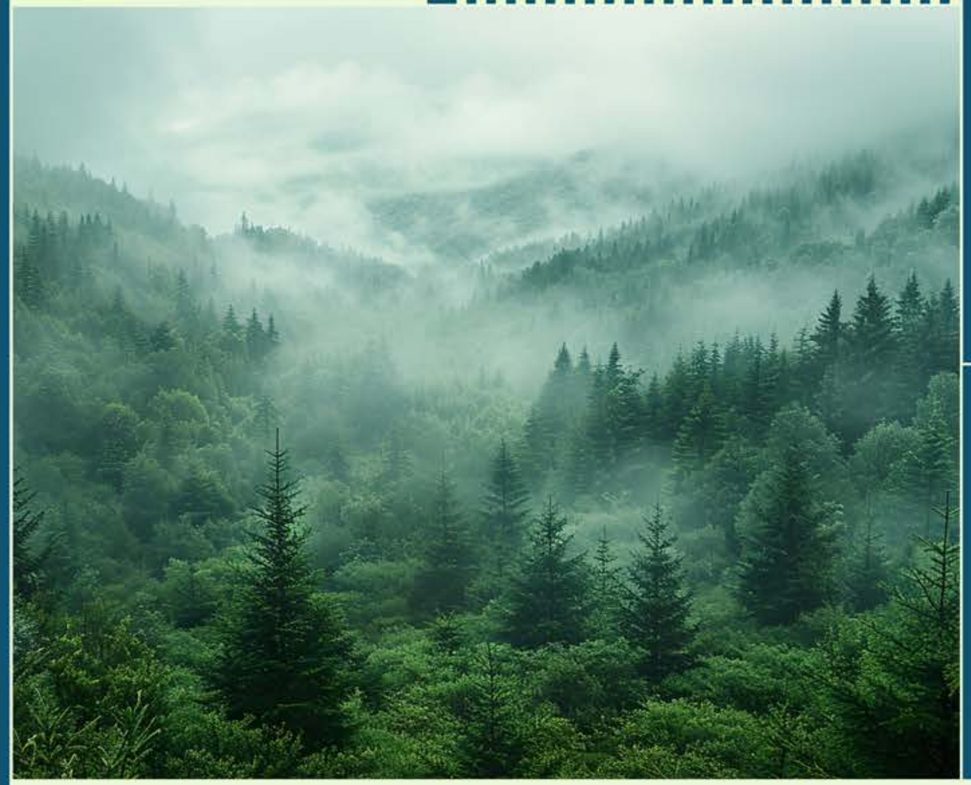


AI-powered GRC

From reactive compliance to proactive strategy

Table of contents

Section 1: Executive summary

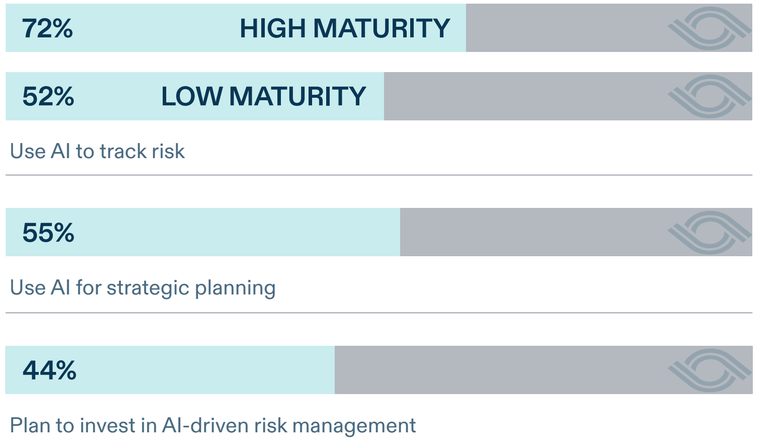
To unlock AI's full potential in GRC, integration, governance, and cross-functional alignment are critical. Forty-eight percent of organizations say they're using AI extensively, but dig deeper, and you'll find **many are stuck in pilot mode, struggling to turn experiments into real performance.**

What sets leaders apart isn't how much AI they've adopted – it's how well they use it to drive decision-making. The best organizations don't see AI as just another tool. They treat it as an intelligence layer – one that connects regulations, risks, and business choices in real time.

The data are clear:

- Leading organizations are 6x more likely than their peers to apply AI across multiple GRC functions, embedding it into daily operations.
- **72%** of the most mature organizations use AI to track risk proactively, compared to just **52%** at the lowest maturity tier.
- More than half (**55%**) of mature organizations use AI for predictive risk modeling, shaping risk posture, and strategic planning – not just checking compliance boxes.
- Nearly half (**44%**) of the most mature organizations plan to invest further in AI-driven risk management in the next 12 months, doubling down on proven returns.

(FIGURE 1) **AI-driven GRC: The growing divide between high and low maturity organizations**



Source: Optro, September 2024 flash poll of 1,335 information security, compliance, and risk professionals

These organizations aren't just automating. They're building systems that think. They're feeding AI structured data, connecting policies to risks, and aligning compliance with innovation. Meanwhile, less mature firms are stuck with scattered tools, manual processes, and isolated automation. **The most advanced teams don't just adopt AI – they build for it, making compliance a strategic advantage.**

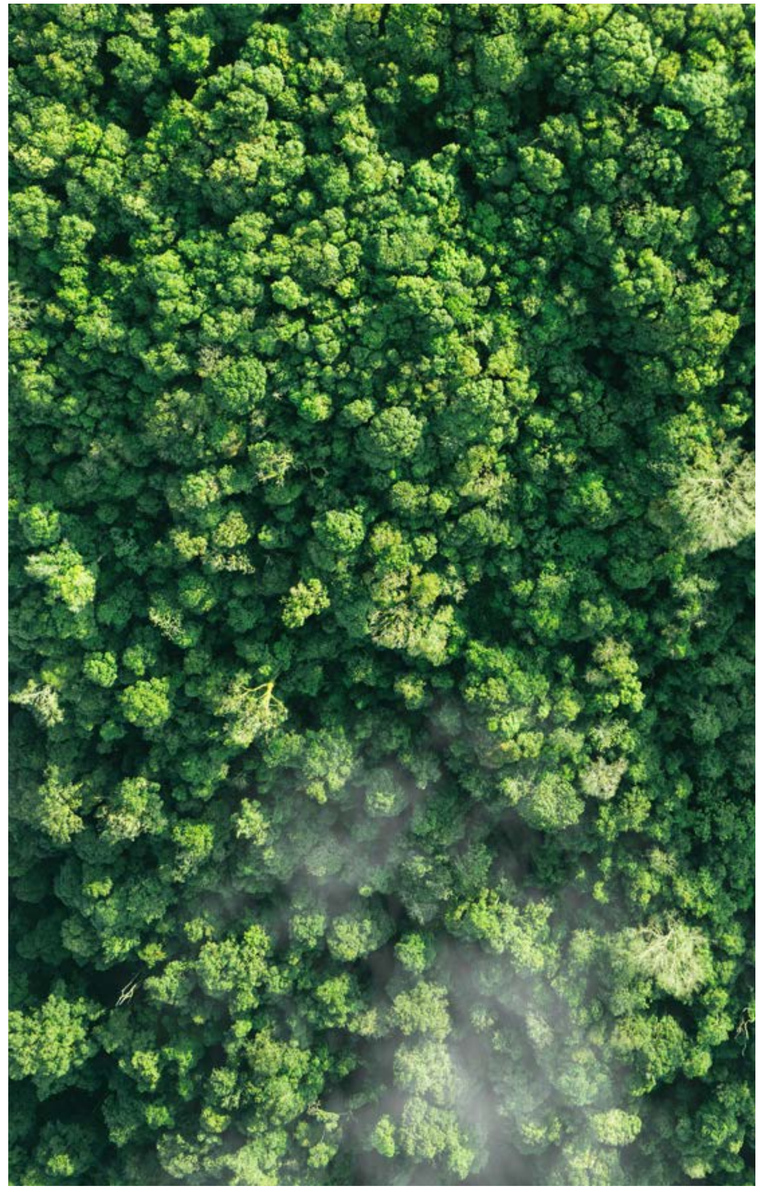


Image credit: Igor Omilaev

Section 2: The maturity journey: From siloed pilots to strategic intelligence

AI is making real inroads into GRC, but not all progress looks the same. Some organizations are scaling mountains – turning AI into an engine for smarter, faster decisions. Others are still setting up base camp, running disconnected pilots with limited impact.

BASE CAMP

This is where many organizations start. **Only 14% at this level use AI meaningfully in GRC.** Most are experimenting with specific tasks, like document review or automated alerts, but lack cohesion. About 55% use automated tracking, but the data is scattered, and governance is weak. Teams often operate in silos, with just 47% reporting strong cross-functional collaboration. Cultural resistance is common, and many rely on external consultants to make progress.

ASCENSION

At this stage, AI is live, but not yet strategic. Around 34% of organizations use AI in risk and compliance functions, but 85% still report only partial integration. Implementation lacks standardization across teams, and while the technology shows value, **siloed systems and inconsistent data limit its potential.**

SUMMIT

Summit-stage organizations treat AI as core GRC infrastructure. Seventy-six percent of Summit organizations use AI across both risk and compliance. Predictive modeling (used by 55%) and automated workflows (52%) are standard tools. AI isn't an add-on. It's part of the infrastructure. These teams have moved past efficiency and are expanding capability, using AI to simulate risk, support innovation, and drive strategy.

Execution, not ambition, defines the climb

What separates the base from the summit isn't vision. It's execution. Climbing this mountain requires organizations to move from pilot programs to full production, with strong governance and trustworthy data.

At Base Camp, AI is still in the lab. In Ascension, it's operational but narrow. **By the time organizations reach Summit, AI is integrated into daily workflows and strategic processes.**

Another key shift is from tactical to systemic use. At lower levels, AI is used for isolated tasks like policy summarization. As maturity grows, it connects across workflows and functions. Summit organizations use AI in twice as many GRC functions as their less mature peers.

WHAT PROGRESS LOOKS LIKE

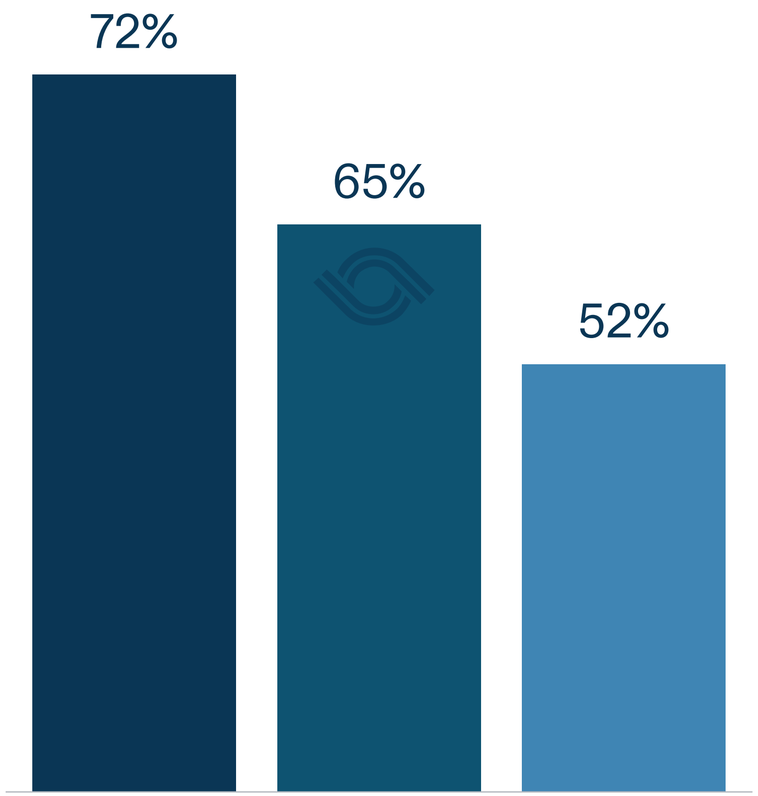
Progress isn't just about adding more tools. It's about building smarter systems:

1. Moving from proof of concepts (PoCs) to full-scale deployment
2. Connecting siloed workflows across teams
3. Replacing fragmented automation with coordinated, contextual intelligence

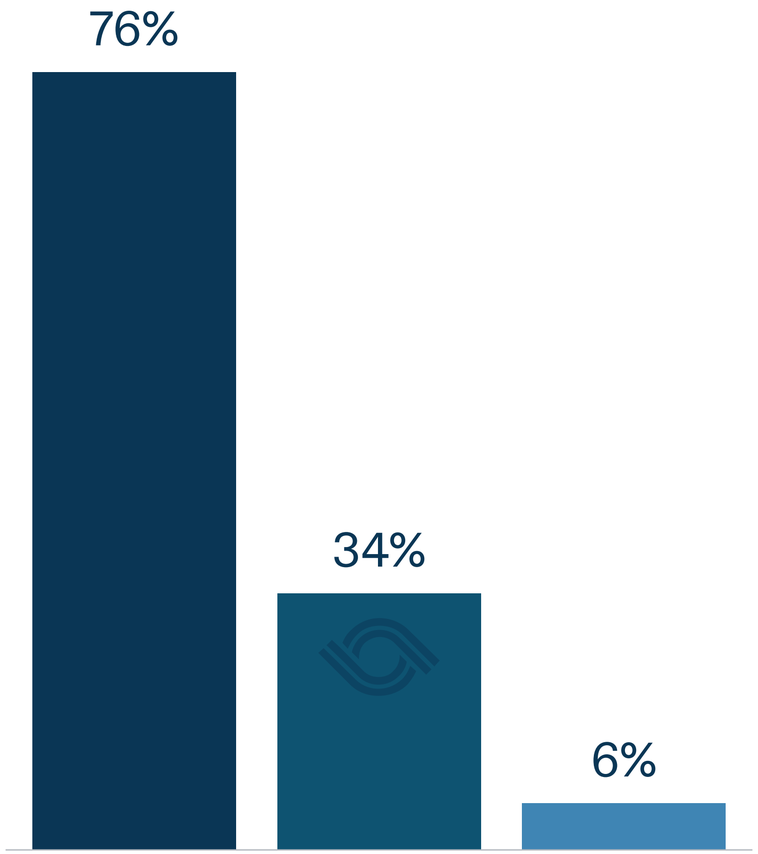
Mature organizations don't rush to the top. They build methodically, acclimating at each altitude. **The goal is not just doing things faster, but doing them smarter – and turning compliance from a checkbox into a lever for growth.**

Section 3: The AI ceiling: How maturity shapes strategic value

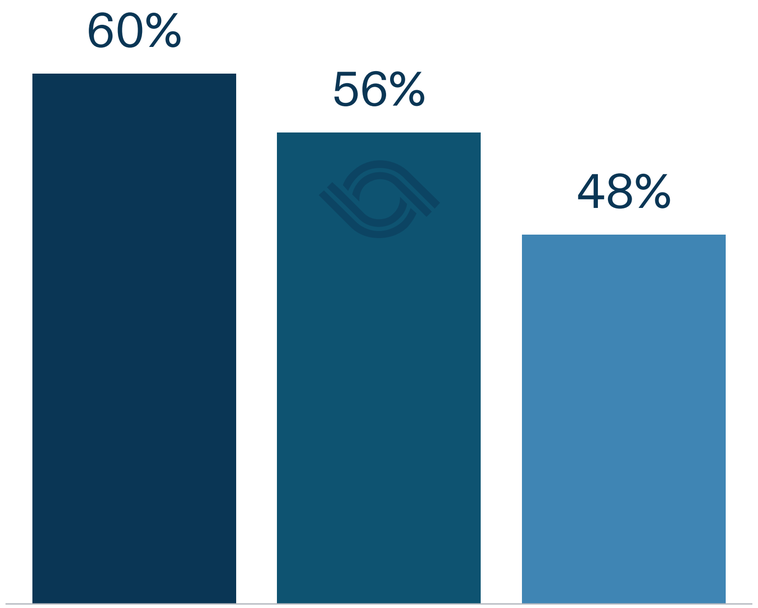
Every organization using AI in GRC runs into a limit: an “AI ceiling” that defines how much strategic value they can extract. And that ceiling is not set by technology. It’s set by maturity.



72% of Summit-stage organizations use automated alerts compared to **65%** Ascension and **52%** Base Camp.



76% of Summit-stage organizations are already using AI in compliance and risk management compared to **34%** Ascension and **6%** Base Camp.



60% of Summit-stage organizations use AI-powered automation for regulatory change monitoring compared to **56%** Ascension and **48%** Base Camp.

Organizations that have climbed further in their AI journey are already seeing meaningful gains: faster responses to risk, smarter compliance, and a more agile business posture. They're not just managing risk; they're shaping it.

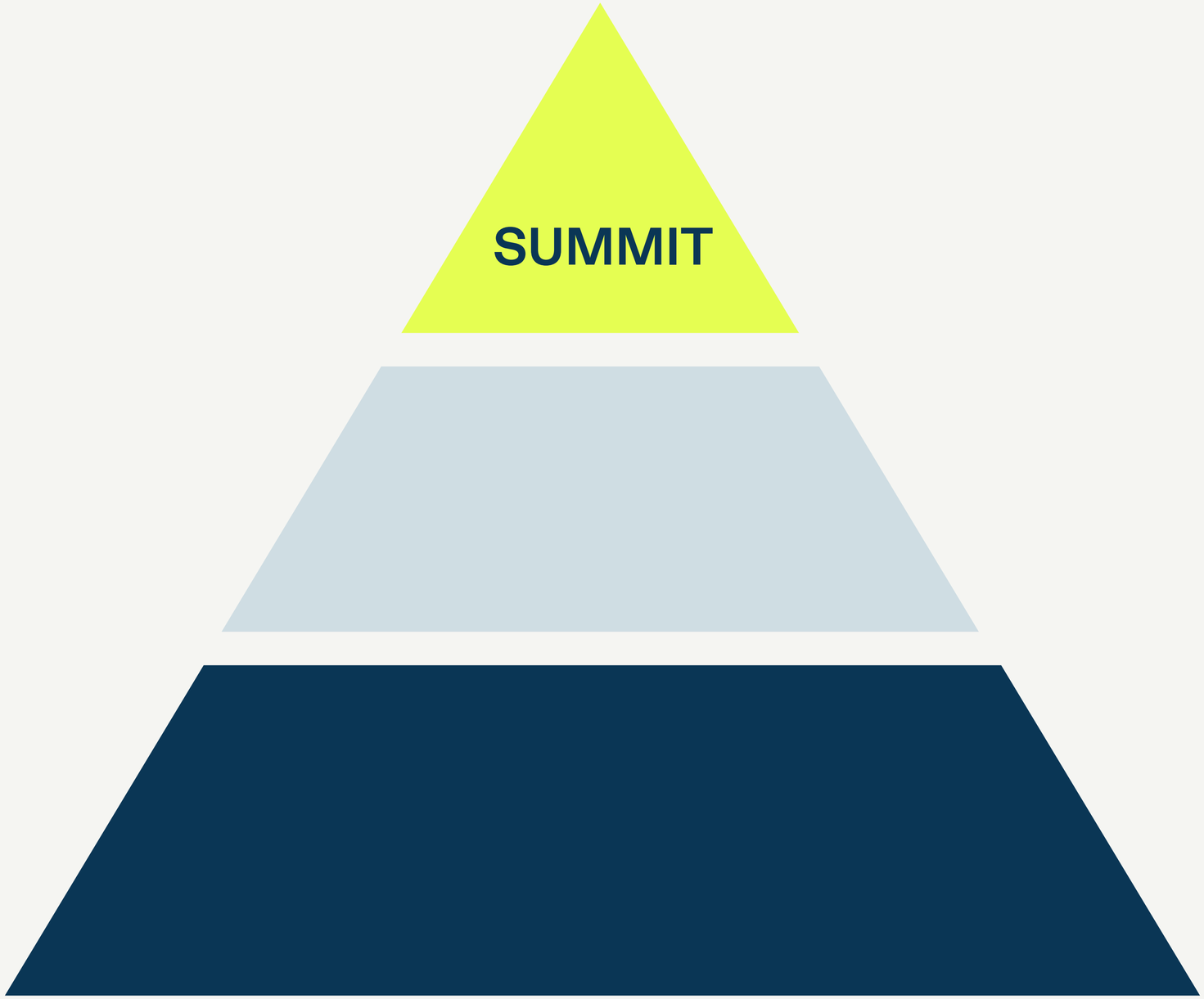
SUMMIT STAGE:
Organizations lead the way

They're **45%** more likely than their lower-maturity peers to believe AI can significantly accelerate operations, whether it's spotting emerging risks, automating approvals, or managing regulatory change. For them, compliance isn't a bottleneck; it's a catalyst.

These leaders are also much more aggressive in how they apply AI. **Seventy-two percent** use automated alerts (compared to 62% across the board), and they're six times more likely than Base Camp peers to deploy AI across multiple GRC functions. Over half (**55%**) use predictive modeling to simulate regulatory impact before implementation – a sign they've moved from reacting to anticipating.

They also integrate more deeply. Cross-domain orchestration – where AI connects infosec, audit, compliance, and risk – is twice as common in Summit Organizations compared to lower tiers. One respondent put it clearly: Their goal is a system that can "automatically track, interpret, and apply regulatory changes across global jurisdictions." For the most mature firms, that vision is already in progress.

But not everyone has cracked the code.

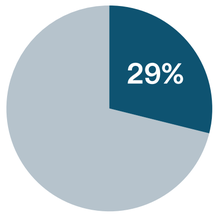


ASCENSION STAGE:
Trapped by the process-technology gap

Organizations in the middle tier have the right tools or the right processes, but rarely both. Integration is a major hurdle. In the UK, for example, only **29%** of organizations use ad hoc assessments to update compliance programs, compared to **41%** globally.

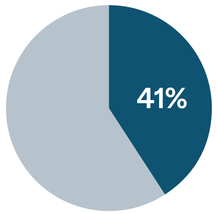
They've seen success in isolated use cases, but those wins don't scale. The result is a landscape of "islands of excellence" – pockets of advanced capability surrounded by bottlenecks. AI shows promise, but siloed systems and governance gaps hold it back.

UK

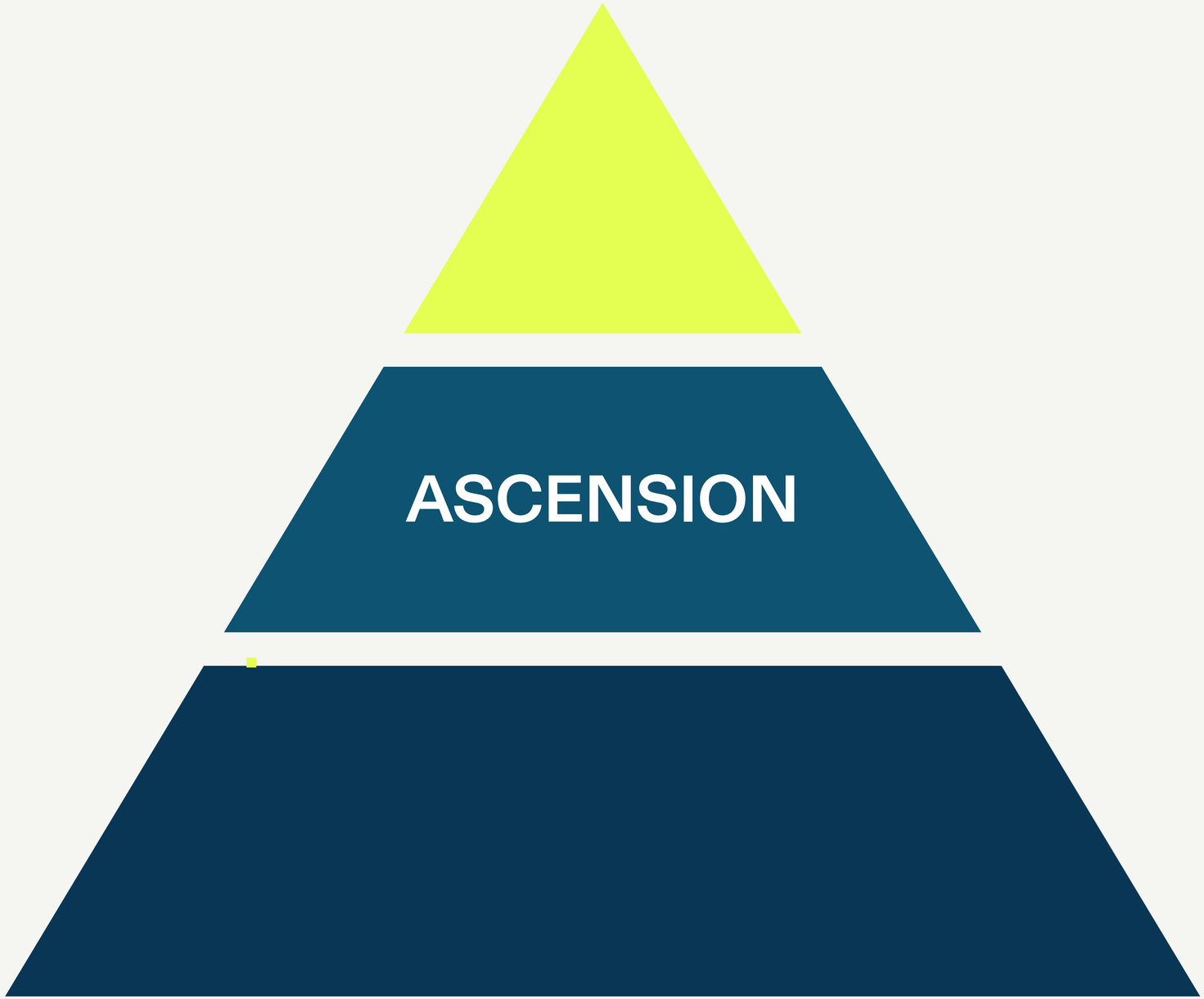


29% of UK organizations use ad hoc assessments to update compliance programs

GLOBALLY



41% of UK organizations use ad hoc assessments to update compliance programs globally



BASE CAMP:
Compliance as a cost center

At the lowest maturity level, organizations are stuck in reactive, manual workflows. AI is limited to small pilot projects that rarely scale. Only **18%** report integration across audit and compliance functions, compared to **39%** at the Summit. And 41% still rely on spreadsheets, emails, and static documents, tools that make intelligent AI adoption nearly impossible.

Even though many of these firms are satisfied with their current tools, **nearly half (48%) say managing regulatory change is a top challenge.** Their fragmented systems isolate GRC from business strategy, and cultural resistance, underinvestment, and unclear leadership priorities slow them down even further.

(FIGURE 2A) **Respondents report integration across audit and compliance**

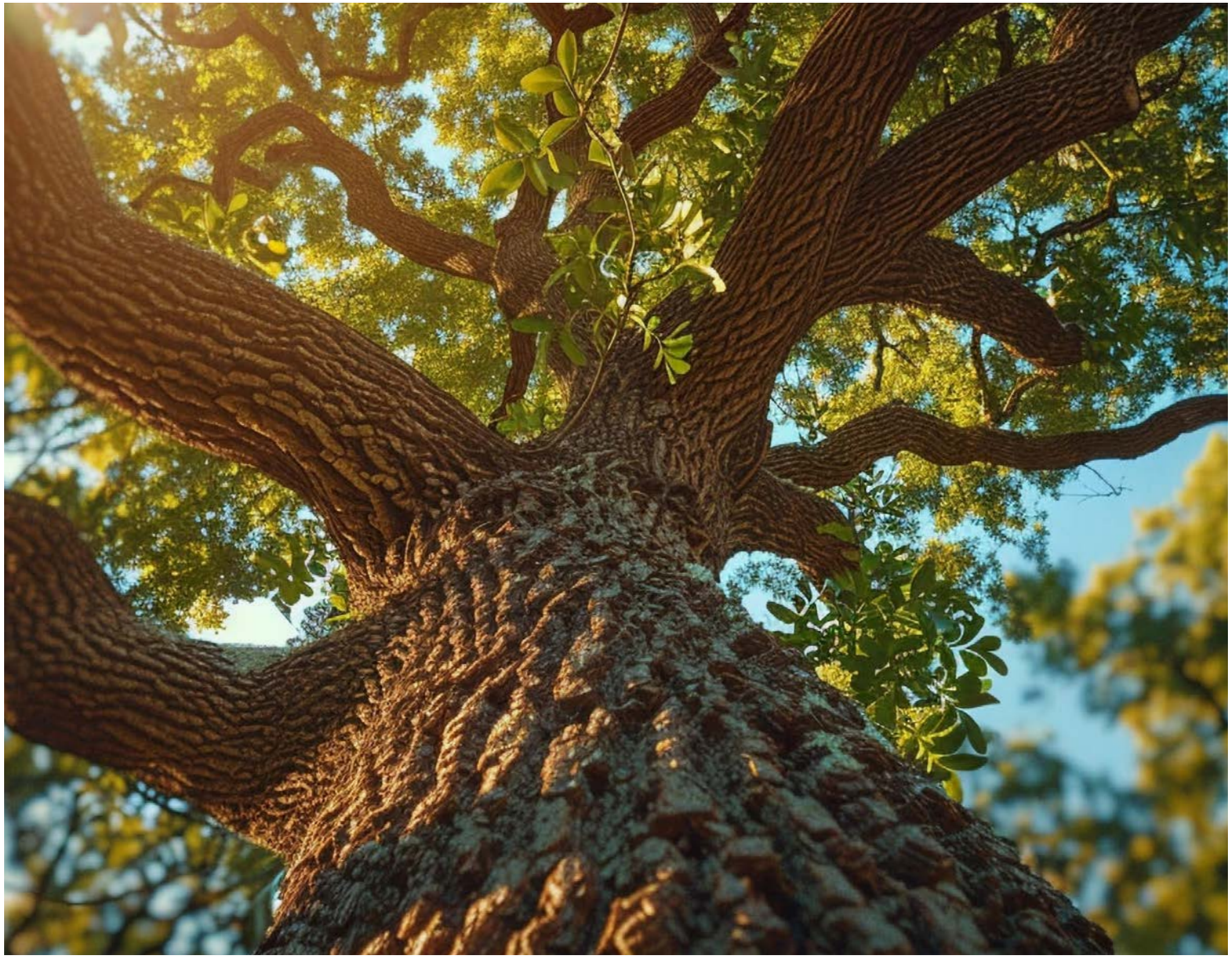
(FIGURE 2B) **Organizations rely on spreadsheets, emails, and static documents**

The AI ceiling is organizational, not just technical

To move beyond their current ceiling, organizations need more than new tech. **They need structural change: cohesive data models, integrated workflows, and executive alignment.**

The key is context. Systems need to connect regulations to internal controls, risks, and metrics. Only then can AI deliver trustworthy, explainable insights that people will act on. Interestingly, only **20%** of UK respondents identified a lack of AI automation as the primary problem, which suggests that the real issue isn't the tools. It's the foundation they're built on.

Organizations that are breaking through the ceiling aren't just reacting faster. They're modeling scenarios, quantifying impacts, and using AI to drive the business forward. They're not asking if AI can help. Instead, they're building systems where it already does.



(FIGURE 3) **UK respondents identified lack of AI as primary issue**

Source: Optro, September 2024 flash poll of 1,335 information security, compliance, and risk professionals

Section 4: Risk tolerance and trade-offs

As organizations climb the AI maturity curve, something important shifts: their relationship with risk. Instead of minimizing it at all costs, mature organizations start making smarter trade-offs, balancing speed, precision, and innovation with real-time insights guiding the way.

This isn't recklessness; it's confidence **grounded in data and supported by systems that can model outcomes before decisions are made.**

Context enables intelligent risk

High-maturity organizations understand the "why" behind AI decisions. They don't just get alerts, they get insight. Contextual data connects regulations to processes, risks to controls, and controls to outcomes. This allows them to ask: Is this a risk we need to avoid, or one we can manage?

Instead of slowing things down, Summit-stage organizations are speeding up, with fewer missteps and less rework. They've supplemented audits and checklists with advanced capabilities. They're simulating scenarios, testing risk posture, and aligning decisions with strategy.

The cost of immaturity: Rigid or reckless

At the other end of the spectrum, less mature organizations often fall into extreme positions. Some become overly cautious, avoiding any action that might introduce exposure, and in doing so, stall innovation. Others move too fast, deprioritizing compliance just to hit deadlines, and unknowingly taking on risks they can't see.

Without connected, data-driven systems, these teams can't properly evaluate trade-offs. Decision-making becomes inconsistent, based on gut instinct, static policies, or outdated spreadsheets. The result? A fragile posture that either slows the business down or leaves it exposed.

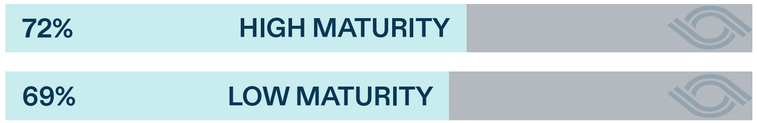
Strategic risk as a competitive edge

For Summit organizations, risk isn't the enemy – it's a variable to be managed strategically. They adapt controls instead of defaulting to rigid rules, using predictive models to surface early warning signs and head off issues before they escalate.

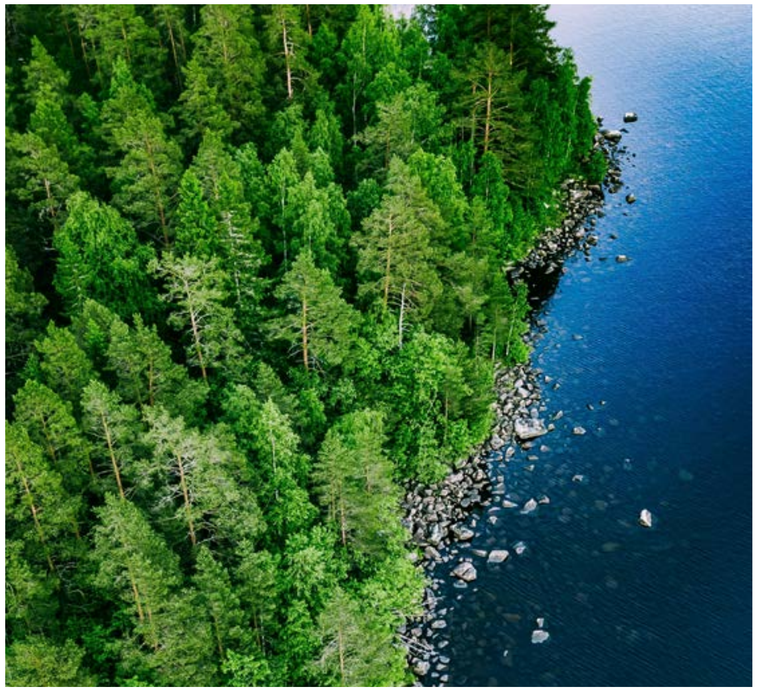
They also measure differently. Forty-six percent track compliance ROI based on its ability to enable better decisions. Real-time monitoring replaces manual validation, which means fewer fire drills and more focus.

The results speak for themselves: **72%** of Summit-stage organizations agree that embedding compliance into innovation helps scale faster with fewer disruptions. And **69%** say AI is helping them manage regulatory change more effectively, turning what was once a bottleneck into a growth accelerator.

(FIGURE 4) **Summit organizations embedding compliance into innnovation vs. leveraging AI for quicker scaling**



Source: Optro, September 2024 flash poll of 1,335 information security, compliance, and risk professionals



Section 5: Pain points and promise: Where the gaps still exist

Even AI-savvy organizations face friction when it's time to scale. Two issues consistently show up across all maturity levels: integration gaps and explainability. These aren't minor hurdles; they're structural weaknesses that can stall momentum and limit trust in AI systems.

Integration: The biggest roadblock

Integration is consistently the top issue across maturity tiers. Only **39%** of organizations report strong integration between compliance, infosec, and risk. That leaves the majority navigating partial or weak linkages – where workflows break, insights don't travel, and silos persist.

Foundational issues remain at the lower end of the maturity scale. Data is still scattered across spreadsheets and inboxes. In the U.S., **45%** of respondents say manual work and inefficient tools are their biggest regulatory challenges, well above the **38%** global average.

Mid-tier organizations have different problems. They've adopted more advanced tools, but integration often depends on brittle point-to-point connections that aren't built for scale. Nearly **60%** rely on third-party consultants for compliance support – and that number jumps to **67%** in the U.S. These firms are getting short-term results, but still lack internal capability to run intelligent, connected compliance operations.

Even respondents who say they're satisfied with their current tools admit they've made compromises. Surface-level wins often hide deeper problems, like fragmented data and misaligned systems, that create long-term risk.

(FIGURE 5A) **US respondents more likely to struggle with manual work and insufficient tools**

(FIGURE 5B) **US respondents more likely to rely on third-party consultants for compliance support**

Source: Optro, September 2024 flash poll of 1,335 information security, compliance, and risk professionals

Explainability: The trust barrier

The other major challenge is explainability. For many organizations, this is the last-mile problem. They've got AI tools, but they don't fully trust the outputs – and without trust, adoption stalls.

Over half of respondents say they need better accuracy and transparency before expanding AI in compliance decisions. And in heavily regulated industries, that's non-negotiable. You need audit trails, defensibility, and clear reasoning for every decision made. If an AI system flags a risk but can't explain why, compliance teams often override or ignore it.

That's why **context is critical.** AI doesn't just need raw data –
it needs structured, connected content that links decisions to regulations, policies, and controls. Without that, even accurate results can feel unreliable.

The promise is real, but work remains

The organizations making the most progress are the ones closing these gaps. They're not just buying tools – they're building systems that share data across functions, explain decisions in plain terms, and grow more capable over time.

Scaling AI in GRC doesn't just mean more automation. It means smarter integration and deeper transparency. Until those are in place, even the best AI can fall short of its potential.

Section 6: From efficiency to intelligence

The AI journey in GRC doesn't end with automation – it begins there. Successful organizations move beyond saving time to making better decisions faster. They eliminate manual work and build intelligent systems that operate in context, adapt in real time, and ultimately support autonomous compliance.

It's not just about doing things more efficiently. It's about doing them intelligently.

Stage 1: Base camp – Automation without context

At the early stage, organizations are focused on removing friction. They deploy AI to handle repetitive tasks like evidence collection, document review, and policy mapping. These efforts ease the workload, but they rarely transform how compliance operates.

Automation remains narrow and fragmented. Each tool does one job. These are the "islands of automation" where tasks get done faster, but insights don't move across systems. Manual processes are still common. Thirty-four percent cite reducing manual burdens as a top priority, and **45%** of U.S. respondents say manual work remains a major challenge in adapting to regulatory changes.

Stage 2: Ascension – Connecting systems, building intelligence

At this stage, the focus shifts from speed to visibility. Organizations start linking AI systems across compliance, risk, audit, and infosec. They invest in dashboards and analytics to provide unified views of risk and regulation. Contextual data starts flowing between tools.

Sixty-two percent of organizations use automated alerts, but many still struggle to act on them. Feedback loops are often missing, and governance structures lag behind. Half still rely on manual tracking, and only **15%** report strong integration between compliance and related functions.

The result is a patchwork: Some departments use AI effectively, while others lag behind. These are "islands of excellence" – valuable but disconnected.

Stage 3: Summit – Operationalized context, intelligent compliance

The most mature organizations have made the leap. They've operationalized context. AI systems are fully embedded in day-to-day compliance, risk modeling, and regulatory tracking. These organizations don't just automate; they anticipate, adapt, and act.

They're twice as likely to use AI across multiple GRC domains. Predictive modeling helps them simulate regulatory impact. Real-time data links policies to risks and triggers workflows that adjust autonomously as conditions change.

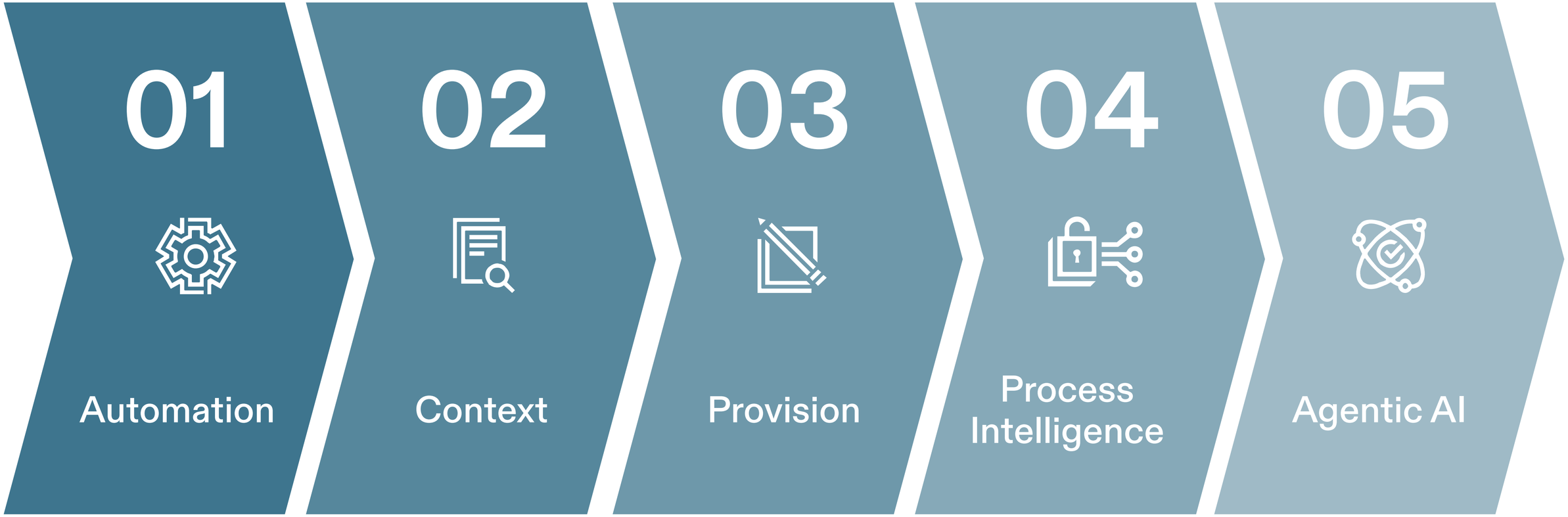
Eighty-four percent agree that embedding compliance into innovation workflows accelerates development and reduces disruption. Compliance becomes an enabler, not a roadblock.

These organizations are laying the foundation for the next phase: agentic AI, where systems operate semi-autonomously, making decisions based on pre-defined parameters, real-time data, and strategic goals.

Where intelligence meets autonomy

The trajectory is clear: Automation gets you efficiency. Context gives you intelligence. But to reach autonomy – the stage where AI doesn't just support decisions but initiates them – you need both. And you need them working together.

That's where mature organizations are headed. They're not just building faster systems. They're building systems that learn, adapt, and guide the business forward.



Section 7: Preparing for agentic AI: The next frontier in GRC

For leading organizations, the next step in GRC isn't more automation, it's autonomy. They're preparing for a future where AI systems don't just recommend actions; they take them. **These systems, known as agentic AI, are designed to operate within guardrails, make decisions, and continuously adapt based on real-time conditions.**

It's a powerful shift. And it's already underway.

What agentic AI looks like

Agentic AI doesn't replace oversight, it makes it smarter. These systems escalate incidents when thresholds are breached. They initiate audits without waiting for a prompt. They update policies automatically when a regulation changes. They generate reports, trigger vendor reviews, respond to internal inquiries, and even adjust controls, all without waiting for human intervention.

More importantly, they learn as they go. These systems improve over time, reducing false positives, anticipating regulatory impact, and responding at the speed of business.

Building the foundation for autonomy

Agentic AI doesn't work in isolation. **It depends on a solid foundation: structured, contextual, continuously updated data.** Without that, even the most advanced tools can't make safe or strategic decisions.

Summit-stage organizations are already putting the pieces in place. They've invested in real-time policy assessments, predictive scoring, and multi-jurisdictional simulations. They're moving from static policy reviews to systems that automatically align with evolving regulations.

And they're not just adopting tools – they're designing systems. Systems that connect compliance to strategy, that operate across domains, and that scale without losing control.

Governance for autonomous action

As AI begins to act on behalf of the business, governance becomes critical. Mature organizations are setting up tiered decision frameworks, audit logs, and escalation paths. They're aligning legal, compliance, IT, and business leadership to make sure AI doesn't just act fast, but acts responsibly.

This governance isn't a constraint. It's what makes autonomous action safe and scalable.

Why this matters now

The benefits are significant: faster response times, streamlined operations, and real-time regulatory adaptation. But the bigger value is strategic. **Agentic AI turns compliance from a defensive shield into an operational advantage. It shifts GRC from a lagging function to a leading force.**

The organizations investing in this now aren't just preparing for change. They're positioning themselves to lead it.

Section 8: From vision to execution: The strategic roadmap for AI-driven GRC

The most mature organizations aren't just using more AI – they're using it better. They've aligned people, processes, and platforms to unlock scalable, measurable, and strategic value. Their success comes not from chasing tools, but from building the right foundations: governance, data context, and intentional design.

But strategic vision only matters if it's actionable.

Whether your organization is just starting out or pushing toward full autonomy, here's how to progress based on your current maturity.

Stage 1: Base Camp – Build automation with the future in mind

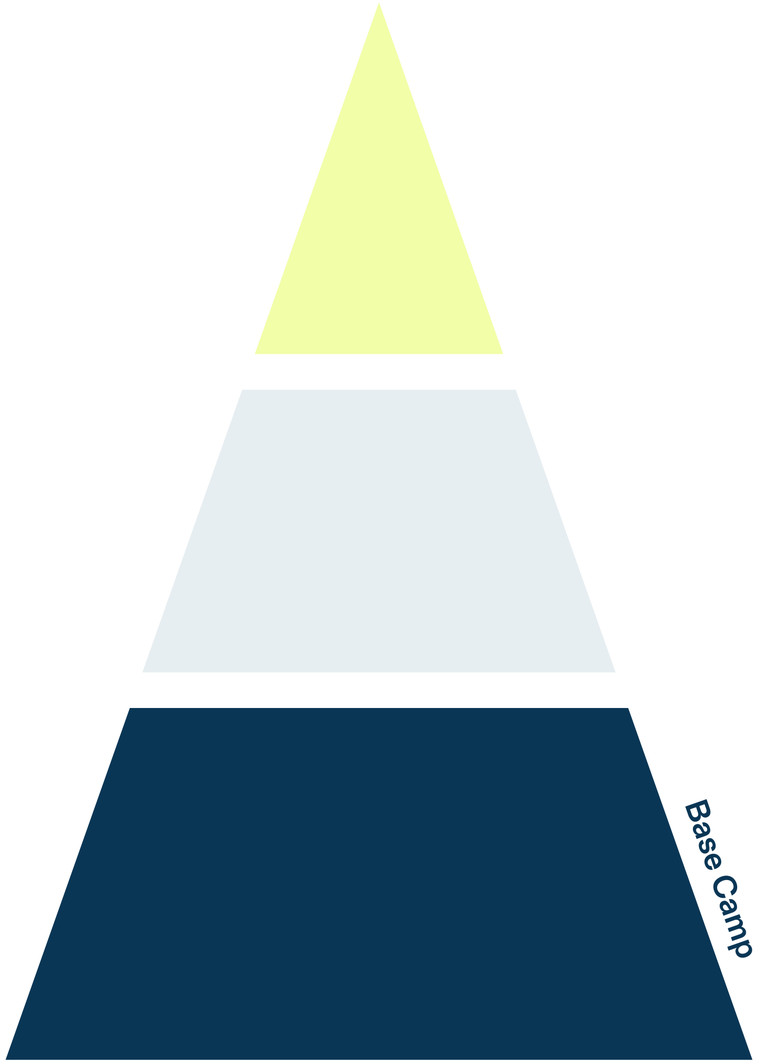
At this stage, workflows are manual, and tools are fragmented. The first priority is simple: reduce friction. Target high-volume, repetitive tasks like evidence gathering, policy mapping, and control tracking with automation that delivers fast wins.

To move forward:

- Standardize regulatory data and tag it to risks and controls.
- Begin building basic contextual links – even simple structures will help future AI systems understand relationships.
- Secure executive sponsorship to expand beyond isolated pilots.
- Create a clear roadmap that connects today's automation to tomorrow's intelligence.

The goal is not just to automate, but to set the stage for scalable, connected AI.

Base Camp - Build automation



Key actions

- Target high-volume, repetitive tasks (evidence gathering, policy mapping, control tracking)
- Standardize regulatory data and tag it to risks and controls
- Secure executive sponsorship beyond isolated pilots
- Create a clear roadmap connecting current automation to future intelligence

Milestones

- Move from 55% to 70%+ automated tracking
- Reduce manual work burden (currently 47% cite as major challenge)
- Establish basic contextual links between policies and controls
- Scale beyond pilot programs to production use

Outcomes

- Eliminate friction in repetitive compliance tasks
- Build foundation for machine-readable regulatory data
- Gain organizational buy-in for AI expansion
- Set stage for scalable, connected AI systems

Level 2: Ascension – Shift from fragmented automation to connected intelligence

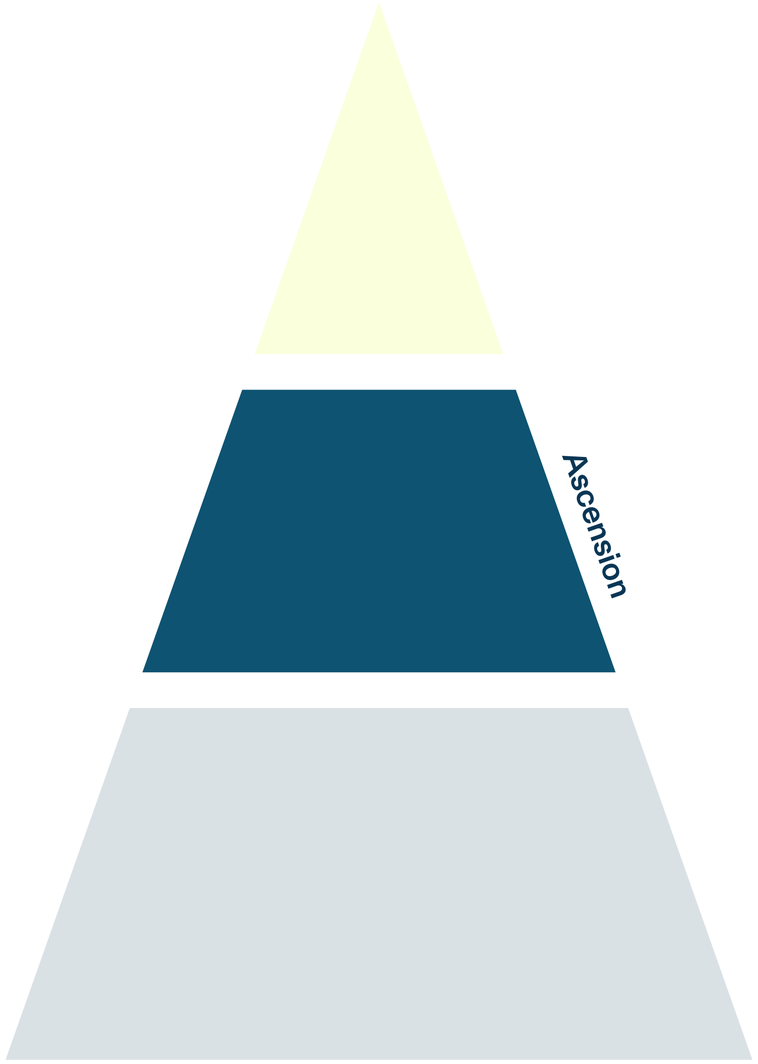
These organizations have AI tools in production, but integration is patchy. Systems may work, but they don't yet work together. Only **39%** of respondents report strong integration between compliance, infosec, and risk teams.

To move forward:

- Invest in platforms that unify compliance data across teams.
- Map regulations to internal controls, audit trails, and change workflows.
- Implement dashboards, predictive alerts, and simulations to make risk visible.
- Establish cross-functional workflows with clearly defined roles and escalation paths.
- Launch pilot projects around predictive modeling with measurable KPIs tied to decision speed and quality.

At this stage, the foundation exists. The next step is connecting systems and layering in real-time context.

Ascension - Connect intelligence



Key actions

- Invest in platforms that unify compliance data across teams
- Map regulations to internal controls, audit trails, and change workflows
- Implement dashboards, predictive alerts, and simulations
- Establish cross-functional workflows with defined roles and escalation paths
- Launch predictive modeling pilots with measurable KPIs

Milestones

- Achieve strong integration between compliance, infosec, and risk
- Deploy automated alerts across operations
- Reduce reliance on third-party consultants (currently 60% rely on them)
- Implement real-time monitoring and validation

Outcomes

- Move from "islands of excellence" to connected systems
- Gain unified visibility across risk and regulation
- Enable faster response times and fewer manual validations
- Build contextual intelligence that travels between functions

Level 3: Summit – Scale intelligence and prepare for autonomy

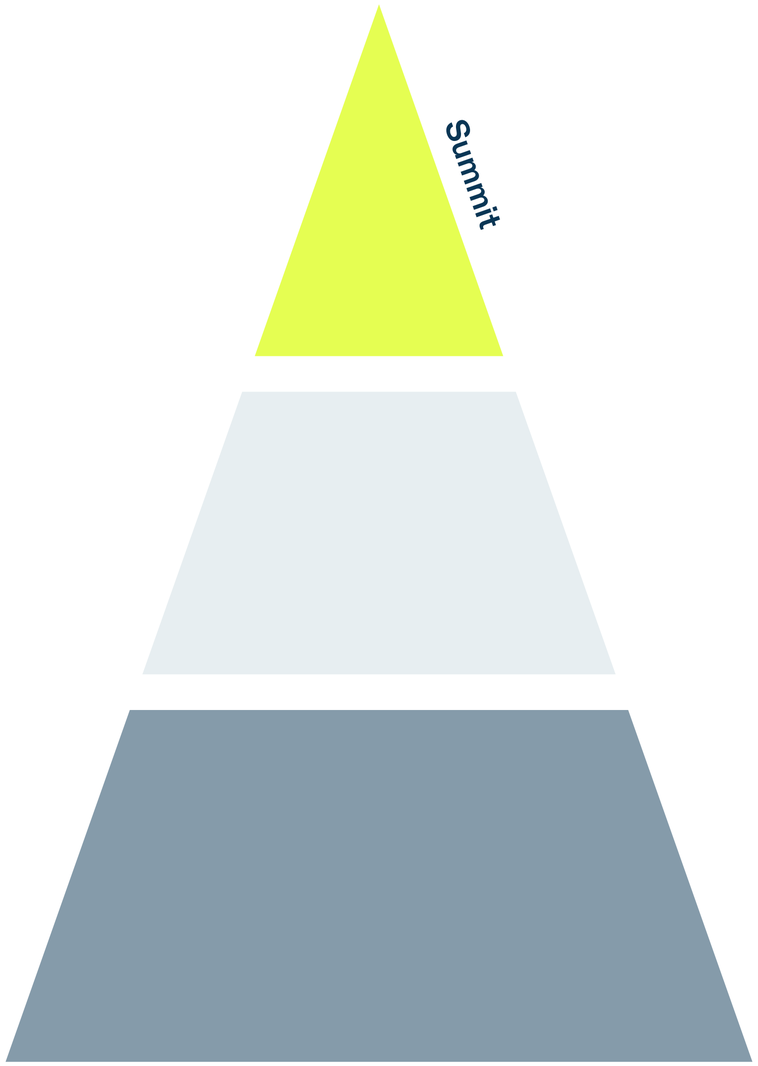
Summit organizations are already operating intelligent, integrated GRC systems. Their next challenge is preparing for agentic AI: systems that can act semi-autonomously within clear boundaries, making smart decisions based on context, thresholds, and real-time inputs.

To stay ahead:

- Ensure contextual intelligence is dynamic and spans all compliance domains.
- Design systems with tiered decision rights, audit logs, and policy-as-code structures that support autonomous action.
- Implement feedback loops so AI learns from regulatory updates and operational outcomes.
- Enable agentic workflows, where AI can trigger audits, file reports, or adapt controls automatically.
- Measure ROI not just in time or cost saved, but in business performance, agility, and risk mitigation.

The goal now is to go from intelligent compliance to autonomous resilience, where systems learn, adapt, and operate at business speed without losing control.

Summit - Scale for autonomy



Key actions

- Ensure contextual intelligence spans all compliance domains dynamically
- Design systems with tiered decision rights, audit logs, and policy-as-code
- Implement feedback loops for continuous AI learning
- Enable agentic workflows (auto-trigger audits, file reports, adapt controls)
- Measure ROI in business performance, agility, and risk mitigation

Milestones

- Deploy AI across multiple GRC domains (6x more likely than Base Camp)
- Achieve 55% predictive modeling adoption
- Reach 70% automated alert implementation
- Enable automated workflow capabilities
- Establish semi-autonomous decision-making within guardrails

Outcomes

- Transform compliance from bottleneck to business catalyst
- Enable real-time regulatory adaptation and simulation
- Prepare foundation for fully agentic AI systems
- Turn GRC into competitive advantage and strategic differentiator

One journey, many starting points

Wherever you are on the AI maturity curve, the path forward is the same: Use today's capabilities to build tomorrow's potential.

High-performing organizations didn't get there by rushing – they advanced step by step, from automating the basics to integrating intelligence to designing for autonomy. What separates leaders is their clarity of vision and the discipline to build toward it.

The most successful teams understand this: Every layer of maturity isn't just about improving compliance; it's about unlocking competitive advantage.

Section 9: Appendix

- **RESEARCH METHODOLOGY**
  The survey included 403 respondents sourced from a leading global online panel provider. They were selected from the panel based on geographic and role-based quotas, as well as screening questions based on role in audit and compliance, decision making role, company size, and how long they have been in their audit role. Selected respondents were further screened based on self-reported audit and compliance knowledge and attentiveness to survey questions.

- **ROLE QUOTAS**
  The survey divided respondents into four broad roles: C-suite 54%, Lead 36%, Manager 8%, Other 2%. Respondents were asked to select which role – from a list of 23 options – most closely described their primary responsibility, even if none were quite right or even if they performed more than one of these roles. Answers were consolidated into those four broad roles.

- **GEOGRAPHIC QUOTAS**
  The survey included respondents from the U.S., Canada, Germany, and the UK.

- **INDUSTRY**
  Although no industry-level quotas were deployed, we monitored the data to ensure that no single industry was over-represented in the data. The final breakdown of respondents by industry is as follows: Financial Services 24%, Insurance 20%, Technology 14%, Retail / Ecommerce 13%, Industrial and Manufacturing 12%, Energy & Resources 8%, Business / Professional Services 3%, Life Sciences (including healthcare and pharmaceuticals) 2%, Telecommunications 2%, and Transportation and Logistics (including supply chain) 1%.

- **RESPONDENT SCREENS**
  - Role: All respondents were required to indicate that they were responsible for or had influence in evaluating and/or selecting audit compliance solutions or software for their organization.

  - Company size: All respondents must self-report that their companies have a minimum of 1,000 employees. All potential respondents from smaller companies were excluded. In total, the survey includes 67% of respondents from companies with 1,000 to 4,999 employees, 24% from companies with 5,000 to 9,999 employees, 4% from companies with 10,000 to 24,999 employees, 3% from companies with 25,000 to 49,999 employees, and 1% from companies with 50,000 or more employees.

  - Time in IT: Respondents must have spent a minimum of 3 years managing, planning, or purchasing compliance and/or cyber risk management software services or infrastructure in order to qualify for the survey. In total, 37% of respondents have spent 3 to 5 years in this role, 51% have spent 6 to 10 years in this role, 11% have spent 11 to 15 years in this role, and 1% have spent 16 years or more in this role.

  - Information level: In our experience, it is possible to have “qualifying respondents” who nevertheless prove to have too little information or knowledge about the space to provide useful data from which to draw insights. We therefore apply an “information” screen to respondents as well. Specifically, we ask whether or not respondents could explain certain terms to their colleagues if asked to do so. In order to qualify for this survey, a respondent must say “yes” to this question for the term “GRC (Governance, Risk, and Compliance)”.

  - “Attention” level: It is easy for respondents to speed through surveys or not pay enough attention to provide useful data. We make an effort to exclude these respondents as well, as they provide generally less useful data. In this survey, respondents were screened out for “attention” reasons if they said they could explain the made-up term “CRISM Framework” to a colleague in the same question used for the Information Screen noted above.

- **RESPONDENT SCREENS**
  It is technically impossible and improper to list a margin of error for a survey of this type. The respondents for this sample were drawn from an online panel with an unknown relationship to the total universe, about which we also do not know the true demographics. As such, the exact representativeness of this, or any similarly produced sample, is unknown.


Optro