Thoropass™

2026 State of Audit & Compliance *Report*

Enterprise security and compliance in the age of AI

Table of Contents

Thoropass

Executive Summary

This year’s survey reveals an industry caught between two forces: the pressure to adopt AI quickly and the imperative to govern it responsibly.

Thoropass surveyed 536 security and compliance leaders to understand how organizations are adapting as AI becomes a core part of the corporate technology landscape. The research explores how companies are evolving their security and compliance strategies to manage the growing use of both enterprise and employee-driven AI tools across the organization.

The study also examines the audit landscape, highlighting the challenges teams face with current audit workflows and how organizations are managing increasing audit demands.

AI has outpaced governance

AI is fast becoming the defining compliance risk of 2026, and most organizations are ill-prepared. More than eight in 10 leaders now see AI as a material risk. Over half worry most about AI-driven data exposure, and a similar number believe an AI incident is the risk most likely to spark regulatory or customer fallout.

At the same time, 69% say AI adoption is moving faster than their security and compliance controls. The gap between how AI is used and how it's governed is getting wider.

Compliance teams feel that tension every day. They don't want to slow the business down, but they're responsible for making sure AI rolls out safely. While product and sales chase the upside, security and compliance are building the guardrails that let innovation scale without creating tomorrow's headline.

Organizations see the risk. Now they have to close the gap.

Fragmentation creates compliance risk

Compliance programs look mature on paper, but they're feeling the strain. Most organizations run multiple external audits each year, and more than half say their programs are mature, with defined metrics and monitoring in place. This isn't a lack of structure. The friction shows up in execution.

Nearly 91% have had to resubmit evidence because of auditor feedback or miscommunication. More than half cite evidence collection across scattered tools as their biggest bottleneck, and managing multiple frameworks remains the top compliance challenge. Four in 10 teams duplicate work across frameworks, and 38% aren't confident they'd pass an unplanned audit tomorrow.

This isn't about burnout. 96% actually say compliance is manageable. It's about fragmentation. Evidence lives in too many systems. Auditor expectations shift. Frameworks overlap but don't align cleanly. Preparation stays reactive when it should be continuous.

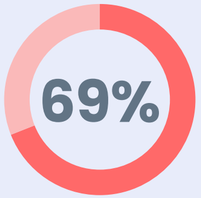
Integrated compliance is the future

Our findings point to a structural shift: compliance is moving from a certification exercise to a continuous risk management function.

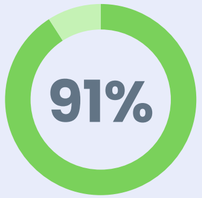
Organizations are increasingly investing in compliance to reduce risk (64%), meet cyber insurance requirements (60%), and satisfy regulatory obligations (57%). Meanwhile, 93% agree that AI-powered audit preparation would improve readiness and free teams to focus on strategic risk management.

The path forward is clear: integrate platform and audit workflows, shift from event-based audits to continuous readiness, and consolidate frameworks to eliminate duplicate work.

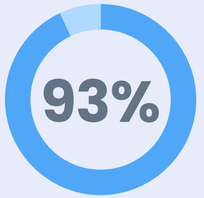
Organizations that close the AI governance gap and reduce operational fragmentation will gain more than audit efficiency, they'll gain speed, predictability, and trust.



say AI adoption is outpacing their security and compliance controls.



report having to resubmit evidence due to auditor feedback or miscommunication.



agree that automating audit preparation with AI would improve continuous readiness and free teams to focus on strategic risk management.

Thoropass

Part I: Key Findings

AI, audit overhead, and compliance as risk management

Compliance programs have never been more mature, nor more strained. Teams are managing higher audit volumes even as friction persists throughout the process. The rapid rise of AI is introducing an entirely new category of risk that is outpacing security and compliance governance at most organizations.

Programs are mature, but challenges persist

Audit volume and compliance maturity are high

Most organizations are running multiple audits annually:

- 83% completed 2-6 external audits in the past 12 months (and another 13% completed seven or more).

Compliance programs are, overall, relatively mature:

- 58% of respondents describe their programs as having defined metrics, predictability, and/or continuous monitoring capabilities.

Audit inefficiencies remain

While almost all respondents claim that their compliance workload is relatively sustainable, there is friction in the process: Most of them also report experiencing audit process problems. Over half sometimes need to resubmit audit evidence due to miscommunication, while more than a third report this happening either often or almost always.

Framework sprawl and evidence maintenance

“Managing multiple frameworks and audits” is the top-ranked compliance challenge, followed closely by “keeping evidence continually audit-ready”, suggesting that even mature programs struggle with the coordination and documentation overhead of overlapping compliance requirements and too many frameworks.

Risk and insurance lead compliance spending

The primary drivers for 2026 compliance investment are risk reduction and security maturity, cyber insurance requirements, and regulatory obligations.

The shift to technology-driven audits

Respondents overwhelmingly agree that automating manual and repetitive work around compliance and audit preparation with AI will enable them to maintain continuous audit readiness while allowing them to redirect efforts to focus on more strategic risk management initiatives.

Part II: Survey Results

Emerging risks

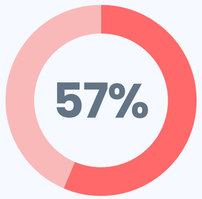
The compliance landscape is defined by contradiction. Organizations have built mature, sustainable programs for managing multiple annual audits. At the same time, they're grappling with persistent operational friction and an entirely new category of AI-driven risk that most aren't equipped to govern.

Compliance threats are escalating with AI

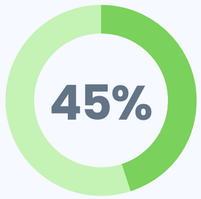
AI has moved from emerging technology to compliance imperative in record time, and the security leaders in this report are highly aware of AI's impact: AI-related incidents have overtaken every traditional threat category as the most likely to trigger regulatory consequences.

AI is now the #1 anticipated source of regulatory and audit consequences.

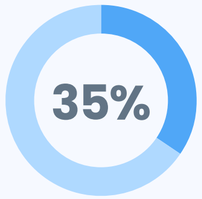
A majority (57%) believe that AI-related data misuse or exposure is most likely to result in regulatory action, audit findings, or customer fallout in 2026 — higher than any other incident type. In addition, 4% are concerned about regulatory or audit scrutiny of AI usage specifically, and 35% cite lack of audit evidence for AI-related controls as a top concern.



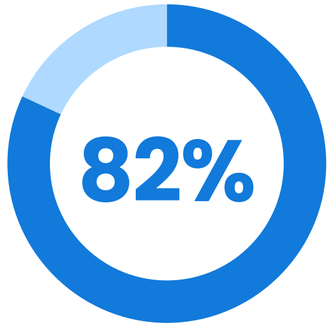
believe AI-related incidents most likely to trigger regulatory action.



concerned about regulatory scrutiny of AI usage.



cite lack of audit evidence for AI-related controls.



see AI as an active and material compliance threat.

AI governance has emerged as a top-five compliance challenge:

- AI governance and controls ranked #5 among pressing compliance challenges.
- This is nearly equal to the perennial "reducing audit cycle time", indicating that AI governance has rapidly become as pressing as longstanding operational challenges.
- More than eight in 10 (82%) see AI as an active and material compliance threat.

Key takeaways

Recognition without readiness

The large majority of security and compliance leaders see AI as a material risk, yet most admit their controls haven't caught up.

This gap between awareness and action is where compliance threats escalate: organizations know they're exposed but haven't yet built the audit evidence, policies, and controls to demonstrate governance.

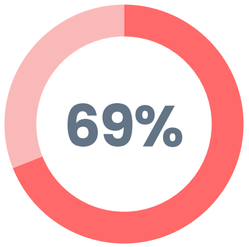
Speed and stakes

Just two years ago, AI governance barely registered as a compliance concern. Now it's the defining challenge of the next audit cycle: more than half believe AI-related incidents (globally, not necessarily at their own organizations) are the most likely to trigger regulatory compliance consequences, audit findings, or customer fallout.

The race to AI is outpacing compliance

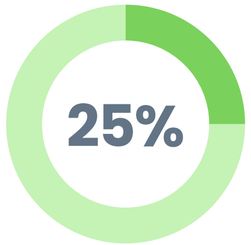
Competitive pressure to adopt AI has created a governance gap that organizations are aware of but struggling to close.

The gap between AI adoption and controls is significant:

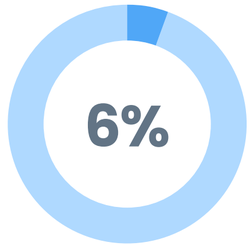


say AI adoption is ahead of their security and compliance controls.

27.6% "far ahead" and 41% "slightly ahead"

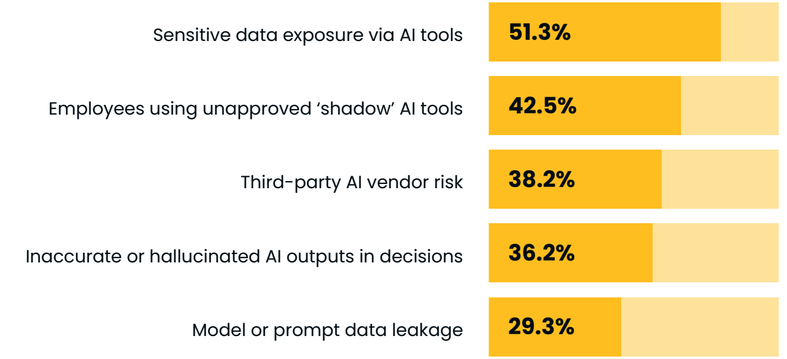


report that AI adoption and controls are mostly aligned.



say security/compliance is ahead of AI usage.

Top AI-related risks reflect this gap:



Thoropass

Key takeaways

Compliance teams caught in the middle

The sales, product, and business sides of companies are racing to capture AI's productivity and competitive advantages. However, security and compliance teams are trying to build guardrails around technology that's evolving faster than policy frameworks can keep up.

Not blockers, but enablers

Compliance teams are concerned about being seen as the blocker to their organization's AI adoption even as their number one AI-related priority is finding solutions that allow their org to take rapid advantage of AI in a secure and compliant manner.

Advantage vs. audit risk

The 31% of organizations that report alignment between AI adoption and compliance governance controls have a potential advantage not just in risk posture, but also in audit readiness. For the majority still playing catch-up, the question is whether they can close the gap before the next audit cycle, or a regulatory inquiry forces the issue.

Top security concerns for 2026

What happens when adoption outpaces controls? This governance gap is already influencing how organizations think about risk. The breach concerns that top the list for 2026 reflect a security landscape transformed by AI and data exposure, with traditional threats like ransomware and software vulnerabilities falling behind.

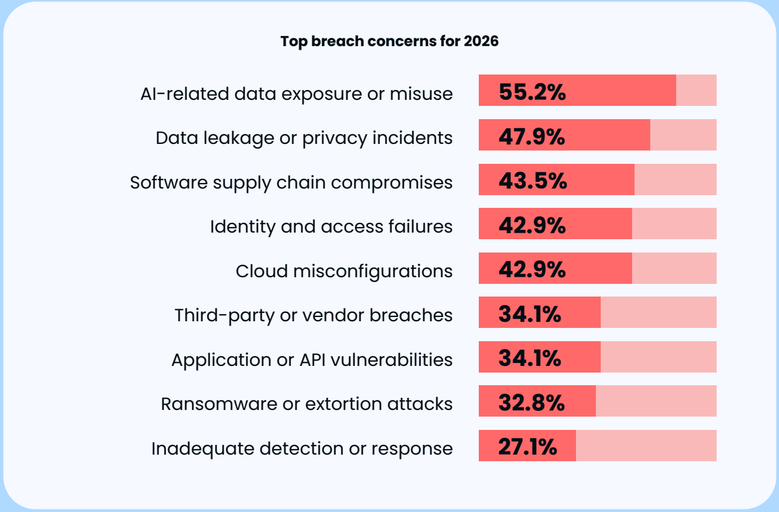
Top breach concerns for 2026

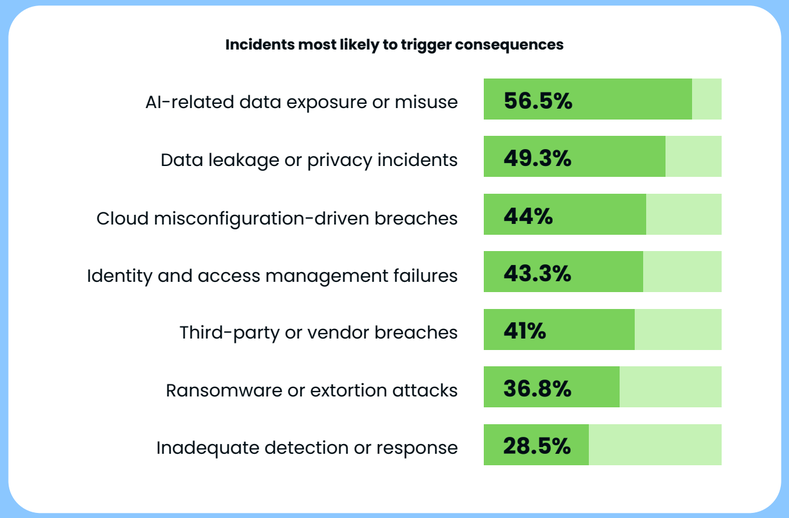
AI-related security breaches have surpassed every traditional security threat to become the number one anticipated source of regulatory, audit, and customer consequences.

Incidents most likely to trigger regulatory, audit, and/or customer consequences

AI-related incidents have sped ahead of longtime traditional security concerns to become the #1 anticipated source of regulatory, audit, and customer consequences.

Security leaders are more worried about data flowing out through AI tools, cloud misconfigurations, and third-party integrations, than they are about extortion attacks.





Key takeaways

The rise of data-centric threats

Four of the top five concerns involve data leaving the organization in unauthorized ways (AI exposure, data leakage and privacy incidents, supply chain compromises, and cloud misconfigurations).

Breach concerns vs. breach impact

The threats organizations worry most about are also the ones they believe will trigger the harshest regulatory and customer fallout. AI-related incidents top both lists. Beyond breach likelihood, leaders are worried about breach impact in a regulatory environment that's increasingly focused on data protection and AI accountability.

Audit issues, failures, and friction points

Even mature compliance programs are grinding through inefficiencies that increase cost, delay certifications, and introduce unnecessary risk. The breakdowns are not isolated, they appear across evidence collection, framework management, auditor coordination, and audit predictability.

Evidence breakdowns: resubmission, staleness, and fragmentation

- 91% of organizations must resubmit evidence, and 37% do so often or almost always.
- 53% struggle with collecting evidence across multiple tools.
- Nearly 35% say evidence isn't auditor-ready when submitted.

The root issue is fragmentation. Evidence lives across cloud providers, HR systems, identity platforms, ticketing tools, and spreadsheets — with no unified system of record. This fragmentation creates cascading failures:

- Evidence is outdated by the time it's reviewed.
- Teams duplicate work across frameworks.
- Audit becomes a scramble rather than a continuous state of readiness.

Multi-framework sprawl and duplicate work

Managing multiple frameworks ranks as the #1 compliance challenge. SOC 2, ISO 27001, PCI DSS, and emerging AI governance requirements all introduce overlapping controls with slightly different evidence expectations.

Without consolidation:

- 41% cite duplicate work across frameworks as a bottleneck
- Teams struggle to maintain a single source of truth
- Documentation is repeatedly recreated instead of mapped once and reused

Despite years of automation tools entering the market, manual evidence collection still ranks #3 among challenges, suggesting automation adoption is incomplete or that tools fail to unify fragmented systems. AI governance now ranks nearly equal to reducing audit cycle time as a top challenge, signaling that compliance complexity is expanding, not stabilizing.

Auditor handoff failures

70% of organizations experience at least one significant handoff problem. There is no single dominant failure point — breakdowns occur across the entire audit lifecycle:

- Coordinating submissions
- Translating controls into acceptable evidence
- Evidence not accepted as-is
- Expectation misalignment
- Remediation tracking

Four of the top five bottlenecks involve the internal team auditor interface. Two recurring friction points highlight a structural gap:

- Controls are implemented in one way but must be documented differently for audit
- Evidence collected internally is not “auditor-ready”

When coordination happens via email chains and disconnected systems, friction multiplies. Leadership visibility suffers, and compliance teams spend hours building status updates instead of strengthening controls.

Auditor instability and quality concerns

More than a third (37%) of organizations changed auditors in the past three years.

The top reasons:

- Auditor quality and expertise
- Cost

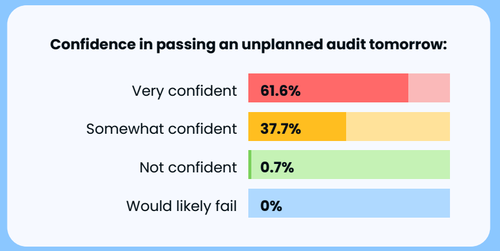
Frequent switching introduces institutional knowledge loss, resets expectations, and further reduces predictability. Organizations are searching for consistency, domain expertise, and audit partners that can scale alongside them.

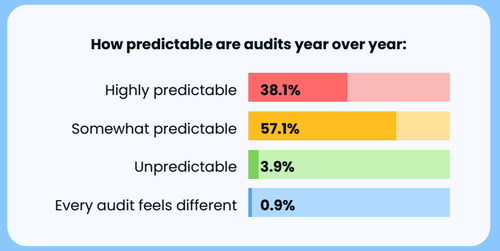
Confidence gaps and audit unpredictability

Audit friction ultimately shows up in confidence and predictability metrics:

- 38% are not fully confident they would pass an unplanned audit
- Only 38% describe their audits as highly predictable
- 62% characterize audits as less than highly predictable

Even though 96% say their workload is “supportable,” that does not mean it is smooth or efficient.





Thoropass

Key takeaways

Multi-framework frustration

When a company needs to complete a security audit, it wants a faster, more predictable (in cost, time, and process) way to certify without sacrificing quality or exhausting internal teams. But managing multiple frameworks and audits ranked as the #1 compliance challenge, ahead of every other operational pain point.

Each framework introduces its own evidence requirements, control mappings, and auditor expectations. Without consolidation, teams end up doing duplicate work (41% cite this as a bottleneck) and struggling to maintain a single source of truth (20% say this breaks down).

Supportable does not equal smooth

The vast majority of respondents (96%) say their compliance workload is sustainable, yet:

- 91% have to resubmit evidence due to miscommunication
- 53% struggle with evidence collection across multiple tools, and nearly
- 35% report that the evidence their teams collect isn't auditor-ready

Audit risks and downstream outcomes

When 38% of respondents aren't fully confident they'd pass an unplanned audit tomorrow, and 62% describe their audits as less than highly predictable, the downstream risks are real: delayed certifications, deal friction, and exposure in the event of a regulatory inquiry. Organizations that reduce this friction (through platform consolidation, auditor alignment, or both) will be out in front of competitors.

Part III: AI, Continual Readiness, and Closing the Compliance Gap

Even as programs have matured, the infrastructure supporting them has not kept pace. Organizations are managing more frameworks, facing new AI-driven risks and regulations, and navigating audit processes that remain stubbornly unpredictable, even after years of investment.

The challenges and frustrations revealed in this survey share a common root cause: fragmentation. Evidence lives across dozens of disconnected tools. Auditor expectations don't align with how teams collect and format documentation. Multi-framework models and requirements create duplicate work. And AI governance exists as an emerging mandate without established playbooks or controls.

To achieve audit-ready continuous compliance, the data points toward three principles for organizations to prioritize:

1. Platform and audit integration

When the system used to prepare for an audit is the same system that's used to manage it, the translation problem disappears. Evidence is collected in the format auditors need. Feedback happens in real time, and interpretations stay consistent year over year because everyone operates from the same source of truth.

2. Continuous readiness

The 38% who expressed concern over passing an unplanned audit reveal that, too often, compliance is still treated as an event rather than a state. Automated evidence collection and continuous monitoring transform audit preparation from a periodic fire drill into an always-current snapshot of your security posture.

3. Multi-framework consolidation

The number one compliance challenge cited in this report is managing multiple frameworks. Smart companies are adopting smarter architecture, not adding headcount. Mapping controls across frameworks, eliminating duplicate evidence requests, and coordinating audits through a single workflow reduces the coordination burden that's straining even mature teams.

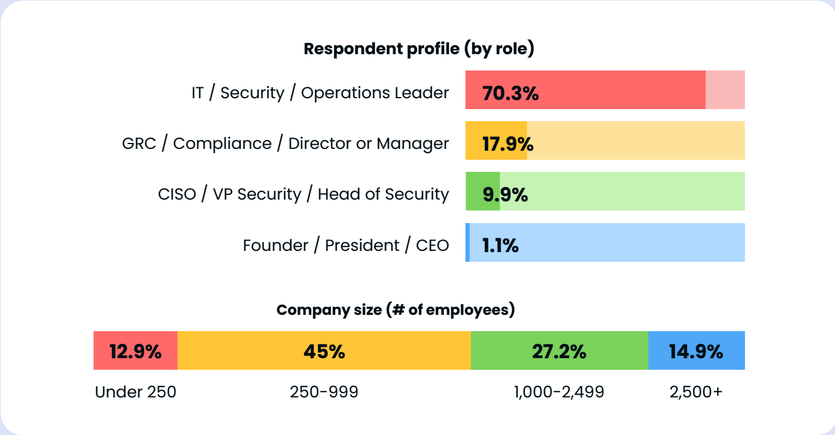
Closing the gap between AI adoption and governance, between evidence collection and auditor expectations, and between audit volume and team capacity are the ones that recognize compliance as a risk management function — not only within their security teams, but across their entire organization.

In conclusion

Compliance is no longer a back-office certification function. It is infrastructure. When governance lags adoption, risk compounds. When workflows are fragmented, friction scales. But when evidence, auditors, and controls operate within a unified system, predictability returns. The companies that treat compliance as a strategic operating capability, not a periodic obligation, will be the ones that innovate with confidence while others scramble to catch up.

Methodology

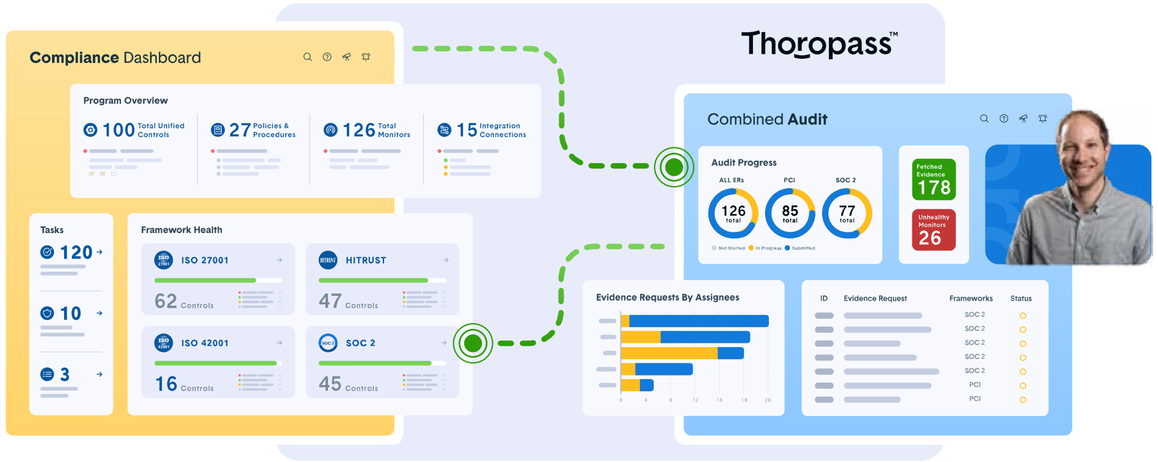
To understand the current state of audit processes, compliance, and how AI is affecting both, we surveyed 536 InfoSec leaders across SMB to enterprise organizations, ranging from 50 to 5,000+ employees.



The End-to-End Cybersecurity Auditor

Thoropass brings auditors, automation, and your compliance data into one platform — using AI to collect and validate evidence while in-house experts guide you from controls to attestation, without surprises.

Talk to an Expert ⟶



Thoropass