the absence of consequences. But a tool that hasn't failed a test it hasn't *taken* yet isn't evidence of readiness.

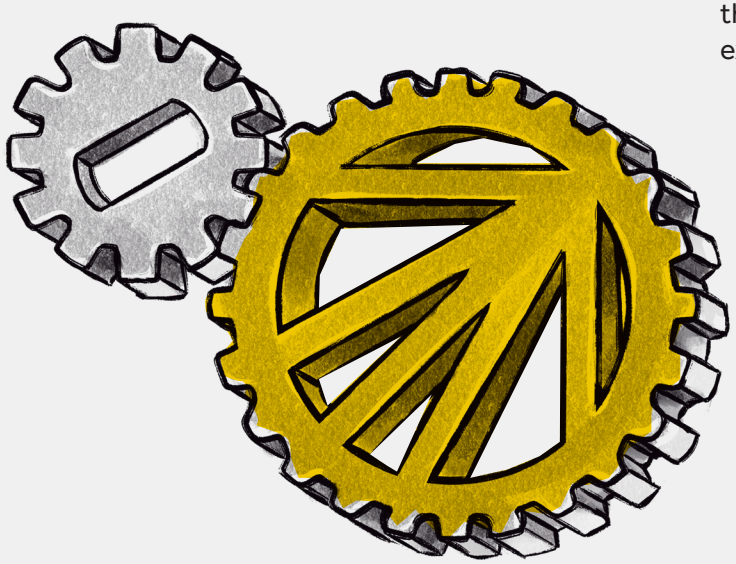
The tools work fine. They're just not doing compliance.

A quarter of respondents (25%) cited system limitations as a factor in their ratings: tools hampered by poor integration, outdated architecture, and an inability to keep pace with regulatory change. Some go further: they're not convinced their tools are doing compliance work *at all*.

A tool can be frictionless and still leave the organization exposed. Tool capability is rarely the limiting factor. The more common constraint is the absence of anyone whose job it is to make sure compliance is actually happening across the organization.

> **"Most of those tools don't address compliance specifically. They help us reduce vulnerability on spam, phishing, and managing emails, but I'm not sure they specifically help us address compliance. I'm not sure that if a new compliance requirement came out, I could rely on any of those tools to make sure I'm meeting it."**
>
> - IT Manager, Software/Technology, 51-100 FTEs

> **"There really is no catch-all to make sure that every single department is maintaining compliance. So as long as everything is being passed down correctly, we should be fine… but ultimately, there's no one to spot check, double check, or maintain compliance across the entire company. That's a glaring hole."**
>
> - CMO, Financial Services, 1,001-1,500 FTEs



That observation comes from a leader at a thousand-plus-person company. The same gap exists at fifty people; it's just less visible.

The tool is only as good as the person running it

One in five respondents (21%) identified user adoption and training as the limiting factor on their tools' effectiveness.

> **"The data you get is only as good as the person who can interpret it."**
>
> - IT Manager, Real Estate, 501-1,000 FTEs

Expertise isn't a feature you can add to a platform. It has to come from somewhere else.

> **"It's not so much about the tools and their functionality. It's more about my team and the experts I have utilizing those tools, and their ability to solve problems or find workarounds when the tools aren't sufficient."**
>
> - CEO, Professional Services, 6-20 FTEs

The gap a better platform won't close

Leaders who acknowledge their tools' limitations describe the same gap: everything they need to *demonstrate* compliance sits in a different system from everything they need to *practice* it.

> **"I simply don't know if it's catching all the requirements I should be meeting, all the reports I should be filing."**
>
> - Owner, Professional Services, 6-20 FTEs

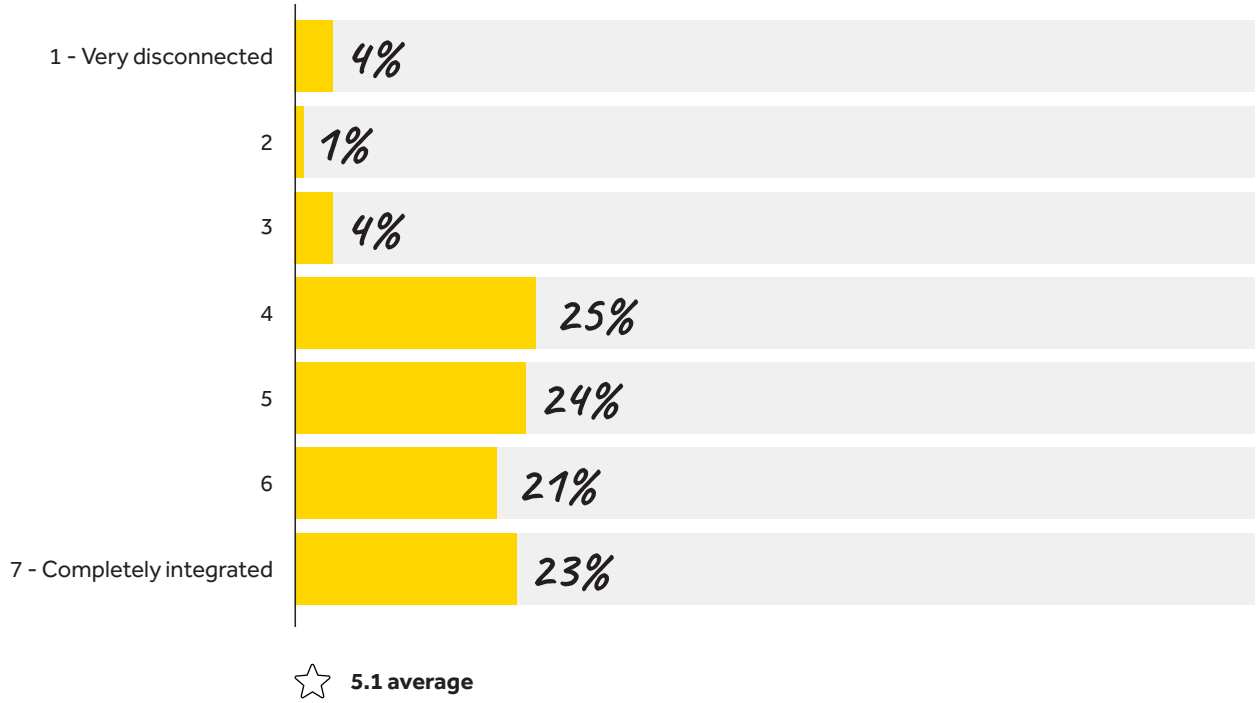
The leaders who feel this most acutely have already figured out that a better tool won't close it. The disconnect they're describing is a structural problem, and it has a structural answer.

> **"It would be nice if we could get everything in one spot—no extra steps, everything streamlined through one platform. Right now we're using a couple of different systems and it sometimes feels like there are gaps."**
>
> - Director, Healthcare, 21-50 FTEs

Cybersecurity *& tooling*

Cybersecurity and compliance: connected in theory, siloed in practice

To what extent are compliance and cybersecurity connected within your organization?



Two functions, one risk

On a 7-point scale, respondents rated the integration of compliance and cybersecurity at an average of 5.1, with 72% citing integrated controls as a factor in their rating.

> **"Everything falls under security in terms of compliance. There is risk associated with non-compliance, so we decided it makes sense to look at all of this as managing risk."**
>
> - CTO, Software/Technology, 6-20 FTEs

What the numbers *can't* tell us is how many of those 72% have built that integration, and how many are simply assuming it's there.

Integration by delegation

For the majority of SMB leaders who describe their compliance and cybersecurity as connected, the connection runs through a single point: an IT person, an MSP, or a third-party vendor who handles both. What looks like integration is, in most cases, consolidation.

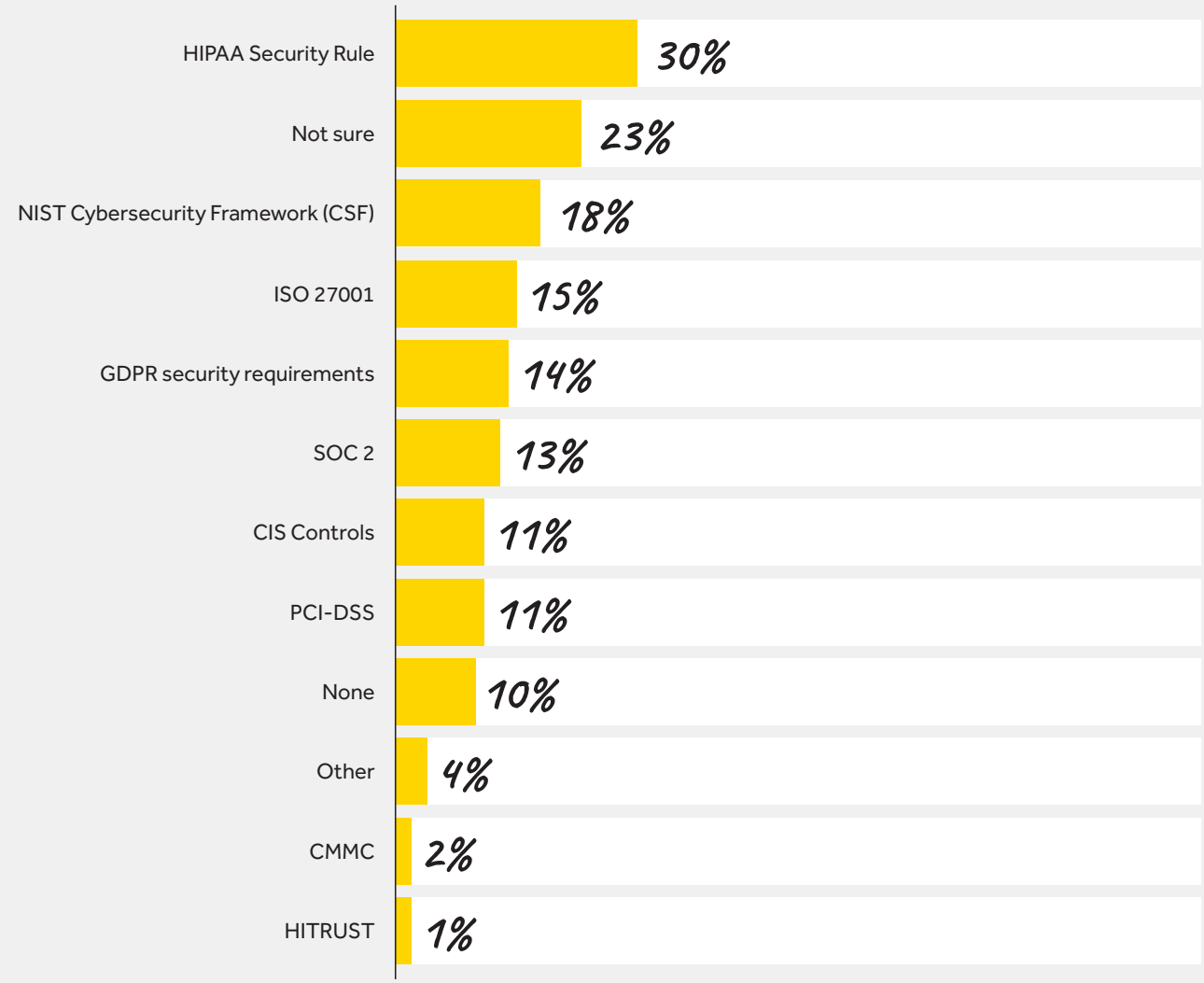
> **"It's the same person we outsource to who handles our compliance and our cybersecurity protections. It's not something we think about day to day internally. It's something that happens out of sight, out of mind."**
>
> - Director, Retail/e-commerce, 6-20 FTEs

> **"Our MSP cybersecurity controls make sure that we are in compliance and protect any data that we have."**
>
> - COO, Non-profit, 21-50 FTEs

Seventeen percent of respondents explicitly described their cybersecurity and compliance as externally managed, and most admitted they lacked visibility into what that management actually involved. Consolidated ownership is the right foundation when the partner treats the two functions as genuinely interdependent: surfacing how a security finding affects compliance posture, how a regulatory requirement shapes the security program, and reporting on both in terms leadership can act on. A partner who holds both functions *without* connecting them can produce the same invoice without producing the same protection.

Framework adoption driven by mandate, not strategy

Which cybersecurity frameworks or standards do you actively follow?



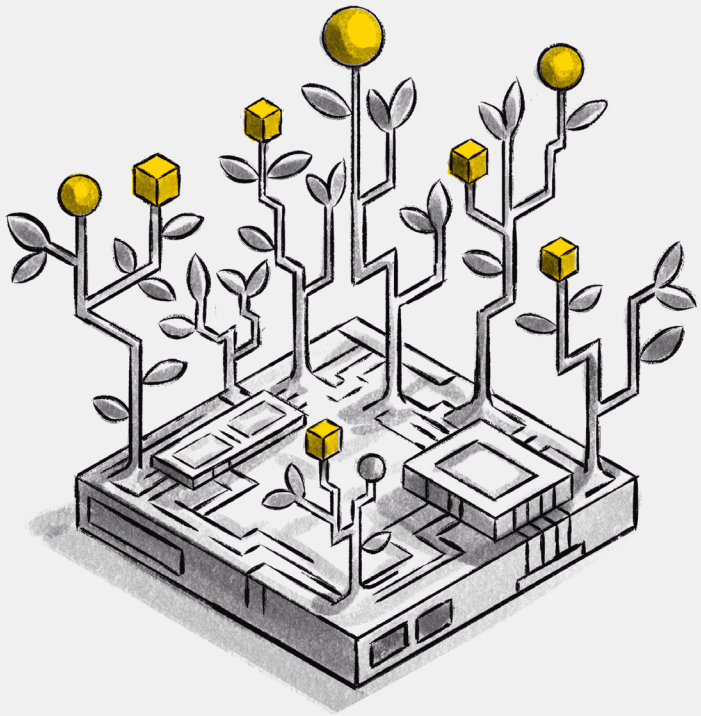
No single cybersecurity framework dominates the SMB landscape. HIPAA Security Rule leads at 30%—largely because it isn't optional. NIST CSF follows at 18%, ISO 27001 at 15%, SOC 2 at 13%. About a quarter of respondents said they weren't sure *which* frameworks they follow, and 10% follow none.

More than half of respondents (54%) said their framework decisions were driven by regulatory or compliance requirements: a federal mandate, a client requirement, an insurance condition, and so on.

> **"All compliance is pretty much driven by our customer base. They pretty much require what they need of us. Any software framework we have in place is to specifically satisfy what's required of a customer base."**
>
> - Director, Manufacturing, 201-300 FTEs

> **"What makes us use SOC 2 is that it's a requirement for our industry. It's not a matter of choice. It's mandatory."**
>
> - IT Manager, Real Estate, 501-1,000 FTEs

Frameworks adopted under external pressure still provide real protection. The limitation is that mandate-driven adoption tends to produce minimum-viable compliance: organizations do what's required, for the audience requiring it, and stop there. A framework adopted to satisfy a client requirement and a framework adopted to manage organizational risk can look identical on paper and function very differently in practice.



SOC 2:

the framework that's voluntary until it isn't

77% of organizations now require compliance with frameworks like SOC 2 from their vendors. Most SMBs only start the SOC 2 process after a customer demands it.

SOC 2 (Service Organization Control 2) is an independent audit framework that proves a company has effective controls in place to protect customer data. No government agency enforces it. What makes it consequential is who does: the enterprise customers who increasingly require it before they'll sign with you.

The reason is downstream risk. When a large customer hands data to a vendor, that vendor becomes part of their attack surface. SOC 2 is how procurement teams verify (without doing the audit themselves) that the vendor's controls are real. For SMBs that sell to mid-market or enterprise customers, the question isn't whether SOC 2 will land on the desk; it's when. And by the time it does, the deadline belongs to the customer, not the SMB.

How SOC 2 works

SOC 2 is conducted by independent CPA firms that evaluate whether an organization meets the Trust Services Criteria: Security (required), and optionally, Availability, Processing Integrity, Confidentiality, and Privacy. The output is a report, not a certification; every report's controls depend on what the business chose to be evaluated against, which is why two SOC 2-compliant companies might be following completely different sets of controls.

	Type 1	Type 2
What it proves	Controls are designed correctly at one point in time	Controls operate effectively over a 3-to-12-month period
Typical timeline	1.5 to 3.5 months	6 to 18 months
Typical cost (all-in)	$15K to $40K	$30K to $150K
What enterprise customers usually want	Sometimes accepted as a starting point	The standard ask

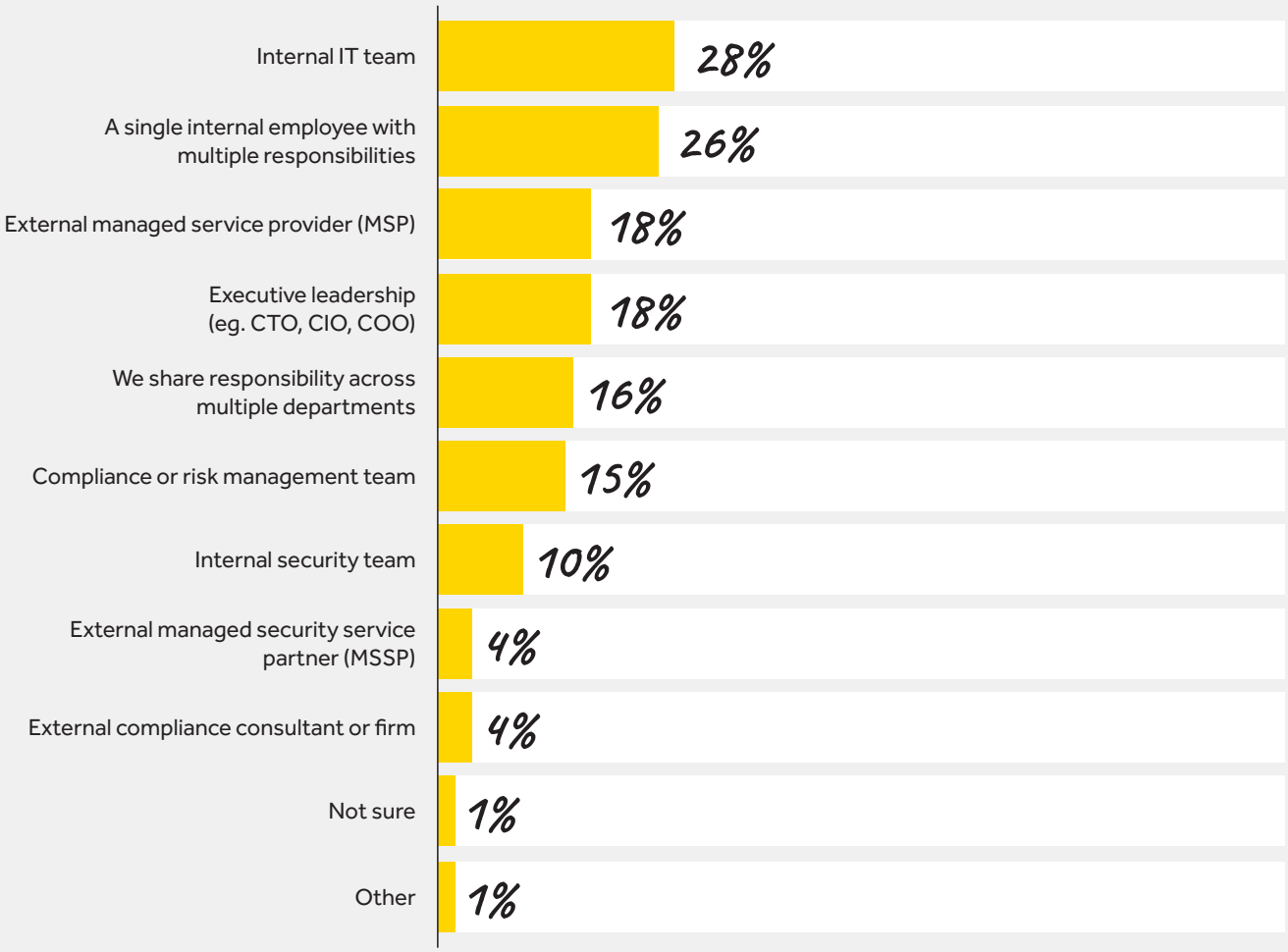
Most SMBs who need SOC 2 will eventually need Type 2. Type 1 is sometimes accepted as a placeholder, but enterprise procurement teams generally treat it as a stepping stone, not a destination.

The cost of starting late

A Type 2 report can't be produced on demand. The audit examines an observation period of 3 to 12 months: the clock starts when the controls go live, not when the customer asks. Auditors carry 4-to-8-week scheduling lead times on top of that, and rushed implementations cost 30% to 50% more than planned ones. Most customers won't wait 6 to 12 months for a business to produce a report. They'll sign with a vendor who already has one.

Compliance ownership is diffuse; accountability disappears with it

Who in your organization is primarily responsible for day-to-day cybersecurity and compliance tasks?



At most SMBs, responsibility for day-to-day cybersecurity and compliance is spread across multiple functions, roles, and individuals. Internal IT teams lead at 28%, followed closely by a single employee with multiple responsibilities at 26%. Executive leadership and MSPs each account for 18%. Shared responsibility across multiple departments comes in at 16%, compliance or risk management teams at 15%, and dedicated internal security teams at just 10%.

The compliance desk of one

The most telling number is the 26% relying on a single internal employee with multiple responsibilities. A quarter of SMBs have concentrated their entire cybersecurity and compliance function in one role… and with it, every question about where the organization actually stands.

When compliance ownership lives in one person, the program becomes visible only to that person. Leadership can't independently assess the organization's posture, verify what's being done, or identify what's missing. The compliance function *operates*, but it operates as a closed loop. What's inside it is largely a matter of trust.

The 18% who've handed it off entirely

Eighteen percent of respondents rely on an external managed service provider for day-to-day cybersecurity and compliance ownership. These are the organizations that have decided both functions are too complex, too dynamic, and too consequential to manage as a side responsibility.

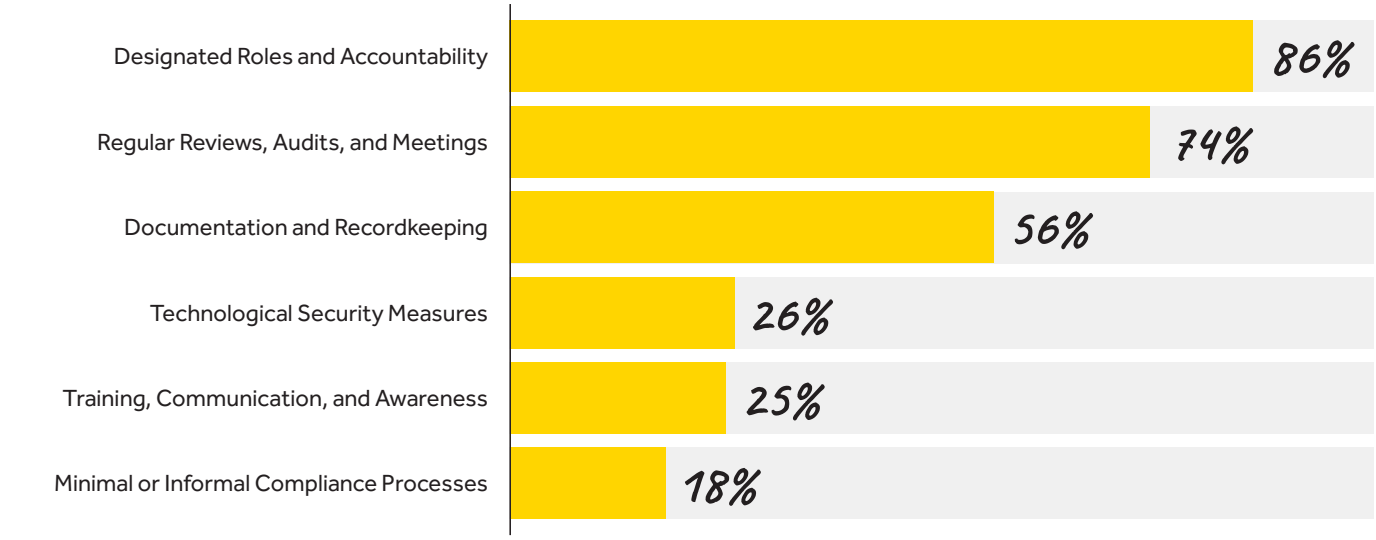
It's the only model in this data that doesn't depend on a single person, doesn't pause when someone leaves, and doesn't require leadership to already know the right questions to ask. That institutional continuity is structurally absent from every other model in this data.

Whether it's *delivering* on that potential rarely shows up in how leaders describe their own programs.

Processes, challenges, *& measurement*

Most SMBs "have compliance"; fewer can describe what it looks like

Describe any internal processes or policies you've put in place to maintain compliance.



Nearly nine in ten SMB leaders report having compliance infrastructure. Eighty-six percent report designated roles and accountability. Seventy-four percent conduct regular reviews and audits. Fifty-six percent maintain documentation and recordkeeping systems.

Those numbers don't describe a compliance shortfall in the traditional sense: a shortage of intent, awareness, or effort. They describe something more specific: organizations that have built something, believe it's working, and may not have a clear basis for that belief.

"Designated roles" frequently means a single person. "Regular reviews" ranges from rigorously structured quarterly audits with documented version histories to ad hoc check-ins triggered by whatever comes up. The categories are broad enough to hold both; and the data can't distinguish between them.

> **"We have dedicated compliance owners, a centralized GRC, executive oversight, a formalized policy suite and control document repositories, risk assessments, internal control reviews, internal audits, remediation processes, training, phishing simulations, and off-boarding compliance."**
>
> - COO, Financial Services, 1,001-1,500 FTEs

That description represents one end of a very wide distribution. At the other end, another picture emerges.

Unwritten, undocumented, assumed

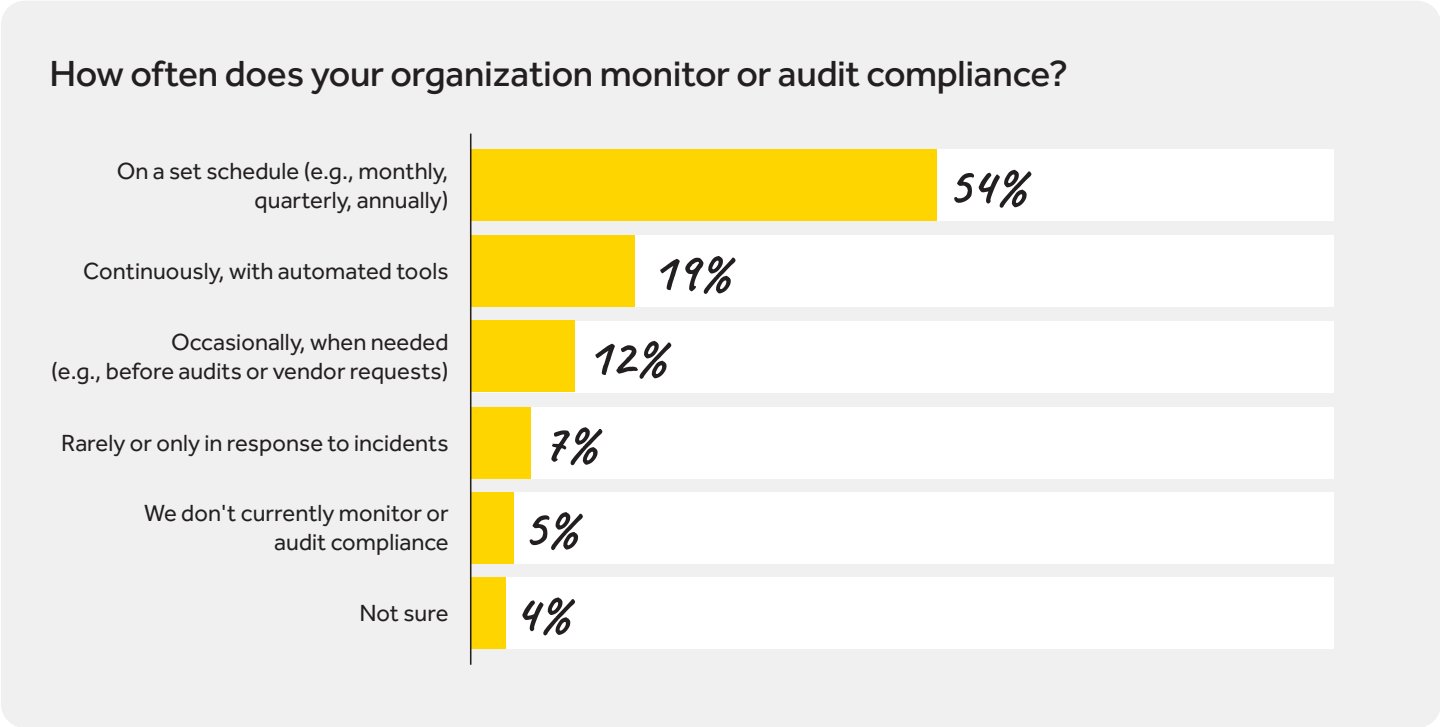
A broader pattern runs through this data: compliance processes that *function*, but exist primarily in someone's head, in an informal routine, or in a binder that gets updated when someone remembers to.

> **"Our compliance processes aren't necessarily documented. We pretty much do the same thing we've been doing for the past 32 years. The processes are sort of unwritten. We really don't keep a lot of digital records—just to try to avoid anybody being able to hack the system. For the most part, they're just a physical copy under lock and key."**
>
> - IT Manager, Software/Technology, 51-100 FTEs

Thirty-two years of institutional knowledge can survive a lot: personnel changes, audits, growth. The one thing it can't survive is being asked to prove itself. And protecting physical records from a digital breach doesn't address the auditor who asks for documentation, the client who requires a compliance attestation, or the ransomware that doesn't need to touch a filing cabinet.

But the more consequential pattern isn't undocumented processes. It's leadership that has lost the ability to describe what the organization's compliance program looks like at all.

Monitoring happens on a schedule (until it doesn't)

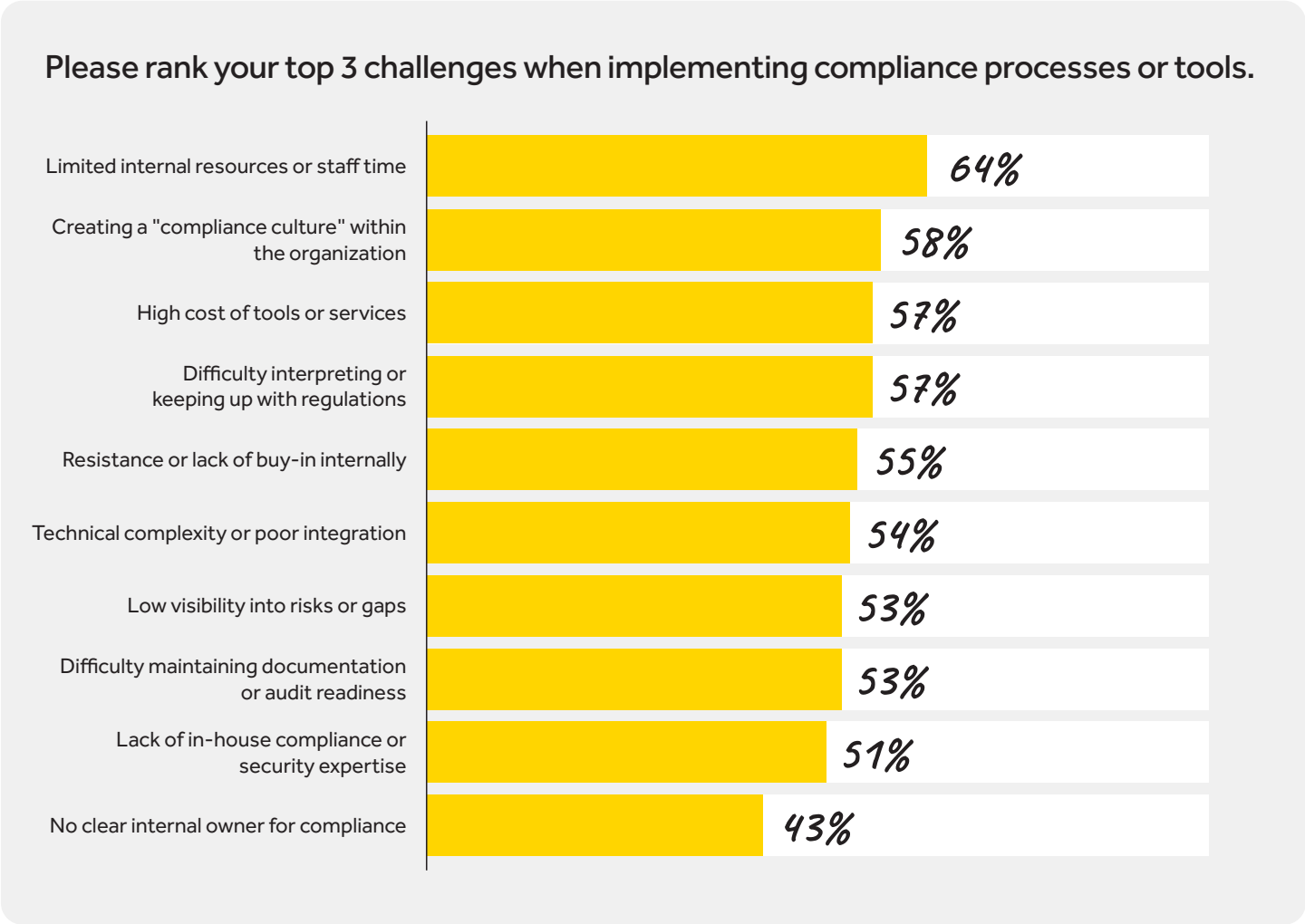


More than half of respondents (54%) monitor compliance on a set schedule: monthly, quarterly, or annually. Nineteen percent monitor continuously using automated tools. At the other end: 12% monitor only when something forces the issue, 7% rarely or only after an incident, and 5% don't monitor at all.

The 19% with continuous automated monitoring have largely solved the problem this question is measuring. For everyone else, the frequency of monitoring is only part of the picture: "set schedule" covers a wide range of rigor, from formal audits with documented version histories to a quarterly check someone assumes is happening.

The 24% who monitor occasionally, rarely, or not at all are the most exposed group in this data. They're also the most likely to discover that a regulatory change has been in effect longer than they realized.

Resources are the constraint everything else runs into



Limited internal resources or staff time ranks first among compliance challenges, scoring 64%—well ahead of everything else on the list. Creating a compliance culture ranks second (58%), followed by the cost of tools or services and difficulty interpreting, or keeping up with, regulations (57% each).

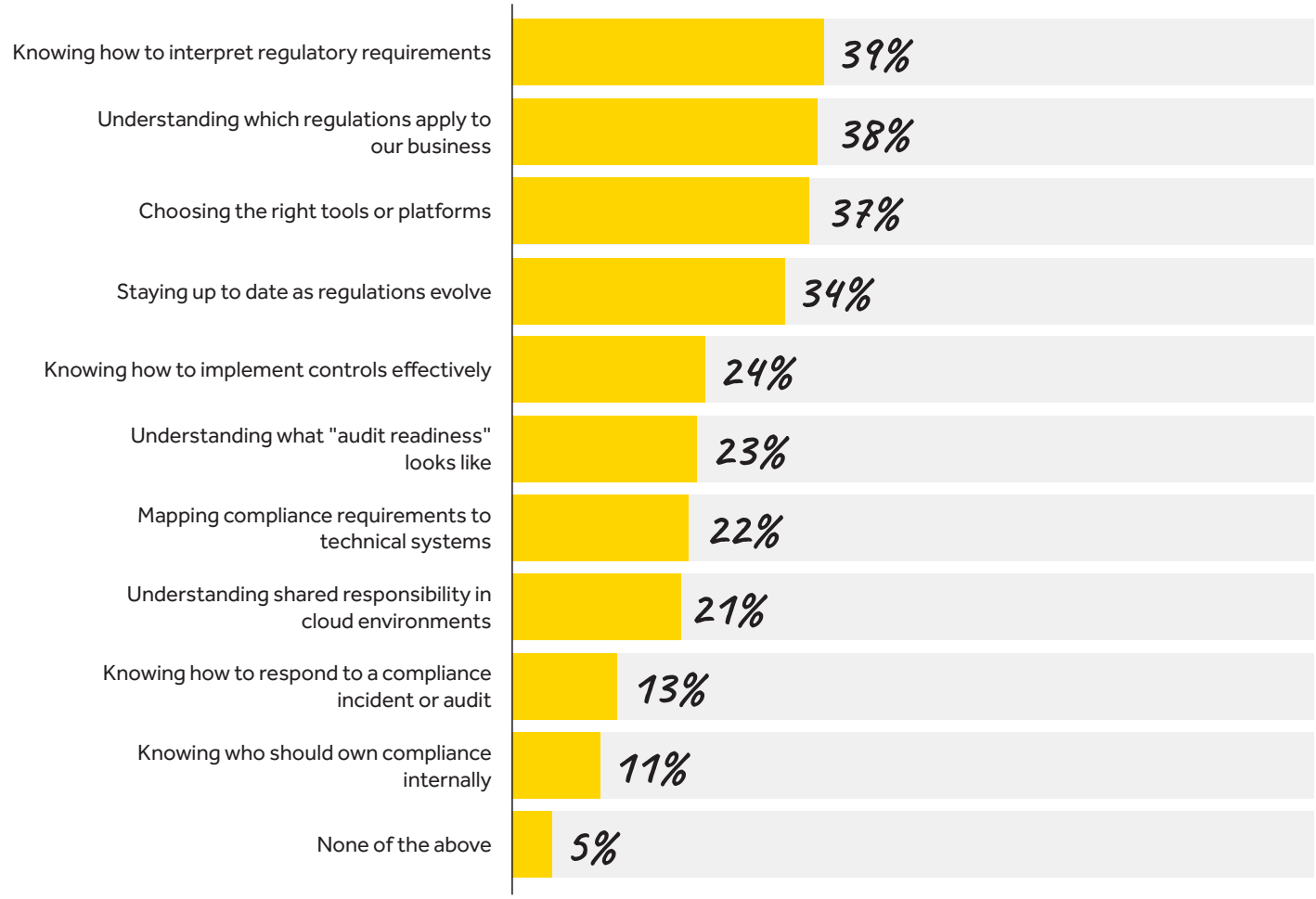
The more telling finding is what ranks lower. The bottom three items—lack of in-house expertise, no clear internal owner, and “we haven't faced major challenges”—share a common trait: they require an external reference point to recognize. A resource constraint is felt directly. The absence of expertise an organization has never had, the accountability gap that’s always looked like shared responsibility, the risk that hasn't materialized yet: none of these register as problems from the inside.

In other words, self-assessment has a structural ceiling here. An organization can audit what it knows to look for, but it can’t audit what it doesn’t know is missing. The challenges that rank lowest in this data aren’t low because they’re rare; they’re low because the people experiencing them have no basis for recognizing them as problems.

Knowledge gaps *& future needs*

SMBs can't self-diagnose their most persistent compliance gaps

What are the biggest knowledge gaps that exist for you or your team regarding compliance?



The most common knowledge deficits in this data all occur upstream of execution: before implementation is possible, before tools are selected, and before anyone asks whether the right regulations are even on the list. Thirty-nine percent cited difficulty interpreting regulatory requirements. Thirty-eight percent said they don't know which regulations apply to their business. Thirty-seven percent don't know how to choose the right tools.

The regulation problem

Regulations are frequently written for organizations that don't resemble most SMBs: too large, wrong industry, different jurisdiction, or different operating model.

> **"Not knowing which regulations apply means we might miss things… or we might overprepare."**
>
> - COO, Non-profit, 21-50 FTEs

Both outcomes are expensive. Overpreparing wastes resources organizations don't have. Missing things creates exposure they can't see. Regulatory ambiguity has a second dimension: pace. Rules change across administrations, across states, and as new technologies emerge. Several respondents cited AI specifically as an area in which the rules haven't caught up with what they're already doing.

> **"We're working on an AI chat and potentially an AI voice bot; and it seems like it's a little bit more of the wild west in the AI world versus the more traditional. You're trying to adopt new things and hoping you're not missing something you need to be complying with."**
>
> - Director, Legal Services, 21-50 FTEs

The vendor assumption problem

Not every compliance risk registers as one. The assumption that software vendors handle compliance so the organization doesn't have to rarely surfaces as a concern, because the people who hold it don't know to question it.

> **"There's a certain level of complacency by management, thinking that because we hired a vendor to provide the software, they're responsible for preventing cybersecurity incidents. Most of the time they are. But there's inevitably some configuration that we as an organization are responsible for."**
>
> - IT Director, Professional Services, 201-300 FTEs

SaaS applications handle some compliance requirements by default, but they don't handle all of them. Few organizations can clearly describe where their vendor's responsibility ends and theirs begins, and that boundary is where exposure accumulates.

NIST CSF:

the framework you've probably already promised to follow

82% of denied cyber insurance claims involved policyholders whose MFA implementation didn't hold up under investigation.

The NIST Cybersecurity Framework (CSF) is a voluntary set of cybersecurity practices developed by the federal government. No regulator enforces it, and no customer demands certification, because there isn't one. What makes it consequential for SMBs is that most cybersecurity insurance policies already require the controls NIST recommends.

When an SMB applies for or renews cybersecurity insurance, the questionnaire asks whether multi-factor authentication is enabled across all systems, whether endpoint detection is in place, whether backups are tested and isolated, whether an incident response plan exists, and whether security awareness training is ongoing. These aren't arbitrary questions; they're NIST CSF controls, translated into yes-or-no items.

Many SMBs answer "yes" without verifying. The IT person says it's handled, the MSP says it's covered, and the box gets checked.

The trap inside the questionnaire

Denied claims trace back to a consistent pattern: a gap between what the policyholder attested to in the application and what was actually deployed when the incident occurred. MFA enabled on email but not on VPN. Backups configured but never tested. An incident response plan written but never rehearsed. Endpoint detection licensed but not deployed across all devices.

The denial comes after the incident, when forensic investigators verify the controls listed on the application. By then, the business is paying out-of-pocket for ransomware recovery, breach notification, legal fees, and lost operations: costs the policy was meant to cover.

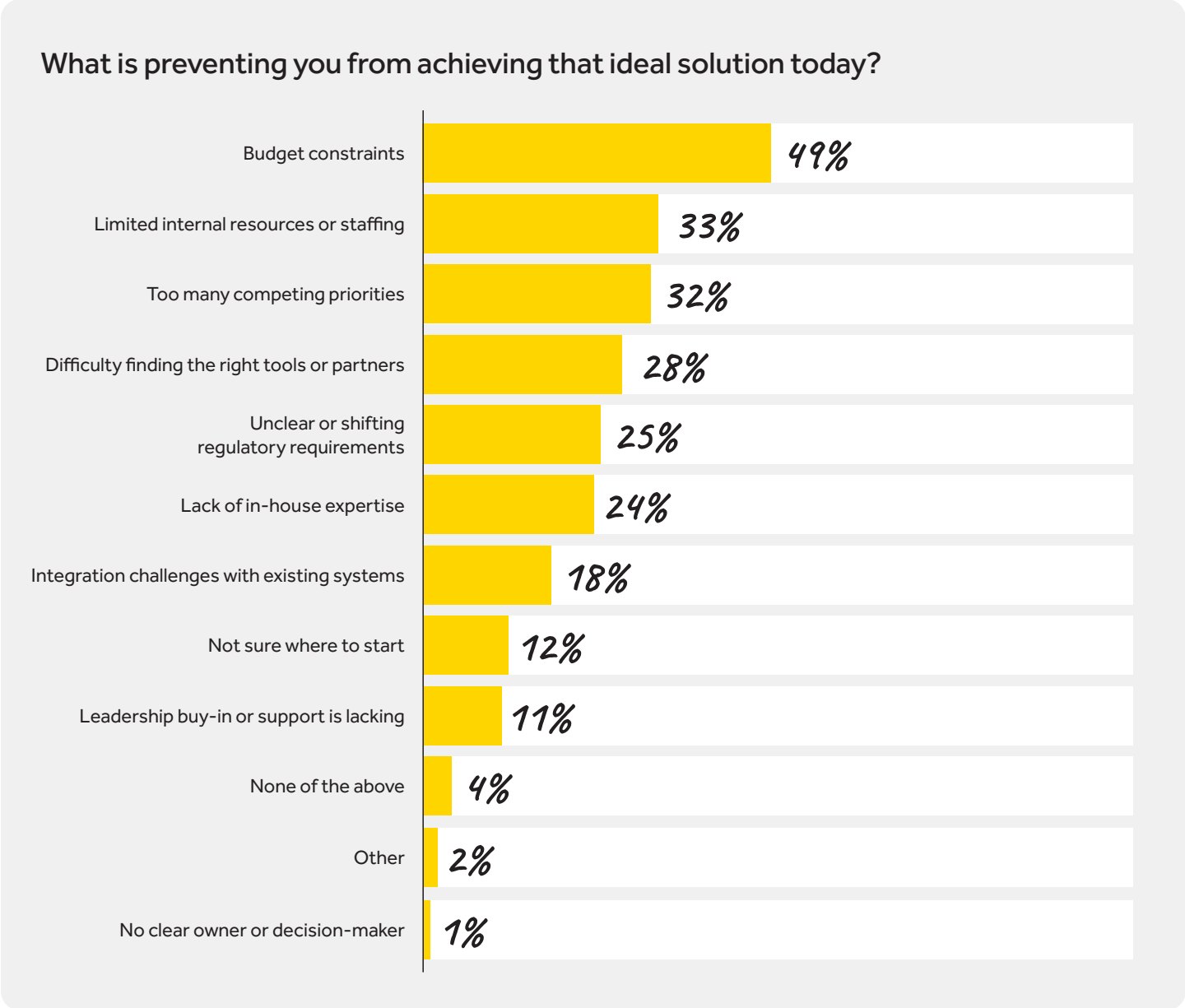
The exposure most SMBs don't see

NIST CSF doesn't have a November deadline, primes cutting suppliers, or False Claims Act exposure. What it does have is something more universal: every SMB with cyber insurance has implicitly agreed to a set of controls. Few have verified those controls match what's running.

The gap between what's been attested and what's actually running is closeable, but only through structured comparison: what your policy requires, what NIST CSF defines, and what your environment has. It's not the kind of work most internal teams are positioned to do, because it requires fluency in both insurance underwriting language and cybersecurity controls.

Budget, resources, and leadership:

the barriers that reinforce each other



Budget constraints rank first among barriers to the ideal compliance solution, cited by 49% of respondents. Limited internal resources rank second at 33%. Competing priorities rank third at 32%.

Those three barriers are related, and they're also circular: organizations that don't prioritize compliance don't budget for it, don't staff for it, and then cite the absence of budget and staff as the reason they can't move forward. The data doesn't fully distinguish between organizations that genuinely can't afford better compliance and those that haven't decided it's worth the investment.

The leadership problem

> **“I’ve struggled with this for years: showing the owners the repercussions of not complying, the possible costs, the fact that the company could be out of business. It just falls on deaf ears. When it comes to something as simple as using strong passwords, we haven’t even managed to get past that one.”**
>
> - CTO, Software/Technology, 6-20 FTEs

That’s a CTO who’s been making the compliance case and losing—to an ownership team that has heard the argument, understood the stakes, and chosen to do nothing.

Leadership resistance takes different forms. Indifference is the most common: compliance sits on the back burner until something external forces it. For some organizations, the resistance is more deliberate.

> **“Some of our leaders have ideas that wouldn’t be compliant. Occasionally the highest level of leadership has wanted to take the risk of falling afoul of compliance regulations. It’s a constant struggle to make sure everyone understands you can be easily flagged; and we really don’t want them to finally understand that because something bad happens. It’s an ongoing, heated conversation.”**
>
> - CMO, Professional Services, 21-50 FTEs

Indifferent or actively resistant, the outcome is the same: an organization that remains exposed while the people responsible for fixing it wait for permission or a crisis.

When mission competes with obligation

> **“We have a challenge around whether to invest more in our operations—which includes compliance and security—versus increasing our investments in the community, which is our mission and reason for existing.”**
>
> - CEO, Non-profit, 6-20 FTEs

That’s a genuine resource allocation dilemma—and one of the more sympathetic forms the barrier problem takes. The same leaders who cite these barriers can describe, in precise terms, what they’d pay to have.

SMBs want a partner, not a platform...

and they know what that looks like

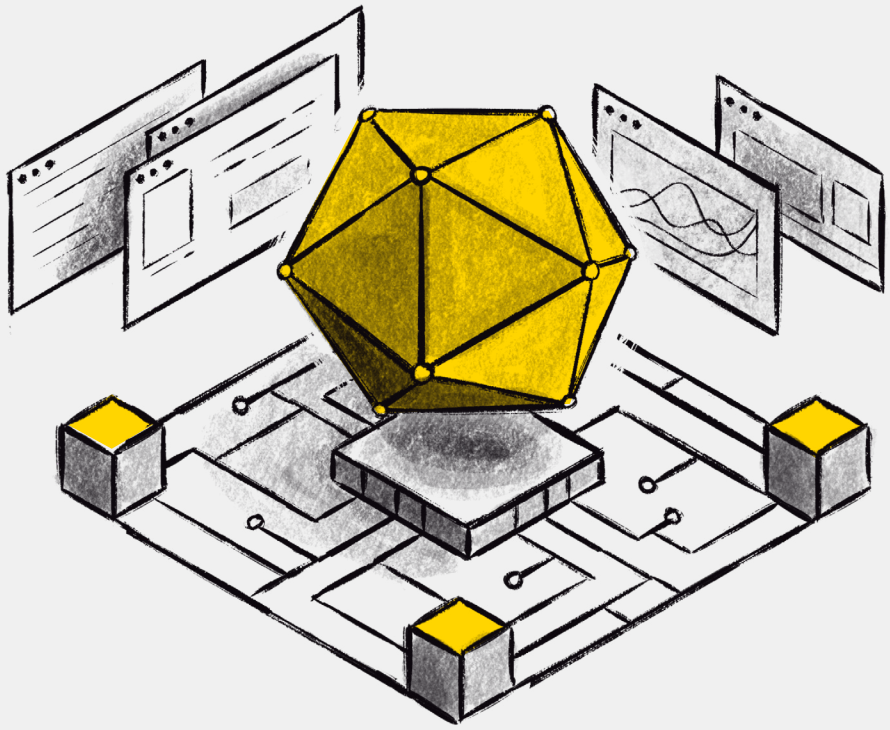
When SMB leaders describe their ideal compliance solution, the wish list moves past tools quickly. What they're reaching for is something tools can't provide by definition. Automation is table stakes, cited by 58% of respondents as an essential feature. But running alongside it is a second desire that no platform satisfies: a human layer that can answer a question, flag something the client wouldn't have known to ask, and implement what it finds.

Proactive automation, and a human layer on top

> **“An ideal compliance solution would be something we don’t have to think about. It’s proactive. It does the work for us, running and updating without us having to be reactive when changes are made.”**
>
> - Owner, Other, 51-100 FTEs

> **“I’d want real-time updates when something changes that affects my business. A checklist or dashboard tailored to my specific work would be huge. But I’d also love support that feels human, not just a chatbot sending me links to articles. Give me someone I can actually talk to if I’m stuck. Keep it simple, make it clear, and help me stay out of hot water without having to become a legal expert.”**
>
> - Owner, Other, 6-20 FTEs

Simplicity is the third most-cited feature requirement in this data. The ideal solution has to work for organizations that don’t have the internal expertise to run something complicated.



Implementation, not just identification

> **“I suppose it would be a third party that stayed up-to-date on all compliance, was knowledgeable about our business, had the authority to implement compliance, and we trusted them to do so.”**
>
> - Director, Retail/E-commerce, 6-20 FTEs

“Had the authority to implement” is a precise ask from someone who’s likely experienced the alternative: a partner who identifies problems and stops there. A minority of respondents went further still, describing not just implementation but *anticipation*.

> **“They are experts in their field, they tell us about changes that are on the horizon, and they allow us to make adjustments in our business according to what upcoming regulations are.”**
>
> - Owner, Retail/E-commerce, 51-100 FTEs

That description came from someone who already has this kind of partner. Most don’t.

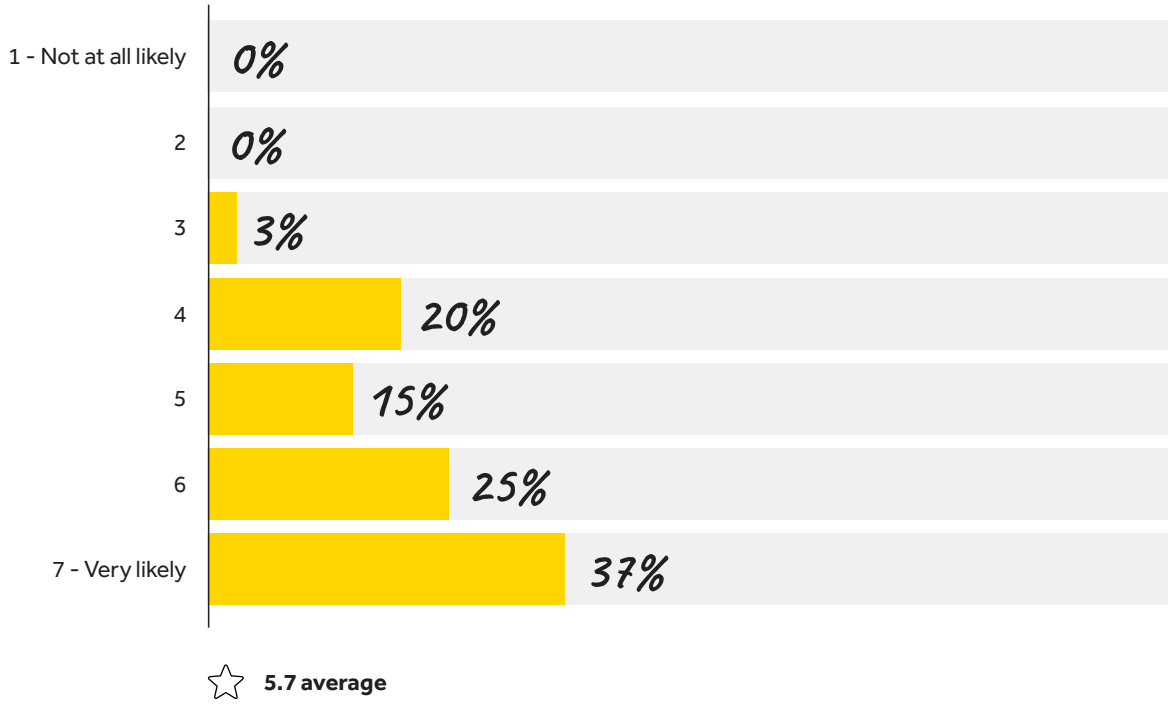
A model of engagement, not a category of software

> **“I would say the magic wand would be providing a part-time IT specialist that could speak to the system requirements we have in place, the regulatory requirements we’re meeting, and how we’re protecting our data, so I’d be able to describe that to others.”**
>
> - Chief Compliance Officer, Financial Services, 6-20 FTEs

A compliance officer who can’t describe their company’s compliance posture to others is the natural endpoint of a program built to satisfy requirements rather than inform leadership. What these respondents are describing—automated, proactive, human-backed, and capable of briefing the people at the top—is a model of engagement, not a category of software.

The *standard* worth holding your MSP to

If your MSP or IT provider offered compliance assessment and ongoing support services, how likely would you be to adopt them?



Sixty-two percent of SMB leaders rated their likelihood of adopting compliance assessment and ongoing support services from their MSP at 6 or 7 out of 7. Nobody rated below a 3. The average was 5.7 out of 7. The appetite is there. The question is whether the provider can meet it.

The qualitative data makes clear what "worth buying" means to them. It begins with proactive engagement: the most common complaint about existing MSP relationships is *posture*, not capability.

> **"They're the experts, so I sort of rely on them—but a lot of times they're reactive, and that's what's challenging."**
>
> - IT Manager, Software/Technology, 51-100 FTEs

When the MSP is "the expert," clients defer. But when that expertise isn't applied proactively, the client is exposed… often without knowing it.

Some SMBs are already running dedicated compliance platforms and evaluating MSPs against them on concrete terms:

> **"What is their value proposition? How can they help reduce the amount of audit time and increase the likelihood of a successful audit for my organization?"**
>
> - Director, Software/Technology, 201-300 FTEs

Those are the right questions. The standard these leaders are describing is specific: show up, follow through, and treat each situation as particular rather than generic.

> **"We don't want to be treated like one of ten other companies. If you're not in salesperson mode—if you're there as an advisor and support, patient, and offering real solutions—then you'll be taken seriously."**
>
> - CMO, Healthcare, 201-300 FTEs

> **"It's got to be done right: clear communication, real support—not just another service they tack on and disappear. Not just another monthly charge with no follow through."**
>
> - Owner, Other, 6-20 FTEs

A managed relationship delivers accountability, visibility, and genuine expertise; and the organizations in this study were describing exactly that. Certified compliance experts who embed controls into daily operations. Continuous monitoring that surfaces gaps before regulators do. Framework mapping across every major standard. Leadership briefings that keep executives informed. That's what a purpose-built partner brings—and for SMBs, it's worth asking for.

Choosing a cybersecurity & *compliance partner*

The questions every SMB should ask

Choosing the right cybersecurity and compliance partner is one of the most consequential vendor decisions an SMB can make: it determines whether the organization has genuine protection or the appearance of it. The nine categories below cover the questions worth asking—and the answers worth requiring—before any partner relationship begins.

1 How will you assess where we stand?

Before any partner can protect your organization, they need to understand it. A capable partner begins with a detailed review of your controls, your actual regulatory exposure, and a prioritized roadmap for addressing what's found, mapped to recognized frameworks: NIST CSF, CIS Controls, ISO 27001, or whichever standards govern your industry.

Questions to ask:

- What does your initial assessment process look like, and what frameworks do you use?
- Will you produce a prioritized remediation roadmap?
- What's included in the assessment, and what costs extra?

If a partner's onboarding process skips directly to tools and service agreements without a structured assessment first, that's a signal about how they'll operate across the relationship.

2 Which compliance frameworks do you cover, and how do you determine which ones apply to us?

One of the most consistent findings in this survey is that SMBs frequently underestimate their regulatory exposure. Organizations subject to HIPAA, PCI-DSS, GDPR, CCPA, CMMC, SOC 2, or an expanding list of state privacy laws often discover it later than they should: sometimes only after a client requirement or audit forces the question.

A capable partner maps your full regulatory environment: what applies to your industry, your data, your customers, and your geography, *including* obligations you haven't identified yet. They should also be able to map your cybersecurity insurance policy's required controls against your actual environment, since that gap is one of the most common sources of denied claims.

Questions to ask:

- Which compliance frameworks does your team have certified expertise in?
- How do you determine which regulations apply to a business like ours?
- Can you map our cybersecurity insurance policy requirements against the controls we actually have in place?
- How do you handle frameworks that are still evolving (new state privacy laws, AI regulation, updated federal guidance)?
- If we're subject to multiple frameworks, how do you manage overlapping requirements without duplicating work?

Framework coverage that matches your actual exposure is a baseline requirement.

3 How will you keep us continuously protected?

A compliance assessment is a snapshot; but the regulatory environment, your technology stack, and your threat landscape are all moving targets. An organization that was compliant in January may not be in June. Without continuous monitoring, nobody finds out until something external forces the question.

Questions to ask:

- Do you offer 24/7 continuous monitoring, or scheduled reviews?
- How are we notified when something changes in our compliance posture or threat environment?
- What does real-time audit support look like? Can you respond to a compliance inquiry on short notice?
- How do you handle regulatory changes that affect our obligations mid-year?

The distinction between continuous monitoring and periodic audits is one of the clearest dividing lines between partners who provide genuine protection and those who provide documentation that protection exists.

4 What happens when something goes wrong?

Every security and compliance program is eventually tested. When an incident, a breach, or an audit arrives, the question is whether your organization has a partner who can respond effectively.

Questions to ask:

- Do you provide incident response services, or do we need a separate vendor for that?
- What does your breach containment and recovery process look like?
- Do you offer disaster recovery planning as part of your engagement?
- If we faced a regulatory inquiry or audit tomorrow, what role would you play?

A partner who helps you prevent incidents and disappears when one occurs is only half a partner.

5 How do you address the human side of the risk equation?

Most security incidents trace back to human behavior: a phishing email clicked, a password reused, or a procedure skipped. Most compliance failures have similar origins: a policy nobody was trained on, a process that existed only on paper, or a culture that treated compliance as someone else's job.

Questions to ask:

- Do you provide phishing simulations and security awareness training for our employees?
- How do you help build a compliance culture across the organization?
- How do you measure whether training is actually changing behavior?

Tools and monitoring address part of the risk. Training and culture address the rest.

6 How will you keep our leadership genuinely informed?

Fourteen percent of SMB leaders in this research described their compliance confidence as borrowed: drawn from a partner they trust, whose work they've never independently verified. A capable partner closes that loop, equipping leadership with visibility into what's being managed, what it means for the business, and what requires attention.

Questions to ask:

- What does board-level reporting look like, and can you tailor it for a non-technical audience?
- Do you offer vCISO services for ongoing strategic guidance?

The goal is to ensure leadership has enough visibility to ask the right questions, and enough information to recognize a good answer.

7 Can you grow with us?

A capable partner scales with your organization and treats it as particular.

Questions to ask:

- Have you worked with businesses in our industry before, and how does that shape your approach?
- Do you offer both fully managed and co-managed models, depending on what our team can handle internally?
- How does your engagement change as our business grows, adds locations, or faces new compliance requirements?
- If we were considering a merger, acquisition, or new line of business, could you support the compliance and cybersecurity due diligence?

Longevity in a compliance and security relationship is an asset—*if* the partner is growing alongside the organization.

8 How will we know the investment is working?

The most common measure of compliance tool effectiveness in this survey was the absence of consequences: leaders assume that if nothing has gone wrong, their tools are working. That's a poor measurement standard. A compliance program that hasn't been tested hasn't proven anything yet.

Questions to ask:

- What metrics do you use to demonstrate improvement in our security and compliance posture over time?
- How do you tie your services to measurable outcomes (reduced incidents, faster recovery, audit readiness)?
- Do you provide regular executive-level reviews that document progress?
- How do you report on ROI for an SMB that needs to justify this investment internally?

That's what accountability looks like. Require it.

9 How will we know who is responsible for what?

Every major compliance framework assumes a shared responsibility model. Some controls have to be implemented by the partner. Some have to be owned by the customer. Some involve both, with handoffs and dependencies. When that division of labor isn't documented upfront, the gaps appear under audit pressure or after an incident.

A capable partner walks into the engagement with a written responsibility matrix that names every major activity, who owns it, and how the handoffs work. Without one, the partnership runs on assumption.

Questions to ask:

- Can you walk me through a sample responsibility matrix for a client like us?
- Which controls or tasks remain the customer's responsibility, even with full managed service?
- How do you document handoffs between your team, our internal staff, and any other vendors involved?
- How often is the matrix reviewed and updated?

Longevity in a compliance and security relationship is an asset—if the partner is growing alongside the organization.

Ready to see where you stand?

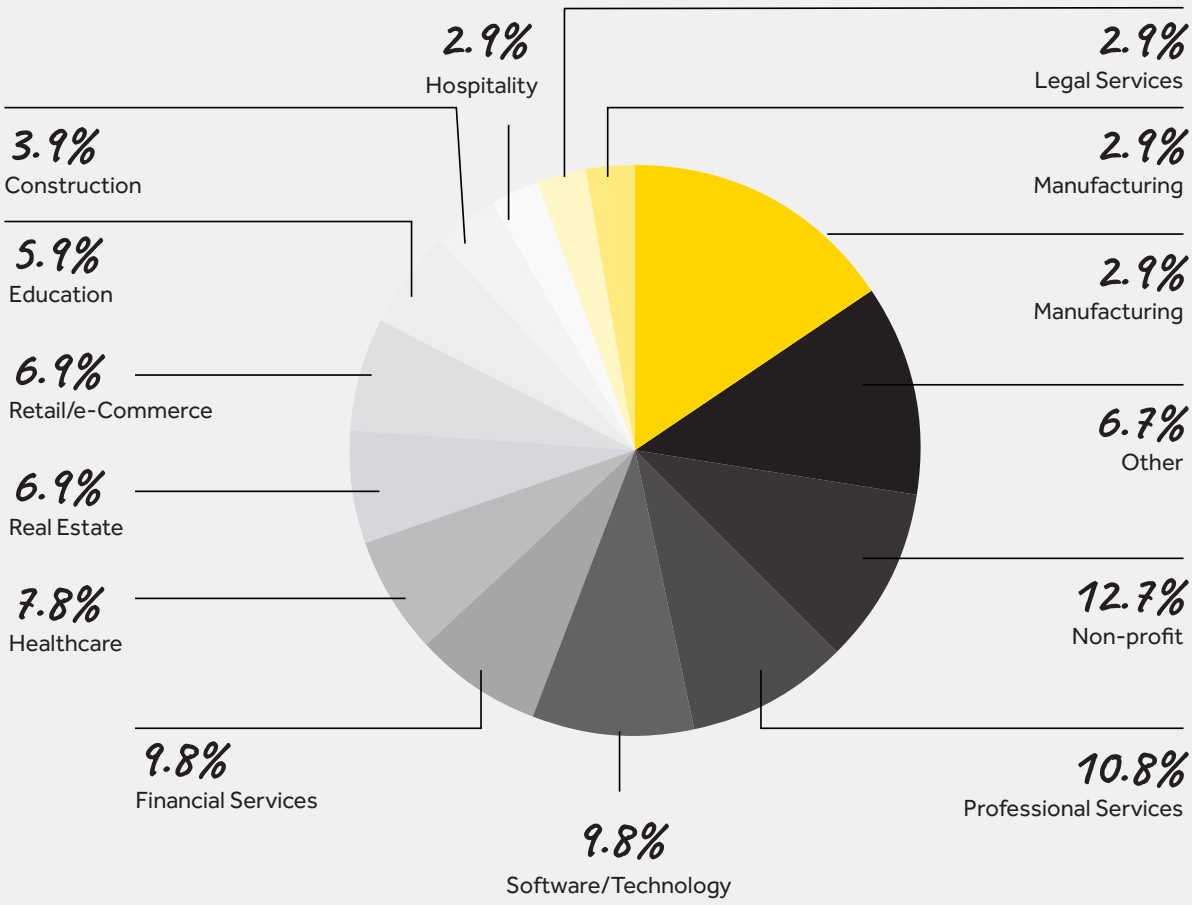
A compliance confidence score only means something if it's been tested. Propulsion's assessments give leadership a clear, honest picture of where the organization stands, and what it takes to stay there.

Get an honest assessment →

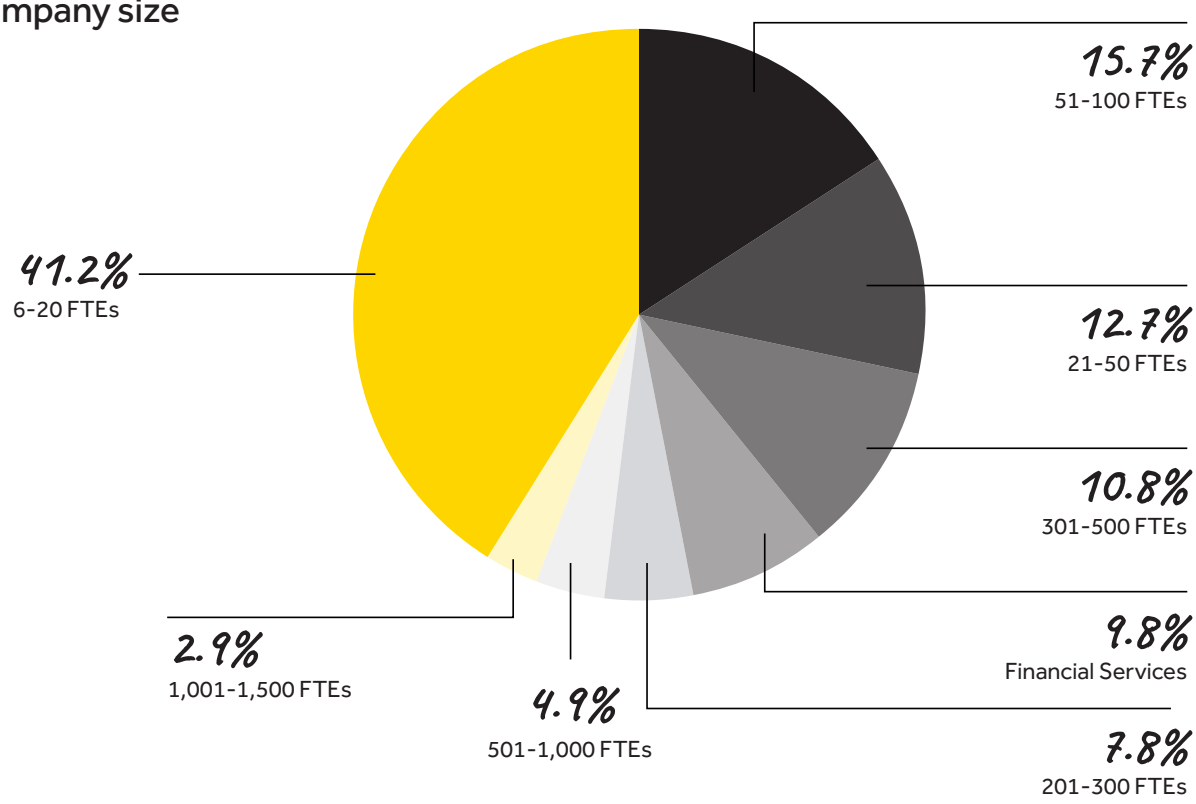
Propulsion

About our respondents

Industry



Company size



Role