SureCloud GRC Survey 2025

Understand the Real Risks and Obstacles Faced by UK Leaders

SURECLOUD®

Executive Summary

87%

87% of Enterprise executives claim preparedness for a major GRC event—but their own survey responses expose systemic, ongoing issues: fragmented tools, manual processes, skills shortages, and budget constraints. Among SMB organisations, 95% of leaders report a similar level of confidence, yet that assurance is built on widespread reliance on spreadsheets, limited resources, and a reactive approach to certification.

"Enterprise" refers to organisations surveyed with greater than 1,000 employees, whilst "SMB" covers those organisations with 51 to 1,000 employees.

"Scaling or growing teams" are those with fewer than 25 dedicated GRC employees. 63% of SMBs had only between 1-5.

How can both groups project readiness while facing deep operational cracks? This disconnect is the central tension, the “risk reckoning”, facing UK organisations today.

By integrating insights from both segments for the first time, this report highlights the growing pressures on SMBs who are often overlooked in GRC (but are now facing real uncertainty about how to move forward) as well as the persistent operational gaps undermining enterprise confidence. Together, these findings reveal the disconnect between perception and reality that continues to define governance, risk and compliance (GRC) management in 2025.

For large enterprises, complexity and multi-framework compliance drive inefficiency and persistent blind spots. For SMBs, resource scarcity and fragmented manual controls create a different, but equally dangerous landscape.

Across all sizes, the real risk is not a breach or audit failure, but the mistaken belief that legacy methods- spreadsheets, manual workarounds, and disconnected tools, offer genuine control. Even the organisations that feel most prepared continue to face major breaches, underscoring the gap between perceived confidence, actual practice and true resilience.

Across this report, SureCloud has uncovered where these perceptions diverge from reality, what is uniquely challenging in each segment, and how leaders can close the gap between confidence and capability.

> “The biggest risk isn’t a breach or fine. It’s thinking everything is under control when it isn’t.”

Introduction – The New Realities Facing GRC Leaders

UK businesses of every size face unprecedented pressure to manage risk, maintain compliance, and adapt to fast-evolving regulatory demands. But the true experience of governance, risk, and compliance (GRC) is anything but uniform.

For large enterprises, the landscape is dominated by complexity: sprawling business structures, layers of oversight, and the constant challenge of integrating multiple frameworks and technologies; a scale of responsibility that often exceeds the capacity of even well-established, but relatively small, GRC teams.

Smaller organisations are also navigating the same regulatory environment, but must do so with even leaner teams, smaller budgets, and limited capacity or knowledge that clouds their vision.

On the surface, confidence in GRC programs remains strikingly high. Enterprise executives, backed by significant investment and formal policies, are quick to cite preparedness and board-level engagement. SMB leaders, meanwhile, take pride in agility, visibility, and the ability to do more with less.

Yet beneath the optimism, both segments acknowledge ongoing struggles: persistent manual workarounds, fragmented tools, skills shortages, and the relentless pressure to "do more with less." For many, the real challenge isn't a lack of ambition, it's the operational reality of sustaining GRC maturity amid resource and complexity constraints.

For the first time, SureCloud's Risk Reckoning brings together these two perspectives in a unified study. Drawing on survey data from nearly 200 executives and leaders across the market in both large enterprises and small businesses, this report delivers the UK's only end-to-end GRC maturity snapshot.

By directly comparing the experience of enterprise and SMB organisations, it surfaces not just universal truths and sector-wide challenges, but also the unique pain points and opportunities for progress that define each segment.

The Goal: Closing the persistent gap between GRC confidence and capability, making it easier than ever for teams big or small to improve their security posture.

Who Should Read This?

For Enterprise GRC Leaders

If you're responsible for risk, compliance, or audit across a large, complex organization, this report provides a reality check on operational blind spots and strategic opportunities.

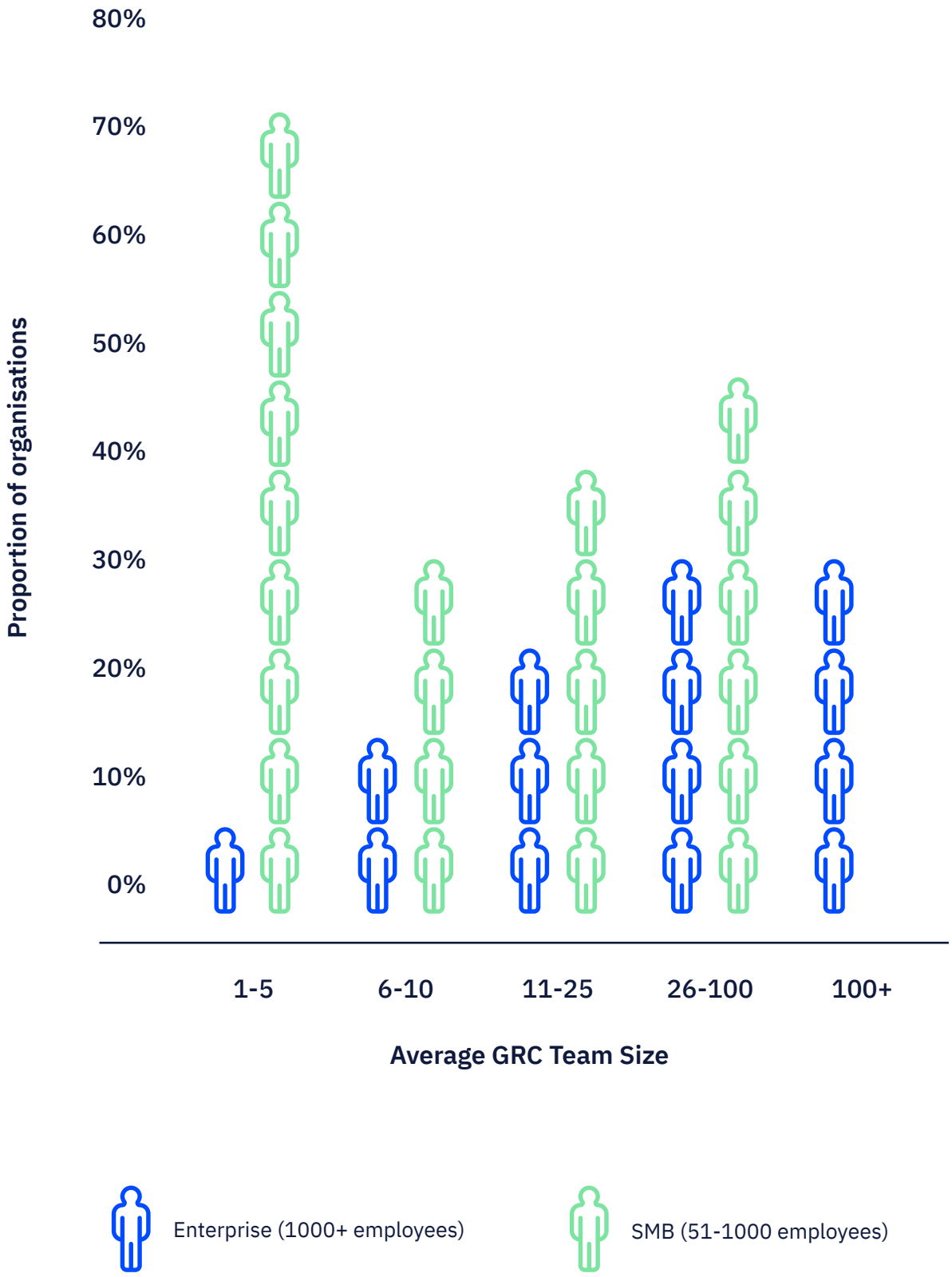
For Mid-Market & SMB Teams

If you manage risk and compliance in a smaller organization this report surfaces those unique challenges for lean teams. Discover practical strategies to move beyond spreadsheets, automate the essentials, and achieve real control and resilience, even with limited capacity.

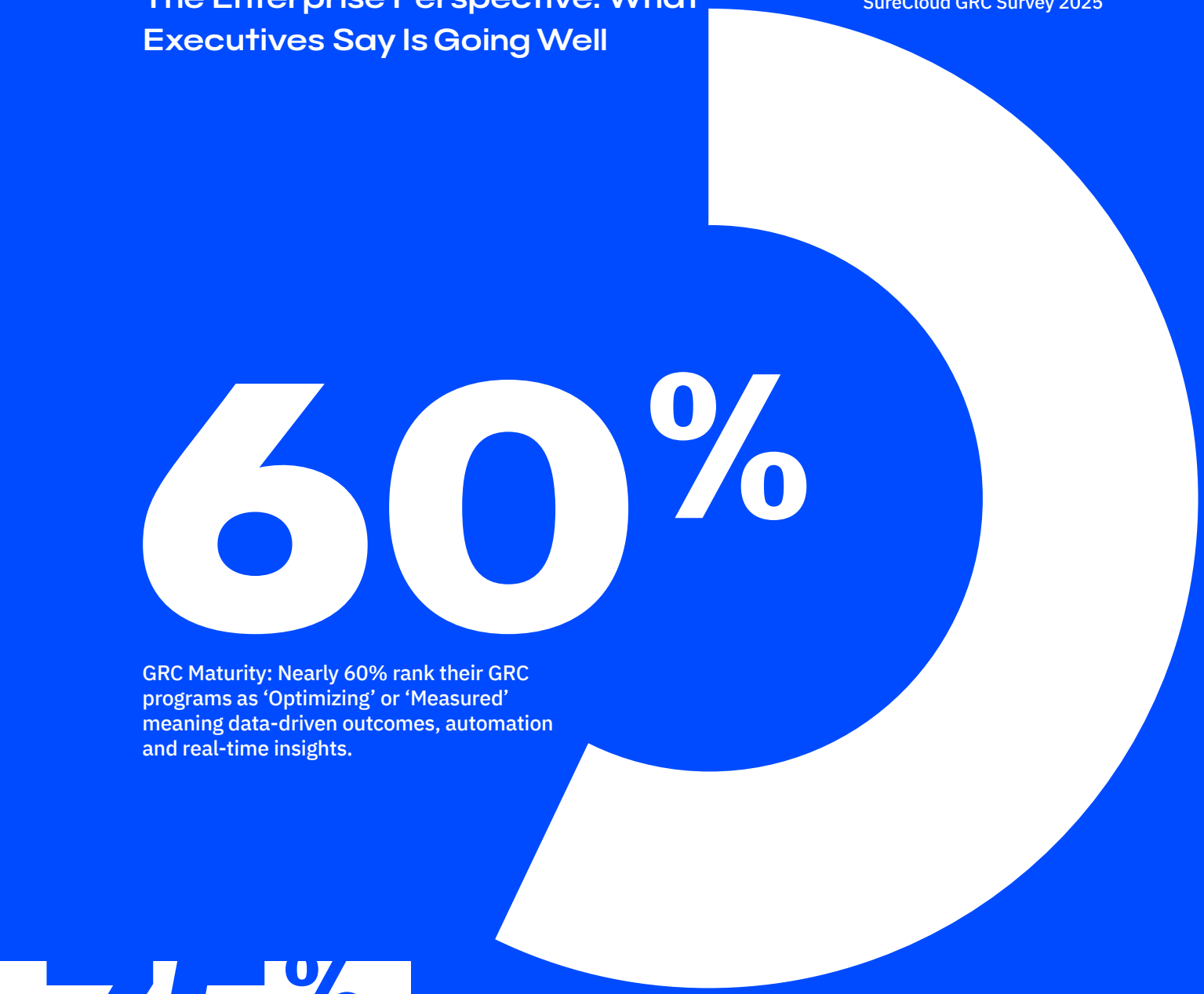
For Advisors, Consultants, and Solution Partners

If you advise or support UK organisations on risk and compliance, this analysis offers data-driven insights to sharpen your recommendations. Understand what's working, what isn't, and where your customers need the most help- whether they're navigating enterprise complexity or SMB realities.

GRC Team Capacity by Business Size



The Enterprise Perspective: What Executives Say Is Going Well



60%

GRC Maturity: Nearly 60% rank their GRC programs as ‘Optimizing’ or ‘Measured’ meaning data-driven outcomes, automation and real-time insights.

75%

Board Engagement:

GRC is discussed at board level in 75% of firms with nearly half of this figure addressing it in 2/3rds of meetings.

59%

Resource Investment:

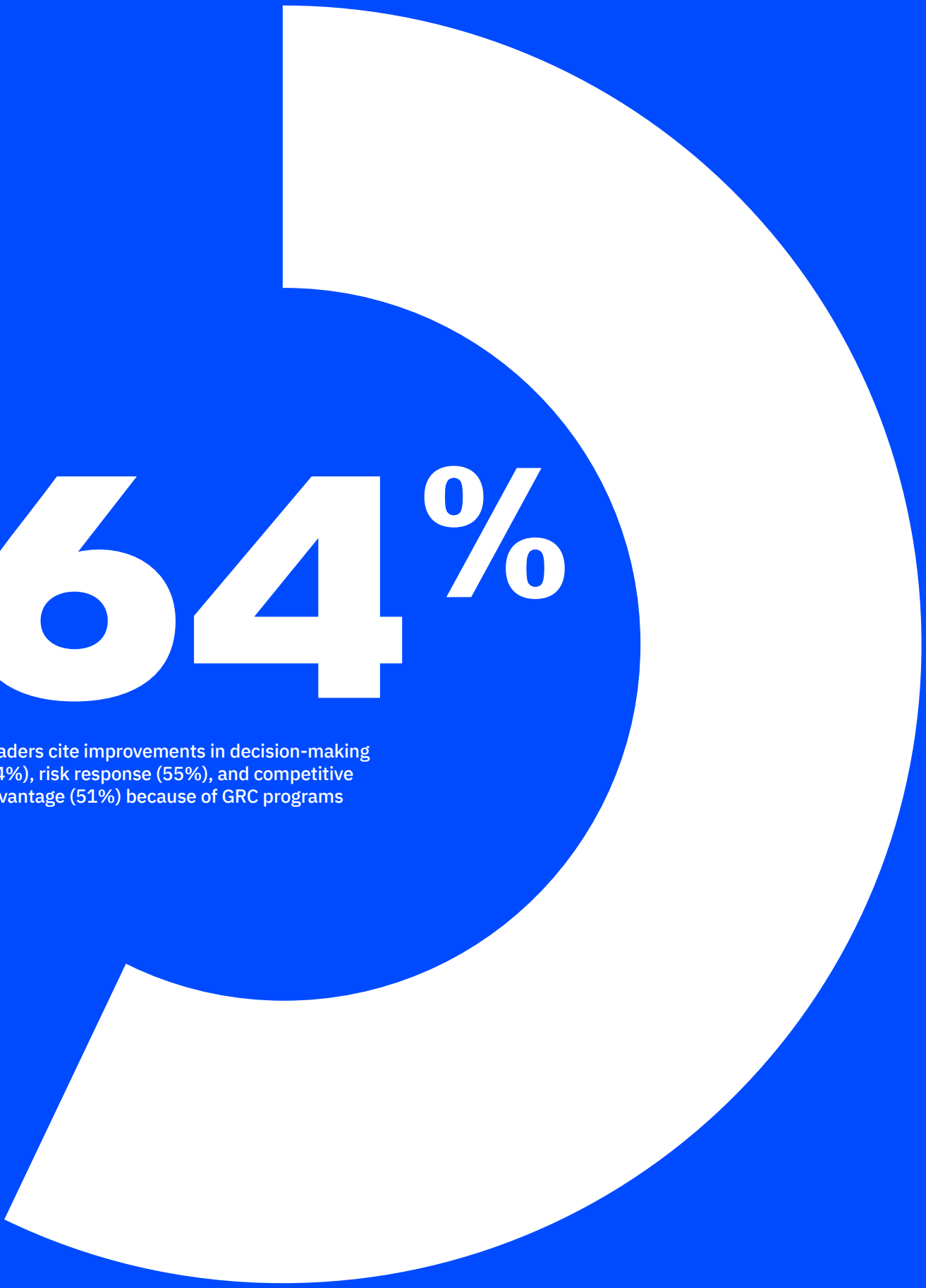
59% of firms have 25+ full-time GRC staff; 28% have 100+.

74%

Integrated Tooling:

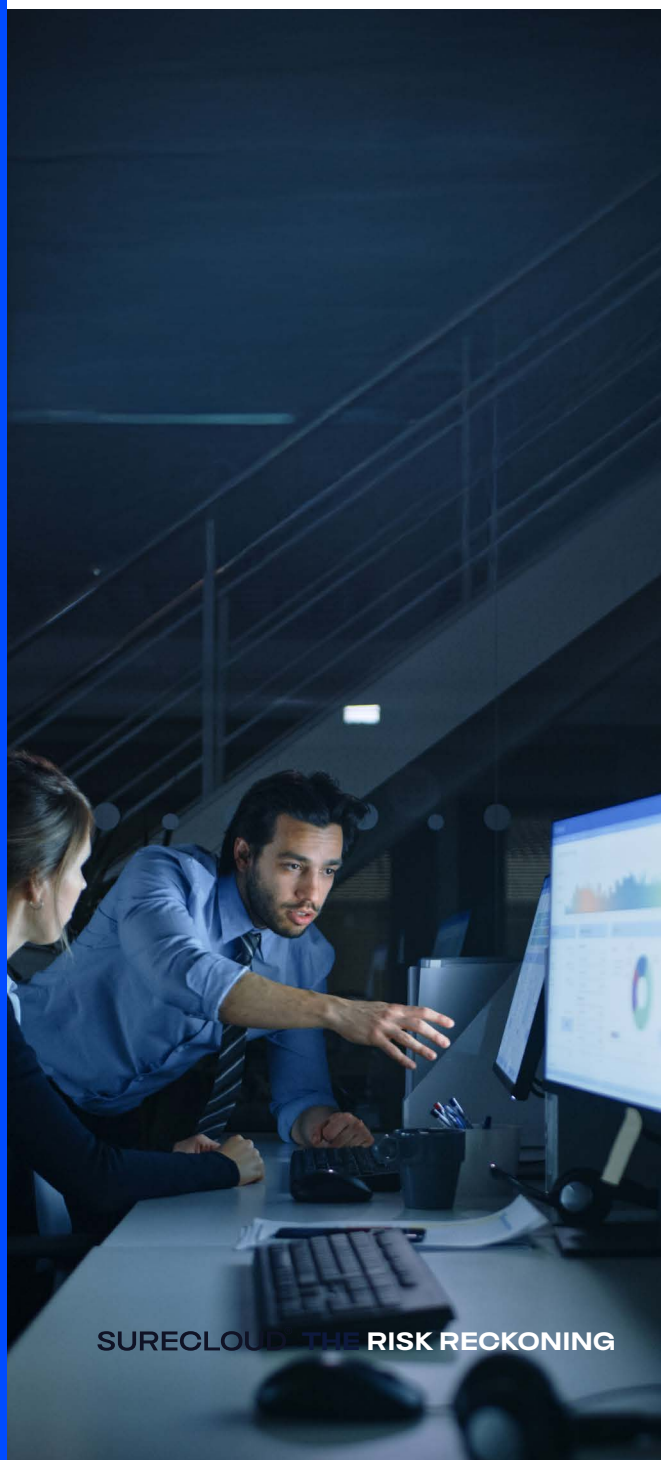
Enterprises enrich GRC tools with further point solutions providing threat intelligence (74%), continuous controls monitoring (67%), and automated reporting (66%).

Tangible Business Impact



Leaders cite improvements in decision-making (64%), risk response (55%), and competitive advantage (51%) because of GRC programs

Enterprise leaders across the UK are outwardly optimistic about the state of their GRC programs and when asked directly, they point to several clear indicators of success:

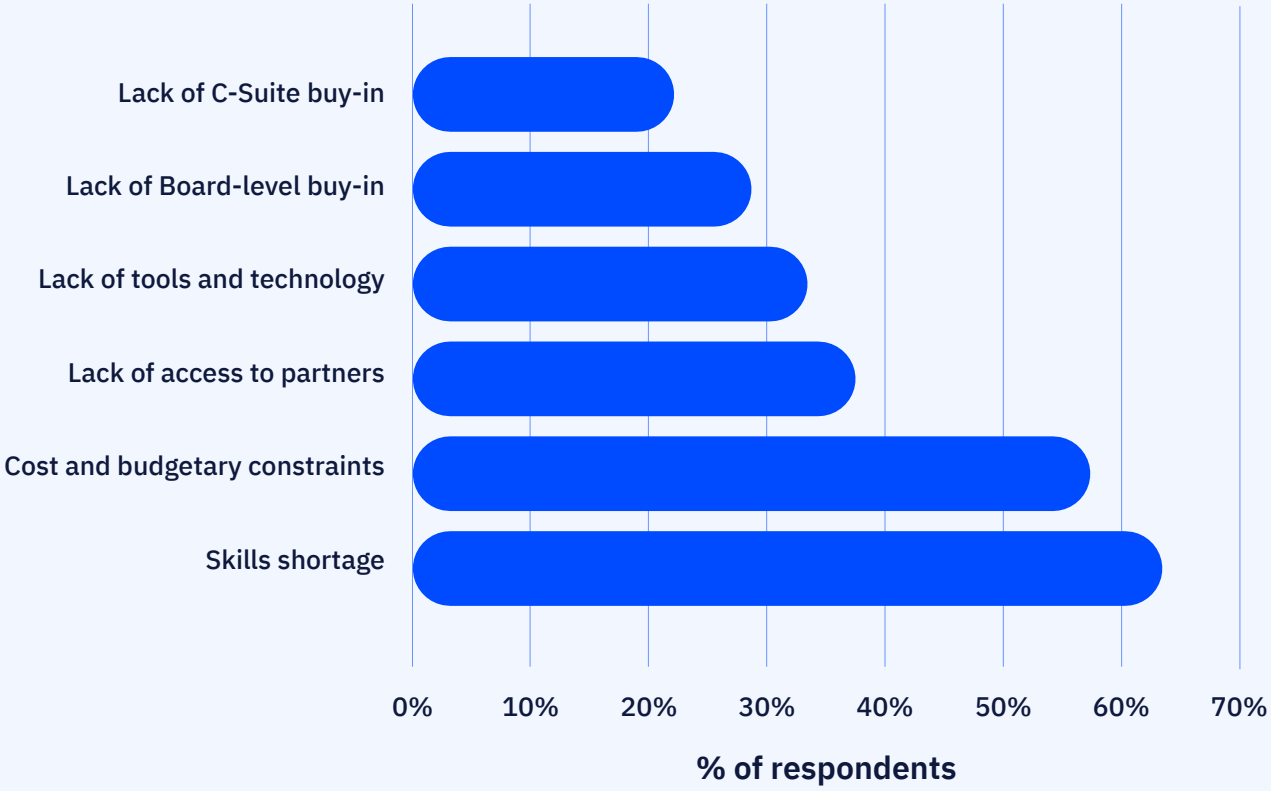


- **Significant investments:** Most organisations (59%) have dedicated more than 25 full-time employees exclusively to GRC tasks, and over a quarter (28%) employ 100 or more. On top of their chosen GRC platform many enterprises are also buying advanced point solutions around cyber threat intelligence (74%), real-time controls monitoring (67%), and automated reporting (66%).
- **Engaged stakeholders:** At 75% of companies GRC is regularly discussed at board meetings. Nearly all C-level executives (90%) and most board members (64%) are directly involved in key governance decisions.
- **Measurable benefits**: Executives note tangible business improvements since actively measuring GRC effectiveness, such as better decision-making (64%), better response capabilities (55%), and competitive advantage (51%).
- **High maturity and preparedness:** Most business leaders consider their programs mature, with nearly 60% rating them “Optimizing” or “Measured,” and a full 87% claiming their organization is prepared to handle a significant GRC event today.

Things look solid from the top when GRC works by most conventional measures. Based on these results alone, executive optimism is relatively easy to justify, and many organisations seem truly prepared.

But there’s more here than meets the eye. Most of these metrics depend on what organisations choose to measure and how well they report it. A closer look at the rest of the survey results reveals a much different, more complex, and nuanced story.

Top Barriers to GRC Effectiveness for Enterprises



The Reality Check

63% **Talent & budget gaps:** lack internal GRC expertise; a further 57% cite constrained budgets.

49% **Regulatory overload**: enterprises manage 5+ major regulations and struggle to keep up.

60% **Manual workflows:** 60% of enterprises still rely on spreadsheets; 64% use manually created dashboards.

62% **Fragmented tooling:** use 4+ GRC tools whilst less than half have integrated them.

Despite projections of confidence by leaders, the reality for their practitioners is knowledge gaps, manual workflows and distributed data sets. The benefits of board involvement and high tool investment are lost as different departments and global regions are forced to collaborate and find meaning in a complex IT, cyber or enterprise technology ecosystem.

The Foundations Perspective: What SMB Leaders Say is Going Well

Smaller organisations share some similarities to those larger enterprises, reporting high levels of GRC confidence, even in the face of resource and staffing constraints.

When surveyed, leaders highlighted several key strengths and points of pride:

- **Resourceful teams:** SMB GRC professionals consistently "make it work," leveraging spreadsheets and manual processes to maintain oversight and adapt to evolving regulatory demands. Even when dedicated tools or budgets are limited, 70% believe they have adequate to even high capacity with flexibility for additional or urgent tasks.
- **Agility and adaptability:** Smaller teams cite agility as a core advantage, emphasizing their ability to pivot quickly and address compliance requirements on short notice, often without formalized process or large-scale systems.
- **Commitment to capability:** Despite limited headcount, 2/3rds of small teams rate their own GRC capacity as "moderate to good," meaning they cover the essentials but occasionally face some weakness. However this is underscored by a strong culture of accountability and willingness to improve. 31% had made their first investment to either an in-house solution or a legacy GRC platform.
- **Growing leadership engagement:** Board and executive attention to GRC is on the rise, as leaders recognize the increasing impact of risk and compliance on organisational outcomes, even if formal engagement trails larger organisations.

From a distance, these factors suggest scaling teams are confident, adaptable, and determined to maintain compliance regardless of circumstance. The numbers point to a clear sense of preparedness and ownership. Yet, as with their enterprise peers, a closer look at the survey data reveals persistent challenges beneath the surface and a more complicated path to sustainable GRC maturity.

93%

Incident Confidence:
SMB GRC leaders believe their teams are prepared for a major GRC event.

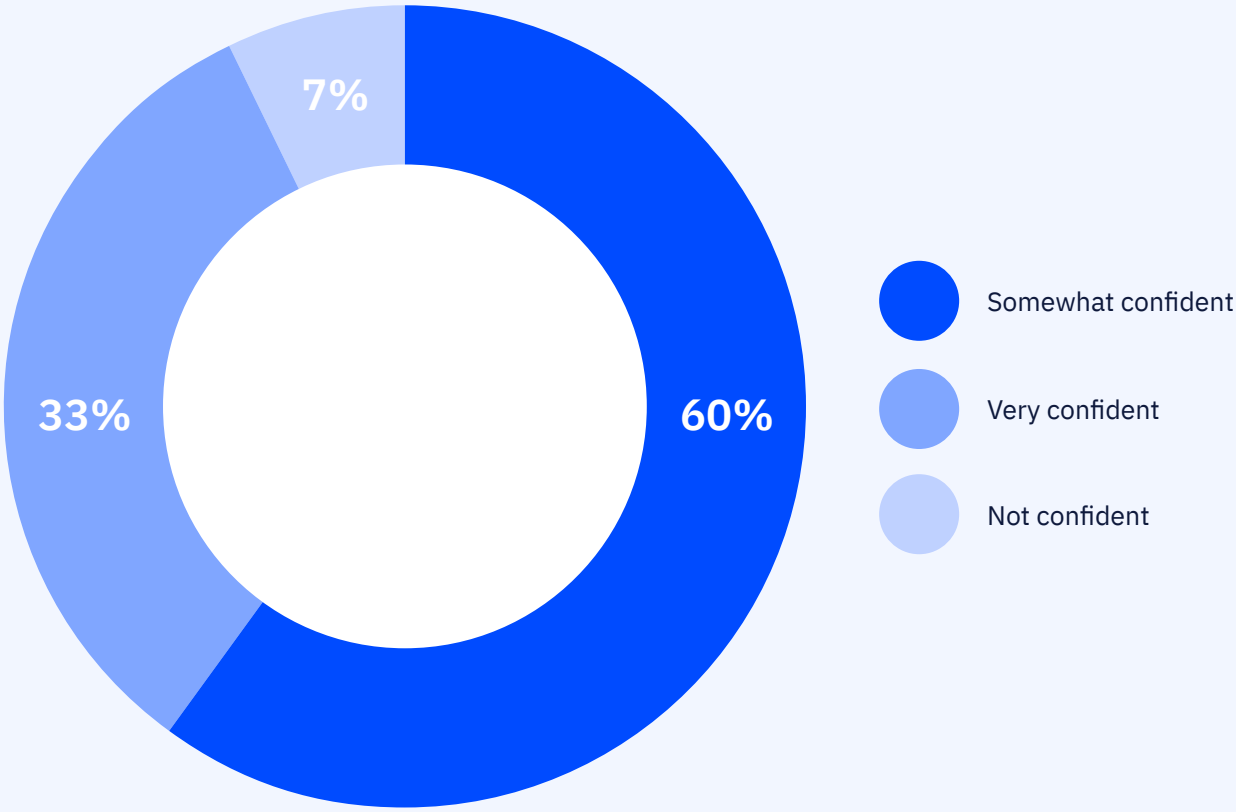
86%

Affordable Methods:
of all SMB respondents use spreadsheets or manual processes in some capacity, credited primarily due to their affordability and ease of use.

63%

Perceived Capability:
Nearly 2/3rds of small teams rate their GRC capability as "moderate to good."

Confidence of SMBs Against a Major Compliance or Cyber Incident in the Next Year



The Reality Check

86% **Spreadsheet reliance:** 86% of SMB organisations use spreadsheets and other manual methods; among teams with 1–5 GRC professionals, this rises to 100%.

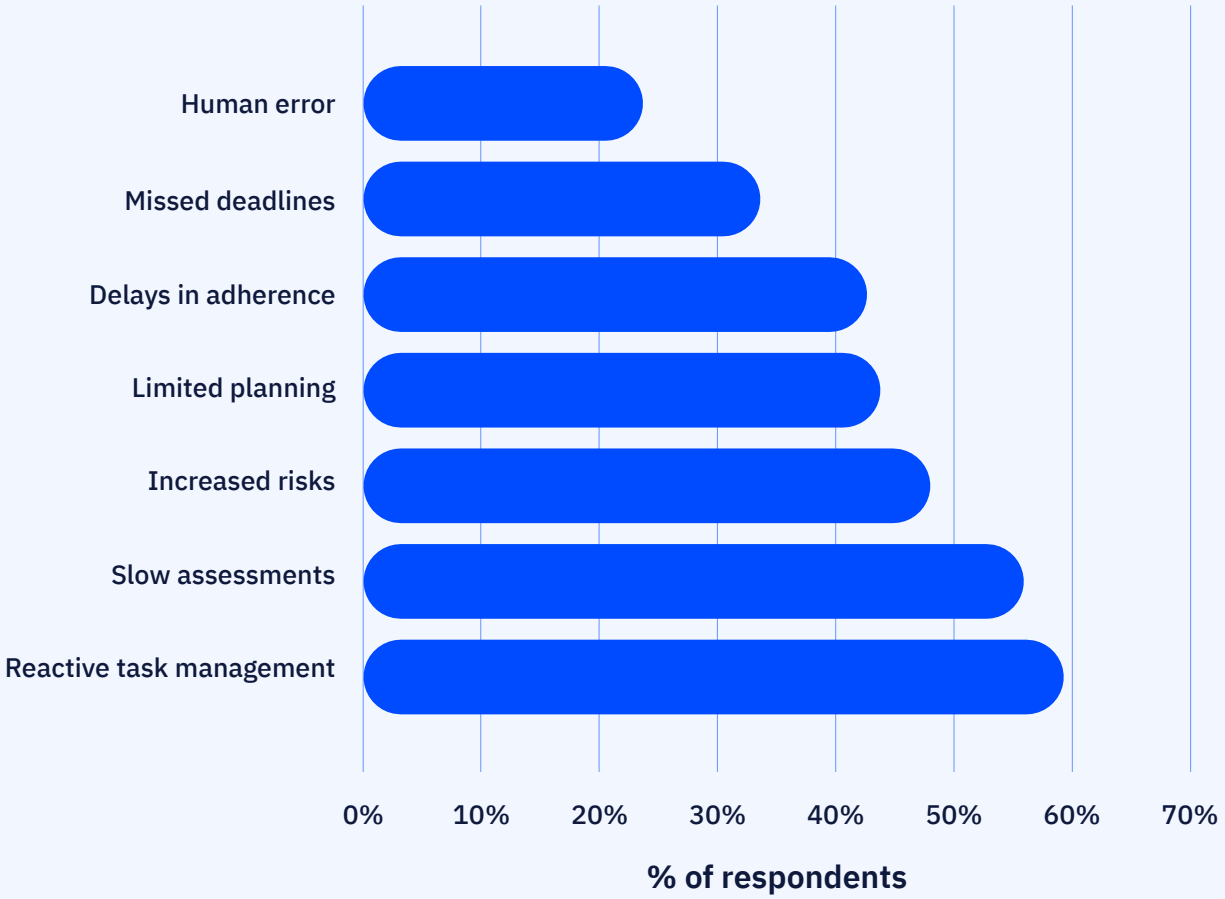
84% **Capacity strain:** 84% of SMB respondents cite limited team capacity as the main cause of reactive task management and slow risk assessments.

41% **Breach exposure:** 41% of SMB organisations have experienced a breach in the past 36 months.

58% **Reactive State:** cite reactivity as the biggest barrier to their effectiveness. Meanwhile only 6% believe they have the resources to be proactive. Low budgets keep SMBs reliant on spreadsheets, with cost and simplicity as the top two drivers for remaining. Most teams only consider switching to modern GRC platforms in response to incidents, rather than as a proactive measure.

Despite a belief in their capability and preparedness for an event, many SMB teams suggested a reality that highlighted their own knowledge gaps. Heavy spreadsheet reliance, slow assessment processes and a high proportion of data breaches shows an overconfidence that needs to be addressed not just with a larger investment but smarter methods.

Top barriers to GRC effectiveness for SMBs



Executives in both segments project confidence, but survey responses uncover meaningful contradictions about the state of GRC.

"... less than half having achieved full integration."

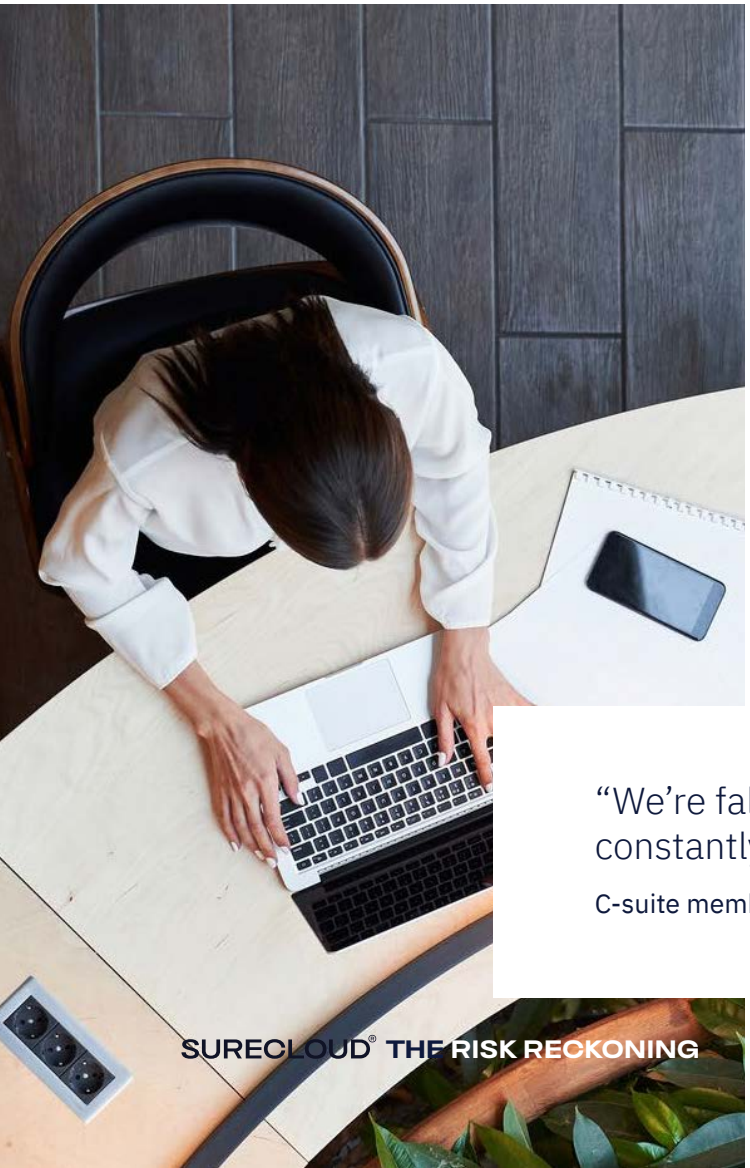
- **Tools and processes are fragmented:** Among Enterprises, organisations use multiple different GRC tools or processes, with less than half having achieved full integration. In SMBs, tool fragmentation is less about paid software and more about the layering of spreadsheets and manual, informal solutions. In both groups, disconnected approaches limit real-time visibility and slow down effective decision-making.
- **Manual workflows persist:** 60% of Enterprises and 86% of SMBs rely on spreadsheets for at least some of their GRC processes. Among the smallest SMB teams (those with 1–5 dedicated GRC professionals), spreadsheet use is universal.
- **Talent, budget, and capacity gaps:** Nearly 2/3rds of Enterprise respondents cite skills and budget shortages as barriers to GRC advancement. In SMBs, over 1/2 say limited team capacity and lack of specialist skills force them into reactive practises. GRC responsibilities are either distributed across multiple roles or shared against multiple responsibilities, heightening the risk of oversight lapses.
- **Persistent risks and incident-driven change:** Cyber threats, data privacy, and regulatory demands are top concerns for both groups. 41% of SMB organisations have experienced a breach in the last three years, often serving as the trigger for modernisation or tooling upgrades, rather than a proactive motivation.

These contradictions don't undermine overall optimism, but they do complicate it. For both Enterprises and SMBs, the combination of fragmented tools, manual processes, and resource gaps leaves significant blind spots and operational risk. Closing the gap between confidence and control remains the defining challenge.

Enterprise	SMB
Optimism masks operational blind spots	Confidence hides resource constraints and manual workarounds
Disconnected systems limit real-time visibility and slow decision-making	Reliance on spreadsheets and informal processes leads to unseen vulnerabilities
Persistent GRC problems become normalised, and innovation feels risky	Capacity and expertise gaps force teams into reactive, incident-driven management

Enterprise confidence is high, but the scale and complexity of GRC infrastructure can create significant, often invisible, challenges. When programs appear mature supported by dedicated teams and advanced tooling, it's easy to miss the cracks beneath the surface. Issues like tool sprawl, reporting delays, and incremental risk become routine rather than triggers for improvement.

As a result, progress slows and innovation can stall. Programs that seem stable from the outside may operate in a cycle of maintaining the status quo, rarely interrogating the systems and assumptions that create their risk posture. The more mature a GRC function appears on paper, the less likely leaders are to ask what's still missing.



For small businesses and mid-market organisations, the challenge is fundamentally different: less complexity at scale, and more about sustaining control with fewer resources.

It is rare for teams to have the luxury of proactive GRC improvement. Over half of SMB respondents cite limited team capacity as their biggest operational barrier. Whilst leaders are proud of their ability to "make it work," this normalization of workaround culture can leave major risks undetected until a crisis forces change.

Progress is measured in survival and compliance rather than transformation. As a result, many SMB teams remain in a perpetual cycle of reaction, firefighting, and incremental fixes, without the bandwidth or resources to build lasting resilience.

> "We're falling behind when it comes to constantly changing regulations."
>
> C-suite member of a £1 bn+ revenue organisation

Openly acknowledging the challenges facing GRC is uncomfortable, but it's essential for progress.

For many organisations, the "risk reckoning" begins when leaders choose to confront not just the most visible threats, but the operational gaps fragmented tools, manual workarounds, skills shortages, or capacity constraints that have become business as usual.

For enterprises, these gaps are often hidden behind complexity. Mature programs can mask real issues under layers of process, investment, and reporting. Integration is elusive, and persistent challenges like tool sprawl, delayed insights, and regulatory fatigue can become normalized, slowing real improvement. As a result, risk is not just an external threat, but a by product of systems that look robust, but struggle to adapt.

For SMBs or scaling GRC teams, the reckoning is shaped by resource limitations. Confidence and agility have helped teams survive, but the cost is perpetual overwork, fragmented oversight, and vulnerability to the unexpected. The normalization of spreadsheets, workarounds, and reactive management creates gaps that only become visible when incidents force a change. Without new approaches, teams risk being stuck in a cycle of firefighting and incremental fixes.

But this reckoning is also an opportunity. When leaders in both large enterprises and growing teams recognize that persistent challenges are not signs of failure—but signals for improvement—they can move from optimism to action.

- **Better visibility means better decisions:** Whether it's integrating separate tools, simplifying the stack, or performing a complete audit of all IT assets, gaining a comprehensive real-time view of risk and compliance is the key to targeted and proactive actions.
- **Clarifying accountability and responsibilities reduces cost and confusion:** Both enterprises and SMBs benefit when GRC roles are explicit, evidence is easy to collect, and reporting isn't an afterthought.
- **Fixing persistent challenges supports retention and resilience:** Modernizing workflows reduces burnout, increases satisfaction, and allows scarce expertise to be used strategically, not just tactically.
- Maturity is a differentiator: Whether through platform integration, smarter workflows, or clearer reporting, organisations that can demonstrate true control, not just the appearance of it, will stand out to customers, partners, and regulators alike.

Risk isn't going away. If anything, it's multiplying. The organisations most willing to face uncomfortable truths about their GRC posture and address them will be best positioned to respond, recover, and lead.

Strategic Takeaways for Action

01

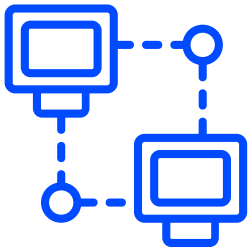
Improve visibility for better decisions:

Integrated platforms (for Enterprises) or consolidated processes (for SMBs) are key to accurate risk awareness.

02

Clarify accountability:

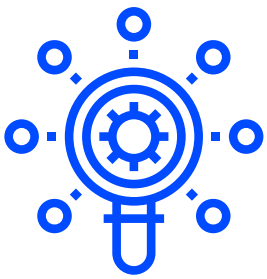
Streamlined roles and clear responsibilities reduce confusion and compliance costs across all organization sizes.



03

Fix what's broken:

Modernizing outdated workflows, whether integrating technology or reducing manual work prevents burnout and attrition.



04

Challenge the status quo:

Maturity doesn't just mean 'optimised'; leaders in both large and growing teams must reassess assumptions continuously.

Enterprise vs. SMBs: GRC at a Glance

	Enterprise	SMB
Confidence in GRC Preparedness	87% claim preparedness for a major GRC event	95% claim preparedness; confidence often based on manual methods
Main GRC Tools	60% use spreadsheets (alongside other tools); but dedicated GRC platforms more common	86% use spreadsheets; 100% of 1–5 person teams rely on them as main or supplementary tool
Integration & Fragmentation	62% use 4+ GRC tools, only 45% have integrated platforms	Average of 2 tools. Most have fragmented, manual/informal solutions (spreadsheets, email).
Resource & Capacity Gaps	63% report skills gaps; 57% cite budget constraints	Over half cite limited team capacity as a key barrier
Regulatory Burden	49% struggle to keep up with 5+ major regulations	Regulatory deadlines are a top driver for modernisation
Board/Leadership Engagement	GRC discussed at board level in 75% of firms	Engagement increasing, but less formalized
Drivers for Tooling	Investment in automation, cyber intelligence, reporting	Cost and simplicity are top drivers; modernisation is often crisis-driven
Persistent Risks	Cyber threats, regulatory complexity, talent shortages	Same, but amplified by small team size and reactive approaches

Whilst the gap between perception and reality is vast, this hasn't stopped an ambitious motivation for the future.

Top 5 UK Certifications of 2025	Respondents covered / chasing
UK GDPR (UK's specific General Data Protection Regulation)	73%
Technology Code of Practice (TCoP)	62%
ISO/ IEC Standards (e.g. ISO 27001)	50%
NIST Framework (from the U.S. National Institute of Standards and Technology)	49%
EU NIS2 Directive (Network and Information Security Directive 2)	47%

Respondents at both the enterprise and SMB scales showed a clear weighting towards UK and EU regulations, with data privacy and commercial technology standards as the number one drivers either due to associated fines or barriers to partnership for non-compliance. North American regulations like SOX, SOC2 and HIPAA appeared only for organisations with global operations

Top 5 Desired GRC Capabilities	Representative respondents
Real-time risk intelligence	55%
Continuous controls monitoring	53%
Regulatory change alerts / notifications	45%
AI based monitoring and insights	38%
Cross-entity mapping	18%

VS

Top 5 GRC Objectives for 2026	Representative respondents
Strengthening broader cyber security	47%
Leveraging AI for human efficiency	46%
Improve risk-insights in decision making	42%
Enhance visibility and oversight	38%
Standardize GRC processes	34%

When it comes to objectives and improvement, leaders know where they want to go; there's a desire for more AI, better oversight and stronger ties between GRC and cyber, but they are still navigating how to get there, with a gap in what that looks like for technology capabilities.

Organisations want AI to help their teams work smarter, but only a third are asking for AI features in GRC tooling. There's a top-down intent to use AI, but little knowledge of how it can practically help and an uncertainty in the new risks that generative AI or LLMs present once adopted.

Likewise, whilst process maturity is seen as important, there's no clear consensus on what tools will get them there, with risk and compliance capabilities overstating governance with little mention of workflows or policy.

What is certain, is that traditional tools are being less emphasized with a preference for proactive and intelligent systems (real time alerting, AI efficiencies and automation) over static dashboard reporting.

For both Enterprises and SMB organisations, the path forward in GRC is not just about adding tools or updating policies- it's about building a sustainable, adaptive, and visible control environment that scales with risk.

SureCloud's vision for the future of GRC is unified and actionable:

01 **Built for risk prevention and continuous compliance:** Enterprises and growing teams alike will need to shift from reactive, fragmented workflows to integrated, real-time oversight. For large organisations, this means leveraging intelligent platforms to consolidate multiple systems, automate evidence collection, and surface risk insights across complex business units. For SMBs, it means moving beyond spreadsheets, adopting processes and tools that make compliance effortless, minimizing manual workload, and providing true visibility without breaking the budget.

02 **Confidence, best practice, and assurance- delivered faster:** Regardless of size, organisations that put visibility at the heart of GRC will gain the agility to keep up with regulatory change, respond to incidents, and drive continuous improvement. By making risk, compliance, and controls easy to monitor and act on, leaders can future-proof their businesses, designing innovative products, launching new services, or entering new markets without losing control and facing financial, legal or reputational damages.

03 **The real risk isn't just a breach or fine, it's thinking everything is under control when it isn't:** In both Enterprises and SMBs, the danger lies in assumptions. SureCloud enables leaders to move beyond surface-level confidence, with practical, data-driven insights that drive improvement and assurance for every level of maturity.

The next generation of GRC is about delivering real-time insights and targeted automation. SureCloud offers two platforms to meet this challenge:

FOUNDATIONS

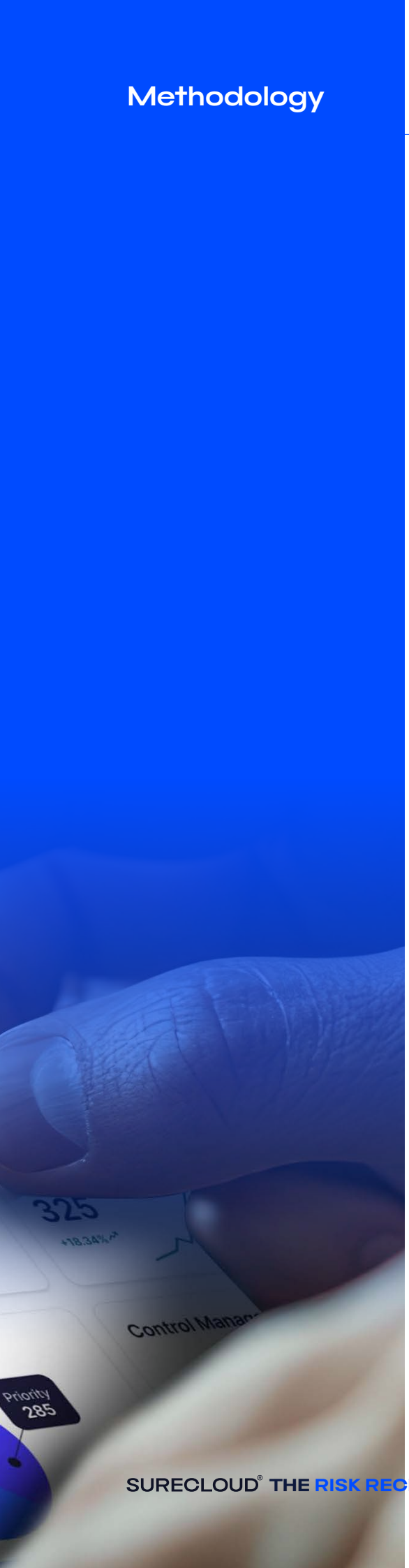
Foundations, our purpose-built solution designed specifically for growing teams and SMBs. Designed for effortless control, Foundations ensures quick compliance towards frameworks like ISO/IEC 27001, GDPR and SOC2 through ready-to-use controls, unified first and third-party risk management, and reporting that focuses on the impact of your decisions and lets you move away from spreadsheets.

ENTERPRISE

And Enterprise, the most intelligent GRC platform. Powered by event-sourced architecture, SureCloud helps teams prioritise what matters most with contextual risk scoring, cross-framework control mapping and real-time reporting that puts outcomes at the forefront. SureCloud Enterprise lets mature teams scale with confidence, simplifying their GRC complexity and refocusing towards organisational resilience.

Whether you're scaling up or already managing complex environments, SureCloud enables you to put visibility and control at the heart of your GRC strategy. Because only when you can see what's coming can you decide what happens next.

Methodology



Enterprise Segment

Report findings are based on a survey and select interviews of 152 UK senior executives working in GRC roles at organisations with revenue of over £50m, conducted by CIO Dive on behalf of SureCloud. 81% of those polled held a C-suite role, with the remaining 19% describing their job as EVP, SVP, or VP. Respondents were from a range of industries, including technology, information & communication, manufacturing, retail, transportation & logistics, and financial services. The research took place between March and April 2025.

Foundations Segment

Survey of 43 UK executives and middle management in organizations between 51–1,000 people, conducted by SureCloud via the Wynter research platform. 35% of those polled had a C-suite role, the rest were intentionally selected from senior management positions across information security and compliance. Titles included Head of, Director, and Lead. Respondents represented a range of industries, including government, non-profit, technology, financial services, and real estate. The survey took place in July 2025.

SureCloud Summary

SureCloud Ltd. has two decades of experience as a leading provider of Governance, Risk, and Compliance (GRC) solutions since its founding in 2006. Headquartered in the UK, with offices in the US, SureCloud supports a global portfolio of organisations with its holistic and intelligent GRC platform. Whether addressing cyber risk, data privacy, third parties, or compliance demands, SureCloud has a proven record of empowering organisations to continuously identify, manage and automate their risk and regulatory alignment.