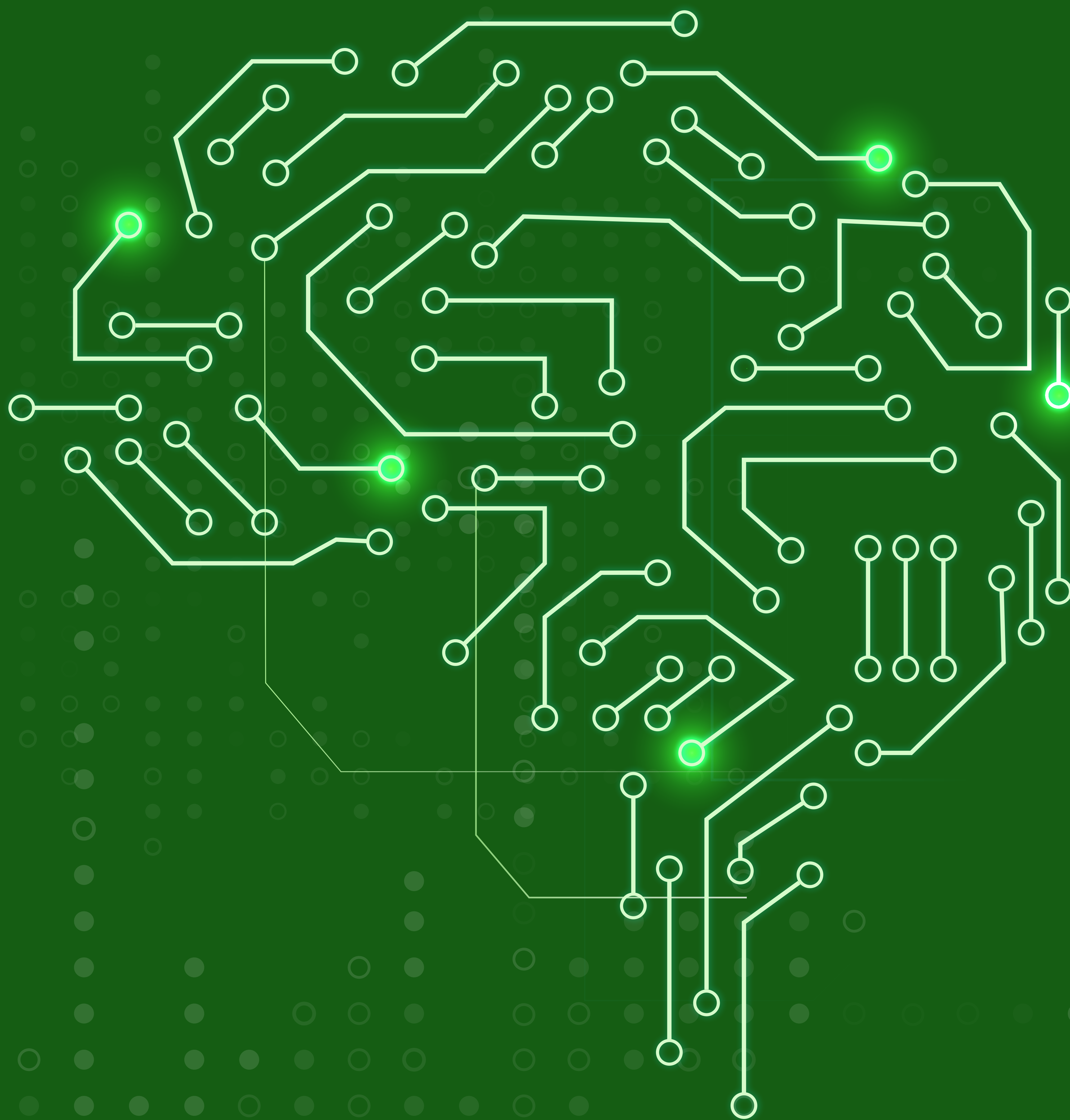


Thoropass™

AI and the future of audits: 500+ security leaders on how they're leveraging AI



Ninety-six percent. That's how many IT and security leaders say their organization already uses AI in compliance or audit processes.

If you're still on the fence about AI in auditing, you're in the minority. The question has already shifted from "should we adopt?" to "how are we using it and are we using it well?"

The answer, for many teams, is "not yet."

Organizations are deploying AI across risk assessment, control testing, and report generation—but adoption doesn't equal optimization. Most are still figuring out where AI delivers real value and where human judgment remains non-negotiable.

This guide breaks down how organizations are actually using AI in their audit workflows: the use cases that work, the benefits they're seeing, the risks they're managing, and what they expect from their audit partners.

Key Insights

1

Nine out of 10 of GRC professionals we surveyed say their organization **already uses AI in compliance and audits**, with an internal AI usage policy in place.

2

At the same time, just **40% of organizations use compliance-specific AI tools**. Two-thirds of respondents describe their organization's use of AI as "advanced" or "integrated," still have loose deployment and some untapped use cases. Unsurprisingly, most organizations are looking to work with partners proficient in AI: **seven out of 10 say AI capabilities are "very important" when selecting an auditor**. Worryingly, half that number say their auditor is "very advanced" in AI workflows.

3

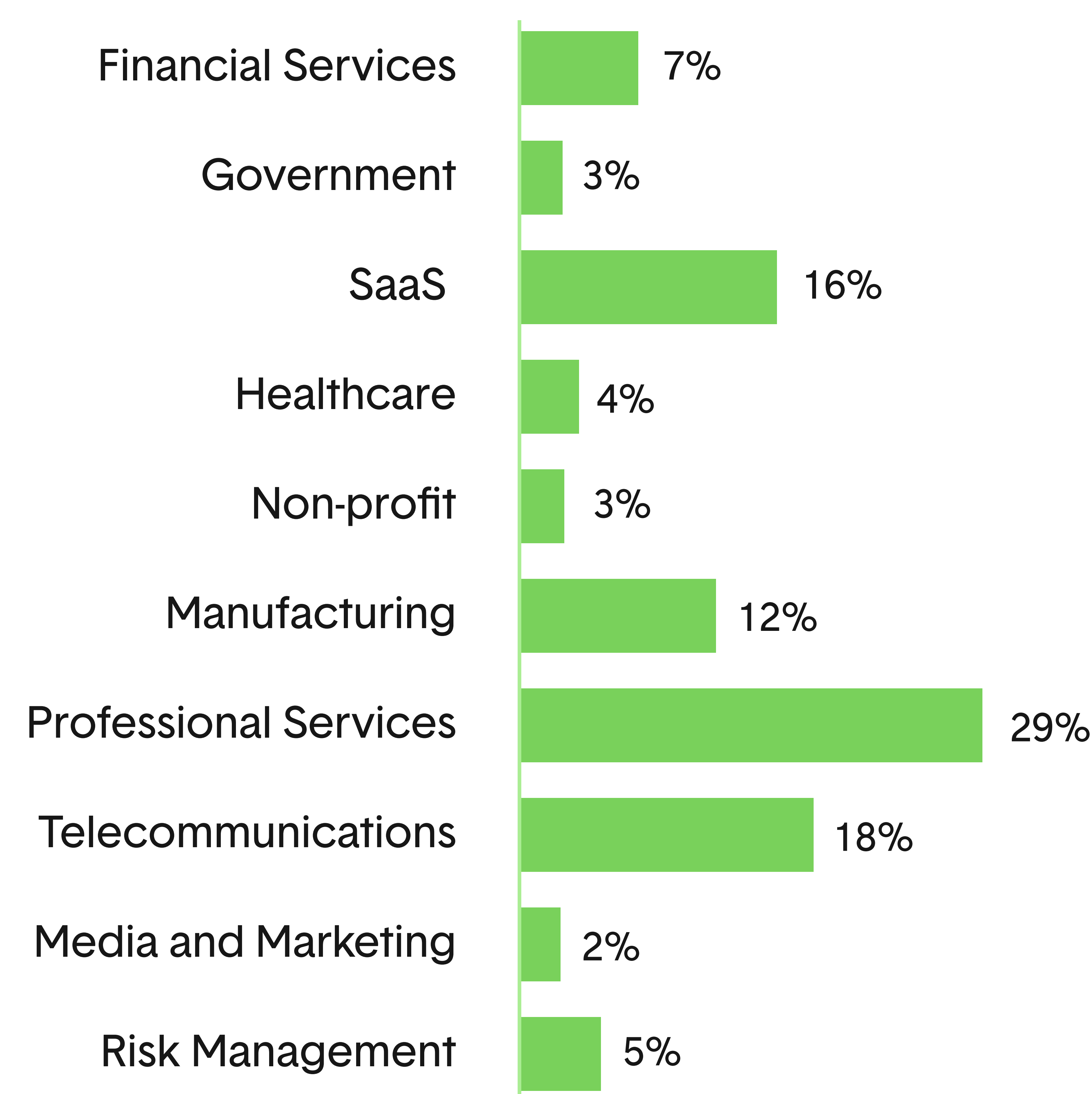
Respondents list the three biggest impacts of AI as **time savings, consistency in documentation, and improved visibility**. Early efficiency gains and room for growth in some use cases. More than half of respondents say AI cut audit times by 50% or more, but there's still room for growth: just a quarter of organizations use AI for evidence review.

4

Looking forward, our GRC respondents expect to see a fundamental shift in the industry, with **AI speeding up audit processes, sharpening threat detection, and having a continued impact on productivity**. Respondents are also clear on current limitations: **over half say AI can handle only some compliance workflows**. In other words, organizations need the expertise of a GRC team and a strong audit partner to direct better, more scalable adoption of AI.

Methodology

We surveyed 548 IT and security professionals who manage or contribute to external audits for frameworks like SOC 2, ISO 27001, and PCI DSS. Respondents spanned industries—professional services, telecommunications, SaaS , and manufacturing made up the largest segments. Financial services, healthcare, government, and non-profit organizations also contributed perspectives.



548
professionals

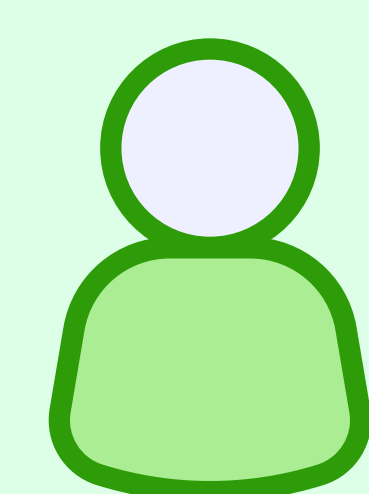
These aren't junior staffers. Half hold senior leadership titles—VP, Director, or Head of Function. Another 19% sit in the C-suite or at board level. Middle management accounts for 25%. In other words, we're hearing directly from the people making decisions about AI in compliance.

19%

Sit in the C-suite
or at board level

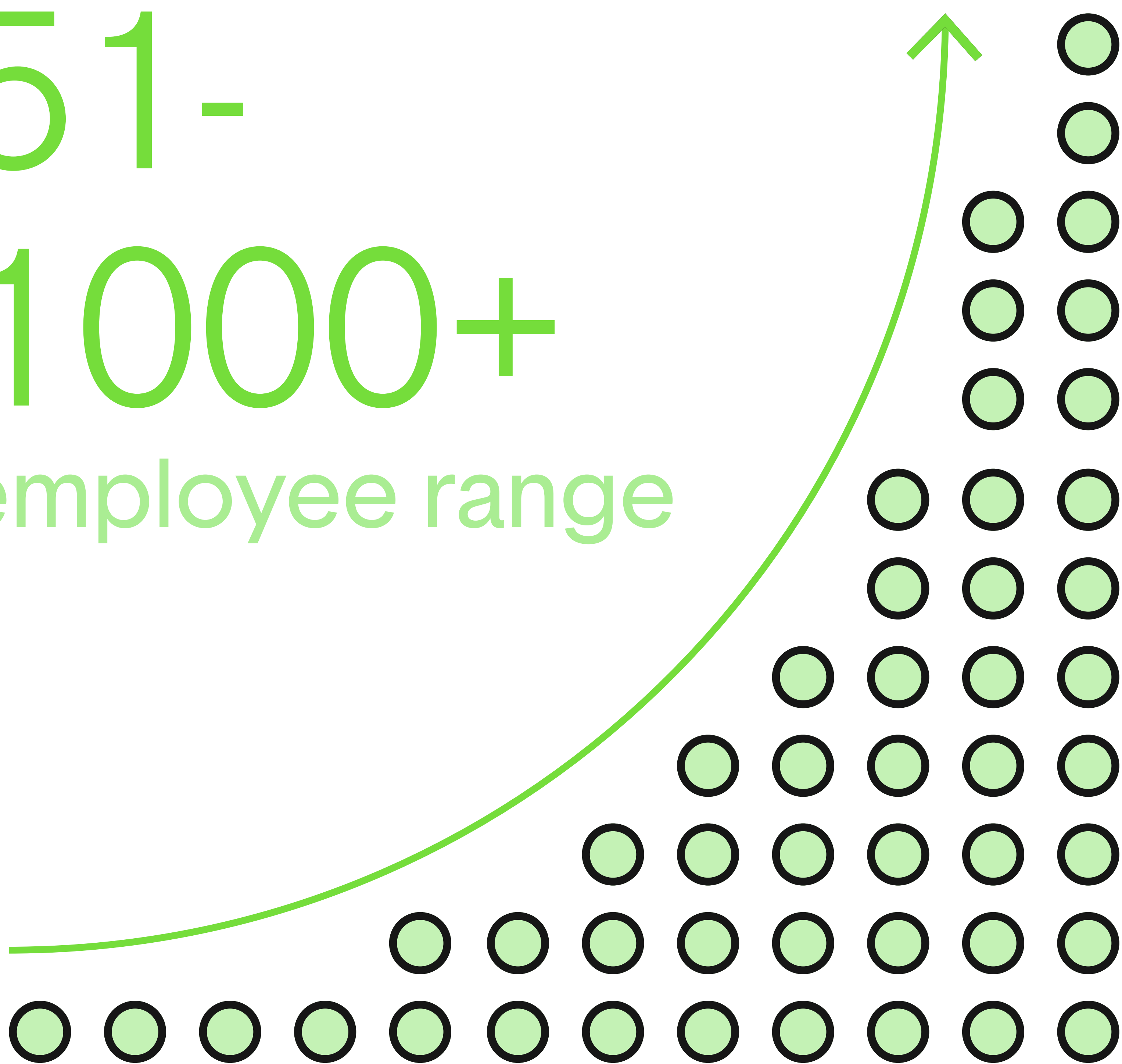
25%

Middle management



Company sizes ranged from 51 employees to over 1,000, with the largest cohort (33%) coming from enterprises with 1,000+ people. Compliance teams varied too—38% have 10 or more employees dedicated to security audits, while 36% operate with teams of 6–10.

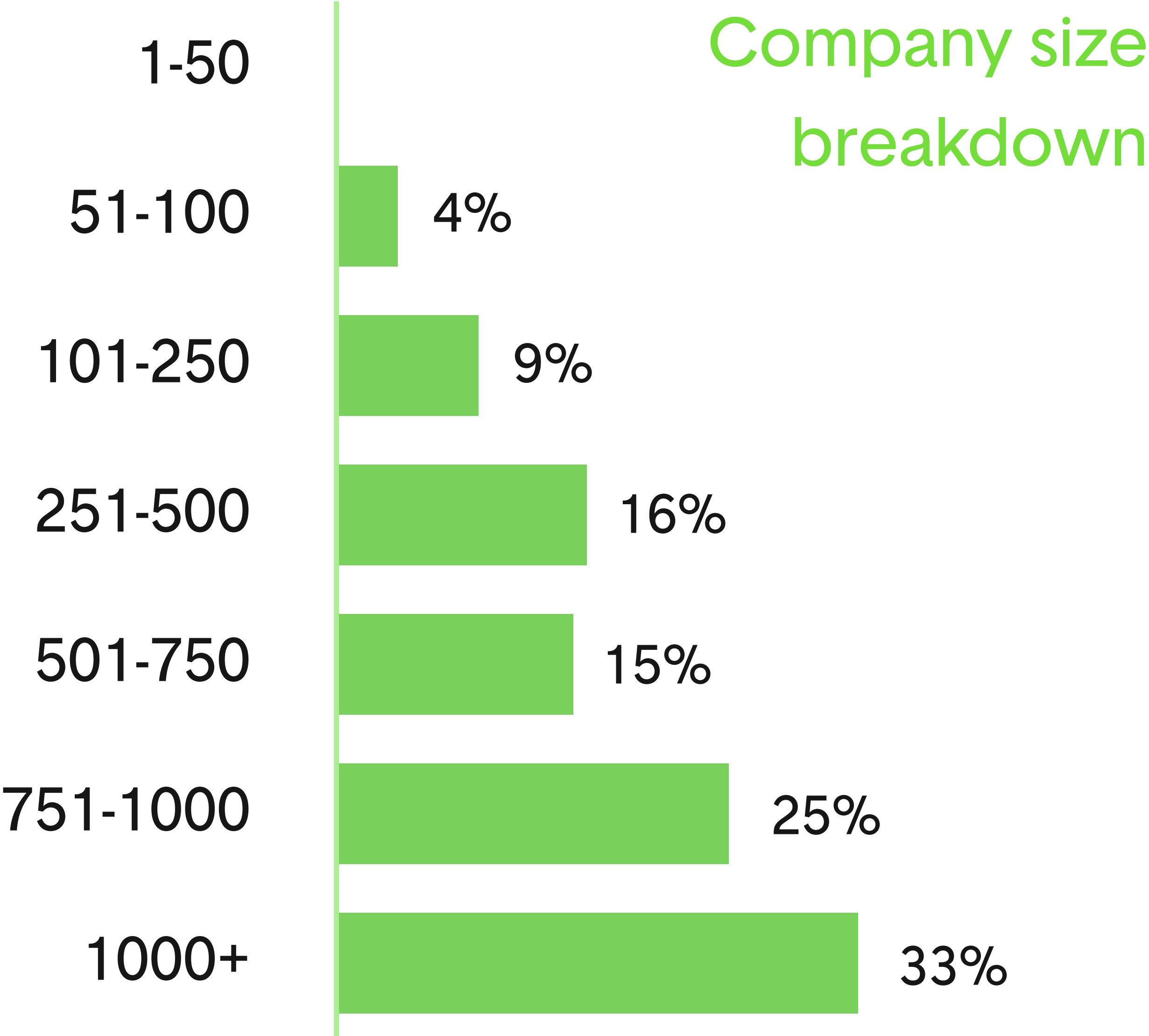
51-
1000+
employee range



33%
Coming from enterprises
with 1,000+ people

38%
Have 10 or more employees
dedicated to security audits

36%
Operate with teams of 6–10



62%
0-10 employees

38%
10+ employees

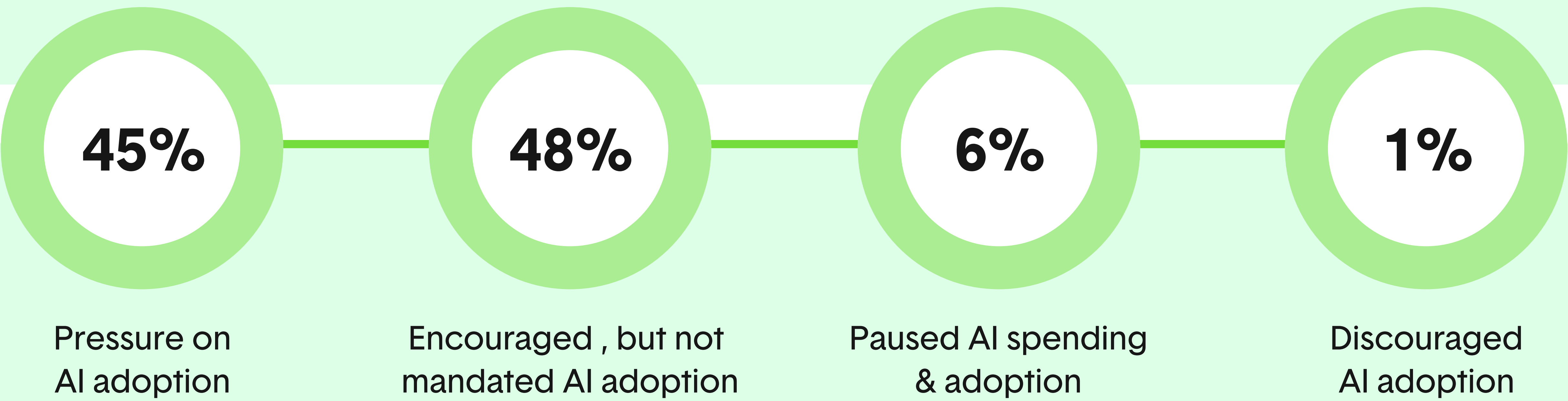
Compliance team size breakdown

AI is here: How organizations are using it today

Almost every organization has adopted AI; the more interesting question is how they're doing it and who's driving the push. Our survey reveals clear patterns: adoption is coming from the top, general-purpose tools are outpacing purpose-built solutions, and some use cases have taken off while others lag behind.

Leadership is driving adoption

This isn't a grassroots movement. AI adoption in compliance is being pushed from executive suites and boardrooms. Nearly half of respondents (46%) say that their leadership mandated AI use. Another 45% describe leadership as encouraging, but not requiring AI adoption. Only a sliver (6%) report that their organization has hit pause on AI spending, and just 1% say leadership actively discourages it.



CISOs and CIOs are the primary champions, leading adoption efforts at 34% of organizations. Department heads follow at 25%, with engineering or data teams close behind at 24%. Company boards and advisors drive adoption at 8% of organizations, while external consultants play a role in just 4%. Once tools are adopted, IT overwhelmingly owns the keys—93% of respondents say IT is the primary team overseeing AI usage across the organization.

At the same time, organizations have governance infrastructure in place. A striking **95% of organizations have established internal policies for responsible AI use in compliance and audit**—covering approved tools, formal oversight processes, and limits on which systems can be accessed.

Has your organization developed any internal AI policies?

95% YES

NO



“

All organizations want their people to use AI because they see it as an efficiency boost. Leadership says, 'Use AI, you're more efficient, it's less cost.' But the reality is they give people an enterprise ChatGPT license without much training on how to actually use it in day-to-day work. That's where the tension and drop-off exist—people don't actually know how to optimize AI to make themselves more efficient.”

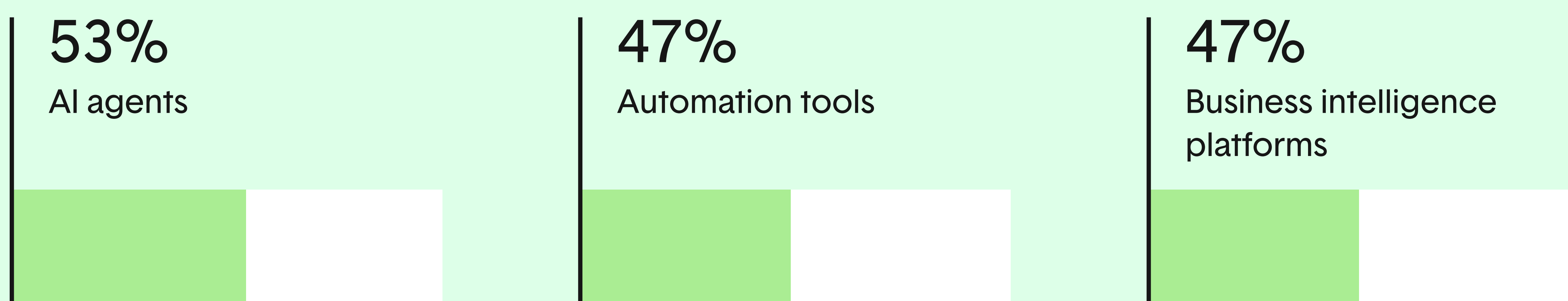
Leith Khanafseh, Audit Managing Partner at Thoropass



You probably don't have a good grasp on how AI is used within your org

Adoption may be nearly universal, but a closer look at what people are using reveals a more nuanced story. General-purpose LLMs dominate: 90% of respondents use ChatGPT, Claude, Gemini, Perplexity, or similar tools in their compliance work. Vendor-deployed AI features—capabilities automatically baked into existing software—come in second at 67.2%.

From there, adoption drops off. AI agents are used by 53%, while automation tools (47%) and business intelligence platforms (47%) hover around the halfway mark. App-building and low-code tools trail at 35%. Compliance-specific AI? Only 40% of respondents use purpose-built solutions.



Most teams are adapting general-purpose tools to specialized workflows rather than investing in tailored automation. That's not inherently wrong, but it does raise questions about how much efficiency organizations are actually capturing—and whether governance is keeping pace.

Self-assessments of AI maturity skew optimistic. About a third (33%) describe their organization as "advanced"—meaning AI-driven automation spans their audit processes. Another 33% say they've reached "integrated" status, with AI woven into compliance workflows. Only 16% describe their use as "structured" (enterprise tools with custom prompts), and just 19% remain at the "basic" stage, dabbling with free tools for occasional tasks.

“

Seeing 90% of auditors using AI sounds impressive, but what does that actually mean? From what I've heard, many firms just make an LLM available, and professionals use it as a glorified search engine—asking questions to teach themselves about unfamiliar cloud environments. It's more of a resource rather than embedded AI workflows actually changing what's being done. I haven't seen a lot of great solutioning from AI tooling yet.”

Chris Beiro, Senior Director of InfoSec Solutions at Thoropass



Where AI is making an impact

Certain use cases have emerged as clear winners. Risk assessment tops the list at 62%, with control testing, report generation, and regulatory research close behind—all above 50% adoption. Evidence collection and review, however, trail noticeably despite being natural fits for automation.



62%

Risk assessment with above 50% adoption

These patterns make sense. AI thrives on volume, pattern recognition, and consistency. That’s exactly what’s needed when parsing regulations, generating documentation, or churning through repetitive assessments. The technology excels at tasks that would otherwise consume hours of analyst time without adding strategic value. "There's a lot that an auditor does that is repetitive and mundane, like reviewing policy documents and trying to find relevant language to test a control," says Beiro.

“You can have AI do that much more effectively: review the evidence, write a summary of what it found for a human auditor to validate. That's a great administrative burden lifted off the team's shoulders.”

Risk assessment offers similar potential. Rather than manually combing through technical data, teams can let AI surface insights faster—provided they validate the output. The key is treating AI as a thought partner, not an oracle.

“

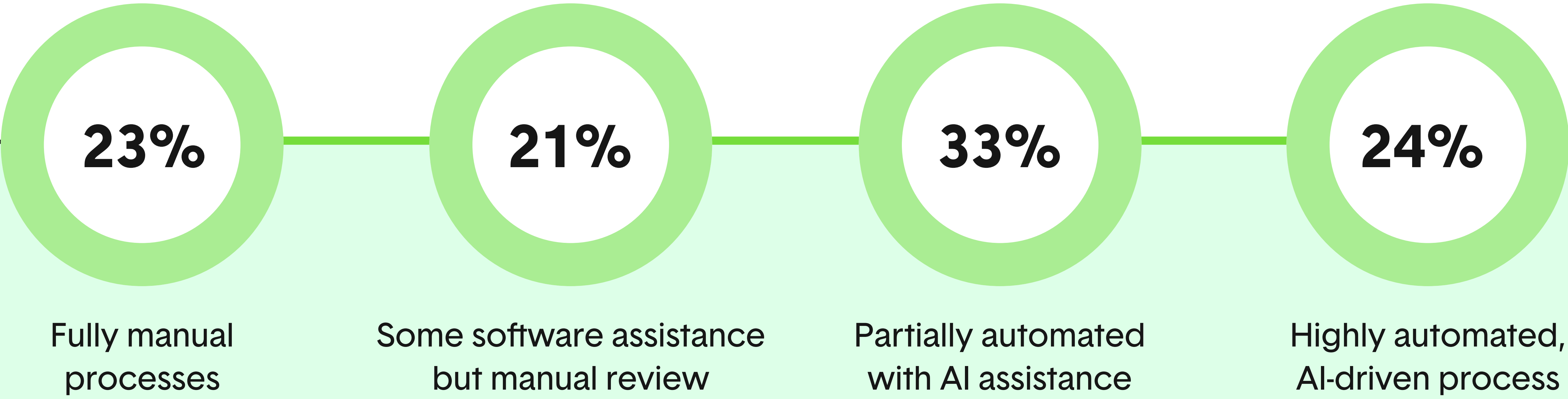
If you feed AI your vulnerability scans, pentests, or technical assessments, it does a pretty good job of identifying risks to your business: how big or small they are, and how you might mitigate them. Used correctly, it could be really powerful. Obviously it could make mistakes, so you'd want a human to validate and be a thought partner. But the potential is there.”

Leith Khanafseh, Audit Managing Partner at Thoropass

The evidence collection gap

One glaring exception: evidence collection and review. Despite being tailor-made for automation, these tasks remain stubbornly manual. Fewer than half of respondents use AI for evidence review, and only about a quarter have achieved highly automated, AI-driven evidence processes. The rest still rely on fully manual workflows or software with heavy human oversight.

How does your organization currently handle evidence collection and review?



“

A lot of evidence collection is actually controlled by the auditor. The auditor tells you what to submit and has to approve the mechanism for submission. There's resistance from auditors, and part of it is because many auditors aren't technical. They don't really understand the technology. They see something new, and they're afraid of it rather than embracing it. That's why AI hasn't penetrated evidence collection the way you'd expect."

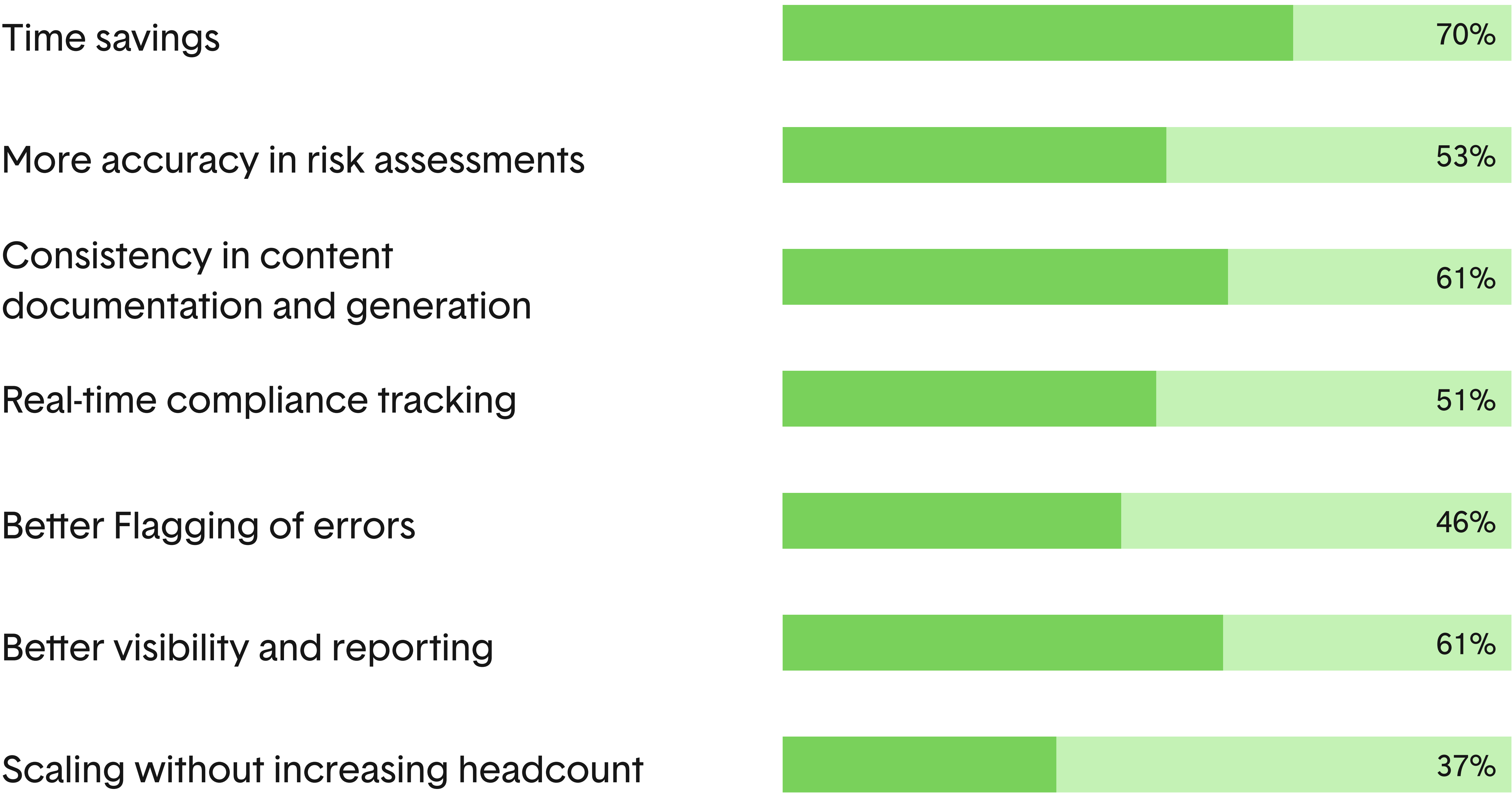
Leith Khanafseh, Audit Managing Partner at Thoropass

This gap represents low-hanging fruit. Organizations that bridge it—by working with auditors who embed automation into their processes—stand to unlock major efficiency gains in one of auditing's biggest time sinks.

The benefits organizations are experiencing

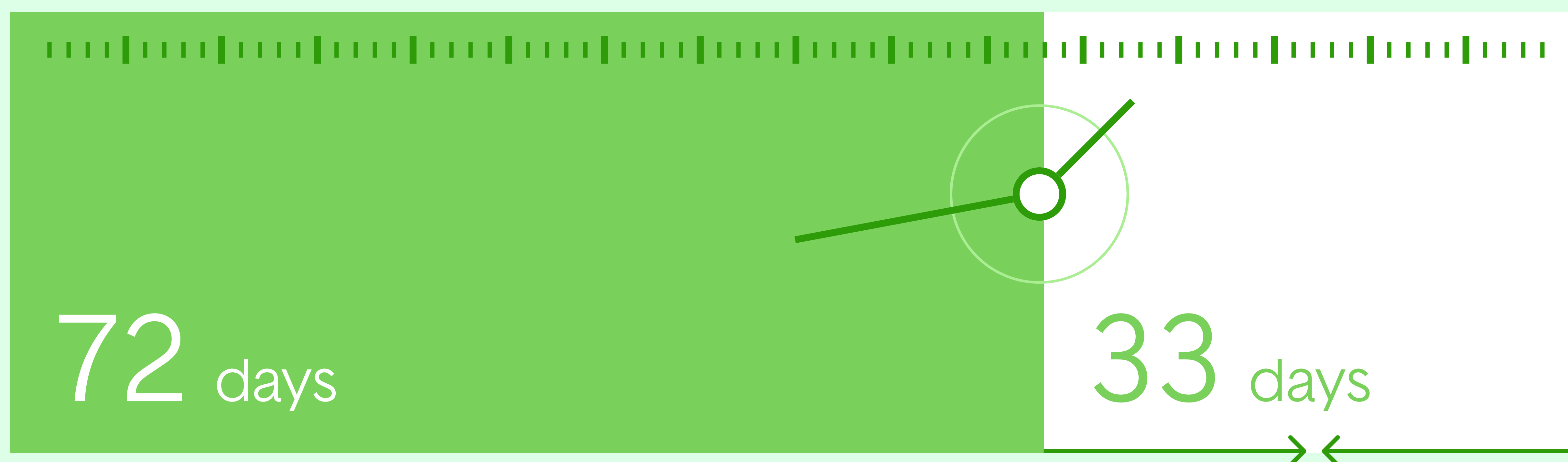
When asked what AI actually delivers, respondents pointed to three standout benefits: time savings (70%), consistency in documentation (61%), and better visibility and reporting (61%). Real-time compliance tracking and more accurate risk assessments also ranked highly, each cited by more than half of respondents. For resource-strapped teams, one benefit stands out: 37% say AI has enabled them to scale compliance efforts without adding headcount.

What are the primary benefits you've experienced from AI adoption?



The impact on audit timelines backs up the enthusiasm. Nearly all respondents say AI has accelerated their audits, with more than half reporting improvements of 50% or greater.

How has AI impacted your audit efficiency and timeline?



Thoropass has witnessed similar transformations internally. "We started deploying AI in our audits in February of this year," Khanafseh shares. "Average audit duration dropped from around 72 days to 33 days. That's more than half—and it's because AI is making our auditors and processes much more efficient."

Speed isn't the only gain. Confidence matters too. "There's less surprise in the audit because customers know almost immediately whether what they're submitting will be acceptable—and why," Khanafseh explains. "The timeline shrinks, but they also have more satisfaction going in. It makes the customer more confident heading into the audit."

AI is everywhere — but that doesn't mean it's always effective

Widespread adoption masks a messier reality. AI tools have real limitations, implementation varies wildly in quality, and compliance professionals harbor complicated—sometimes contradictory—feelings about what automation means for their work and careers.

Risks and limitations

The top concern among compliance professionals about AI's shortcomings is that the technology still demands human oversight. This is a clear acknowledgement that automation doesn't eliminate the need for expert judgment, particularly in the compliance space.

Other pain points:

- Lack of compliance-specific knowledge
- Inconsistent outputs from identical prompts
- Garbage-in-garbage-out data quality issues
- Prohibitive costs for regular use
- Integration issues with audit platforms
- AI hallucinations
- Low user adoption
- Security concerns around AI tools

What limitations have you encountered in your current AI tools?

- 38% Lack of compliance-specific knowledge
- 31% Inability to integrate with adult platforms
- 14% Doesn't pass security frameworks/data security concerns
- 32% Reliance on poor data (garbage in, garbage out)
- 36% Inconsistencies across sessions (same prompt delivers different answers)
- 19% Hallucinations
- 18% Low user adoption
- 31% Expensive to use on a regular basis
- 40% Requires human oversight
- 15% None

Beiro notes that AI is prone to generating bad responses, which can rattle someone's trust: "That's why the mindset should be: use AI as a first step where you have a human come in behind to validate that the response is accurate. Down the road, we may get to a state where there's more reliance on AI output. But it's not there yet."

Getting value from AI also requires more upfront work than many expect. Organizations can't just plug in a tool and watch productivity soar—there's real engineering involved.

“

There's probably a thought out there that you can just pick up an AI tool and inject it into your workflow. But what we're finding is you have to do a fair amount of engineering—refining your prompt structure to get to the use case you want. It's not lift and shift. You have to be intentional about what you want it to do, build a plan, and iterate."

Chris Beiro, Senior Director of InfoSec Solutions at Thoropass

Auditing introduces its own risks beyond the usual AI pitfalls. The very capabilities that make AI powerful—image manipulation, text generation—can be weaponized to fabricate compliance.

“

There's a perception in the infosec auditor community that AI can be used to doctor or fake evidence. It's trivially easy to feed a screenshot into ChatGPT and say, 'Change these details to make me look like I'm doing the right thing.' From an audit perspective, that's a real risk we have to contend with."

Leith Khanafseh, Audit Managing Partner at Thoropass

The shadow AI challenge

Beyond sanctioned tools lurks a growing phenomenon: shadow AI. Employees use whatever works—authorized or not—to get their jobs done faster. This creates tension between individual productivity and organizational security, when organizations aren't sure where or how their teams are using AI.

"I saw today that shadow AI is outpacing enterprise AI solutions," Beiro notes. "People just grabbing tools to support their day-to-day work is more popular—and maybe more impactful—than companies trying to take an enterprise solution and embed it into formal workflows."

That popularity comes with a cost. When employees choose their own tools, they're often selecting free tiers with weaker data protections—and they're rarely thinking about what happens to the information they feed into those systems.



"If it's unauthorized and you're dealing with sensitive information under non-disclosure agreements, whatever you put in the LLM can be used to train the engine and it can be shared. Some tools—the free versions especially—will share what you create with the community. You can't be using sensitive information from your organization or your clients; that's very risky."

Chris Beiro, Senior Director of InfoSec Solutions at Thoropass

Job security and satisfaction: A complex picture

AI stirs up complicated emotions in the compliance workforce. Over a third of respondents (36%) admit that fear of becoming irrelevant or replaceable by AI-adopting professionals influenced their decision to use these tools. Nearly a quarter (23%) say they're "very concerned" that AI will make their role redundant. Another 14% worry about job security if they don't adopt AI.

AI impact on job security:

27% Not concerned

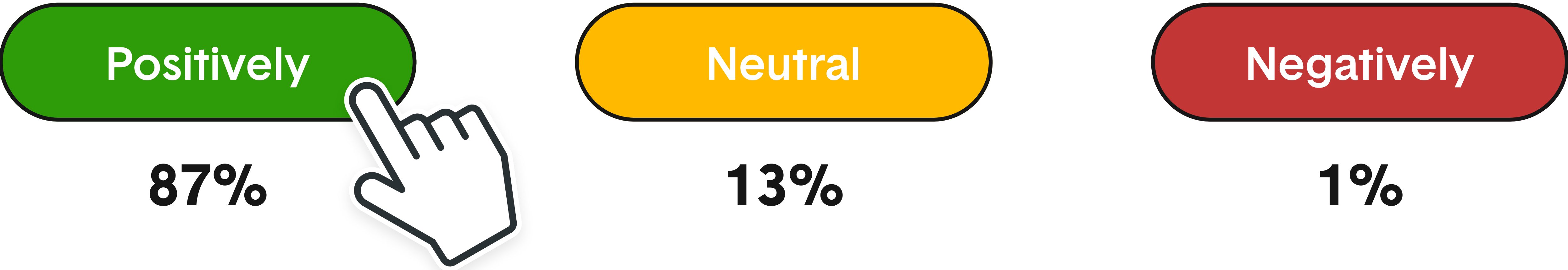
36% Concerned but willing to adopt AI to add value to my role

14% Concerned about job security if AI is not adopted

23% Very concerned that AI will make my role redundant

And yet enthusiasm runs high in parallel. A remarkable 87% say AI adoption has positively influenced their job satisfaction—they feel more likely to stay in their role with new tools at their disposal. Perhaps most telling: 77% would switch employers for a workplace with stronger AI adoption.

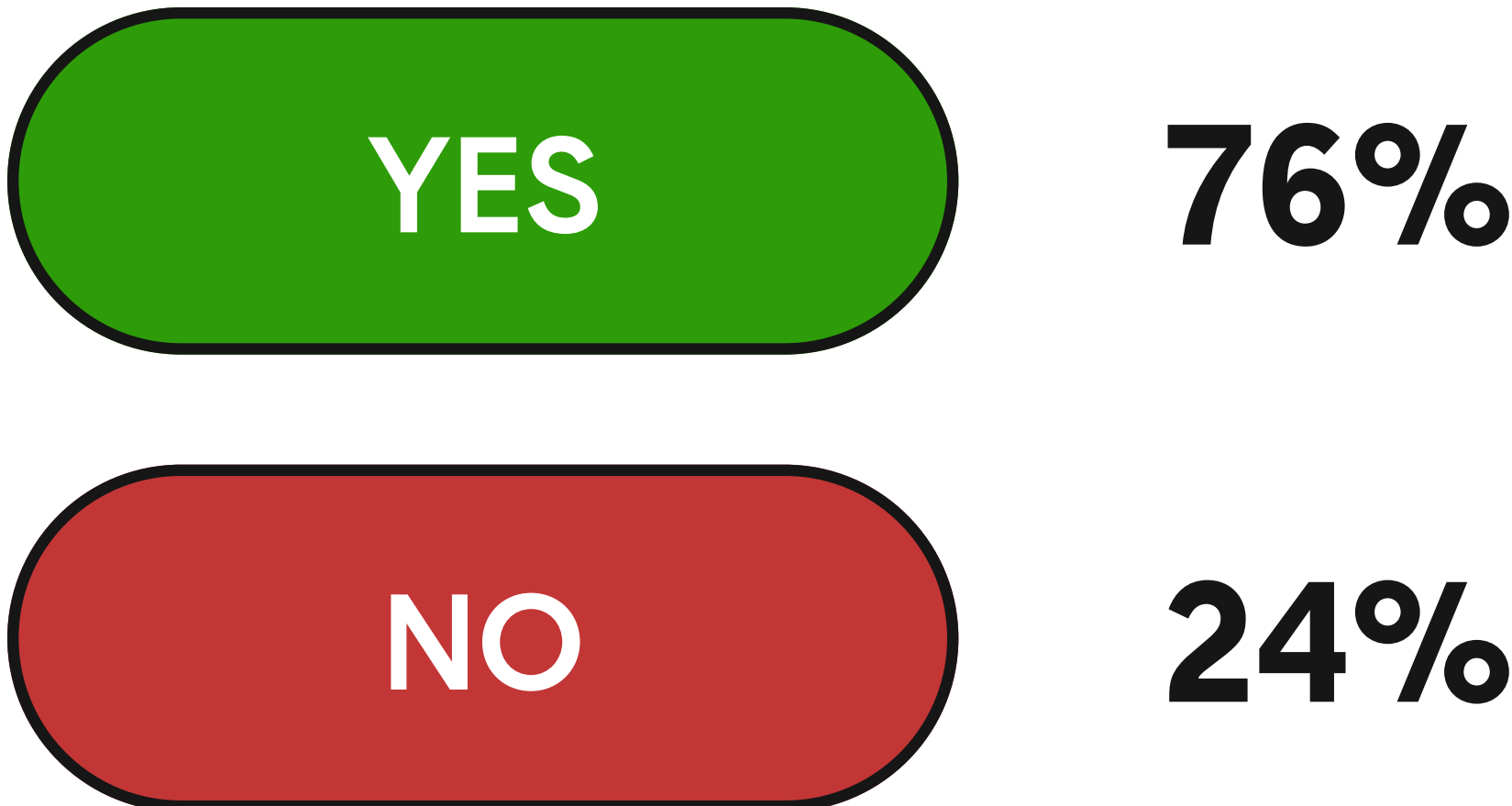
How does AI adoption influence your job satisfaction?



- Positively** — I'm more likely to stay in my role with a range of opportunities and new tools at my disposal
- Neutral** — I'm unsure about the direction the organization is taking in regards to security and AI
- Negatively** — I'm considering/actively looking for a new role

This tension defines the current moment: professionals are worried about being replaced, yet energized by what the tools enable them to accomplish.

Would you consider changing employers to be in a workplace with greater adoption of AI tools?



“

"There's a lot of buzzwords around AI, and as humans we're inherently risk-averse. We hear it and we're terrified of being replaced by algorithms and robots. Having used it, though, I don't think AI will ever fully replace a human—at least in the context of GRC. The humans that get replaced are the ones who don't use AI to be better at their jobs. It's like when computers were introduced—people who learned to use them kept their jobs, and people who couldn't probably lost them. AI is going to be similar."

Leith Khanafseh, Audit Managing Partner at Thoropass

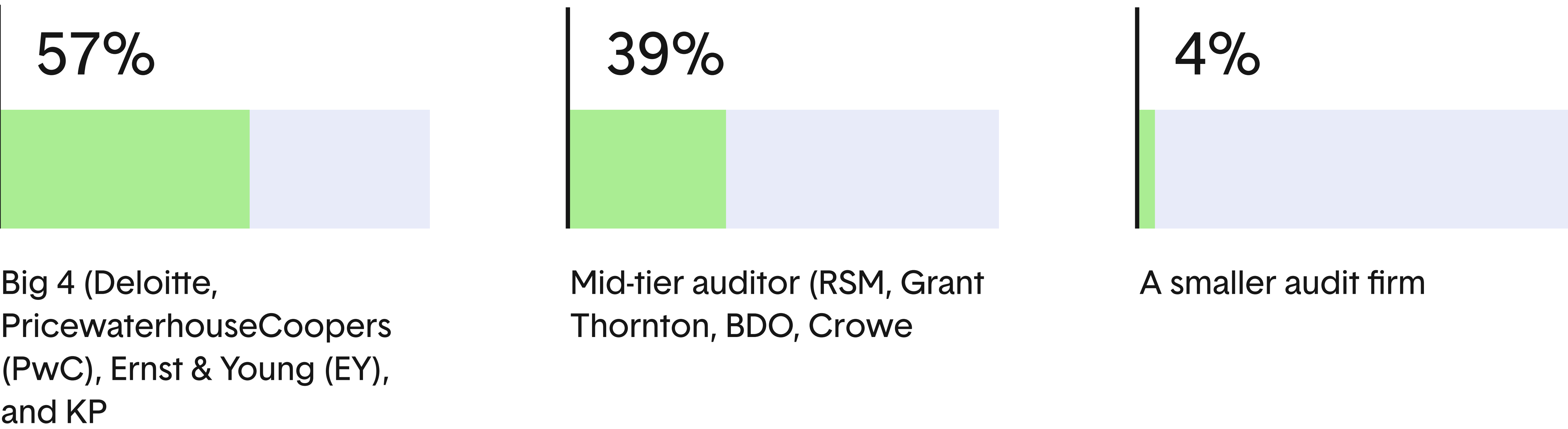
The Thoropass vision for AI in auditing

As organizations wrestle with AI adoption, they're scrutinizing their audit partners more closely, expecting not just capability but also genuine guidance on what works and what doesn't.

What organizations want from their audit partners

Most respondents work with established firms—57% use Big 4 auditors (Deloitte, PwC, EY, KPMG), while 40% engage mid-tier players like RSM, Grant Thornton, BDO, or Crowe. Regardless of firm size, expectations around AI have spiked considerably: 69% now rate AI capabilities as "very important" when selecting an auditor.

Who is your primary external auditor?



Just like 96% of respondents' organizations use AI, 96% of respondents' auditing firms also use AI in some capacity. But how advanced is their usage?

Here, reality lags expectations. Just 38% describe their auditor as "very advanced" in AI, while more than a fifth wish their auditor would catch up.

How important are AI capabilities when selecting an auditor?

- 69% Very Important
- 16% Not required, but preferred
- 8% Not required, must be able to prove efficacy before use
- 6% AI capabilities are not allowed, vendors using AI will not be considered
- 1% Not important
- 0.2% I don't know

How would you describe your auditor's use of AI?



That gap creates an opportunity for audit partners willing to lead rather than follow. Organizations want more than tools—they want partners who understand how to deploy AI while maintaining audit integrity.

Where AI will have the biggest impact

Looking two to three years out, our survey respondents see AI reshaping compliance fundamentally.

Their top predictions:

Looking two to three years out, our survey respondents see AI reshaping compliance fundamentally.

- Faster audit processes
- Sharper threat detection
- Boosted compliance team productivity
- Stronger auditor-client relationships
- Accelerated organizational scaling
- Always-on compliance monitoring

Where do you see AI having the biggest impact in compliance or audit over the next 2-3 years?



The through-line? AI excels at volume, consistency, and continuous vigilance, enabling a shift from periodic fire drills to ongoing assurance. The organizations that crack this model first will operate with a fundamentally different compliance posture than their competitors.

How Thoropass weaves AI into auditing

Thoropass operates on a simple principle: automate the grind, preserve the judgment. That philosophy manifests in both customer-facing features and internal audit operations.

First Pass AI

Traditional audits involve exhausting back-and-forth. Auditors request evidence. Customers submit something. It's incomplete or formatted wrong. Follow-ups ensue. Multiply that across hundreds of requests and frustration mounts on both sides. The process becomes burdensome for everyone involved.

First Pass AI short-circuits this cycle. "Once a customer satisfies a request for evidence, it gives them real-time feedback so they don't have to wait for the auditor," Khanafseh explains. "It tells them, 'This made the mark,' or 'You missed the mark in these three places—fix it now, because if you submit it, the auditor is probably going to come back with the same feedback.' The customer can address issues before they become problems."

The payoff: fewer cycles, faster closures, and calmer customers who enter audits with genuine confidence.

Smart Sort

Many organizations run compliance in one GRC platform and audits in another—creating tedious mapping work. Smart Sort eliminates that friction. Customers can dump data from any GRC platform, and the system automatically matches evidence to Thoropass's audit requirements.

"Instead of going line by line for each request, figuring out what it's asking, and manually attaching evidence," Khanafseh describes, "you just dump everything in and it sorts automatically." No more laborious matching across hundreds of requests. Upload, sort, move on.

Internal audit tooling

Behind the scenes, Thoropass auditors rely on proprietary tools that accelerate their work; most notably, Copilot, which tackles the information overload inherent in control testing.

"Think of a control as an instruction—part of a recipe for your security program," Khanafseh illustrates. "If you say you do background checks on employees, the auditor gets all the information on new hires and verifies whether you did a background check for each one during a specific period. You can imagine that's a very laborious process—going line by line could take eight hours for one control."

Copilot changes the math. It takes an initial pass at the auditor's checklist and the submitted evidence, surfacing findings with specific references. Instead of hunting through stacks of documents, auditors jump directly to relevant pages and validate what Copilot found.

"It tells the auditor: for this person, I found this thing on this page," Khanafseh explains. "The auditor goes to that specific piece of evidence and validates whether it's actually there. It really enhances the auditor's ability to get through information quickly and with more accuracy."

That's the model in action—AI handling initial analysis, humans validating conclusions. The "human in the loop" principle Thoropass experts emphasize is essential for responsible AI use in compliance.

AI is table stakes—execution is the differentiator

Everyone's using AI. That's no longer a competitive advantage. What separates leaders from the security teams that are falling behind is how they use it.

The benefits are proven: audit cycles cut in half, documentation that stays consistent, and visibility that doesn't require a fire drill to achieve. But the risks are just as real. AI hallucinates. It lacks compliance intuition. It can't tell you when something feels off. Treat it as infallible, and you'll learn that lesson the hard way.

The playbook isn't complicated. Let AI handle what it's good at—volume, repetition, pattern-matching. Keep humans where they belong—making judgment calls, validating outputs, catching what the algorithm missed. And invest in training, because a tool your team doesn't know how to use is just shelfware with a subscription fee.

One more thing: your auditor matters. The firms that figured this out early are already delivering faster, smoother engagements. The ones still debating whether to adopt AI are the ones creating the friction you're trying to eliminate.

AI won't replace compliance professionals. But compliance professionals who master AI will replace those who don't.

Ready to see what AI-augmented auditing looks like in practice? Explore how Thoropass combines intelligent automation with expert judgment to deliver faster, more confident audit experiences.

Thoropass[™]