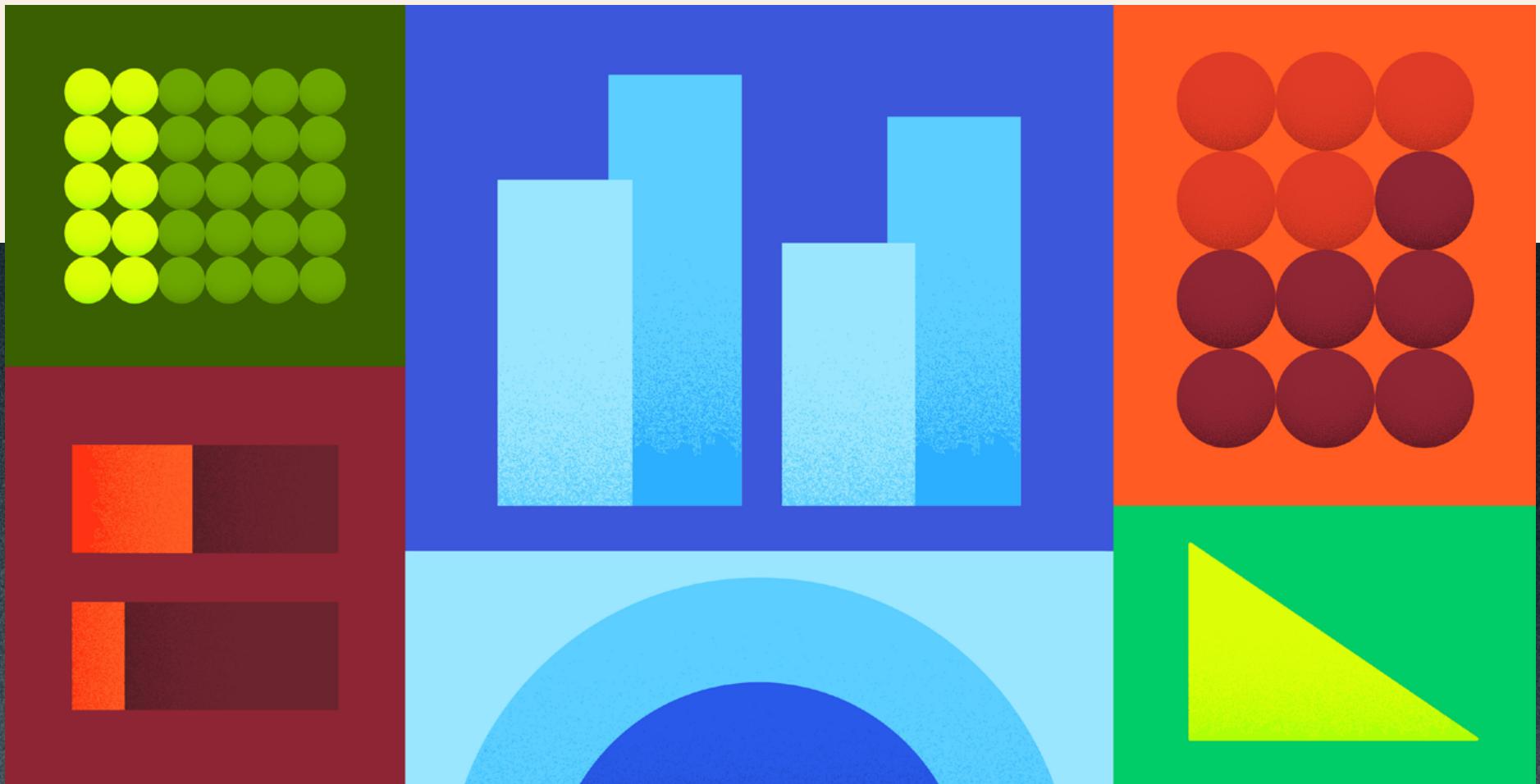


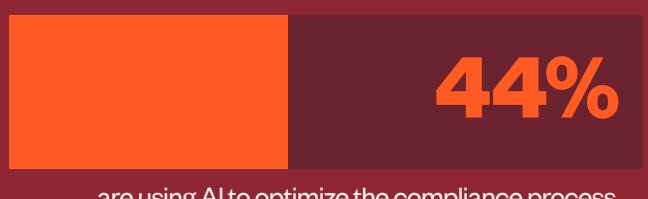
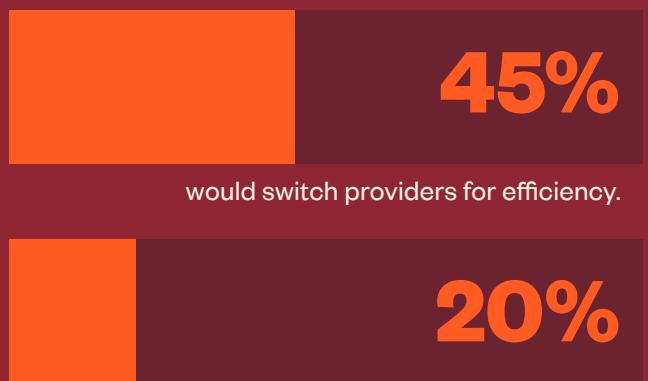
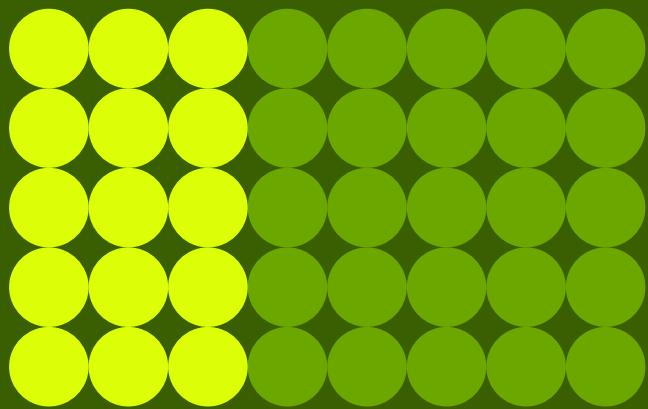
2020 COMPLIANCE BENCHMARK Report



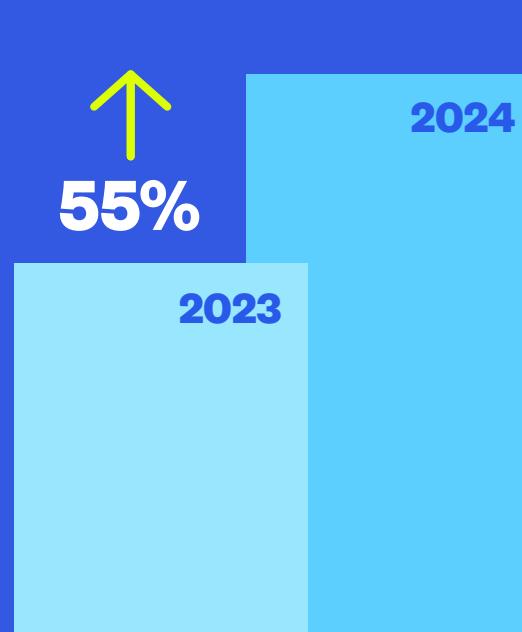
Contents

| | |
|--------------------------------|----|
| Key findings | 3 |
| Executive summary | 4 |
| Introduction | 5 |
| Major themes | 6 |
| Benchmark data | 16 |
| Conclusion & methodology | 19 |

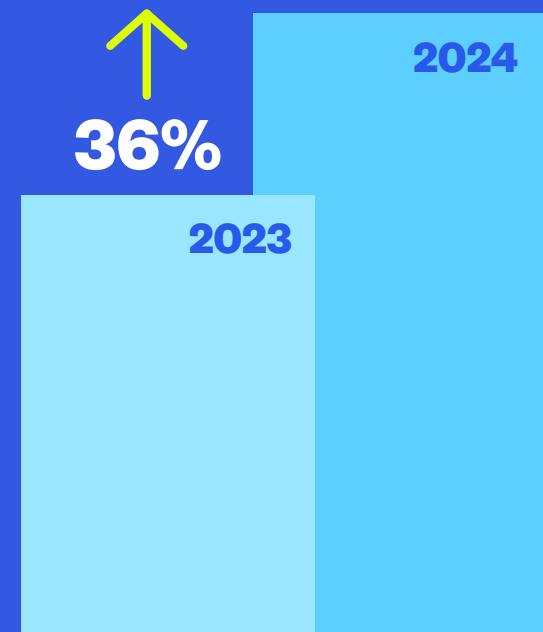




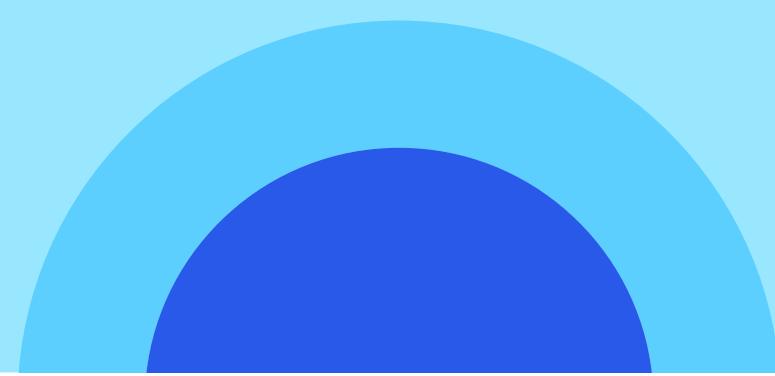
The why behind compliance



Validating IT controls



Establishing trust with
customers and stakeholders



2/3
of teams spend at
least three months
and more than \$100K
annually on audits.



17% increase
from 2023 

34%

lost business due to a
missing certification.

Top 3 reasons
companies choose
an auditor:

- #1** experienced team
- #2** report quality
- #3** tech-enabled audit

32%

22%

19%

Executive summary

This year's survey data revealed four major themes:

1

Quality: Not all reports are created equal.

Companies have noticed a difference in report quality among auditors, and respondents ranked quality highly when it comes to choosing an auditor.

2

Efficiency: Companies must do more with less.

Teams reported spending many months each year preparing for and conducting compliance audits, but few have dedicated compliance staff, and budgets are shrinking. As a result, audit efficiency is vital.

3

Culture of security: It's more than checking the box.

The motivations behind compliance programs are shifting. More companies are focusing on building trust with customers rather than simply doing the basics required for compliance.

4

Partnership: Experience + tech are the winning combination.

Best-in-class companies prioritize experienced, tech-enabled auditors that can serve as compliance partners rather than one-off vendors offering a rushed or cheap audit job.



Introduction

With evolving regulations, increasing cyber threats, and growing consumer awareness of security and privacy concerns, organizations today face a myriad of compliance challenges. A robust compliance program is not just a regulatory requirement but also a strategic imperative for mitigating risks, ensuring business continuity, and maintaining customer trust.

In 2024, audit quality and efficiency are more crucial than ever. In addition to heightened regulatory scrutiny and the increasing complexity of compliance requirements, many companies have reduced headcount, forcing them to make do with fewer internal resources than ever before.

Companies are responding to these resource limitations in different ways, with varied effects on their security postures. Some seek out new automation tools to help streamline audits and other compliance processes, making their compliance strategy more efficient without diminishing its effectiveness. Others have resorted to quick audits from discount providers or, even worse, deprioritized security altogether, leaving their organizations at greater risk of cyberattacks.

A-LIGN's fourth edition of the Compliance Benchmark Report delves into these key themes, which emerged from our annual survey of nearly 700 business leaders and compliance professionals. Our data shows that the most successful companies continue to prioritize security while finding ways to manage the audit process efficiently. This report will shed light on the current state of compliance and offer insights into best practices for achieving compliance excellence.



A culture of security requires broad collaboration and honestly transparency among all stakeholders throughout your business.”



Brandon Thompson
CISO, A-LIGN



Quality:

Not all reports are created equal.

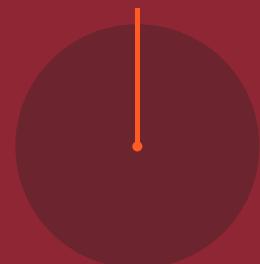
Compliance reports serve as a vital means of demonstrating the state of an organization's compliance strategy to various stakeholders, including customers, regulators, shareholders, and leaders. Accordingly, the quality of compliance reports holds immense significance, as reflected by the overwhelming majority of respondents in our survey (69%) who deemed it "extremely important."

More to the point, **22% of all companies surveyed said their top reason for choosing an auditor was report quality**, with even higher percentages for the IT services industry (29%). An exhaustive report is crucial for these companies, as facing a data breach can have dire consequences. An IT services company that suffers a cyberattack can look incompetent, permanently damaging brand reputation, not to mention the costs required to bring security up to par.

What factors make a compliance report **top quality**?

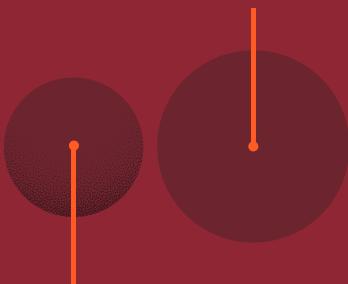
31%

Trusted auditors with a positive market perception



21%

Report provides thought leadership / best practices



9%

Number of controls tested

19%

Professionally designed report

19%

Length of report

19%

19%

19%



But what does “quality” really mean? Our data shows that auditor expertise plays a critical role. The top two factors organizations use to determine whether a report is high quality are the auditor’s reputation and an explanation of best practices, industry benchmarks, or other helpful content in the final report. Companies want their audit reports to come from an experienced compliance partner who can offer practical guidance about how to improve their security posture.

Not all auditors live up to this ideal. For organizations that have used multiple auditors in the past, **79% said they noticed a difference in quality among auditors**, and **11% said they received audit reports that were too short**. Not all audit reports — or auditors — are created equal.

A high-quality compliance report ensures that audit information is presented clearly, facilitating effective decision-making regarding compliance management. But bad decisions aren’t the only consequence of a low-quality report — **38% of organizations have had a report rejected** by a vendor or prospect, leading to additional time and money spent to produce an acceptable report or, worse, a lost business deal. Choosing a compliance partner with a track record of quality reports can ultimately save companies time, money, and frustration.

69%

said the **quality** of compliance reports is **extremely important**.

79%

noticed a **difference in quality** between auditors.



One of the things that I think a lot about is what the audit assessment means in terms of representing the security posture of the company. If we have a good SOC 2 report, it means a lot of the harder questions don’t get asked.”



Mark Petry

Cyber Compliance & Risk Manager, GoodLeap



Risks of a low-quality audit

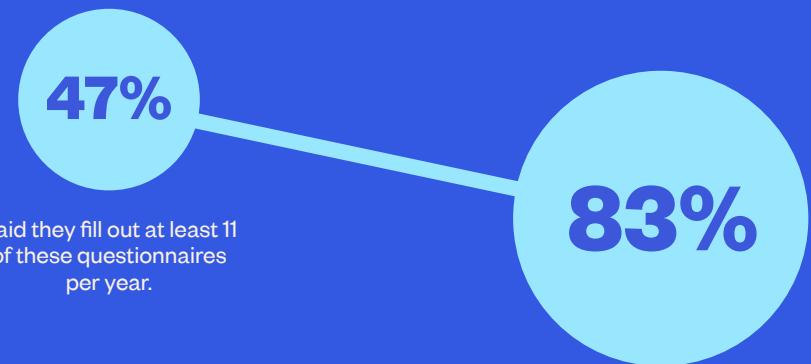
Choosing an audit provider can be tricky. Our data shows that companies value high-quality reports, but **14% say budget constraints are the greatest challenge to the audit process**. When weighing **cost versus quality**, some organizations may be tempted to choose a budget auditor that delivers the bare minimum.

Some of the risks associated with a flimsy report are major: security vulnerabilities, inadequate assurance, negative brand image, and legal liabilities. But even the purely logistical consequences can have a significant impact on a business's day-to-day functioning.

For example, **the vast majority (83%) of respondents have had to fill out a security questionnaire for a vendor at some point, and nearly half (47%) said they fill out at least 11 of these questionnaires per year**. A thorough audit report can make filling out these questionnaires significantly less difficult, and providing one to a vendor can sometimes even prevent them from sending you a security questionnaire in the first place. Considering most companies reported spending up to two hours on each questionnaire, teams can potentially take back days of their time to focus on higher-value work. Plus, having a comprehensive audit report on hand can show potential clients or business partners that the organization understands the importance of security and has already taken steps to improve it.

Cost vs. quality

Flimsy reports can make filling out questionnaires a daunting task.



have had to fill out a security questionnaire for a vendor at some point.

What department owns
compliance?



Efficiency:

Companies have to do more with less.

66%
of teams spend at least **three months of the year** on audits.

45%
would switch audit providers for
a more efficient process.

In the pursuit of high-quality compliance audits, organizations are met with significant resource deficiencies. In our survey, companies reported that their greatest challenge in the audit process is limited staff resources dedicated to compliance. **Only 20% of companies have a dedicated compliance department** — the majority put their IT department in charge of compliance.

For many organizations, this hunger for efficiency may stem from a lack of overall compliance strategy. **Nearly all (96%) of the companies surveyed believe consolidating multiple audits could save them time, money, or both.** Despite this fact, **only 16% reported that they consolidate their yearly audits into a single event.** The overwhelming majority (83%) conduct multiple audits per year but plan for each one individually. This piecemeal compliance process can lead to unnecessary work in the form of duplicated

evidence gathering, especially if the organization chooses different vendors for each audit (and our data confirms that **nearly 80% of companies use more than one auditor**).

One potential solution to the efficiency problem is artificial intelligence. With the right automation, organizations can improve their overall security strategy and better adhere to compliance standards such as SOC 2, ISO 27001, and more. Luckily, **44% of companies are already using AI** to optimize the compliance process — and few have not considered AI as a potential compliance aid. Still, it is important to remember that AI is a new resource for many industries, and the **role of AI in compliance** continues to evolve.



The benefits of audit consolidation

It's clear from the survey results that most businesses already recognize some of the benefits of audit consolidation — namely, less time and money spent on audits. Let's dive deeper into the advantages of consolidating multiple audits with a single provider:

- Consistency across assessments:** Consolidating audits ensures a consistent, standardized approach to completing multiple assessments. This reduces the risk of errors or contradictions between reports and provides a more comprehensive view of the organization's compliance posture.
- Reduction in duplicate evidence collection:** Organizations can more efficiently collect and organize the evidence required for each assessment all at one time instead of tracking down the same or similar evidence for different assessments throughout the year.
- Auditor time and cost savings:** When working on multiple audits simultaneously, the audit partner can more easily identify and review evidence that is relevant to multiple assessments, reducing the amount of time required to complete each audit (and the cost associated with their work).
- Improved communication:** Consolidating auditors can help improve communication and collaboration between different areas of your organization. A single point of contact can keep everyone on the same page and ensure all compliance activities are aligned with your organization's goals.



In the tech industry, everyone is going through cost-saving measures right now. The most expensive costs are full-time employees (FTEs), which means the cuts start there — and we're having to get the same amount of work done with fewer FTEs."



Meghan Hester

Senior Director of Compliance, Aptiv

What are the main reasons you might **switch audit service providers?**

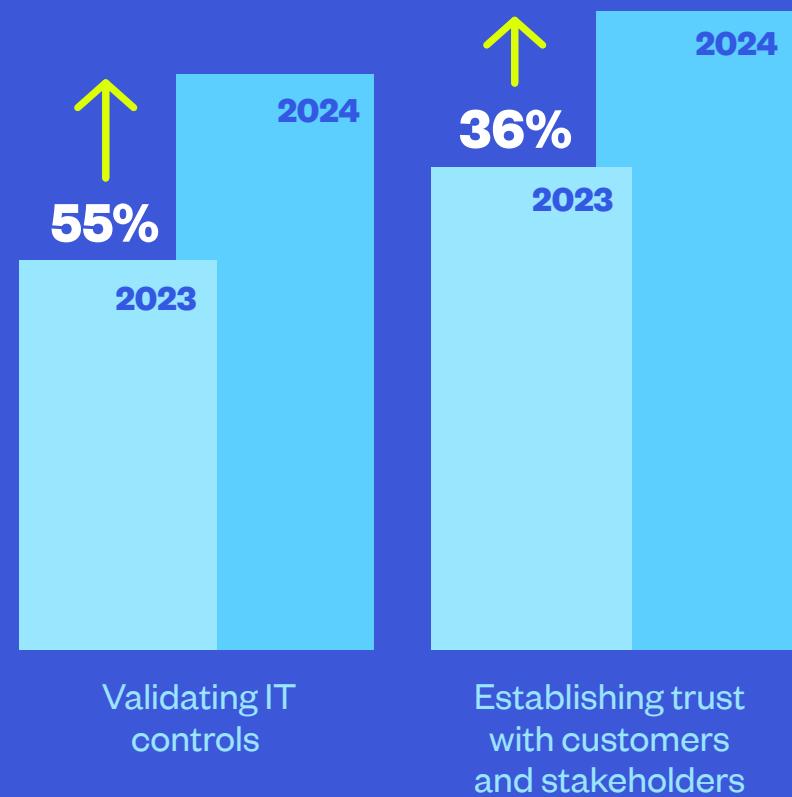


Culture of security: It's more than checking the box.

This year's survey revealed new shifts in the motivations for compliance initiatives. Past surveys indicated that the driving force behind compliance programs was increasing revenue or winning new clients along with pressure from company leadership. These reasons together comprised nearly half of all responses in 2023. This year, they were the two least popular answers.

Compliance is still important for business deals — **34% of companies reported lost business opportunities due to the absence of a crucial certification**, an increase from 29% in the previous year. This statistic underscores the continuing — or possibly growing — value of compliance in today's business landscape. Despite this fact, the data shows a noticeable shift away from revenue as a compliance motivator and toward a culture of security and consumer trust.

The why behind compliance



Regulatory requirements remain a key factor, with nearly a quarter of companies citing them as the primary motivation. However, **establishing trust with customers and stakeholders rose as a motivator by 36%** compared to the previous year. Additionally, **validating the effectiveness of security controls rose in importance by 55%** year over year.

These findings highlight a significant takeaway: businesses are moving away from a check-the-box compliance strategy that prioritizes doing the bare minimum to win over clients and protect the bottom line. Instead, a new culture is emerging, one that values security and trust as valid business concerns in their own right. Companies now recognize the importance of proactive and comprehensive compliance measures to build long-term customer relationships and mitigate potential risks.



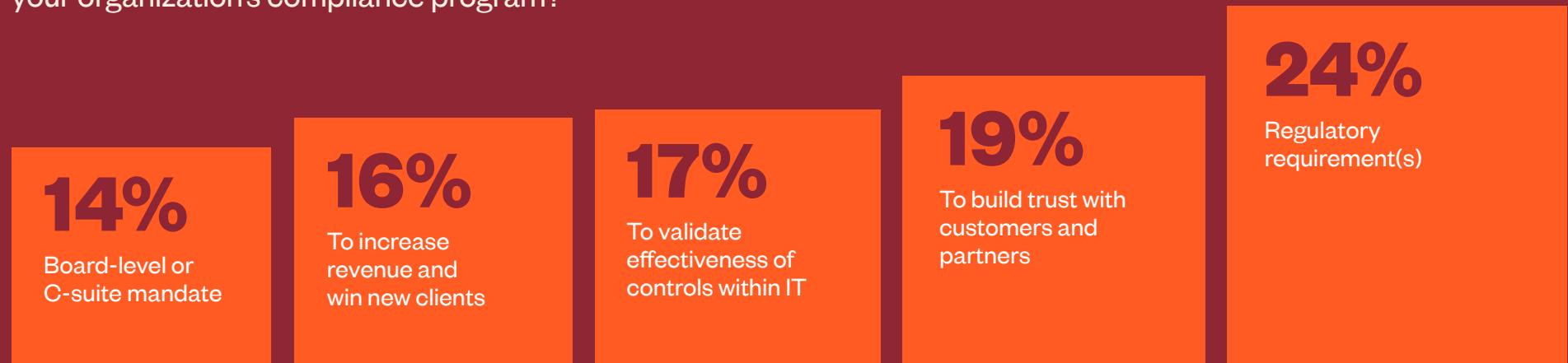
In security, you have the weight of the world on your shoulders. So, I'm always thinking: 'How do I continue to elevate our practices to give our customers the most confidence?'



Noe Ramos

Vice President of Operations, Agiloft

What is the **driving force behind** your organization's compliance program?



Partnership:

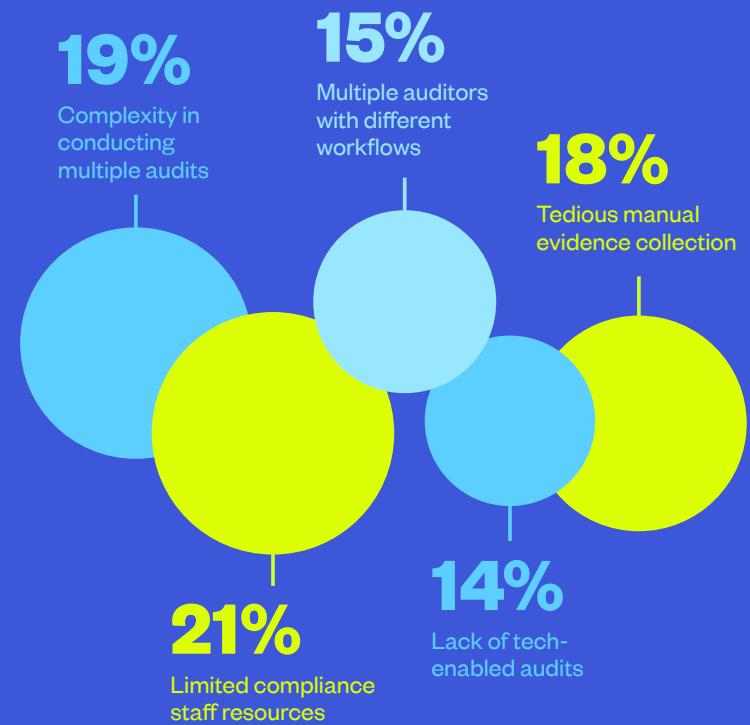
Experience + tech are the winning combination.

The audit process can be a daunting task, especially for organizations with limited resources dedicated to compliance. In addition to limited staff resources (21%), companies reported their top audit challenges to be complexity in conducting multiple audits (19%) and tedious and manual evidence collection (18%).

All of these factors combined can put immense strain on those in the organization responsible for compliance management, who may have little time to devote to a proactive compliance strategy. Instead, organizations end up in a vicious cycle of rushed, reactive audits when a critical issue arises. In fact, respondents in our survey said reactive audits are the greatest challenge to their compliance strategies.

It's no wonder, then, that **32% of companies prioritize auditor experience** as the top factor when choosing a compliance partner. Working with an experienced auditor directly influences the quality and effectiveness of the audit process. Organizations can gain access to a wealth of knowledge and expertise they may not otherwise have, ultimately reducing the burden on the company's limited resources and ensuring a successful audit outcome.

Greatest challenge to your audit process



Greatest challenge to your compliance strategy:

Organization lacks internal leadership.



Organization lacks coherent compliance strategy.



Auditors react to customer demands rather than internal management.



External auditors don't understand our business.



Organization can't keep up with new compliance requirements.



The organization's compliance lags behind in adapting to new technology.



Interestingly, the larger the company, the more likely it is to prioritize auditor experience. The percentage of companies selecting this option increased with each revenue category we tracked in 2024. **Nearly half (46%) of organizations with more than \$1 billion in annual revenue said an experienced audit team was most important.** This data indicates that best-in-class organizations are looking for more than just a one-off auditor. They want a partner who can provide them with the support and guidance they need to navigate the complex and ever-changing regulatory landscape. For these organizations, compliance is not just a checkbox exercise; it is a critical aspect of their overall business strategy.

The survey results also signal that technology, while a powerful tool, is not a substitute for experience. **19% said a tech-enabled audit was the most important factor** for them, compared to **32% who chose an experienced audit team**. Technology can enhance the efficiency and accuracy of the audit process, especially when it comes to evidence collection, but it takes skilled professionals to analyze data, make informed decisions, and provide strategic guidance.



A sharp auditor will not only check the box but will help implement compliance exercises that add value to your organization and ensure that you're safeguarding your precious asset — your brand reputation.”



Mark Petry

Cyber Compliance & Risk Manager, GoodLeap

What to look for in an audit partner

When selecting an audit partner, it's essential to consider several key factors to ensure a successful and efficient audit process. The top three factors organizations prioritize are:

1. Experienced team:

An experienced audit team is crucial for delivering high-quality audits. Look for a partner with a track record of successful audits, a deep understanding of industry-specific regulations, and a team of qualified and certified professionals.

2. High-quality audit report:

The quality of the audit report is paramount as it serves as a critical tool for stakeholders. Consider an audit partner known for producing comprehensive, well-written, and easily understandable reports that meet industry standards and undergo regular peer reviews.

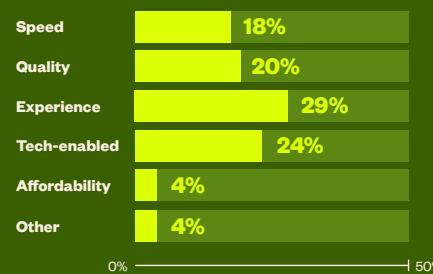
3. Audit management technology:

In today's digital landscape, a tech-enabled audit process can significantly enhance efficiency and accuracy. Choose a provider that leverages technology to streamline evidence collection, automate tasks, and provide real-time insights.

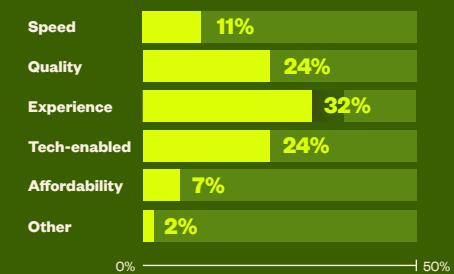
Additionally, organizations should consider a partner that can scale its services to meet changing needs. An audit partner with a wide breadth of services can help you with new audits and certifications as your business grows.

What is most important to you when it comes to **choosing an auditor?** (by annual revenue)

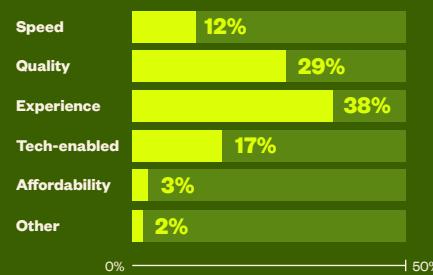
Under \$5M



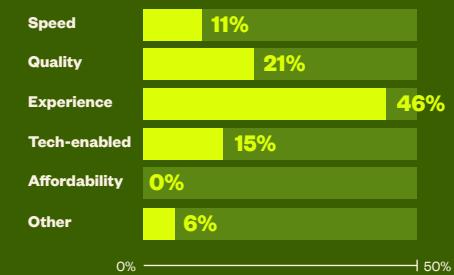
\$5M - 50M



\$50M - \$1B



Over \$1B



Benchmark data

Benchmark data is crucial for a company's compliance strategy as it provides valuable insights into industry standards and best practices. By comparing their compliance efforts with those of similar organizations, companies can allocate resources effectively, prioritize compliance activities, and stay competitive.

As in past reports, A-LIGN has compiled a set of benchmarks related to compliance audits that companies can use to evaluate their current strategy. Any meaningful differences among industries or organization size have been noted for each statistic.

Number of audits each year



Number of audit providers

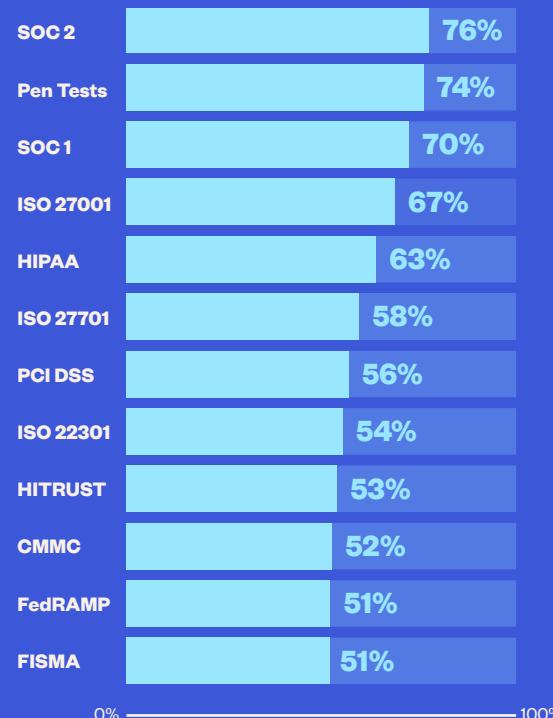


- **IT services companies are 26% more likely to conduct four or more audits per year** compared to the average.
- **Professional services companies are 51% more likely to conduct three or fewer audits per year** compared to the average.

- More than a third of businesses use **four or more audit providers**.
- Large companies with more than \$1 billion in annual revenue are most likely to **use six or more audit providers**.

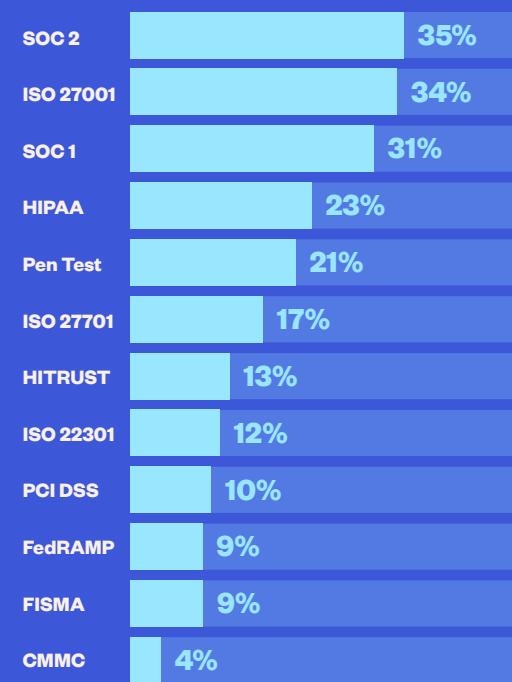
Most common audits pursued

Note: Respondents could choose multiple.

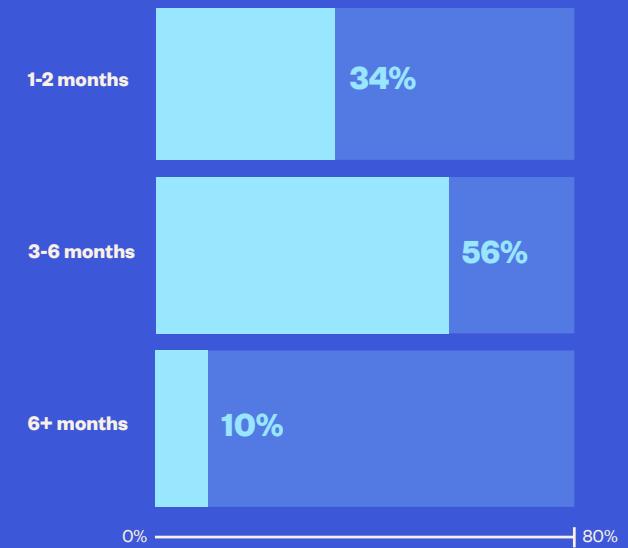


Most impactful audits

Note: Respondents could choose three.



Time spent preparing for audits



- Two-thirds of businesses spend three months or more preparing for audits each year.

By industry:

- Technology: SOC 2
- IT services: ISO 27001
- Healthcare: HIPAA
- Finance: SOC 1
- Manufacturing: ISO 27001
- Government: Penetration Testing

Money spent on audits annually

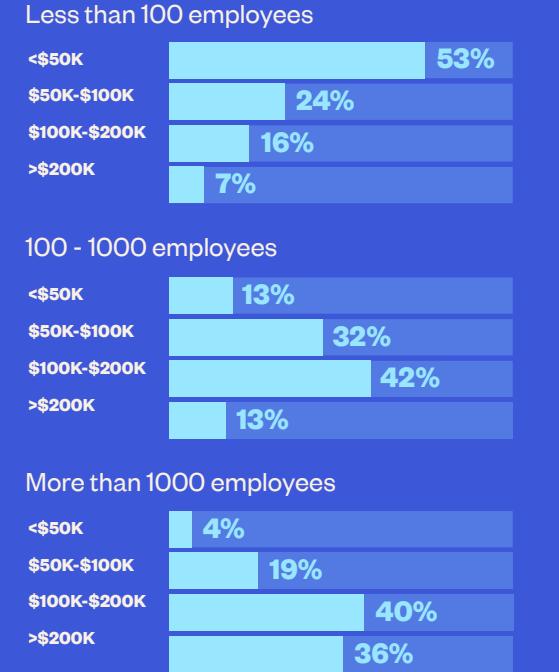
All responses



By annual revenue



By company size



Conclusion

This year's report highlights the growing recognition of compliance as a strategic business imperative. Companies are prioritizing proactive and comprehensive compliance measures to build long-term customer relationships, mitigate risks, and ensure business resilience. The partnership between an experienced audit team and technology is crucial for successful compliance. Selecting the right audit partner is essential for achieving compliance objectives efficiently and effectively.

About A-LIGN

A-LIGN is the leading provider of high-quality, efficient cybersecurity compliance programs. Combining experienced auditors and audit management technology, A-LIGN provides the widest breadth and depth of services including SOC 2, ISO 27001, HITRUST, FedRAMP, and PCI. A-LIGN is the number one issuer of SOC 2 and a leading HITRUST and FedRAMP assessor.

To learn more, visit [A-LIGN.COM](https://www.align.com)

Survey methodology

The survey was conducted by A-LIGN between November 2023 and February 2024. Industries represented include:

- Technology (hardware/software)
- IT services
- Professional services
- Healthcare
- Finance
- Manufacturing
- Government

A total of 686 individuals completed the survey in whole or in part. Results in this report are rounded up or down to the nearest whole percentage.

