Thoropass™

Cybersecurity audit & assurance buyer's guide

Evaluation criteria and tool comparison

Table of contents

Thoropass™

Introduction

Choosing the right IT audit provider is one of the most strategic decisions your company will make. The right partnership doesn't just check compliance boxes—it unlocks revenue by enabling you to compete for enterprise clients, builds customer trust through third-party validation, and improves your security posture through expert guidance.

But many companies don't have an established way to approach this decision, so they rely primarily on brand recognition or price rather than the outcomes that matter most. Unfortunately, many find that legacy auditors coast on their brand reputation without investing in modern technology, delivering exceptional experiences, or understanding your specific business needs—leading to inefficient processes that drain your team's time.

On the other end, price-driven providers may deliver audit reports that lack meaningful findings to help you improve, or worse, produce work that isn't trusted by your customers when they conduct their own due diligence. The best audit experiences combine three elements: proven expertise from experienced auditors, modern technology that automates manual work, and transparent processes that keep you informed throughout the cycle.

This guide will help you avoid the common pitfalls that lead to audit delays, cost overruns, and poor experiences. You'll learn what success should look like, which red flags should eliminate providers from consideration, and the critical questions that separate great audit partners from the rest. Whether you're pursuing your first SOC 2 certification or managing multiple compliance frameworks, the right provider can reduce your audit timeline by 60%+ while delivering better outcomes for your business.

What success looks like: Key outcomes

Thoropass™

Building customer trust and winning business

Successful audits are essential for modern business operations, not just growth opportunities. SOC 2, ISO 27001, and other certifications have become mandatory requirements for enterprise deals—without them, you can't participate in RFP processes for Fortune 500 companies or meet the compliance demands of regulated industries.

This third-party validation of your security practices gives customers confidence to share sensitive data and sign contracts, while also satisfying regulatory obligations that come with significant penalties for non-compliance. Beyond meeting baseline requirements, compliance becomes a competitive differentiator that can accelerate sales cycles and command premium pricing, turning what might seem like a cost center into a strategic revenue driver.

Improving your security posture

The best audit experiences go far beyond checking boxes—they strengthen your actual security posture. Leading auditors provide specific remediation guidance, not just findings, offering gap assessments and ongoing advisory to help you fix issues before they become audit failures. Your audit should provide clear benchmarking against established frameworks, with specific metrics showing where you excel and where improvement is needed.

Real-time monitoring capabilities help maintain compliance between audits, while ongoing compliance advocacy through quarterly check-ins ensures you stay on track. This continuous relationship proves more valuable than one-time audit services, creating a foundation for long-term security improvements.

Operational efficiency and ROI

Modern audit platforms deliver substantial operational benefits through automation. The best providers eliminate 60-80% of manual evidence collection through integrations with your existing tools, translating to hundreds of saved hours annually for your team. This efficiency extends beyond the initial audit—automated evidence collection and continuous monitoring mean subsequent audit cycles require significantly less preparation time, with many companies reducing their second audit timeline by 50% or more.

The financial benefits are equally compelling. Certified companies typically see 10-30% reductions in cyber insurance premiums, with some insurers requiring certifications for coverage. In many cases, the audit cost pays for itself through insurance savings alone, making compliance a clear return on investment rather than just a necessary expense.

How to develop a short list: **Spotting red flags**

Thoropass™

Relationship and trust issues

Do you prefer working with providers you already know?
While existing relationships matter, don't let familiarity override better value. Many companies successfully work with new providers who offer superior technology and expertise.

Are you prioritizing brand name recognition over actual expertise and results?
Legacy audit firms have brand recognition but may assign junior staff to your account and rotate your auditor every year. Look for providers with experienced auditors who understand your industry, regardless of firm size.

Do you have strong customer references to validate their performance?
Always check 3-5 customer references, focusing on companies similar to your size and industry. Ask specifically about timeline adherence, communication quality, and post-audit support.

Are you turned off by aggressive upselling of unnecessary services?
Avoid providers who push extensive professional services or consulting you don't need. The best partners focus on your specific requirements without scope creep.

Technical and platform inefficiencies

Will their platform integrate easily with your existing systems?
Essential integrations include your cloud providers (AWS, Azure, GCP), HR systems, and development tools. Providers should offer pre-built integrations that align with your current stack and needs, to automate evidence collection.

Do you have security concerns about their audit platform?
Your audit provider should meet the same security standards they're auditing you for. Ask about their own certifications, data encryption, and access controls.

Is their platform too complex or difficult for your team to use?
The best platforms feel intuitive and require minimal training. If the demo feels overwhelming, daily usage will be worse. Look for clean interfaces and guided workflows.

Thoropass™

Size, cost and fit mismatches

Are Big 4 firms overkill for your mid-market company?

Big 4 firms often have minimum engagement sizes and processes designed for Fortune 500 companies. Mid-market companies (100-1,000 employees) typically get better service from specialized providers.

Does their pricing model fit your budget reality?

Transparent, fixed-fee pricing works better than hourly billing for most companies. Be wary of pricing significantly above or below market rates —both signal potential problems.

Is your pricing scoped for your business needs?

A price that's tailored to your unique business is typically best. Hourly pricing—often coming with overage rates—can rack up quickly. And without visibility into an audit, it's not always clear why you're even paying for those additional hours.

Do they understand companies of your size and industry?

Industry experience matters, especially in regulated sectors. Your auditor should understand your technology stack, common compliance challenges, and regulatory requirements.

Critical questions to evaluate providers

Thoropass™

Platform and technology capabilities

Does your auditor have a portal for document upload, review, and status tracking?

A centralized platform eliminates email chaos and provides real-time visibility into audit progress. Look for features like automated task assignment, comment tracking, and evidence organization.

How automated is their evidence collection process?

Some providers can automate 70-80% of evidence collection through direct integrations. This includes screenshots, policy documents, access reviews, and configuration exports—all in auditor-ready formats.

What AI capabilities do they use to reduce your manual work?

AI should pre-screen evidence quality, generate policy templates, and suggest control mappings. Some providers use AI to answer security questionnaires and create audit-ready documentation automatically.

How do they ensure your audit information stays fresh and current?

Continuous monitoring detects configuration changes and control failures in real-time. This prevents audit surprises and maintains compliance between certification cycles.

Service delivery and support

Can they complete your audit within your required timeframe?

Establish clear timelines upfront, including evidence review cycles and final report delivery. Through automation and streamlined processes, providers today can often complete in half the time as traditional audit firms.

What security protocols will protect your data during the audit?

Your audit provider should encrypt data, limit auditor access to specific workspaces, and follow the same security practices they're auditing you for.

Will they provide specific guidance on your compliance gaps?

Beyond identifying gaps, your auditor should provide remediation steps, policy templates, and implementation guidance. Some providers offer gap assessments before the formal audit begins.

Thoropass™

Service delivery and support

Can they help with real-time compliance monitoring after your audit?

Ongoing monitoring catches drift and maintains readiness for renewal audits. Look for providers who offer quarterly reviews and automated compliance reporting.

Can they combine multiple frameworks into one audit?

Some auditors enable your organization to combine multiple frameworks and certifications into one audit, where there's significant crossover in evidence and requirements. This can save your team significant amounts of time and consolidate duplicated work on evidence requests.

Experience and fit

Does your auditor have experience with companies in your industry?

Industry experience helps auditors understand your technology stack, regulatory requirements, and common compliance challenges. This leads to more relevant recommendations and smoother audits.

Do they focus on customers of your size?

Providers focused on your segment understand your resource constraints and business priorities. Mid-market specialists often deliver better service than firms primarily serving enterprises.

How technical are your auditors?

Your auditors should understand cloud architecture, APIs, and modern development practices. Technical expertise prevents miscommunications and reduces back-and-forth during evidence review.

What is their pricing model and are there hidden fees?

Fixed-fee pricing provides budget certainty. Ask about costs for scope changes, additional frameworks, and ongoing monitoring to avoid surprises.

How should you evaluate options?

Thoropass™

Creating your decision framework

How should you weigh criteria based on your priorities?

For first-time audits, prioritize guidance and support. For established programs, emphasize automation and efficiency. Always weigh customer references heavily—they predict your actual experience.

How should you prioritize technology capabilities vs. human expertise?

The best providers combine both: experienced auditors supported by modern technology. Choosing a traditional audit firm without the technology to streamline your audit will leave you managing manual work that could be automated and give you little to no visibility into your audit process.

What's the best way to check references?

Ask for references from companies in your industry and size range. Focus on specific questions about timeline adherence, communication quality, platform usability, and post-audit support.

What evaluation mistakes should you avoid?

Are you focusing only on price vs. value delivered?

Calculate total cost including your team's time investment, potential audit delays, and whether you get a baseline or hourly price. An hourly price that looks cheap up front could increase significantly depending on the efficiency of the audit.

Are you thoroughly checking customer references?

Don't rely on testimonials or case studies alone. Speak directly with 2-3 current customers about their actual experience, including any challenges they encountered.

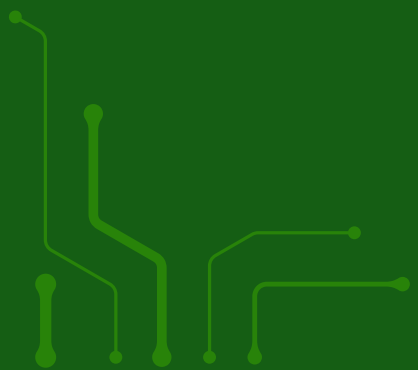
Are you underestimating the importance of platform usability?

A difficult platform creates friction for your team and slows audit progress. If the demo feels clunky, daily usage will be frustrating.

Making the final desicion

The right IT audit provider becomes a strategic partner that transforms compliance from a burden into a competitive advantage. Success depends not just on choosing the right provider, but on how you structure the relationship for long-term value.

The best audit relationships extend far beyond initial certification. Your provider should become an extension of your security team, offering ongoing guidance as your business evolves. Look for partners who demonstrate commitment through proactive communication, regular check-ins, and advisory support between audit cycles.



Thoropass™

Key success factors

Successful audit partnerships share common characteristics:

- **Clear communication protocols that keep you informed throughout the process**
- **Proactive guidance that helps you avoid common pitfalls and stay ahead of changes**
- **Technology integration that eliminates manual work and provides real-time visibility**
- **Continuous improvement that makes each audit cycle smoother and more efficient**

Your audit provider should help you build sustainable compliance processes through automated evidence collection, clear documentation standards, and workflows that maintain compliance as part of daily operations.
Remember that the cheapest option rarely delivers the best outcomes. Focus on total value delivered rather than initial cost, and structure your relationship to support long-term success rather than just meeting immediate compliance needs.

Thoropass™

Thoropass is the modern alternative to legacy security auditors, combining Big 4 rigor with AI-native speed to deliver simply better security audits. Unlike legacy auditors, Thoropass doesn't bury you with black-box processes and manual workflows—your auditor works alongside you, using AI-powered automation and integrations to eliminate the complexity, inefficiencies, and surprises that plague traditional audits.

Learn more at thoropass.com →