Thoropass™

The audit gap report:

How InfoSec teams can bridge the divide between compliance and audit

Table of contents

Thoropass™

Executive summary

Every year, teams invest anywhere from hundreds to thousands of hours preparing for audits, from collecting evidence to monitoring controls and maintaining policies.

Yet when the audit begins, much of that effort doesn't translate. Teams must reformat evidence, respond to duplicate requests, and address new requirements. And all of that disrupts the actual audit. As a result, what should feel like a final lap instead feels like starting over.

This disconnect has a name: **the audit gap**. At Thoropass, we define it as **the breakdown between compliance preparation and audit execution**—a breakdown that drives inefficiency, risk, and frustration across your InfoSec program.

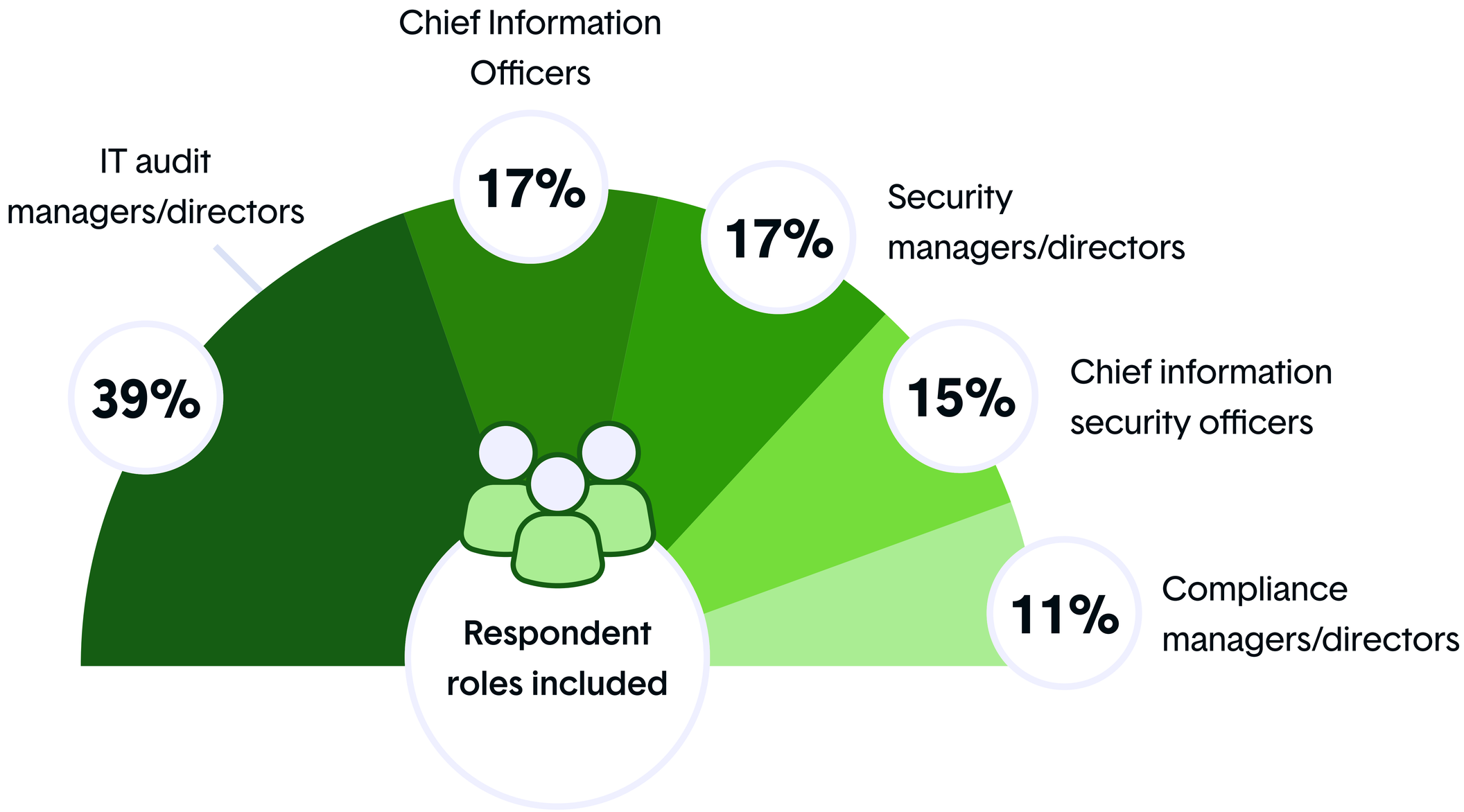
Nearly two-thirds (63%) of InfoSec professionals have experienced delays or increased costs because of this disconnect, according to our recent survey of 546 security and compliance leaders. That's not a minor inefficiency—that's a system-level challenge affecting business agility, customer trust, and revenue.

But there's a path forward. By unifying compliance and auditing into a single, integrated workflow—what we call audit-ready compliance—organizations can eliminate this friction. In some cases, you may even be able to reduce costs by up to 25% and accelerate certification timelines from 12 months to 6-7 months.

Below, we'll break down the anatomy of the audit gap, quantify its impact, and provide a roadmap for closing it once and for all.

Methodology

To understand the current state of compliance and audit processes, we surveyed 546 InfoSec leaders across midmarket to enterprise organizations ranging from 50 to 5,000+ employees.



Frameworks covered included:

52%	42%	29%	29%	28-31%
ISO 27001	SOC 2	HIPAA	PCI DSS	GDPR/CCPA

Most respondents (76%) said they dedicated 6 or more people to audit preparation, with 72% of teams spending **251–2,000+ hours annually** on audits.

The anatomy of the audit gap

Where compliance ends and audit begins (and why that's a problem)

The audit gap isn't a single failure point— it's a systemic disconnect that manifests throughout the compliance and audit lifecycle.

While organizations often attempt to both manage compliance and prepare for audits with a governance, risk, and compliance (GRC) platform, the information auditors seek often exceeds the scope of a GRC platform.

"GRC platforms are good tools for managing compliance, but then when you get into an audit, there's no connective tissue between what that organization has in their GRC platform and what the auditor is requesting," said Chris Beiro, Sr. Director of InfoSec Solutions at Thoropass.

And the organization, of course, has no choice but to follow that auditor's workflow, leading to multiple friction points, including evidence misalignment, communication gaps, tool sprawl, and more.

> *Either you have a good audit firm with a good audit solution, or you have a good GRC platform and it's one that doesn't work with your audit partner. Unless you can tie the two together, there's always going to be a disconnect."*

Chris Beiro
Sr. Director of InfoSec Solutions at Thoropass

The hidden cost of disconnection

All of these inefficiencies add up to more than the sum of their parts. Our research revealed a cascade of impacts, such as:

Resource drain

The human cost of the audit gap is substantial—not just in total hours, but in which hours are consumed. Engineering teams, security architects, and technical specialists are repeatedly pulled from strategic initiatives to handle urgent evidence requests and last-minute documentation needs, disrupting innovation and product development.

Budget escalation

Without addressing the underlying audit gap, investments in new tools and automation often fail to deliver promised efficiencies. Organizations find themselves paying for external consultants or sophisticated GRC platforms, only to encounter the same pain points year after year.

Opportunity cost

Perhaps most critically, the audit gap delays market entry and revenue growth. As certifications take longer to achieve—often stretching to 12+ months for complex audits—organizations miss opportunities to enter regulated industries, win enterprise deals, or expand globally.

One Thoropass customer reported that their previous Big Four audit ran a full year beyond the original timeline, with cost overruns exceeding hundreds of thousands of dollars above the initially allocated budget.

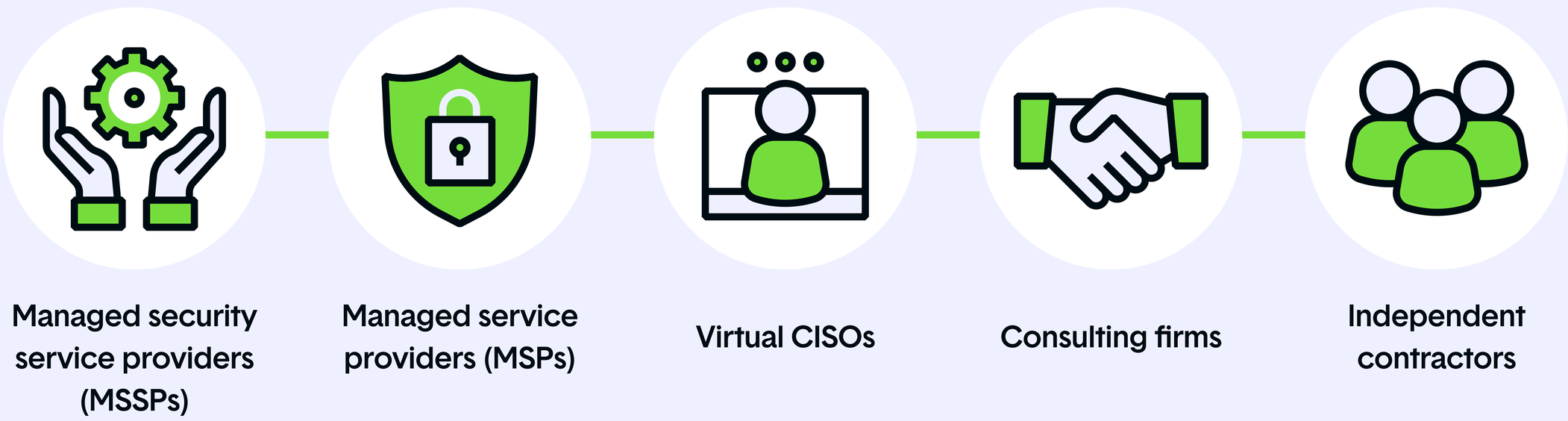
The shape of today's audit gap

Our survey revealed challenges and inefficiencies throughout many of the hundreds—if not thousands—of hours organizations spend on audits.

Top challenges InfoSec teams face

Our survey data paints a clear picture of where the audit gap creates the most friction:

High Costs of External Audit Consultants (47%)



With 92% of organizations relying on external support, it probably comes as no surprise that nearly half of respondents cited cost as their primary challenge. The complexity of modern compliance has created a secondary industry of external support.

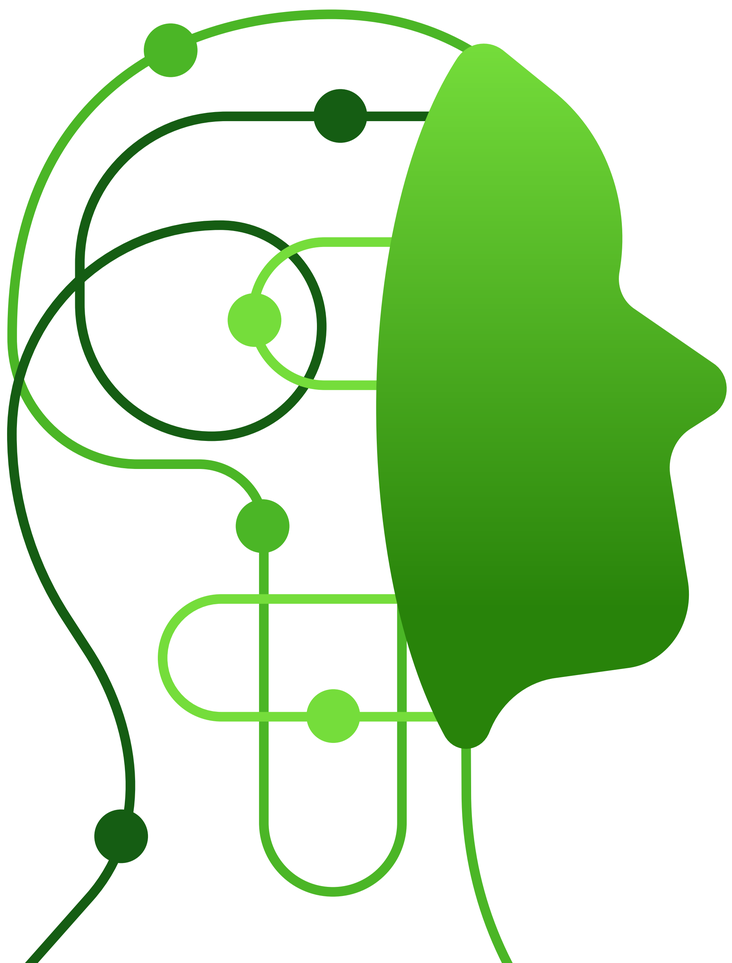
This web of external relationships, while providing necessary expertise, often exacerbates the audit gap.

Each partner brings their own tools, processes, and communication styles, further fragmenting what should be a unified workflow. Organizations find themselves coordinating multiple vendors, reconciling conflicting advice, and managing handoffs between partners who may not communicate directly with each other.

As a result, teams often spend as much time managing their compliance partners as they do managing compliance itself.

Ever-changing regulations (43%)

The regulatory landscape isn't just expanding—it's accelerating. Organizations that once only needed to comply with ISO 27001 and SOC 2 now find themselves navigating a maze of regional and industry-specific requirements.



Compliance professionals are increasingly inquiring about frameworks like:

- **The General Data Protection Regulation (GDPR):** European Union regulatory framework designed to protect user privacy
- **The Digital Operational Resilience Act (DORA):** European Union regulatory framework that aims to increase digital resilience among financial entities and third-party information and communication technology (ICT) providers
- **Cyber Essentials Plus:** United Kingdom regulatory framework run by the National Cyber Security Centre (NCSC) to prevent some of the most common cyber attacks, mandatory for many UK government contractors
- **Information Security Registered Assessors Program (IRAP):** Australian government initiative run by the Australian Signals Directorate (ASD) that assesses the security of ICT providers, mandatory for many Australian government contractors
- **Information System Security Management and Assessment Program (ISMAP):** Japanese government program run by the ISMAP Steering Committee to assess the security of cloud service providers (CSPs), mandatory for many Japanese government contractors

For businesses attempting to expand into new markets or sectors, regulations like these don't just give them a competitive edge—they're often the deciding factor in whether they can operate there at all.

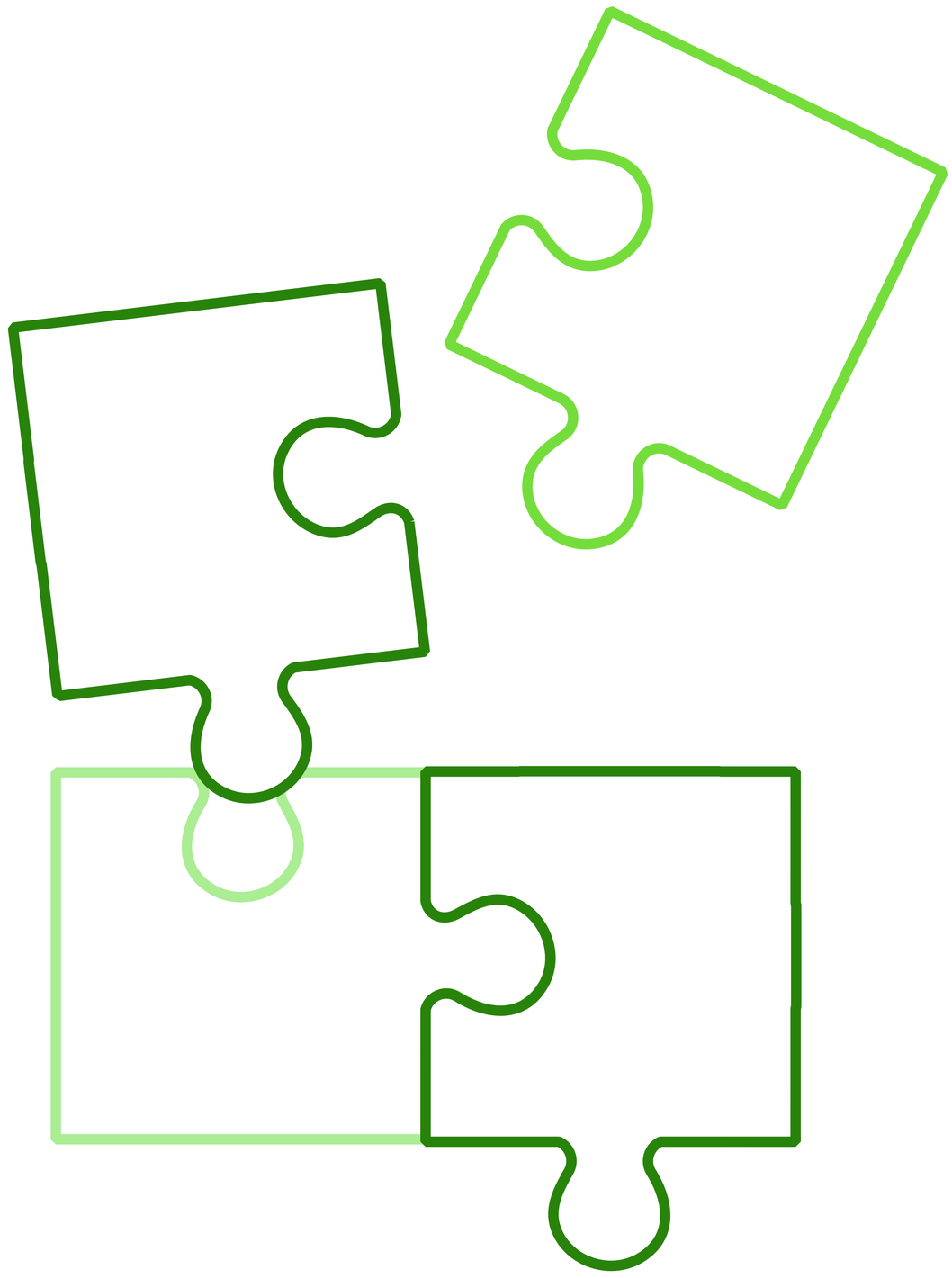
Communication gaps between compliance team and auditor (36%)

More than a third of InfoSec professionals struggle with the fundamental disconnect between what compliance teams prepare and what auditors expect. This typically manifests as "auditor speak" that confuses rather than clarifies.

Even when organizations receive an IRL (Information Request List) from an audit firm, they're often filled with regulatory jargon and vague requirements. Without context or clarification, teams interpret requirements one way, only to discover during the audit that the auditor expected something entirely different—often deep into the audit process.

"At my previous audit company, we would see upmarket customers churn time and time again. There was a massive breakdown between what the automation produced and what auditors would actually accept as evidence," said Elise Spitzer, Sr. Customer Success Manager at Thoropass.

Customers would spend months collecting evidence in their GRC platform, only to discover that their auditor required different formats, requested additional documentation, or rejected automated outputs. At that point, however, it was too late to efficiently course-correct.



Customers would be feeling confident about being audit-ready, but then the auditor would arrive and say, 'I can't accept this evidence. I need you to provide static evidence and walk me through everything manually.' It essentially eliminated any time savings they thought they would achieve."

Elise Spitzer
Sr. Customer Success Manager at Thoropass

GRC teams face gaps in workflow, visibility, and tooling

While compliance and audit technology continues to improve, many organizations still struggle with fundamental workflow challenges.

The spreadsheet paradox

Even as organizations invest in advanced compliance tools, 39% still rely on spreadsheets for critical audit functions. Some compliance professionals are really in love with their spreadsheets.

The challenge isn't the spreadsheets themselves—it's when they become the primary translation layer between GRC platforms and auditor requirements. This creates version control issues, security risks, and efficiency bottlenecks.

The solution isn't necessarily eliminating spreadsheets entirely, but rather integrating them thoughtfully into a more robust compliance workflow where they complement, rather than replace, purpose-built tools.

Platform proliferation without integration

Our survey reveals organizations use an average of 3-4 different tools for compliance and audit management, including SharePoint (33%), custom-built in-house tools (22%), and a variety of GRC platforms—yet these tools rarely integrate seamlessly.

Organizations must manually transfer data between systems, which, in addition to being tedious and time-consuming, often results in duplicated evidence and data entry errors. So, why does this fragmentation occur? Organizations often need to translate between their GRC platform and their auditor's preferred format.

> *When auditors make requests through their own tools—which often lack user-friendly interfaces—organizations on the receiving end just say, 'Forget it, give me an Excel sheet.' It's easier to manage that way, even if it means losing all of the benefits of their GRC platform."*

Chris Beiro
Sr. Director of InfoSec Solutions at Thoropass

Limited visibility into audit progress

Without integrated workflows, organizations lack real-time visibility into audit status. Teams operate in silos, unable to see which controls have been tested, what evidence has been accepted, or where bottlenecks exist.

Critical issues only surface during weekly status calls—by which time they've already caused delays. This lack of transparency creates a cascade of problems: duplicate work, missed deadlines, and last-minute scrambles that could have been avoided with better visibility.

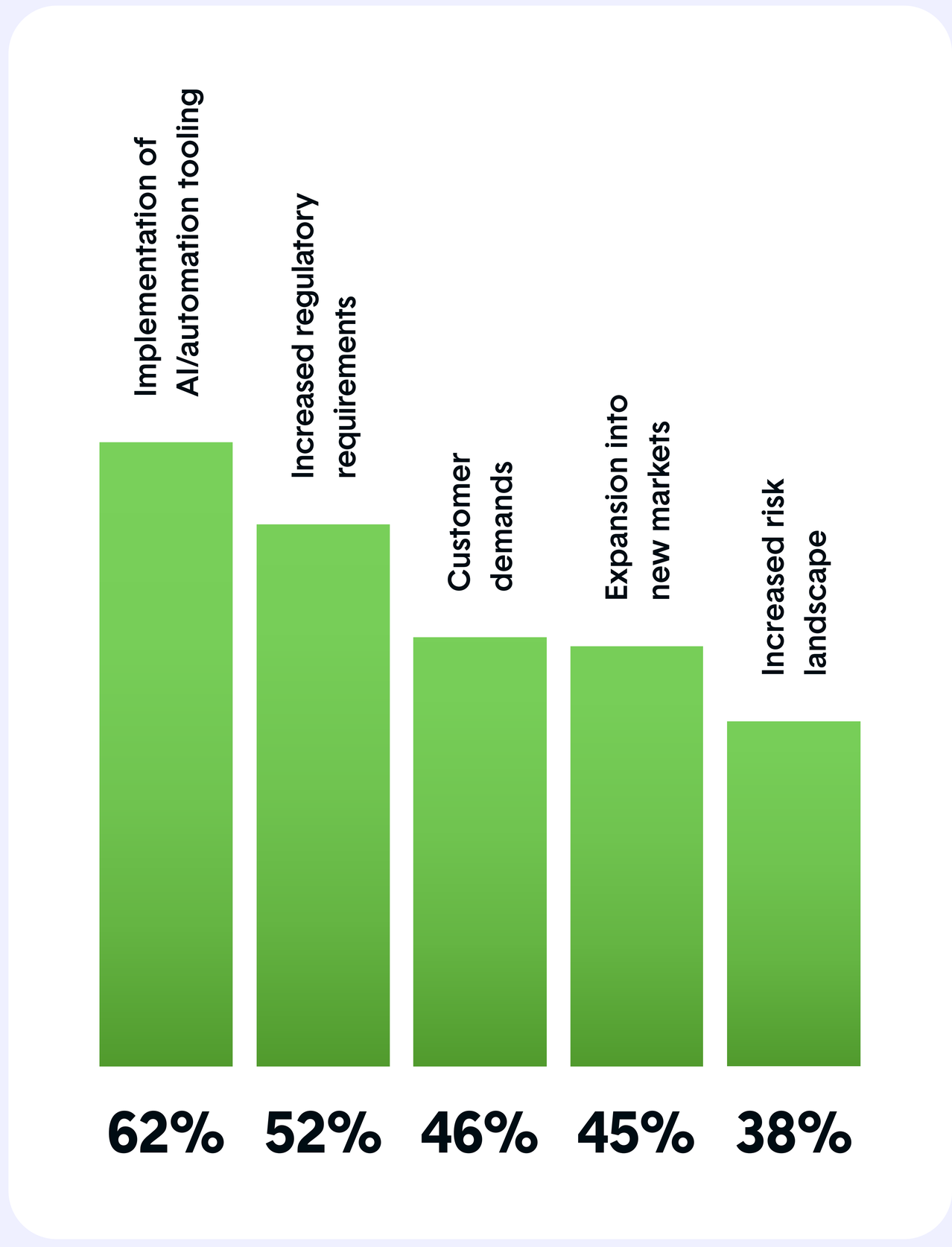
The impact? Increasing budgets, increasing pressure

The financial dynamics of compliance and audit reveal a troubling paradigm: 84% of teams anticipate spending more on compliance and audit in the next 12 months, with 14% expecting increases of over 20%.

While businesses may be increasing budgets in the hopes of solving persistent challenges, additional tools alone rarely do the trick. In fact, they may just exacerbate the inefficiencies caused by tool sprawl. InfoSec leaders, meanwhile, may face increased pressure from executives to hit unrealistic goals.

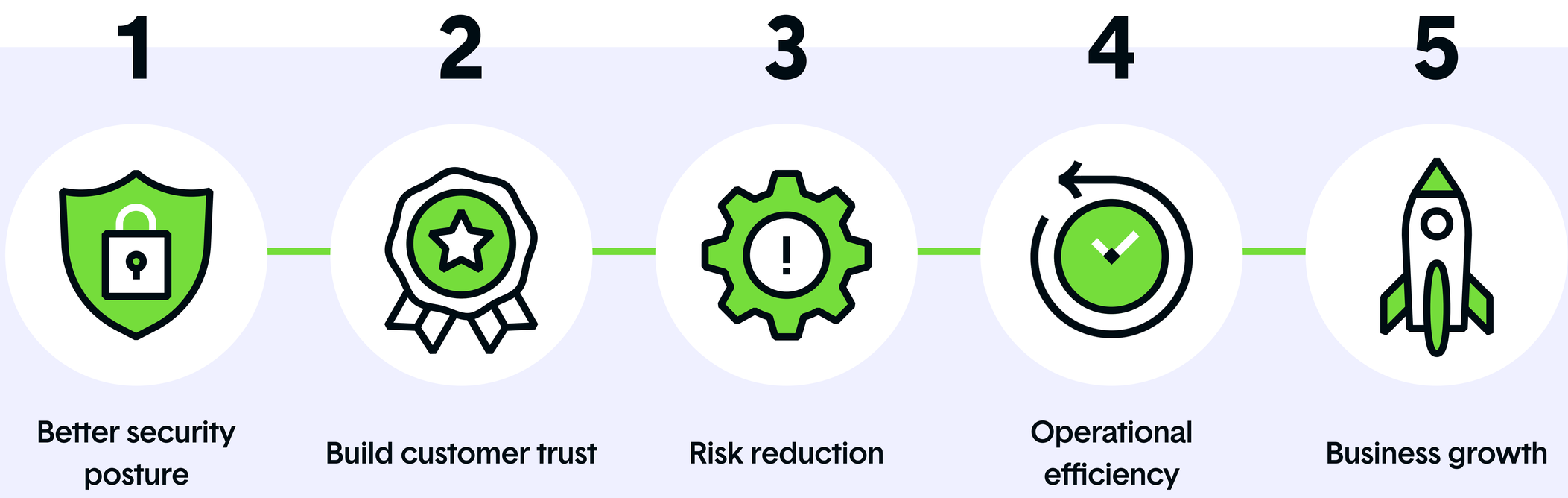
But as long as the audit gap persists, benefits often fail to materialize.

Factors driving these increases include:



What InfoSec teams are looking to drive through compliance and audit programs

While the challenges are clear, so are the goals. Our survey reveals that InfoSec teams aren't just seeking to check compliance boxes—they're looking to drive strategic business outcomes through their audit programs.



The five primary goals

1. Better security posture (72%)

Unsurprisingly, improving security remains InfoSec leaders' top priority. But they increasingly recognize that the benefits of a robust security posture extend beyond the IT department. Strong security establishes credibility, reduces operational risk, and fulfills the requirements needed to enter new markets.

As frameworks evolve to address emerging threats—from AI risks covered by ISO 42001 to privacy concerns in ISO 27701—maintaining a strong security posture becomes increasingly complex and critical.

2. Build customer trust (66%)

Trust has become the currency of modern business, especially in B2B relationships. Organizations can no longer rely on reputation alone—they must provide tangible proof of their security practices through recognized certifications.

Being proactive about compliance ensures organizations aren't just passing audits, but continually and demonstrably improving. Just as important, however, is timeliness.

3. Risk reduction (59%)

The proliferation of frameworks isn't just about compliance—it's about comprehensive risk management across an evolving threat landscape. Beyond avoiding penalties, today's organizations seek to minimize operational, reputational, and strategic risks.

And in an era of massive data breaches, supply chain attacks, and increasing regulatory scrutiny, businesses must continually stay one step ahead.

4. Operational efficiency (58%)

The desire for efficiency isn't just about cutting costs—it's about giving time back to teams, enabling organizations to redirect resources toward innovation and growth instead of compliance administration.

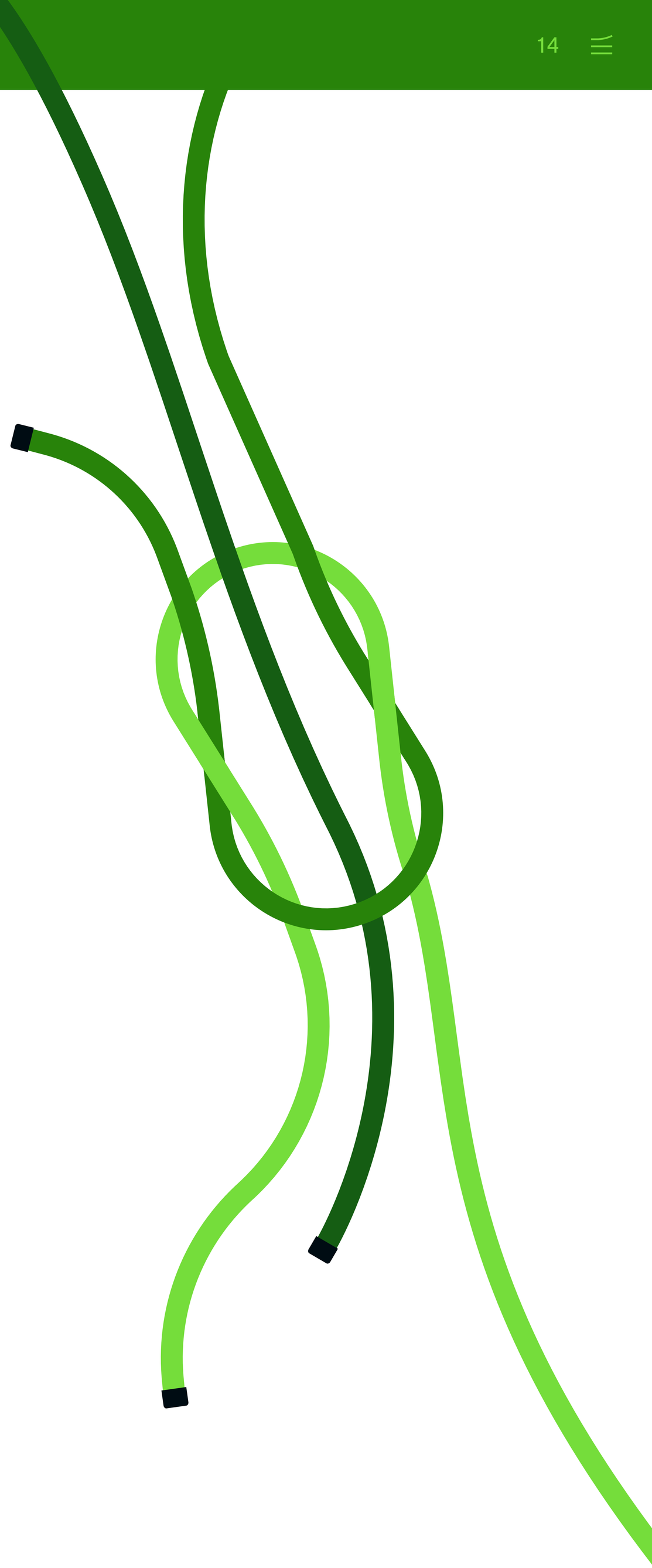
5. Business growth (58%)

Perhaps most tellingly, over half of respondents explicitly connect compliance to concrete business growth opportunities. Whether it's entering the Australian market (requiring IRAP certification), winning federal contracts (requiring FedRAMP or CMMC), or expanding into Europe (requiring ISO certifications and GDPR compliance), compliance has become a growth enabler instead of a cost center.

The interconnected nature of compliance goals: From security to growth

As the goals above demonstrate, compliance objectives don't exist in isolation—they form an interconnected system where success in one area drives progress in others. A better security posture builds customer trust, which opens new markets, driving business growth. Operational efficiency frees resources to focus on risk reduction and security improvements.

The challenge isn't choosing which goal to prioritize—it's recognizing that in today's market, security, trust, and growth are inseparably intertwined.



Closing the audit gap with audit-ready compliance

The path to closing the audit gap begins with technical integration, but not in the way many organizations expect. It's not about adding another tool to the stack—it's about creating genuine interoperability between compliance activities and audit execution.

Systems integration as foundational

Successful integration, Beiro believes, starts with automated evidence collection that auditors actually trust. When systems connect directly to cloud-based environments and automatically pull configurations, it reduces the manual burden on internal teams.

> *The more automated evidence collection integrates directly with auditors' cloud-based environments, the less the customer has to internally chase the audit evidence and artifacts."*

Chris Beiro
Sr. Director of InfoSec Solutions at Thoropass

The key is ensuring that automated evidence collection follows a "least privileged perspective"—pulling only what's necessary, in formats auditors expect, with clear audit trails that demonstrate the integrity of the data.

This allows organizations to ensure that automated evidence collection is pre-approved by auditors, allowing them to feel confident, knowing that they won't have to later double-back on their efforts.

Unifying compliance and audit as a continuous workflow

The traditional model treats compliance and audit as sequential phases—you prepare all year, then scramble during audit season. Audit-ready compliance flips this model, creating a continuous, integrated workflow where compliance and audit activities happen in parallel.

This approach—which reduces surprises, spreads work more evenly throughout the year, and ensures teams aren't caught off-guard by auditor requirements—consists of several components:

Early auditor involvement

Rather than meeting your auditor for the first time when the audit begins, bring auditors into the process from day one. Have them participate in kickoffs, join periodic check-ins, and provide guidance as teams build policy sets and prepare evidence.

Shared platform, shared context

When auditors work within the same platform as compliance teams—with appropriate access controls—they see the same control data, evidence, and documentation. This eliminates confusion about evidence locations, reduces requests for information already provided, and ensures everyone works from the same source of truth.

Continuous feedback loops

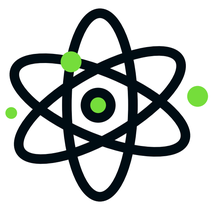
Instead of discovering issues months into an audit, organizations receive near real-time feedback. Regular touchpoints allow teams to course-correct early, before small issues cascade into audit-delaying problems.

Building efficiency with automation and AI

While many vendors tout AI and automation, the real differentiation lies in how organizations apply these technologies. We recommend a two-pronged approach:

1. Intelligent Workflow Optimization:

Beyond basic evidence collection, look for AI that can identify control gaps before auditors do, predict which evidence might be insufficient, and suggest remediation paths based on historical audit findings. The goal is to empower compliance teams with predictive insights, not just reactive automation.



2. Auditor-Side Efficiency:

Look for audit partners who have invested in their own automation, such as automated report generation, streamlined testing procedures, and efficient workflow management. When auditors can work faster without sacrificing quality, the organizations soliciting their services can shorten their audit timelines and reduce costs.

This dual approach addresses both sides of the audit gap simultaneously, ensuring that efficiency gains aren't lost in translation between compliance and audit teams.

Bringing it all together

Of course, technology is just one piece of the puzzle. To achieve meaningful results and lasting change, you'll need to combine multiple elements:

- **Technical excellence:** Integrated platforms, automated workflows, and AI-driven intelligence that actually works in practice—not just in demos. Tooling that actually allows audit teams to migrate away from spreadsheets and manual data entry.
- **Process innovation:** Moving from annual fire drills to continuous readiness, and from siloed tools to unified environments.
- **Flexible implementation:** Recognizing that transformation doesn't happen overnight. For larger organizations, change management may be a journey that lasts years. Start by defining what success looks like, then devising a roadmap to help you get there over time.
- **Human expertise:** Auditors with relevant industry experience who understand both the technical requirements and business context, working hand-in-hand with internal InfoSec teams.
- **Proactive scope management:** Ensuring your audit partner actually reads previous audit reports, reviews network diagrams, and understands your environment before the audit begins. This "right-sizing" of scope means fewer surprises and more accurate timelines.
- **Deadline-driven planning:** Working backward from critical deadlines—whether it's a customer contract requirement or a market entry date—ensures you hit your targets without last-minute scrambles.
- **Post-audit evolution:** The relationship doesn't end with certification. Post-audit reviews translate "auditor speak" into actionable improvements, preparing organizations not just for the next audit, but for evolving regulations and emerging risks.

> *When compliance and audit live in one place, it feels like a collaboration instead of a courtroom."*

Elise Spitzer
Sr. Customer Success Manager at Thoropass

Go beyond compliance

Rather than disruptive events that happen to your organization, audits can become an opportunity to drive continuous improvement. The ultimate measure of success isn't just passing audits, of course—it's what those audits enable.

Uniting compliance and audit in a single, integrated workflow transforms compliance from a business constraint into a competitive advantage with benefits that ripple throughout your organization:

- **Engineering teams** spend less time on evidence collection and more time on innovation
- **Security teams** can focus on reducing risks rather than gathering documentation
- **Leadership** gains visibility into compliance without drowning in details
- **Sales teams** can confidently pursue enterprise deals, knowing they have the certifications that prospects are looking for

With security and compliance increasingly determining market access and customer trust, your next big opportunity might depend just as much on what you build as on how secure you can prove it to be.

Thoropass™