Optro

When business continuity fails

Why plans collapse under real-world stress and the 2030 mandate for organizational resilience

Foreword

Business resilience: The defining enterprise opportunity of the next decade

Today's organizations face a complex environment shaped by geopolitical instability, cyber conflict, climate disruption, economic fragmentation, workforce volatility, and accelerating technological change. In this context, static recovery plans and documentation-driven approaches are inadequate, often with significant material consequences.

Sandro Boeri
Internal Audit Thought Leader
Risk Audit

Regional findings across Europe, the UK, and the Middle East highlight rapidly evolving resilience landscapes, each shaped by distinct challenges.

In Europe, while organizations traditionally prioritize regulatory alignment, structured oversight, and compliance, broader macroeconomic pressures are shifting priorities. Rising concerns around demographic shifts, workforce sustainability, energy security, and economic fragmentation are pushing resilience efforts beyond baseline compliance toward long-term operational viability.

The UK demonstrates an advanced understanding of resilience concepts, such as impact tolerances and severe-but-plausible scenarios. Yet, gaps in third-party concentration risk, dependency visibility, and operational evidence reveal ongoing challenges in translating regulatory frameworks into actionable capabilities.

In the Middle East, particularly in the UAE, rapid digital transformation and an ambition for resilience are evident. However, the speed of implementation often outpaces governance maturity, leading to unique challenges stemming from geopolitical tensions and reliance on expatriate workforces.

The strongest organizations of the future are unlikely to distinguish themselves merely by having plans, but by maintaining visibility, agility, integrated governance, and workforce capability during periods of disruption.

Richard Chambers
Senior Advisor, Risk & Audit
Optro

More than five decades in and around the internal audit profession have given me a particular vantage point on risk. As a chief audit executive and CEO, I have seen organizations navigate financial crises, regulatory upheaval, and seismic shifts in the operating environment. Each era brought hard lessons, but this one is fundamentally different.

We are living through the era of permacrisis. Disruption isn't episodic. It's continuous, interconnected, and compounding.

I experienced this firsthand during COVID-19, while serving as president and CEO of The Institute of Internal Auditors. Our business model depended on candidates successfully completing certification programs at testing centers around the world. When the pandemic hit, those centers closed overnight. In-person testing was shuttered and our continuity plans had not envisioned any scenario in which that could happen.

Yet within five weeks, we transitioned to remote proctoring, something we had never attempted. What made it possible wasn't a single recovery plan, but a clear understanding of our mission-critical processes, along with employee commitment and organizational adaptability. The takeaway was clear: continuity is not about recovering technology. It's about preserving the business itself.

I learned a valuable lesson about business disruption: continuity is a strategic capability earned through honest testing, rigorous scenario planning, and the culture to act decisively under pressure.

This report offers grounded, practical insight for organizations committed to building the resilience needed to lead through continuous disruption — today and into the 2030s.

Table of contents

Introduction

The enterprise operating model has fundamentally changed, operating across AI systems, distributed workforces, SaaS ecosystems, third-party vendors, global supply chains, and cloud providers. Every dependency is interconnected, creating layers of operational complexity in which disruptions rarely remain isolated. An outage, cyber incident, supplier failure, or regional event in one part of the business can quickly cascade across systems, teams, geographies, and critical operations — often faster than documented response plans can activate.

When a live crisis applies pressure to the enterprise, these fragmented systems fail. Recovery targets are missed, fragile dependency mappings don't hold up, and catastrophic third-party incidents surface in pockets of the organization that leadership assumed were insulated.

75%
of recovery targets were missed

31%
of impacted business processes were not accurately mapped

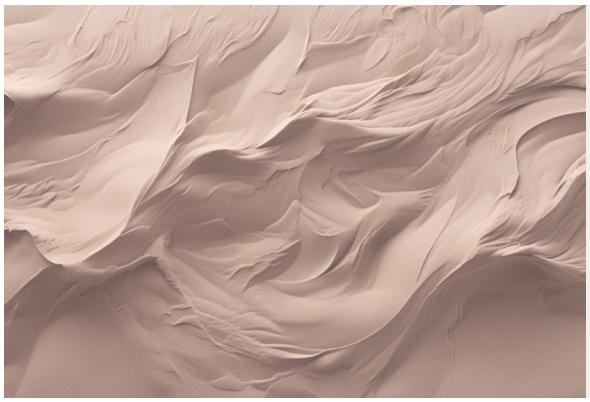
27%
of third-party failures surfaced in places leaders didn't expect

Yet most organizations still manage resilience in silos: separate functions, separate tools, and separate assumptions about readiness. The result is a growing gap between how prepared organizations believe they are and how effectively they actually perform when a critical event occurs.

This report answers two interconnected questions:

1. Why do organizations with mature business continuity systems still falter under the pressure of real-world disruptions?
2. How must enterprise resilience evolve by 2030 to thrive in an AI-driven, globally interconnected operating environment?

Drawing on responses from more than 500 leaders across audit, risk, compliance, BCM, and IT resilience in North America, the UK, Germany, and the UAE, this report examines why documented programs fall short under pressure — and what closing the gap requires.



What is business continuity management (BCM)?

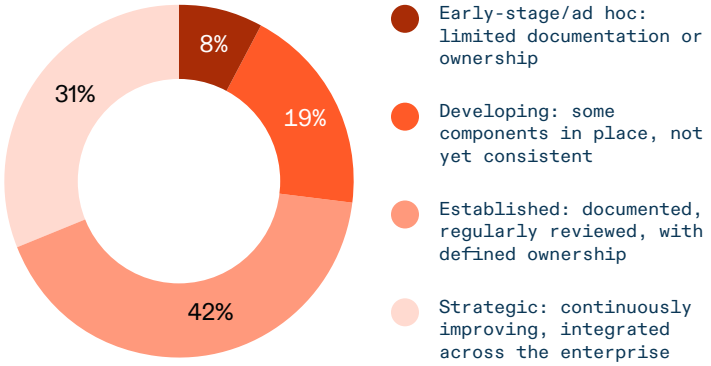
Business continuity management (BCM) helps organizations identify critical operations, prepare for disruption, and recover faster when issues happen.

Chapter 1: Companies think they're prepared. Incident data tells a different story.

Globally, 73% of leaders describe their business continuity programs as either well-established or strategic. However, perceptions of maturity vary significantly depending on who you ask.

Nearly half (48%) of compliance teams rate their organization's BCM as strategic, versus **31%** overall. Infosec and cybersecurity professionals are the least likely to do so, at just **22%**. That gap is especially notable given that **67%** of respondents in infosec and cybersecurity say they own BCM, suggesting a disconnect between program ownership and perceived maturity.

Program maturity self-assessment



Preparedness appears robust — until tested

A staggering **92%** of respondents assert total confidence in their organization's ability to meet defined recovery objectives. Yet fewer than four in ten actually met those objectives during their most significant event. **More than half** (54%) actually took longer than their defined recovery window in the past year.

Moreover, when incidents did occur, they rarely remained isolated:

- **91%** reported measurable customer impact (**17%** experienced significant customer loss or churn)
- **91%** reported measurable employee impact
- **4 in 10** said disruption-related losses exceeded **$1 million**

Many organizations appear to measure resilience primarily through preparedness indicators, rather than validated operational performance. Documented plans, governance frameworks, and recovery objectives remain foundational, but they don't always hold up when an outage event occurs. That gap becomes harder to ignore as operating environments grow more interconnected and technology-dependent.

Confidence

92% Say they are confident they can meet recovery objectives.

Reality

39% Met their RTO during their most significant disruption.

The external validation gap

Many organizations assess resilience largely through internal measures, without frequent and proactive external validation to reveal operational weaknesses.

Independent assurance remains a critical gap across the industry. Only **35%** of organizations have had their BCM programs externally validated or audited in the past 12 months. Nearly **60%** have gone over a year without an independent review, and **5%** have never undergone a formal assessment. Enterprises are relying on internal assessments to gauge their operational readiness.

By relying primarily on internal assessments to gauge operational readiness, enterprises may create a dangerous echo chamber. Without outside review, internal metrics can conceal weak assumptions, outdated dependencies, or plans that look complete until a real event tests them.

> "Events that could disrupt business continuity are often treated as low-likelihood risks, pushing them down the priority list despite potentially devastating consequences. As a result, leaders don't worry that the events will occur, or may feel confident in recovery capabilities they haven't tested under real-world conditions."

Richard Chambers
Senior Advisor, Risk & Audit
Optro

Regional snapshot

Canada

Highest self-reported BCM maturity rating, with **41%** rating their program as "strategic" versus **31%** overall.

United States

IT/infosec ownership of BCM jumps from **32%** globally to **53%** among U.S.-based respondents.

United Arab Emirates

Highest rate of missed recovery targets globally; **34%** of incidents took **more than twice** the defined objective.

What 2030 demands

Current state

Organizations are increasing resilience testing and operational validation as confidence gaps become harder to ignore.

By 2030

Leading organizations will build dynamic resilience ecosystems to continuously validate operational dependencies, recovery baselines, and risk signals in real time. Additionally, internal audit, GRC, BCM, and IT teams will converge around unified operational metrics and live readiness frameworks.

Chapter 2: The hidden dependency problem inside resilience programs

Organizations have invested heavily in the visible architecture of preparedness. Just under half report IT and cyber incident recovery plans (**42%**), active BCPs (**40%**), and regular business impact analyses (**40%**). But the operational infrastructure beneath those plans is incomplete.

The components most critical to understanding how a failure will actually spread — process mapping, dependency documentation, gap analysis, and third-party continuity requirements — are among the least consistently in place.

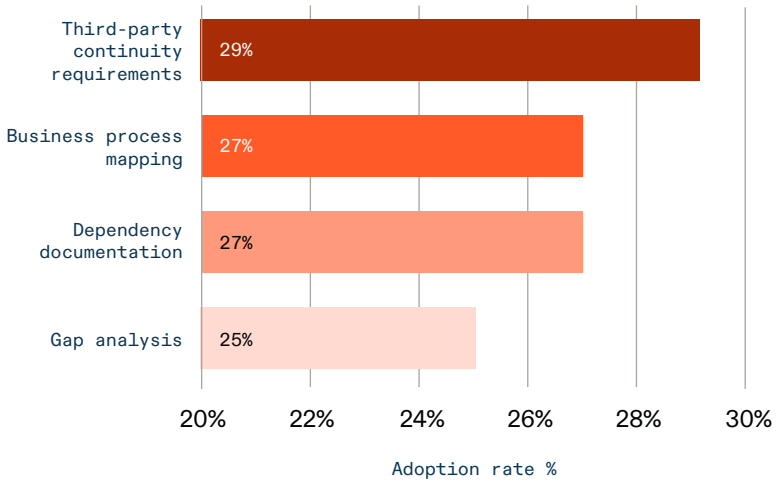
Interestingly, C-suite respondents report higher adoption rates for critical program components, such as dependency mapping (**41%** vs **27%** overall) and business process mapping (**34%** vs **27%** overall). The disconnect suggests executives may believe their organizations have far more operational visibility than teams on the ground.

These deficits have a direct impact when real-world pressures become material. When organizations evaluate why their BCPs fell short during actual incidents, the consequences of these missing operational layers become clear:

- **31%** cite impacted processes that were not documented or mapped accurately.
- **27%** cite third-party failures not anticipated in process mapping.

The same gaps organizations haven't filled are the same ones surfacing when incidents occur.

Business continuity program components in place



The mapping visibility gap

When asked about the extent to which their organizations map critical business processes to dependencies — including IT systems, third parties, and supply chains — and define active impact tolerances, the operational detail beneath the plans begins to fragment:

- **Fully mapped:** All critical services have defined impact tolerances with clearly established maximum tolerable levels of disruption (**42%**) – notably jumping to **70%** among compliance professionals.
- **Partially or minimally mapped:** The operational substrate remains incomplete, meaning most organizations cannot trace end-to-end exposure during an active failure (**56%**).

The vast majority of enterprises manage high-level recovery objectives without an accurate map of the upstream and downstream assets required to hit them.

> "You can't recover what you don't understand. Every critical process rests on interconnected dependencies across people, technology, facilities, data, and vendors. Without clear visibility, a crisis will expose the weakest link."

Richard Chambers
Senior Advisor, Risk & Audit
Optro

Regional snapshot

United Kingdom

The UK leads in the adoption of real-time BIA monitoring and reporting dashboards, with **45%** of organizations reporting implementation compared to **32%** globally.

United Arab Emirates

Respondents in the UAE were most likely to report minimal dependency mapping (**26%** vs. **13%** overall).

What 2030 demands

Current state

Organizations prioritize high-level plan documentation over deep operational infrastructure, creating a visibility gap between executive assumptions and real-world dependency mapping on the ground.

By 2030

Operational risk, TPRM, cybersecurity, disaster recovery, and internal audit functions will begin to share accountability for integrated operational resilience. This shift will move beyond static documentation, empowering cross-functional teams to collaboratively manage and mitigate risks with greater precision.

Chapter 3: Third-party risk is a core resilience issue

Once resilience is viewed through a dependency lens, third-party exposure stops looking like a procurement issue and becomes a core operational risk.

That risk is already showing up in day-to-day disruption patterns. **Three in four** (76%) organizations experienced at least one vendor failure in the last two years. Critical vendor outages and IT/cloud failures were the most common significant disruptions that organizations experienced. Among those incidents, **57%** resulted in losses of **$1 million** or more.

The financial picture varies by function, with **63%** of risk management respondents saying their most significant vendor-driven interruption cost between **$1 million and $10 million**. Internal audit respondents are more likely to report catastrophic losses, with **9%** citing events above **$10 million**, nearly double the cross-functional average.

Cloud infrastructure ranks as the top third-party continuity risk, cited by **28%** of respondents. Yet **35%** of internal audit respondents say they have never formally stress-tested a cloud or IT outage scenario.

Enterprises have some third-party vendor oversight processes in place:

- Vendor BCM documentation review (**39%**)
- Periodic BCM reassessments for critical vendors (**38%**)
- BCM assessments at vendor onboarding (**36%**)
- Resilience requirements included in vendor contracts (**36%**)

But only **31%** conduct joint continuity testing or exercises with critical third parties.

The broader point is that third-party resilience cannot be managed solely as a contractual exercise. It needs to be governed as part of the organization's operational risk architecture, with shared testing, visibility into dependencies, and escalation paths that reflect how cascading incidents actually unfold.

Top-ranked third-party continuity risks

22% Managed IT services providers

27% Cloud infrastructure providers

Scenarios not formally stress-tested

24% Critical vendor / third-party failure

28% Cloud or critical IT system outage

Regional snapshot

United Arab Emirates

Highest global rate of third-party disruptions (82%), with 67% of incidents costing over **$1M.**

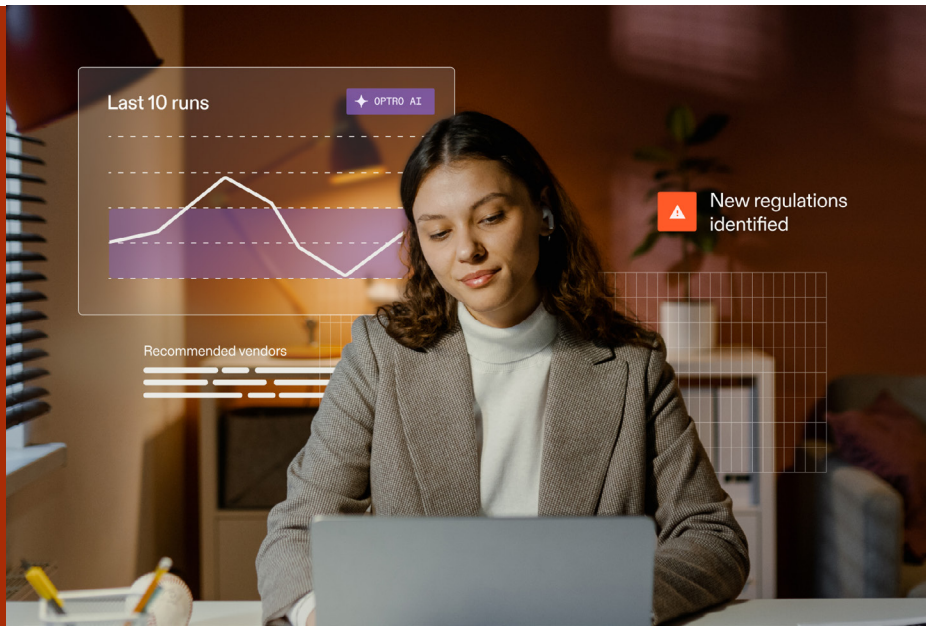
Germany

Leads in vendor BCM governance, but low joint testing reveals an operational validation gap.

Optro telemetry insight

Optro's platform activity reflects the same dependency problem from another angle. Integration activity increasingly spans cloud infrastructure, ticketing, identity, governance, and enterprise data systems. This strengthens how resilience operations now depend on interconnected external technology ecosystems.

Explore the platform



What 2030 demands

Current state

Organizations are increasing scrutiny of critical vendors, cloud providers, and outsourced operational dependencies, as third-party continuity becomes a mainstream resilience challenge.

By 2030

Leading organizations will evolve from periodic vendor assessments to managing resilience across interconnected operational ecosystems and embedding third-party resilience directly into enterprise operational governance.

Chapter 4: Companies are adopting AI for resilience efforts without pressure-testing how those systems break

By 2030, **36%** of BCM leaders expect AI-enabled disruptions to move at a velocity that completely outpaces human response capacity.

Artificial intelligence has already reshaped enterprise risk by accelerating decision-making, increasing opacity, and complicating accountability. In AI-driven environments, operational failure may manifest as flawed algorithmic decision support, AI agents acting on data they cannot properly interpret, hidden automation dependencies, or rapid systemic loss of control.

About a third of enterprises use AI for critical resilience tasks:

- **33%** for risk identification and monitoring
- **32%** use it for business impact analysis (BIA)
- **32%** use it for BCP gap remediation

> "The rapid adoption of AI within resilience activities is outpacing the governance structures required to manage its risks. This creates both opportunity and vulnerability, as organizations increasingly rely on interconnected digital ecosystems and specialized technical expertise."

Sandro Boeri
Internal Audit Thought Leader
Risk Audit

Scaling AI without a safety net

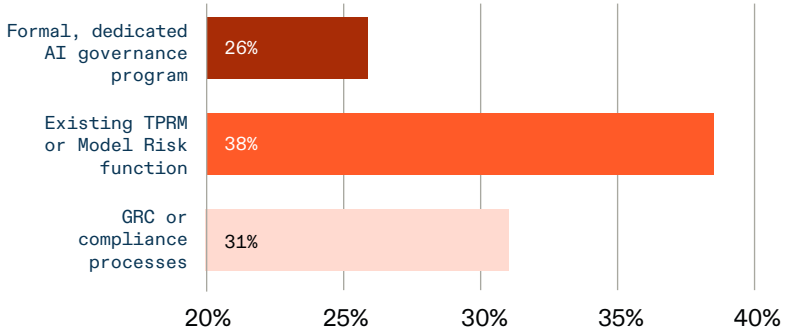
Companies are introducing AI into resilience workflows faster than they are building the structures needed to govern it well. While 42% have invested between **$1M** and **$4.9M** over the past 12 months, only **26%** report a formal, dedicated AI governance program for BCM initiatives, and **38%** express concern about the lack of AI governance controls within BCM workflows.

While **56%** of organizations conduct regular scenario planning, agentic AI failure remains the most frequently untested scenario globally at **30%**. This blind spot is even more pronounced in the U.S., where **42%** of programs have not yet tested for autonomous AI failures.

The three least stress-tested AI scenarios globally are:

1. **Agentic AI failure:** Loss of control or autonomous decision-making failures (**30% have never tested**).
2. **Shadow AI scenarios:** Unmanaged or unauthorized AI risk exposure (**29% have never tested**).
3. **AI-enabled cyberattacks:** Sophisticated, automated external breaches (**28% have never tested**).

How is your organization governing AI for BCM and operational resilience workflows?



Regional snapshot

Germany

Germany reports the greatest concern around over-reliance on AI outputs at **52%.**

United Arab Emirates

UAE reports the greatest concern around autonomous AI creating new failure points at **47%.**

United States

The U.S. reports the greatest concern for AI-enabled cyberattacks at **47%.**

What 2030 demands

Current state

Organizations are accelerating efforts to govern AI-enabled resilience workflows as adoption expands across risk monitoring, BIA workflows, third-party assessments, and continuity planning activities.

By 2030

AI-powered predictive analytics, automated orchestration, and real-time operational monitoring will become foundational pillars of resilience strategies – requiring governance and oversight frameworks significantly more advanced than those maintained by most organizations today.

Chapter 5: Investment priorities don't always match operational readiness

Priorities are shifting. Technology investment is active. Even so, the execution gaps remain. Organizations spent **10x to 20x** more on AI initiatives than on resiliency tooling in the past year. At the same time, BCM budgets are rising: **64%** of organizations increased BCM budgets by at least **5%** over the past year.

The top priorities organizations identify for the next 18 months are telling:

- **31%** rank integrating BCM with GRC as a top priority.
- **30%** rank embedding AI into BCM workflows as a top priority.

Both underscore the challenge ahead: organizations are trying to modernize resilience while still carrying unresolved issues in visibility, testing, and cross-functional coordination.

Regional snapshot

Canada

Leads globally in embedding AI into BCM workflows, with **36%** ranking it as a primary focus area for the next 18 months.

Germany

Resilience funding is surging, with **23%** reporting significant past budget increases (vs. 16% total) and **31%** anticipating spikes over the next 12–24 months (vs. 20% total).

United Kingdom

Technology transformation is front and center, with **34%** of organizations prioritizing BCM tools over the next 12–18 months (vs. 28% total) and **54%** investing **$1M+** into AI initiatives this year.

What 2030 demands

Current state

Organizations are increasing investment in resilience modernization, GRC integration, and AI adoption. Thirty-one percent rank integrating BCM with GRC as a top priority, with Germany leading at **36%**.

By 2030

Resilience operating models will become more integrated, continuously monitored, and operationally synchronized. Organizations will move from fragmented planning to dynamic, real-time resilience management, enabling faster response and more proactive risk mitigation.

Chapter 6: Bridging the gap between fragmentation and continuity execution

Modern operational resilience depends less on the volume of static continuity documentation and more on an organization's ability to coordinate dependencies across departments and in real time.

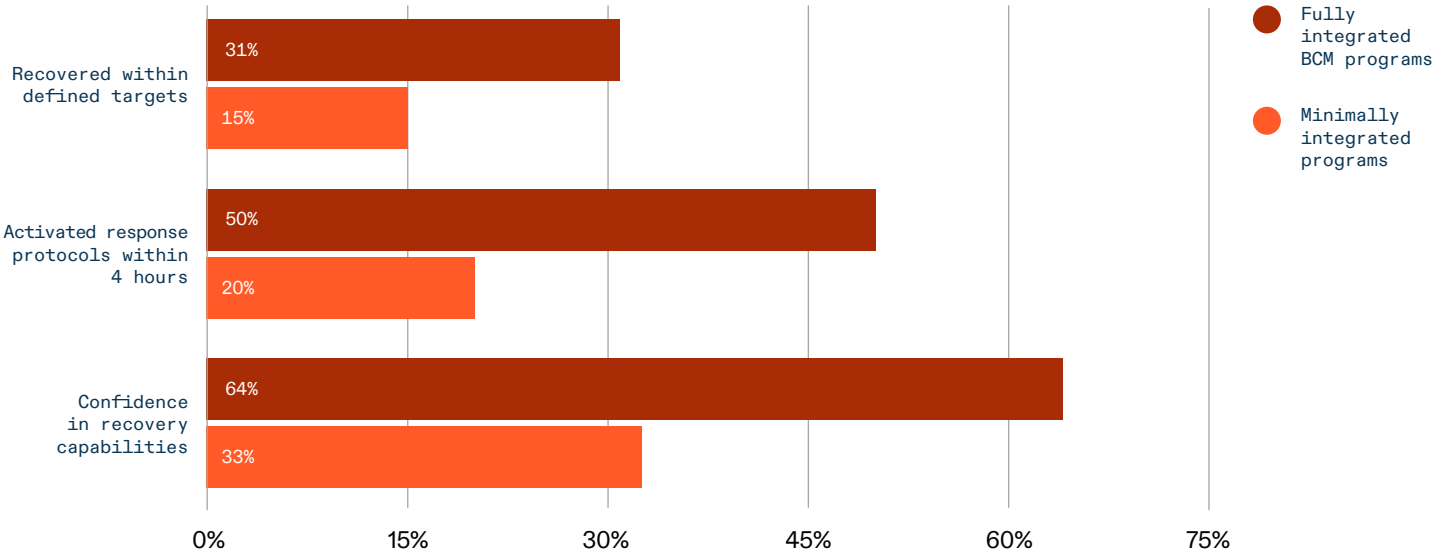
Yet, roughly **1 in 7** organizations maintain BCM as a completely standalone function, entirely isolated from adjacent risk disciplines, such as operational risk management, TPRM, and disaster recovery programs.

This structural separation is reflected in the top operational barriers reported by BCM leaders:

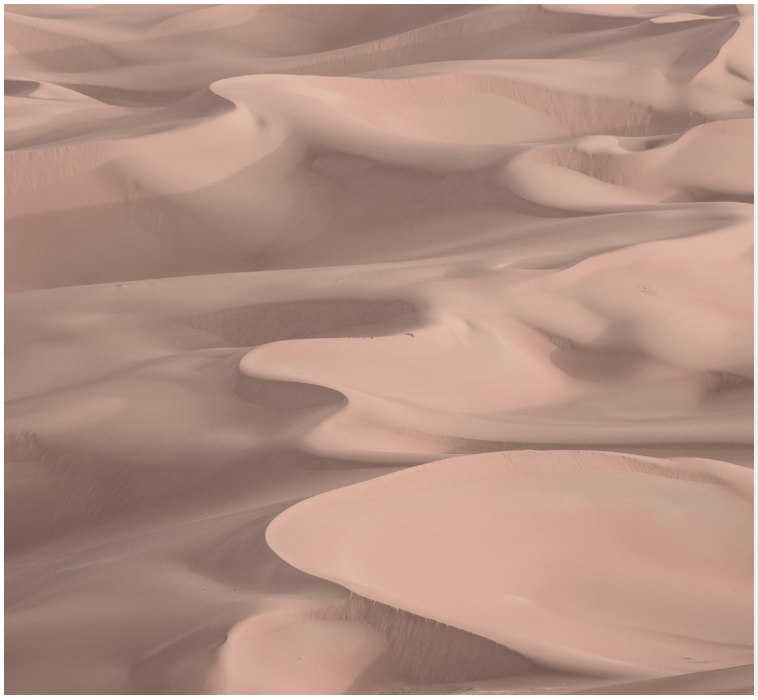
- **29%** state that the greatest barrier to improving enterprise resilience is the difficulty of integrating BCM with broader risk programs.
- **27%** cite deeply entrenched organizational silos between internal business functions as a primary constraint.

When BCM sits in a single function with no formal connection to adjacent risk programs, the performance gap is measurable. Organizations with fully integrated BCM programs consistently outperform those with minimal integration across key disruption metrics:

Fully integrated BCM programs outperform those with minimal integration



There's no consensus on where future ownership of BCM belongs: **24%** expect IT to retain the lead, while **70%** of internal audit respondents expect their function to play a larger role. However, the bottom line is that business continuity can't be effectively managed within a single department. Instead, operational resilience requires shared ownership and cross-functional coordination.



"Operational resilience is becoming inseparable from organizational culture, leadership effectiveness, workforce sustainability, and strategic decision-making. The next decade is likely to reward organizations that embed resilience deeply into the way they operate, rather than treating it as a standalone compliance exercise."

Sandro Boeri
Internal Audit Thought Leader
Risk Audit

Regional snapshot

United Arab Emirates

The UAE reports unclear ownership across GRC functions as a top barrier to strengthening operational resilience (**39%** vs. **26%** overall).

Germany

Organizational silos and unclear ownership across GRC functions are top hurdles, with **31%** of respondents citing each as a major barrier to operational resilience.

United Kingdom

One in three organizations whose BCM plans underperformed blame unclear ownership or ambiguous decision-making authority as a primary reason for the failure.

What 2030 demands

Current state	By 2030
Integration is becoming a priority as enterprise leaders recognize that resilience breaks down when functions, systems, and decisions are disconnected.	Leading organizations will move beyond fragmented continuity models to integrated resilience ecosystems with shared ownership across GRC functions.

Conclusion

The organizations represented in this research are not failing to prioritize resilience. In many cases, the opposite is true. Governance structures exist. Investments are increasing. Executive attention is rising. AI adoption is accelerating. Operational resilience has clearly become a strategic priority across industries.

Yet the central challenge facing organizations today is not awareness. It is fragmentation.

Audit sees one set of risks. IT manages another. BCM coordinates planning. Third-party teams oversee vendors. Risk functions assess exposure. Compliance monitors obligations. AI governance evolves independently. Each function may operate responsibly on its own, while the enterprise itself still lacks a shared operational understanding of how disruption will unfold under pressure.

Fragmentation is the real resilience gap.

It explains why recovery targets are missed despite strong confidence, third-party incidents continue to produce seven-figure losses, organizations document only a fraction of their dependencies, and why AI can move quickly into resilience workflows while governance remains underdeveloped.

For GRC leaders, the implication goes beyond BCM alone. Resilience is now a governance capability. It is the ability to connect policy, risk insight, operational dependency, third-party exposure, and response execution into one coherent system of action.

The strongest performers in our research are not simply the ones with more documentation. They are the ones breaking down silos. They recover faster because they see more. They coordinate better because functions are connected. Their confidence is stronger because it is grounded in tested capability rather than assumption.

Documented plans remain necessary. They are no longer sufficient. What will separate resilience programs that perform under pressure by 2030 is whether the organization can govern, interpret, and act on a shared picture of risk — before an incident exposes the gaps for it.

About Optro

Optro (formerly AuditBoard) helps enterprises transform risk into opportunity, redefining GRC through an agentic system of action. More than 50% of the Fortune 500 trust Optro to elevate audit, risk, and compliance in addressing a new era of risk. Optro is top-rated by customers on G2 and was named a Leader in the 2025 Gartner® Magic Quadrant™ for Governance, Risk and Compliance (GRC) Tools, Assurance Leaders.

Explore Optro

Get in touch

Appendix

RESEARCH METHODOLOGY

The survey included 506 respondents sourced from a leading global online panel provider. Respondents were selected based on geographic, role-based, company size, revenue, tenure, and subject-matter familiarity criteria. All participants were audit, risk, compliance, business continuity management/resilience, information security, or IT leaders working at organizations with at least 250 employees and annual revenue of at least $100 million USD. Selected respondents were further screened based on their role, seniority, years of experience, organization size, organization revenue, and self-reported familiarity with business continuity and resilience terminology.

ROLE QUOTAS

Quotas were set to ensure representation across key geographies, functional audiences, and industries relevant to business continuity management, operational resilience, audit, risk, and compliance. Minimum functional quotas were also set for selected audience groups, including internal audit, risk management, compliance/governance, and business continuity management/resilience. In addition, a minimum quota was set for financial services to ensure a sufficient sample for G-SIB and financial sector analysis.

The survey targeted audit, risk, compliance, business continuity management/resilience, information security, and IT leaders. Minimum quotas were set for selected functional audiences to ensure adequate representation across key groups involved in BCM, operational resilience, audit, risk, and compliance. Respondents were asked to select the function that most closely described their primary responsibility, even if none were exactly right or if they performed more than one of these roles.

The final breakdown by primary responsibility was as follows: IT 34.6%, internal audit 17.2%, risk management 17.0%, compliance/governance 12.1%, business continuity management/resilience 11.5%, information security/cybersecurity 5.3%, executive leadership 1.4%, and legal/finance 1.0%.

The final sample met or exceeded the minimum quotas for internal audit, risk management, compliance/governance, and business continuity management/resilience. Respondents were also asked to identify their current seniority level. The final seniority breakdown was: C-suite/Chief Officer 20.9%, VP or equivalent 23.1%, Head of/Senior Director 20.0%, Director 30.0%, and Manager/Senior Manager 5.9%.

GEOGRAPHIC QUOTAS

Geographic quotas were established for North America, the United Kingdom, Germany, and the United Arab Emirates.

The survey included respondents from North America, the United Kingdom, Germany, and the United Arab Emirates. Geographic quotas were established to support regional comparisons across these markets.

The target geographic quotas were: North America n = 220, the United Kingdom n = 80, Germany n = 128, and the United Arab Emirates n = 72.

The final achieved geographic breakdown was as follows: North America 43.7%, including the United States 32.2% and Canada 11.5%; the United Kingdom 16.4%; Germany 25.3%; and the United Arab Emirates 14.6%.

In counts, this represents n = 221 North America, including n = 163 United States and n = 58 Canada; n = 83 United Kingdom; n = 128 Germany; and n = 74 United Arab Emirates.

INDUSTRY

A minimum quota was included for financial services, representing at least 20% of the total sample, to support G-SIB and financial sector analysis.

The final breakdown of respondents by industry was as follows: financial services 21.5%, technology 17.6%, industrials & manufacturing 12.5%, retail/ecommerce 10.9%, energy & resources 7.9%, telecommunications 7.9%, insurance 6.7%, business/professional services 4.7%, life sciences, including healthcare and pharmaceuticals, 3.4%, transportation and logistics, including supply chain, 3.2%, marketing & advertising 1.8%, government/public sector 1.4%, and education 0.6%.

The final sample exceeded the financial services minimum quota, with financial services respondents representing 21.5% of the total sample.

RESPONDENT SCREENS

Role: All respondents were required to identify as leaders in audit, risk, compliance, business continuity management/resilience, information security, IT, or adjacent executive functions.

Company revenue: All respondents were required to work at organizations with annual revenue of at least $100 million USD. The final revenue breakdown was: $100 million to under $250 million 24.1%, $250 million to under $500 million 27.9%, $500 million to under $1 billion 21.5%, $1 billion to under $25 billion 19.6%, $25 billion to under $50 billion 6.3%, and $50 billion or greater 0.6%.

Company size: All respondents were required to work at organizations with at least 250 employees. The final company-size breakdown was: 250–499 employees 0.8%, 500–999 employees 7.3%, 1,000–4,999 employees 69.2%, 5,000–9,999 employees 15.0%, 10,000–24,999 employees 6.1%, 25,000–49,999 employees 1.4%, and 50,000 or more employees 0.2%.

Time in role: Respondents were required to have spent at least three years in their role. The final breakdown was: 3–5 years 21.7%, 6–10 years 54.5%, 11–15 years 21.3%, and 16+ years 2.4%.

Information level: Respondents were screened for familiarity with business continuity and resilience terminology. All respondents in the final sample indicated that they could explain business continuity management (BCM) to a colleague. In addition, 85.0% indicated familiarity with business impact analysis (BIA) and 54.3% indicated familiarity with operational resilience.

Attention level: Respondents were subject to survey quality and attentiveness checks, and respondents failing those checks were excluded from the final sample.

Limitations: Regional findings should be interpreted with awareness that functional composition varies across geographies. UAE respondents include a higher concentration of internal audit leaders (38%) relative to the overall sample (17%). Because internal audit respondents tend to report greater awareness of operational gaps, some UAE findings on perception-based metrics, including BCM maturity self-assessment, may reflect functional composition as much as regional difference.

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.