Find out more www.thebci.org

bci Thought Leadership

A Year in the World of Resilience 2024

A BCI Report

riskonnect
Integrated Risk Management Solutions™

bci Leading the way to resilience

Contents

Foreword

The BCI are pleased to present the second edition of A Year in the World of Resilience 2024 Report. This annual publication compiles insights from 2024's research reports, highlighting the key themes and trends that have shaped resilience practices over the past year. It serves as both a reflection on the challenges faced in the past twelve months and a guide for resilience professionals navigating complex risks going forward.

The risk landscape over the past twelve months was characterised by its volatility and complexity, driven by geopolitical events and economic uncertainty. 2024 was called "the year of elections", with political instability, cybercrime, and climate-related disruptions creating challenges for organizations who faced multiple, interconnected, and simultaneous crises, complicating response efforts.

In 2024, the role of senior leadership in resilience programs came into stronger focus. The crucial role of senior management in resilience was highlighted in the new BCI's Resilience Framework that defines how executive support is critical in defining organizations' strategic direction towards resilience, and embedding it into organizational culture. When leadership actively supports and governs resilience initiatives, it ensures that these efforts are sustainable, measurable, and continue to evolve. However, senior management's involvement is often divided across competing priorities. This year, cyber resilience—particularly with the integration of artificial intelligence (AI)—took centre stage, alongside regulatory compliance.

Collaboration across departments has also become a defining feature of resilience in 2024, with many organizations forming a "resilience umbrella" that reflects a growing recognition of the interconnected nature of risks. Despite this, silos persist in some organizations, highlighting the need for further progress in aligning cross-functional efforts to achieve true organizational resilience.

AI has been a standout topic this year, as practitioners increasingly explored its potential to enhance resilience. From scenario-building for training and data analysis to bolstering cybersecurity, AI applications are proving to be valuable tools. While more practitioners are making up their minds about AI's role in organizations, particularly within BC and resilience practices, most professionals are taking a wait and see approach to AI. The debate over AI as a resilience enabler or disabler will undoubtedly continue as technologies and controls evolve.

Heightened regulatory pressures emerged as a major concern in 2024, with a record 63.8% of organizations reporting an increase in compliance requirements compared to the previous year. Navigating overlapping regulations, particularly in digital and financial sectors, has been a significant challenge for organizations over the past year.

Looking forward, budgets for resilience programs are expected to remain stable in 2025, though cyber resilience and operational resilience are set to receive increased investment, reflecting their growing importance. AI initiatives are also expected to see higher funding, signalling confidence in technology-driven approaches to resilience.

As the resilience community moves into 2025, the need for strong leadership, effective collaboration, and innovative solutions has never been greater. The lessons from 2024 highlight the importance of integrating resilience into all aspects of organization's strategies in order to remain agile in the face of evolving risks.

I would like to thank everyone who contributed to the BCI's research and shared their expertise throughout the year, helping to make this annual piece possible. We extend special gratitude to Riskonnect for their sponsorship and support in bringing this publication to life. Finally, thank you to the resilience community for their continued commitment to building a more resilient future. We look forward to a new year of progress and collaboration.

Maria Florencia Lombardero Garcia
Thought Leadership Manager
The BCI

Foreword

Riskonnect is proud to once again sponsor the BCI's A Year in the World of Resilience Report for 2024. The BCI conducts thorough and insightful research each year, but this report may be my favorite. It gives us a chance to look back on where we've been while also looking ahead to what's coming. The business continuity and resilience space is rapidly innovating and these results capture that change in a way that should excite us about the future.

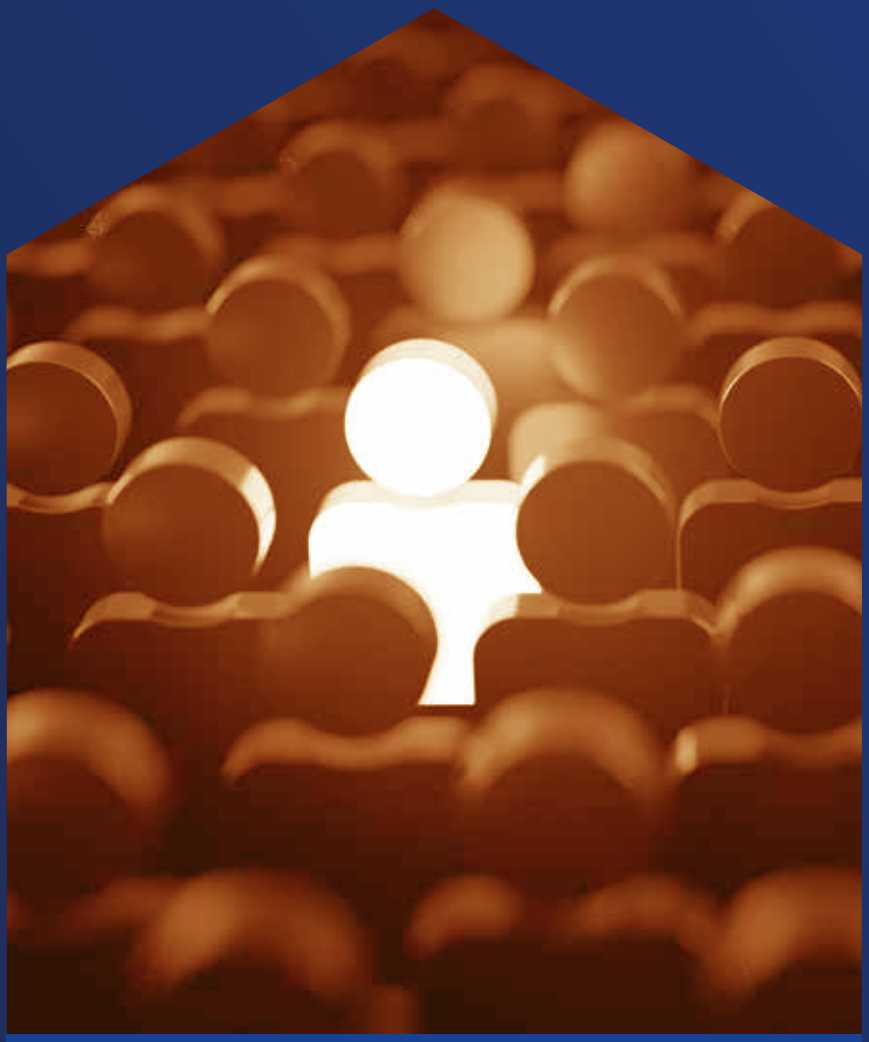
The most encouraging results from this year's report emphasize involvement from senior leadership and the scope of collaboration across risk disciplines. Continued progress in these areas will shape the future of continuity and resilience. The results show that senior leadership is providing strategic oversight in core areas like business continuity (56.8%), cyber resilience (55.1%), and operational resilience (48.7%). Strategic oversight from senior leadership not only provides increased visibility and support for the program but also scales the program to an overall strategic level. A more strategic view builds a proactive rather than reactive approach to continuity. In a polycrisis world, proactivity is your best defense, and strategic oversight from senior leadership offers the building blocks to make it happen.

As Riskonnect is a provider of integrated risk management solutions, it's also heartening to see the level of collaboration across risk disciplines. The BCI calls this the "resilience umbrella" and I'm inclined to call it the "integrated risk umbrella". The results here may seem unsurprising. Business continuity is regularly collaborating mostly with enterprise risk management (77.3%) and cyber security (73.6%). This is likely due to regulations like the Digital Operational Resilience Act interweaving business continuity, technology risk management, third party risk management, and enterprise risk management as components for greater operational resilience in the financial sector. Alternatively, the scale and frequency of cyberattacks have likely caused the increase in collaboration with cyber security. Cyber resilience is no longer just an IT issue, but a strategic, organizational imperative. While insurable risk, and claims management round out the bottom of the list for collaboration, there is great value in connecting these spaces. Both business continuity and insurable risk hold an abundance of business data that can be used to build better resilience. I'm hopeful that we'll see more collaboration here in the future.

Well, another year has closed, and another report is complete. There are many more points I could address but I'll leave you to discover the data from here. I hope you find the insights in the report to be equally as valuable as you prepare your organization's continuity and resilience efforts in the next year.

John Verdi (MBCI)
Senior Director, Professional Services — Resilience & GRC
Riskonnect

1 Executive summary



The success of a resilience program largely depends on strong support from top leadership.

Senior leadership's role in endorsing resilience programs has become increasingly crucial as they set the organization's overarching vision and are therefore best positioned to define its strategic direction and risk tolerance. Building a truly resilient organization requires the active involvement and collaboration of senior leaders across all key areas of the organization. When senior leadership takes the lead in developing and managing resilience initiatives, it ensures these efforts are effectively governed, measured, monitored, and continuously improved for long-term success.

Senior management's role in resilience is split among several priorities

Research shows that overall in 2024, cyber resilience - especially with artificial intelligence (AI) integration - has become top management's primary focus, followed closely by regulatory compliance. Although senior leaders are highly involved across these areas, their approaches vary: regulatory compliance, crisis response, and new technology decisions receive more hands-on management, while business continuity, cyber resilience and operational resilience efforts benefit from broader strategic oversight.

Top three areas where senior management provides strategic oversight

56.8% Business continuity

55.1% Cyber resilience

48.7% Operational resilience

Top three areas with direct involvement from senior management

41.8% Regulatory requirements

32.4% Crisis management

26.4% New technology decisions

Regular collaboration is creating a 'resilience umbrella', although some siloed working practices persist

BC and resilience practitioners regularly collaborate with a range of related departments indicating the formation of a 'resilience umbrella' in some organizations. The top areas for regular collaboration are enterprise risk management and cyber security, which may in part be due to incoming operational resilience legislation for digital and financial sectors. Despite good progress, more work is required in breaking down silos and increasing collaboration,as it is a key factor in following organizational resilience best practice.

Growing awareness of the benefits of AI, although wariness remains

AI has been the subject of much discussion this year and more practitioners have come to conclusions over its use in resilience settings. Fewer organizations than last year are unsure about its role, and more practitioners are deciding whether AI is a resilience enabler or disabler. One in five organizations now see AI as a resilience enabler with the main areas of application being cybersecurity, the creation of scenarios for training and exercising, and data mining. AI will undoubtedly remain a focal point in the coming years as new regulations, such as the EU AI Act introduced in 2024, continue to emerge.

Top five applications of AI in business continuity and resilience operations

24.5%
Cybersecurity

17.5%
Creation of scenarios for training and exercising

15.8%
Data mining/ big data

15.7%
Risk assessment and forecasting

11.6%
Automation/semi-automation of the business impact analysis (BIA)

Reference: How is/will AI be used specifically within your BC/resilience operations? Options: already embedded in our programme and currently introducing into our programme

Most practitioners are happy with their BIA process, and recognize the benefits of technology.

Most respondents are generally satisfied with their current BIA. Many of those that are very happy have recently overhauled the process and those that feel very unhappy are more likely to feel that the process needs assistance from technology. There are few changes in the use of technology this year, but many respondents are considering, or already undertaking, a move to third party software. In terms of using AI in the process, most are wary and would consider using it if they could retain human input. Activities such as inputting sensitive company data currently causes security concerns for practitioners which underlines its relatively early stage in supporting resilience activities.

Regulations, geopolitical concerns, and weather-related events are 2024's top challenges

The most prominent resilience challenge in 2024 is the significant increase in global regulatory requirements, with a notable 63.8% of organizations reporting more regulatory pressures compared to last year. Many organizations have to comply with multiple schemes simultaneously. In addition, geopolitical hazards have emerged as a critical risk this year, with global economic uncertainty being the most frequently cited concern among practitioners. Political instability caused by numerous elections, wars and conflicts, and increasing climate related events all contributed to a challenging risk landscape in 2024

Top three geopolitical trends posing the greatest threats to organizations in 2024

69.9% Global economic uncertainty

49.5% Regulatory changes

45.6% Political stability in key markets

Top three climate related risks posing the greatest threats to organizations in 2024

61.4% Supply chain disruptions due to climate risks

61.4% Physical impacts of climate related events

35.6% Increased insurance costs due to climate risks

Budgets remain stable for 2025 with cyber resilience attracting the most funding

Most respondents feel budgets will remain the same in 2025, as a result of an uncertain economic outlook. However a considerable subset of organizations are expecting an expansion of their budgets in 2025. Cyber resilience will receive the highest increase in spending levels, reflecting senior leadership's priorities. Also, 42.2% of respondent expect an increase in budget dedicated for operational resilience driven by new regulations worldwide. Moreover, 36.2% of organizations are expecting their AI budget to be higher in 2024.

Key areas projected for increased investment in 2025

59.8% Cyber resilience

42.2% Operational resilience

38.5% Business continuity and resilience

2

Strategic leadership of resilience

Strategic leadership of resilience

- This year's top management priorities have been regulatory requirements and cyber resilience
- Management involvement in programmes varies between direct management and strategic oversight. Cyber resilience and business continuity are the top subject requiring senior management strategic oversight whilst regulatory requirements, crisis management and new technology decisions see the biggest direct management involvement.
- Pandemic planning and supply chain management attracts the least involvement from senior management.

The need of senior leadership support for resilience programs has become increasingly clear in BCI research. Active management interest is essential in securing the necessary resources and strategic direction to develop and maintain a robust resilience programme. A true resilient organization is built from the contributions of its people, and it is essential for employees to understand their individual roles within the broader organization. Effective leadership from the top is crucial to fostering this understanding and engagement This chapter delves into the involvement of senior management in resilience activities over the past 12 months.

This year's research shows that the primary concerns for top management are regulatory requirements, cyber resilience and crisis management.

To what degree does senior management get involved in the following subjects?

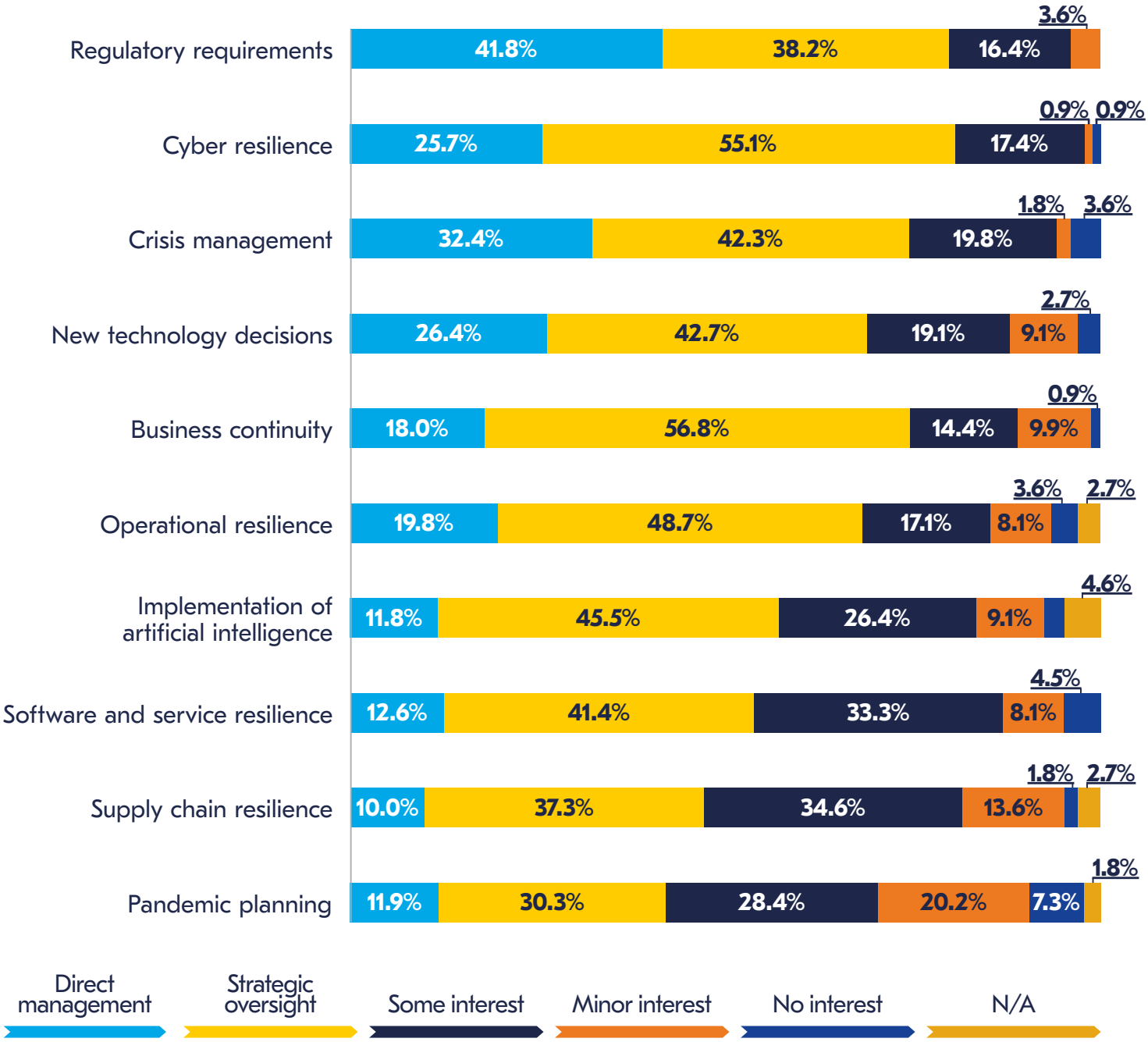


Figure 1. To what degree does senior management get involved in the following subjects?

Increased regulatory requirements

The main concern for leadership teams is the increase in regulatory requirements. In a shake up to 2023's priority list[1], regulations are this year's top-place, a jump from third place.

Across the globe there is an increase in resilience regulations, in particularly those related to critical national infrastructure. Many sectors are affected by national infrastructure regulations, such as energy/utilities, communications, financial services, healthcare, education, transport, education, etc.

In this case it is worth mentioning the EU Directive on the Resilience of Critical Entities that came into effect on January 16, 2023. Member States had until October 17, 2024, to implement national legislation that incorporates the Directive. This legislation seeks to enhance the resilience of critical entities against various threats, including natural disasters, terrorist attacks, insider threats, sabotage, and public health emergencies.

Many organizations have reported increased regulatory requirements this year, including the fast-approaching digital-focused DORA deadline, CPS 230, NIS2, and new guidance from UK regulators for digital service providers about third-party risk considerations, which are all pressing concerns for leadership teams, not least due to the potential risk of heavy fines for organizations that fail to comply, and the new burden placed on management to implement legislation.

"Operational resilience is absolutely key in being able to take the journey to the senior leaders and the reason why we're going to focus further on it next year".

Continuity and Resilience Director, Public Sector, UK

Cyber resilience, an ever-present concern

Forrester's 2025 Predictions report[2] suggests organizations will lose $12 trillion due to cybercrime next year. With cybercrime increasing in complexity and frequency, not least due to the more advanced nature of AI, and prominent cyber-crimes hitting global headlines in 2024, it is understandable that top management remains keen to keep a keen interest on the cyber-security posture of their own organizations. Indeed, cyber resilience was the top concern for management in last year's report. Mirroring this is the BCI Horizon Scan Report 2024[3] which placed cyber-attack as the top short-term risk and cyber security as the top risk over the next 5-10 years. Additionally, the BCI Update Series: Cyber Resilience Report 2024[4] highlighted the expanding commitment from top management to cyber resilience, and a greater allocation of resources in 2024. Two-thirds of respondents (65.9%) reported a high level of commitment from top management to cyber risk, indicating a growing recognition of cybersecurity's critical importance at the highest organizational levels, as well as being indicative of the awareness of the financial and reputational damage a successful attack could wreak. This awareness is demonstrated through increased engagement with cybersecurity topics and exercising at both executive and board levels. However, the report also highlighted the need for ongoing education and awareness efforts in order to ensure comprehensive understanding of cybersecurity risk among top management.

"A lot of increased spending is due to inflationary costs, but budgets have been cut and we have to be really careful about where we spend the money. The focus for us is on cyber, penetration testing and other cyber essentials."

Chief officer, public service, UK

Rising management involvement in crisis management

In last year's report, crisis management placed fifth in the table of top management concerns, but this year it has moved up two positions. This increase reflects the increasingly complex risk landscape that organizations are navigating: 2024's unprecedented number of elections, the influx of new regulations, geopolitical tensions, and increased supply chain vulnerabilities, among others, have created a more complex risk environment.

The BCI Crisis Management Report 2024[5] showed the majority of organizations (75.1%) faced a crisis and activated their crisis management team within the previous twelve months. With organizations now facing a wider range of challenges, business continuity and crisis management programmes have moved to a higher position on senior management agendas to reflect boards concerns. Research shows that senior management is now more involved in crisis response: 44.6%[6] of organizations' top management is involved in the crisis response at points during the process and in the final decision whilst another 31.0% are involved all along the process, taking a controlling role until the final decision.

Top management: Strategic vs. direct involvement

Top management control over the response in a crisis isn't necessarily a good thing. It can make for slow decision making, it can build a culture of fear, and might mean that some voices aren't heard. However an active interest of top management in the crisis response is a very positive sign. To understand this, practitioners were queried into the different ways in which top management approached resilience programmes and in what capacity they were involved.

Strategic oversight and direct management play distinct roles in guiding an organization. Strategic oversight refers to the high-level direction leaders set to achieve long-term goals. It involves crafting vision, establishing priorities, and ensuring that organizational resources are aligned with broader objectives. Leaders focused on strategic oversight generally refrain from involvement in day-to-day operations. In contrast, direct management is when leaders actively oversee specific tasks, manage team workflows, and directly address operational challenges.

While strategic oversight keeps the organization focused on its mission and prepares it for future demands, direct management ensures that the daily functions run smoothly and efficiently. The responses highlighted differing approaches to strategic oversight and direct management.

"Management has targets of what they want to achieve, and we cascade that down, converting strategic plans to tactical and operational plans."

Head of risk and resilience, education, UK

"There's a lot of the strategic oversight in our organization since we are a relatively new program, our steering committee is more involved now than they will be moving forward. They want to make sure that they have a good understanding about the direction the program is taking, but still give us a large amount of autonomy to move the program where it needs to go."

Business continuity manager, health USA

"Management are involved in degrees of threat, risks and effects. We've focused the ownership, leadership, management and good governance of the leadership on high risk, high focus areas."

Continuity and resilience director, public sector, UK

"We have an Executive-level Business Continuity Response Team that would manage the strategic response to a disruption, while we have non-executive groups to manage the operational and tactical responses."

Risk management officer, healthcare, Australia

Strategic overview

A more strategic role is played by top management in business continuity, cyber resilience (including the implementation of artificial intelligence), and operational resilience programmes.

Cybercrime is on the rise, and it is a prominent risk that is likely to remain a concern to management into the future, so a long-term strategic view is required to address the threat. However, cyber security is a specialist industry and, without direct technical knowledge, senior leadership may have to take a more strategic approach, particularly when it comes to AI as there is still a lack of awareness of its potential implications.

> **"Our senior management have a strategic drive to push new technology and that includes AI. We will have to pay a lot of attention to how we are securing those technologies and solutions."**
>
> Business continuity manager, telecoms, Hungary

There is a heightened awareness and interest in resilience in part due to worldwide regulations focused on operational resilience and third party management. However, The BCI Operational Resilience 2024 report[7] found that whilst overall responsibility for operational resilience in the past four years has most frequently sat with the CEO, this year overall accountability is more evenly split amongst other members of the c-suite, such as the Chief Operations or Chief Risk Officer. Some of the regulations on operational resilience affecting the financial sector dictate that a named c-suite officer should be in charge. This goes some way to explain the levels of strategic oversight here, and also the increase in strategic oversight of business continuity (35.8% to 56.8%), which is an important part of resilience programmes.

With the world facing often, sometimes overlapping, crises, leadership teams are now recognising the critical - and competitive - advantage of investing in resilience. Resilience is increasingly being considered not just as a protective measure, but as a strategic priority for sustainable success.

Areas where top management takes a strategic oversight lead

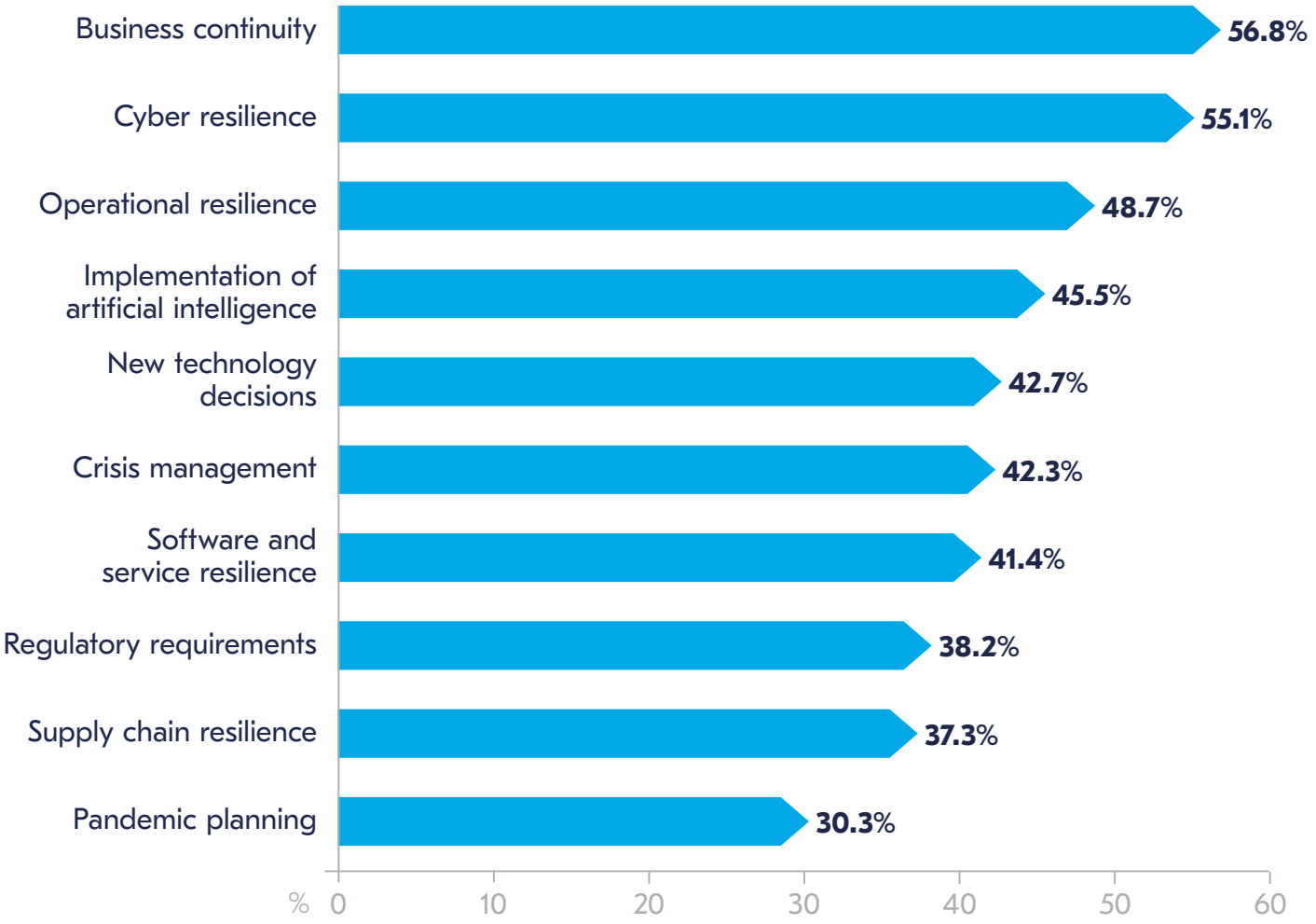


Figure 2. Areas where top management takes a strategic oversight lead

The need to keep pandemic planning in top leadership minds

The 2023 report showed that the strategic oversight of pandemic planning was bottom of the list of areas where leadership took a strategic lead, indicating that organizations were moving away from pandemic planning, in part due to the adoption of plans during COVID-19. However, the risk of a new pandemic remains high on many countries' risk registers, so the importance of continuing to work with leadership to secure support is vital. This year's research also put pandemic planning at the bottom of the list, however this year senior management shows more interest in pandemic planning. 30.3% of organizations senior management have strategic oversight of pandemic planning, compared to only 5% in 2023. This is perhaps in part due to emerging COVID-19 enquiries, such as the UK COVID-19 Inquiry: Resilience and Preparedness Report[8], that highlighted failings and made recommendations to improve future response. This year's global pandemic outbreaks, such as Monkeypox and Dengue Fever, have further raised the profile of pandemic illnesses.

One public sector interviewee reported that pandemic planning was the only programme directly managed by leadership, indicating that it is still a management 'hands-on' topic for certain industries.

"We were pulled into a lot of the decision making around pandemic planning in terms of the impact it had on the organisation and our ability to carry out core functions. Some issues have had long term negative issues for us that we're still working through, with direct management."

Chief officer, public service, UK

"Pandemic planning does still come up and people are still aware of it, but I think on a management level, it's not going to get much attention for now."

Business continuity manager, telecoms, Hungary

Direct management

41.8% of respondents say senior management directly manage activities related to regulatory requirements, the highest percentage of subjects surveyed. This will come as no surprise to practitioners, particularly those in the financial and digital sectors, where some regulations state who in organization's top leadership is ultimately responsible for complying with regulations. Direct management of regulations indicates they are recognised as pressing current risks, no doubt due to imminent deadlines and fines imposed by regulatory bodies.

As we have seen, the increase in crisis management team activations due to an elevated number of crises has prompted a rise in management interest. 32.4% of leadership take a management role here, placing crisis management as the second highest programmes with under direct management.

The growth in remote working has prompted direct management involvement in the introductions of new technology decisions as they can heavily impact organizations. Working from home is a popular choice for many organizations, but home-working practices comes with risks, not least cyber threats created by a lack of security measures on insecure home networks and personal devices, which makes it easier from cybercriminals to access corporate data. Another big vulnerability worth mentioning is due to social engineering and workers being more prone to it in remote environments.

"Senior management directly oversees compliance with regulatory requirements. As an international company, we operate within a complex regulatory landscape, with various regulatory bodies operating at different levels. It is crucial for us to comply with these regulations to avoid potential non-compliance penalties, which can result in substantial fines. Senior management's direct involvement ensures that we stay up to date with regulatory changes and maintain a proactive approach to compliance."

Resilience manager, group business resilience and crisis management, USA

Areas where top management takes a direct management role

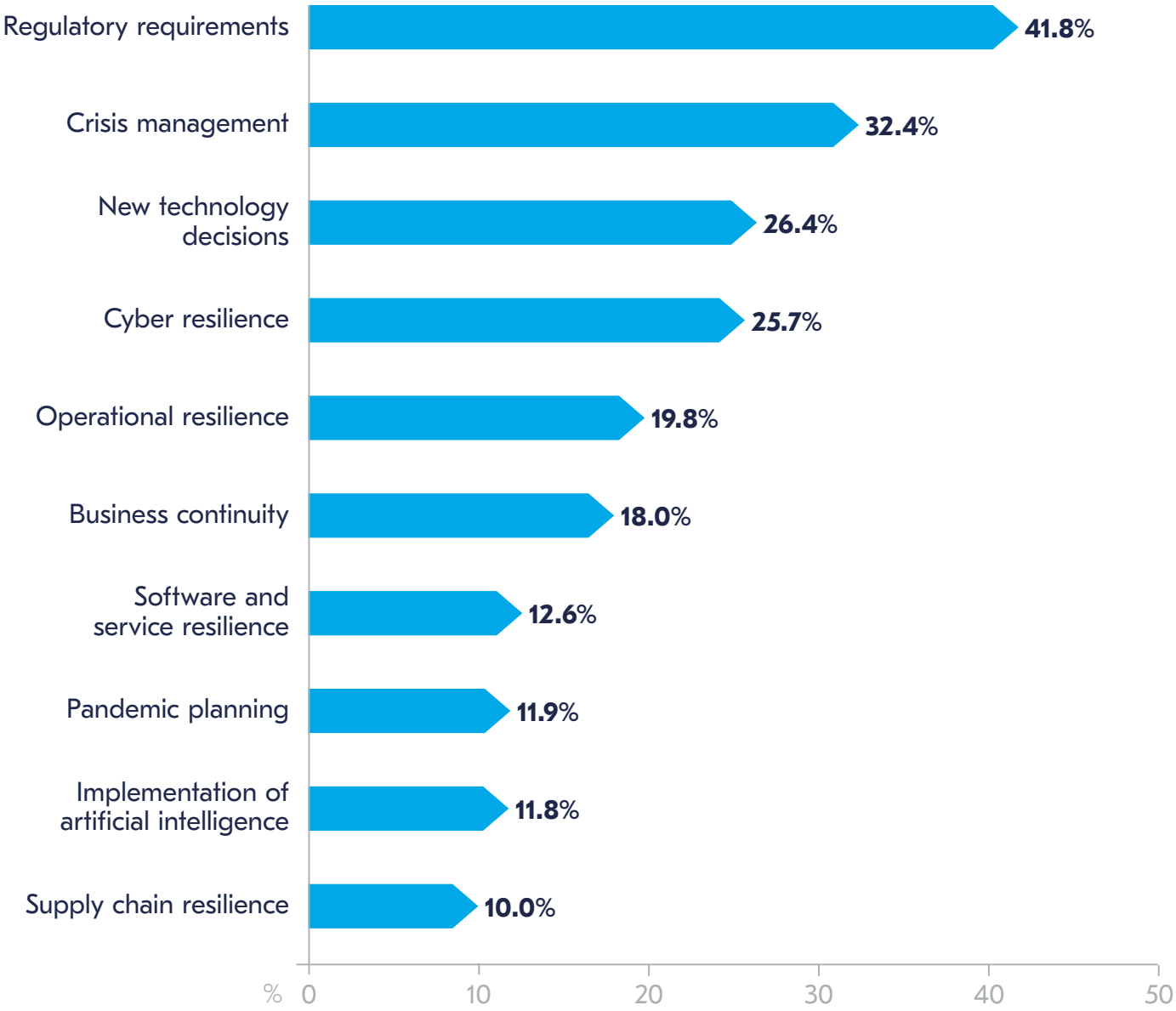


Figure 3. Areas where top management takes a direct management role

Collaboration: ‘The resilience umbrella’

Collaboration: 'The resilience umbrella'

- BC and resilience practitioners regularly collaborate with a range of related departments indicating the formation of a 'resilience umbrella'.
- Top areas for collaboration with the BC function are enterprise risk management and cyber security.
- Despite good progress, more work is required to break down silos in certain areas.

Effective resilience programmes rely on cross-departmental collaborations and the breaking down of siloed practices. Research[9] has shown that resilience is increasingly becoming embedded within organizations But while some organizations are still lacking maturity in resilience leadership, most are now integrating resilient processes as standard practice. Silos are breaking down, reporting structures to boards are streamlining, and business continuity and resilience managers are more frequently involved in strategic discussions.

To understand the current extent of partnerships, practitioners were asked to examine which disciplines of their programmes regularly integrated, interacted, or collaborated with to support resilience and/or risk management efforts. Results indicate that the main related disciplines of resilience are enterprise risk management, cyber security, crisis management, and operational resilience.

77.3% Enterprise risk management

73.6% Cyber security

65.4% Operational resilience

65.4% Crisis management

Perhaps unsurprisingly the highest collaboration rate with the business continuity team is enterprise risk management, followed by cyber security and operational resilience/crisis management tying in third place. This may indicate collaborative working under a resilience umbrella and appreciation of the importance of implementing organizational resilience practices throughout the organization. Incoming regulations and standards may be the driver for this push towards more collaborative working. Legislation such as the EU Digital Operational Resilience Act (DORA) and APRA's CPS 230 all encourage a collaborative approach to resilience across interdepartmental disciplines in order to manage risks.

The collaborative approach has the potential to end siloed working, which research has shown consistently undermines resilience teams. The BCI Crisis Management Report 2024 found that the overwhelming majority of respondents (90.5%) revealed that their team's ability to interact with other functions, as well as a network culture, was a key solution to successfully navigating a crisis. In response, an increasing number of organizations are centralising crisis management structures to address fragmented working, and others are also leaving some space for regional/business led input in order to enhance their crisis response.

However, the need to establish closer relationships with different departments is essential in achieving resilience and achieving fast and effective crisis responses. For example, stronger collaboration between business continuity, resilience, and IT/cybersecurity teams is essential. Persistent challenges in unifying these groups to develop a cohesive cyber strategy stem from siloed organizational cultures. Senior management should lead efforts to foster collaboration and ensure effective integration across teams and functions.

Interviewees explained their collaboration with different organisational functions:

"The department we co-ordinate with most is enterprise risk management. Any big business continuity risk or IT system risk that I discover I channel towards enterprise risk management, so that's a strong collaboration. We also collaborate with the legal department too due to regulatory impacts in the telecoms sector, and facilities because even though a lot of people do work remotely, we have data centres and a lot of the telecom network is on site. If there is a major incident, people need to go on site and actually physically enter systems. It's very important to us that facilities are always accessible."

Business continuity manager, telecoms, Hungary

"We work with all of the organization's departments across the US and UK to protect the business continuity management domain."

Resilience manager, group business resilience and crisis management, USA

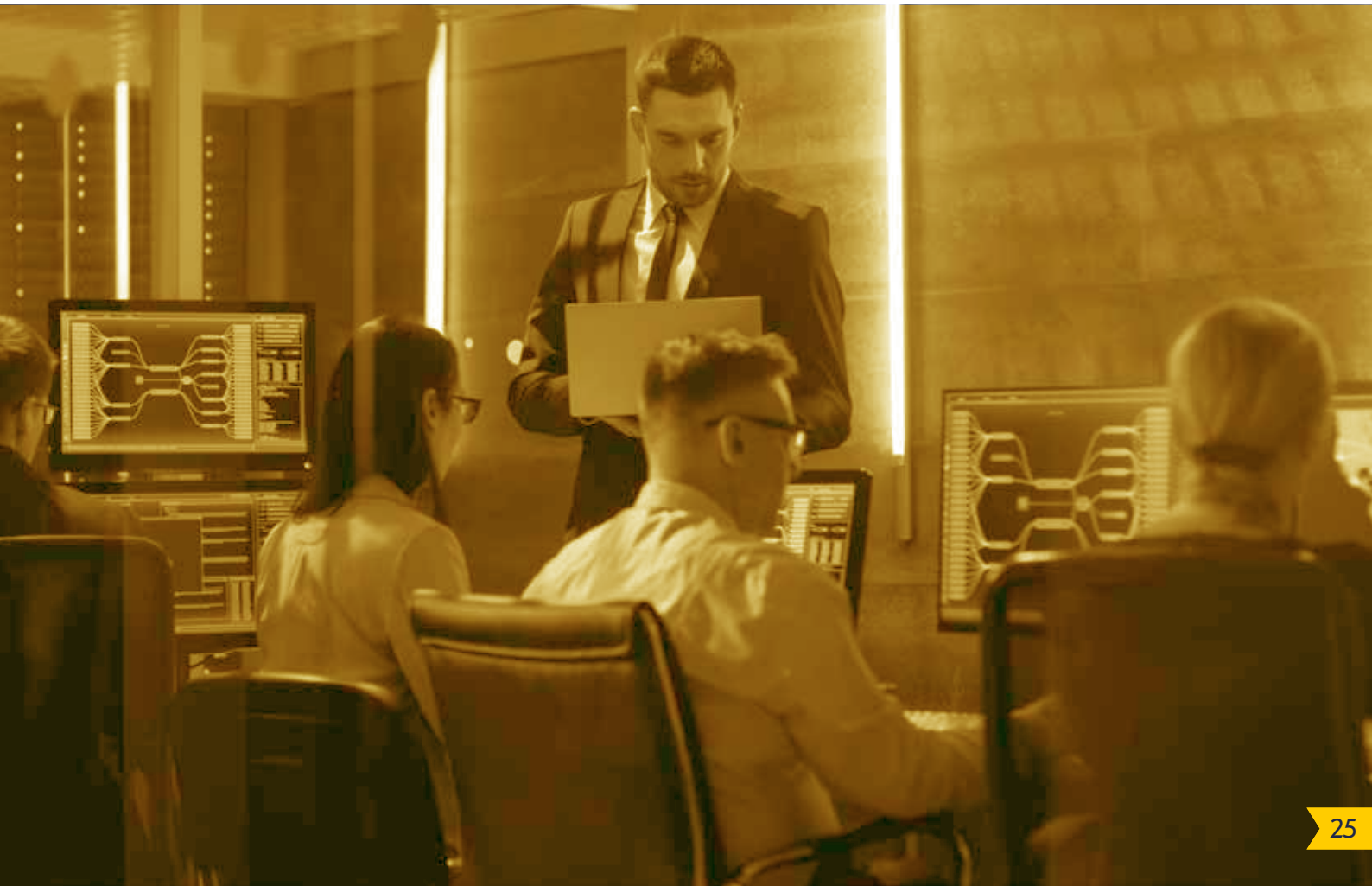
"We've work with the emergency planning side, so I deal with disaster recovery, which is a type of business continuity, but I also get involved with the business continuity side of emergency planning. We bolt the two together, from information assurance to legal and governance and HR as well."

Head of risk and resilience, education, UK

When it comes to the lower end of the collaboration scale, under half of respondents regularly work with Human Resource (44.6%) departments, which is concerning as staff are of intrinsic value in crisis response. For example, the BCI Emergency & Crisis Communications Report 2024[10] highlighted that the predominant cause of breakdown in crisis communication plans is the absence of response from recipients, chosen by 63.4% of respondents. The second most prevalent reason, chosen by 41.0%, is the lack of staff contact information. Additionally, in third place at 35.8% is the lack of understanding about what to do in a crisis. This shows that, despite high levels of training and exercising taking place, more still needs to be done to ensure that staff contact details are up to date. For this, constant collaboration with HR departments is key.

There is an understanding and awareness of the human risk factors as they key cause of crisis and resilience plans failure. However, without the involvement of HR departments, organizations are left exposed when dealing with a crisis which may result costly in terms of finances and reputation.

In addition, environmental, social, and governance (ESG) standards, used to measure an organization's environmental and social impact, garnered under a third of respondents' collaboration partnerships (31.8%). These lower interaction rates indicate a lack of leadership interest in people-focused strategies that may be due to economic pressures, as cost-saving measures often target people-focused initiatives first. Practitioners should ensure that HR and ESG collaborations do not fall off top leadership's radar, despite the prominence of economic, regulatory and cyber pressures that have dominated resilience programmes this year.



What other disciplines does your programme integrate/interact/collaborate with regularly to support your resilience and/or risk management?

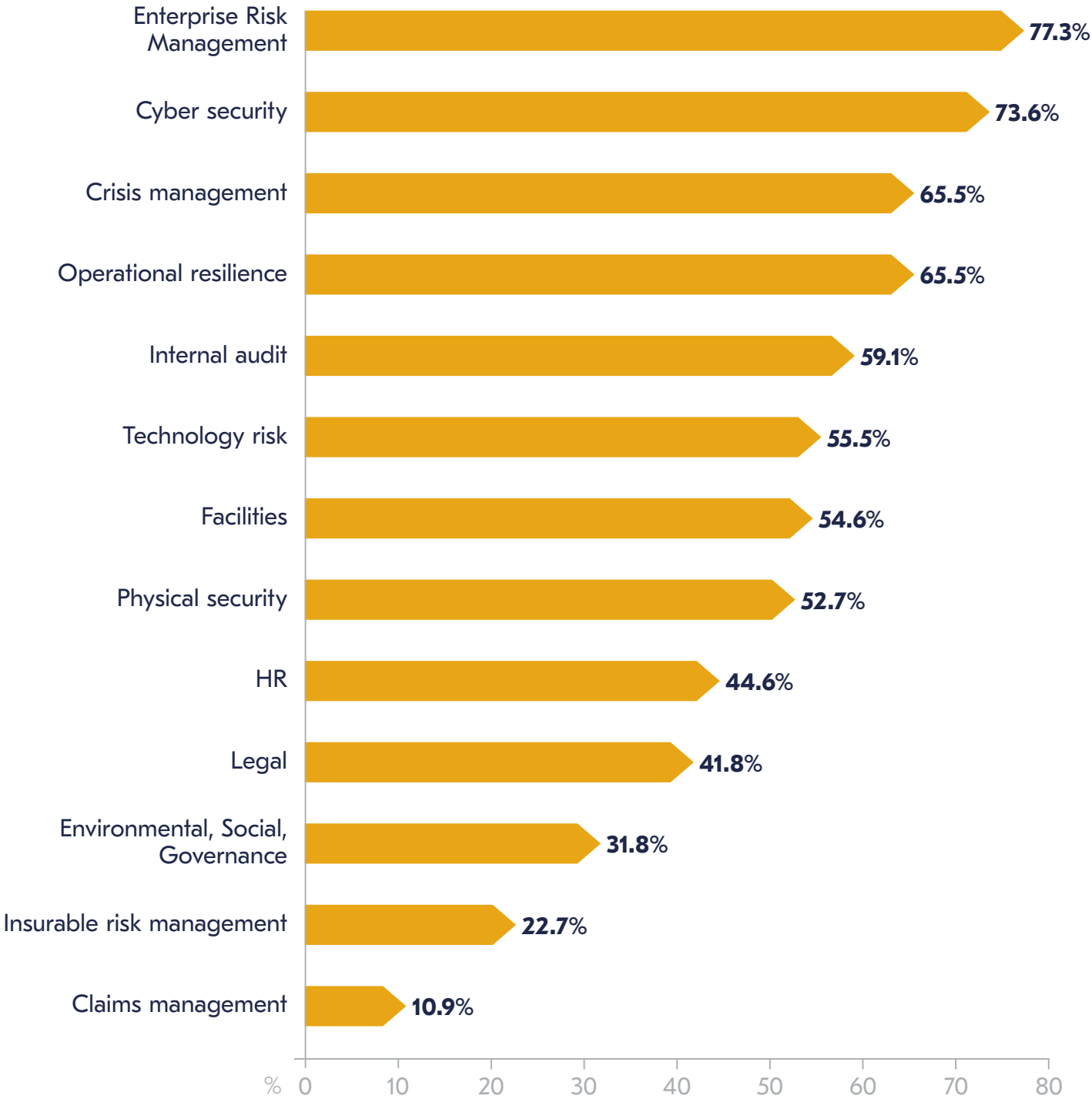


Figure 4. What other disciplines does your programme integrate/interact/collaborate with regularly to support your resilience and/or risk management?

An overview of Artificial Intelligence

An overview of Artificial Intelligence

- More practitioners are making their minds up about AI compared to last year, prompted by new developments both in AI and its regulation.
- Organizations are recognising and considering the positives of incorporating AI in their resilience efforts, however most remain wary.
- Fewer organizations will invest in AI in 2025.

The conversation around AI has gained momentum over the past year, with much discussion about AI's potential to automate, simplify, and potentially improve resilience functions. This chapter looks at how AI is being used, or not, in resilience strategies. Overall, more practitioners have made decisions on AI, but a level of uncertainty remains and will likely stay that way until legislation or regulations emerge to provide guidance.

"I think from a resilience space, there's probably a lot AI could do in terms of like pre planning, but I don't think that our sector has moved into that space at all yet."

Chief officer, public service, UK

The role of AI in organizations

Respondents were asked to consider the role of AI within its functions and, similar to last year's report, there are a wide variety of opinions in the sector. However, this year more practitioners have reached a decision around this topic. 41.3% of respondents were unsure about the role of AI last year, compared to a current 38.46%.

Over 40.0% of practitioners now consider AI a resilience enabler or disabler depending on its use, (2023: 36.4%). There is a slight swing towards distrusting AI in resilience settings. There have been a lot of new technologies launched this year, and equally new regulations have been brought in to safeguard people to the threats posed. However, Could this fast influx of new applications of AI be the reason for practitioners concern?

Indeed, interviews with practitioners showed that many were not introducing AI into certain practices, instead, adopting a 'wait and see' approach. This a was particular concern for the public sector.

"Many people have a certain level of ignorance and fear of AI. Some think it's under consideration because we want to get rid of the people, but that's not correct. I want to try and keep the people but have them doing other things. I don't think we'll see a particular expansion of AI over the next calendar year, but we'll certainly consider the strategy and start thinking about our capital investment. The costs are one thing, but there's the cost of not doing it too."

Chief officer, public service, UK

"We think it's early days as far as AI is concerned and we are watching. We are beginning to see it in some products and ventures, such as supply chains that we're putting in, but we're taking a cautious approach."

Continuity and resilience director, public sector, UK

"In terms of using AI in the BIA I don't know if it's advanced enough, and I know that we are not advanced enough to be able to use it yet."

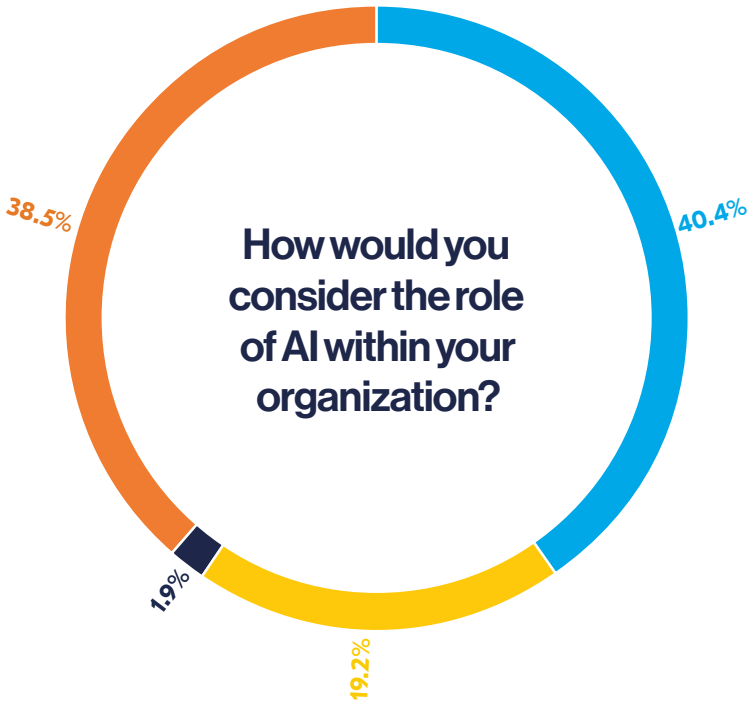
Chief officer, public service, UK

"We don't yet see a level of maturity to use AI in our BIAs. but it will develop, it will come. We just have to keep watching and understand the right time when it's appropriate to use and trust AI."

Continuity and resilience director, public sector, UK

"We're just starting to use AI cautiously. I, personally, am sceptical but willing to give it a try. My concern with AI is that the people that build it have a natural bias of their own that they can project into that model and I'm concerned about that. Eventually it will save a lot of labour intensive, busy work. We are considering introducing it into cyber resilience because it's such a significant threat and we are trying to find strategies to stay ahead of the curve in any way we can."

Resilience Manager, Group Business Resilience and Crisis Management, USA



40.4%
Both, resilience enabler/disabler, depending on the use

19.2%
A resilience enabler

1.9%
A resilience disabler

38.5%
Unsure

Figure 5. How would you consider the role of AI within your organization?

In terms of how important AI will be in supporting resilience activities in 2025, the highest rated answer suggested that AI would not be important to their organization (34.3%), a rise on last year's response (29.8%), which further suggests that more practitioners are making up their minds on how they might employ AI. However, 10.0% of this year's respondents suggested AI would be very important in 2025. In interviews, respondents stated the reasons they regarded AI as very important included their capacity to respond to the increased risk of cyber-attacks, and utilising capabilities to data mine large amounts of internal data were important to them.

"I consider AI a resilience enabler and it's going to be quite important in the next year in activities such as automating reports, providing information faster to assist with timely decision making and to improve activities with our consumers. It then becomes a complementary aid to facilitate resilience as people can respond when required and then focus on other pressing tasks."

Business continuity and governance consultant, social services, Australia

"We're currently introducing AI into the cybersecurity programme. It's very useful to put testing results into AI as it will give you a different lens to look through and challenge information or assumptions."

Continuity and resilience director, public sector, UK

"AI is an enabler - it's a helpful tool to get background knowledge and for table tops and building out different scenarios, and help outline basic BIA information, but you always need that human involvement. That's why I wouldn't use it to fully automate our BIAs, because with AI you run the risk of missing certain things that could be critical."

Business continuity manager, health USA

Just under a fifth of respondents are still unsure, demonstrating that there is still some distance to go before AI is fully understood and accepted by the resilience community.

"I think in the future AI will be far more nuanced about what informs it. I'd like to think that AI could draw lots of things together based on the parameters we give it, such as the kind of scenarios we'd like to see. If we can develop scenarios faster, we can have a broader range of scenarios to tap into."

Chief officer, public service, UK

"We've used AI for monitoring buildings in facilities management and we're researching with our cyber engineers about adaptive security and adaptive resilience, but I think as professionals we need to stand back, watch, and monitor."

Head of risk and resilience, education, UK

"We're waiting for AI guidance from the Australian government who are looking at it as a whole. Currently we're told not to use it in the workplace."

Risk management officer, healthcare, Australia

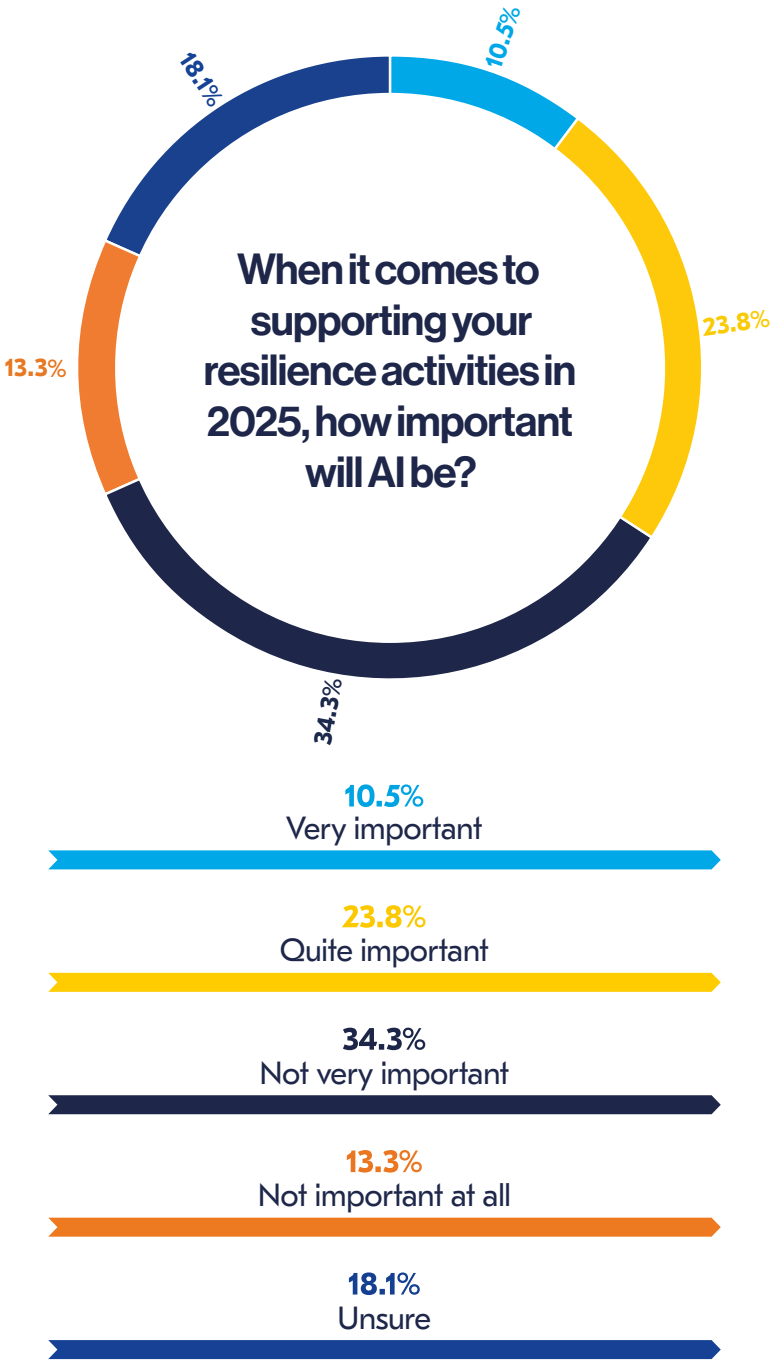


Figure 6. When it comes to supporting your resilience activities in 2025, how important will AI be?

Usage of AI within organizations

The BCI Technology in Resilience Report 2023[11] highlighted technologies used in resilience settings have increased in use by more than 500% since 2019. However, as we have seen so far, the uptake of AI in resilience is restrained. Just 5.9% of organizations currently embed AI practices such as cybersecurity support and risk assessment/ forecasting in their programmes. Authoring crisis communications scripts and post incident/ after action analysis (3.9%) were also highlighted as current uses of AI in organizations in minimal amounts.

The BCI Crisis Management Report 2024 found that some practitioners are using AI in training and exercising scenarios, potentially testing its capabilities in a 'safe' environment. The main uses of AI in training were helping to generate personalised incident scenarios and complex "what if" scenarios to help fully engage staff and thereby enhance resilience. In interviews, practitioners frequently cited their use of Copilot and ChatGPT to write timely crisis response communications in scenario testing.

"We had a very strong initial push with AI and bought software like copilot and rolled out training. Then it died down. So we had a very strong initial push, but there haven't been big developments since then. However, we are working on developing an acceptable use policy for AI because I think people still don't realise that they're feeding company data to all these AI models"

Business continuity manager, Telecoms, Hungary

"We are starting to use AI, such as ChatGTP, but my organization is very keen to be compliant with regulations, so we are very conservative with it. For example, we need to write an application to the supervisory department before using any kind of AI tools. We have used it more in 2024, for things like writing code, and I would like to use it in the future to create training scenarios."

Risk management and BC specialist, manufacturing, Japan

More practitioners have made up their minds on AI and, for some, the benefits are minimal, particularly in the public sector when bank balances are tight and the return-on-investment (ROI) in AI does not show the benefits for the wider society. In interviews, practitioners said they were undertaking a 'wait and see approach' before considering investing resources into AI, but accepted that AI was an incoming risk they would eventually have to address.

Despite its current minimal use, the picture is different when it comes to introducing AI into resilience programmes. The most popular uses under consideration by organizations are cybersecurity, creation of scenarios for training and exercising purposes, data mining, and risk assessment, highlighting practitioners' awareness of AI capabilities and its potential benefits.

A small number of organizations have already embedded AI into their programme or are currently doing so, in different capacities:

24.5%
Cybersecurity

17.5%
Creation of scenarios for training and exercising

15.8%
Data mining/ big data

15.7%
Risk assessment and forecasting

11.6%
Automation/semi-automation of the business impact analysis (BIA)

However, over half of respondents were not considering or will not be introducing AI into their business continuity and resilience programmes at all, underlining the current wariness of AI. This is backed up by the BCI Update Series: Cyber Resilience Report 2024 in which AI placed the fourth greatest threat to organizations over the next five years in terms of cyber security.

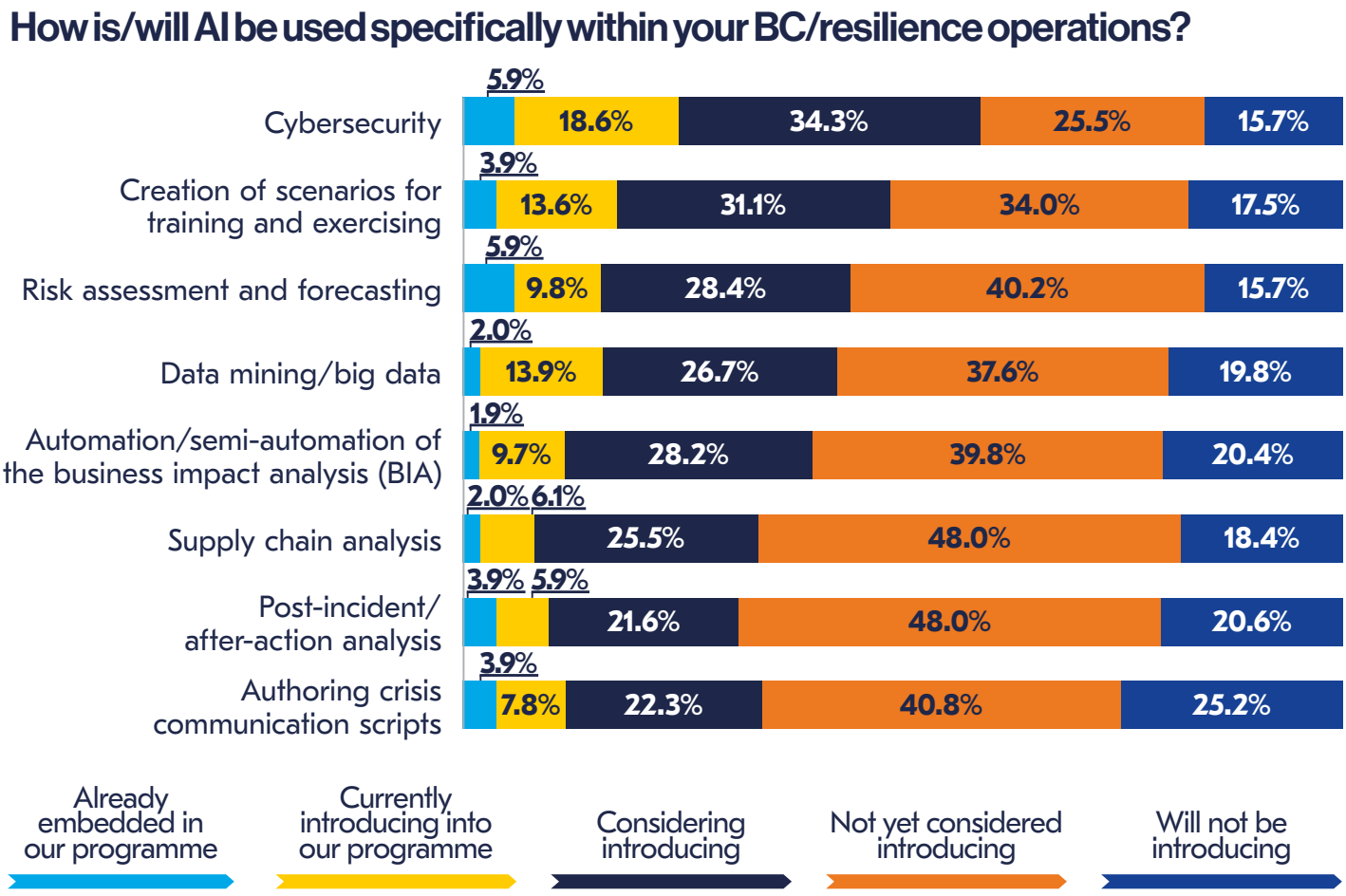


Figure 7. How is/will AI be used specifically within your BC/resilience operations?

AI spending in 2025

As already noted, more practitioners are identifying the benefits and challenges of AI in a resilience setting and this year's research suggests a decrease in spending on AI. Just under a quarter of respondents are unsure about spending on AI compared to last year's third; a further indication that practitioners are starting to make decisions on the use of AI. Interestingly, in 2023 only 9.1% did not intend to spend money on AI programmes over the following year. This figure has now increased to 15.25%. Reasons for less investment in AI may include global economic uncertainty, creating cutbacks in spending, leveraging of free available solutions, and increased leadership interest in regulations and cyber resilience which has taken priority, pushing back the emerging field of AI and its associated purchases, security considerations, and training costs.

Although more people have made decisions about AI over the past twelve months, there is still a long way to go, and AI will certainly be a topic of great interest in 2025. Regulations and frameworks are beginning to emerge, such as the European Union (EU) 2024 AI Act[12] that sets out European laws and a uniform legal framework that guides the development and uptake of AI systems in the private and public sectors. This was the first piece of legislation to address AI safety, and more legislation has now been introduced, with more on the way[13]. This includes the USA's October 2023 executive order for new standards on AI safety and security that requires AI systems developers share safety test results with the US government, and China's new regulation and governance framework for generative AI in 2024[14]. The incoming legislation may have had the effect of putting practitioner's views on hold, regulations, however, pave the way for new technologies, indicating that AI has a prominent future role.

6.7%
It will be much higher

29.5%
It will be somewhat higher

21.9%
It will be the same

2.9%
It will be somewhat less

15.2%
We won't spend any money on this area in 2025

23.8%
Unsure

Figure 8. Overall, how will your organization's spending on AI change in 2025 compared to 2024?

BC practices in 2024: attitudes towards the Business Impact Analysis (BIA)

BC practices in 2024: attitudes towards the Business Impact Analysis (BIA)

- Most are generally satisfied with their current BIA process, and there is a universal understanding of the importance of the BIA process across organizations.
- Nearly 3 in 4 of organizations would automate parts of their BIA process if suitable technology were available. While most organizations are open to using AI for BIA automation in the future, they would like to retain human involvement.

The business impact analysis (BIA) is a fundamental element of standard BC practice, and as such it is vital to understand how processes and attitudes change. This chapter analyses attitudes to the BIA, how technology has touched it over the past 12 months, and practitioners' attitudes to automating the process.

This year, over half of respondents consider themselves moderately satisfied with their current approach to the BIA process, marking an improvement from last year's results. It is also reassuring to note that fewer practitioners (3.85%) do not use a BIA process, an improvement on last year (6.7%). This positive change may be attributed to increased strategic involvement from top management who are in the position to encourage greater participation from various departments into the BIA. In addition, the BCI Horizon Scan Report 2024 found that new global operational resilience incorporates some of the principles of the ISO 22301 business continuity standards, such as identifying critical/important business services, which may promote the importance of a robust BIA process.

"We don't conduct a BIA from the analytical methods in the GPGs, instead our prioritised products are decided by top management."

Risk management and BC specialist, manufacturing, Japan

Less satisfied respondents reported their approach to the BIA process was outdated and needed refreshing to capture the organization's current needs, with issues such as time consuming manual processes and disconnections between BIAs/ current disaster recovery plans causing concerns.

Interviewees reporting they were very happy with their BIAs explained that they had recently overhauled their approach. This underlines the importance of regularly updating BIAs, so they fit an evolving organization's strategic aims and operational processes.

"We've just re-visited our BIA and corporate risk register based on the change of government. With a change of government, we have to consider their funding priorities."

Chief officer, public service, UK

"I'm happy with the BIA process because it's a consultative approach. Everyone is open to ideas and we can have conversations around what is important. It is also very beneficial to encourage managers to take ownership of BIAs."

Business continuity and governance consultant, social services, Australia

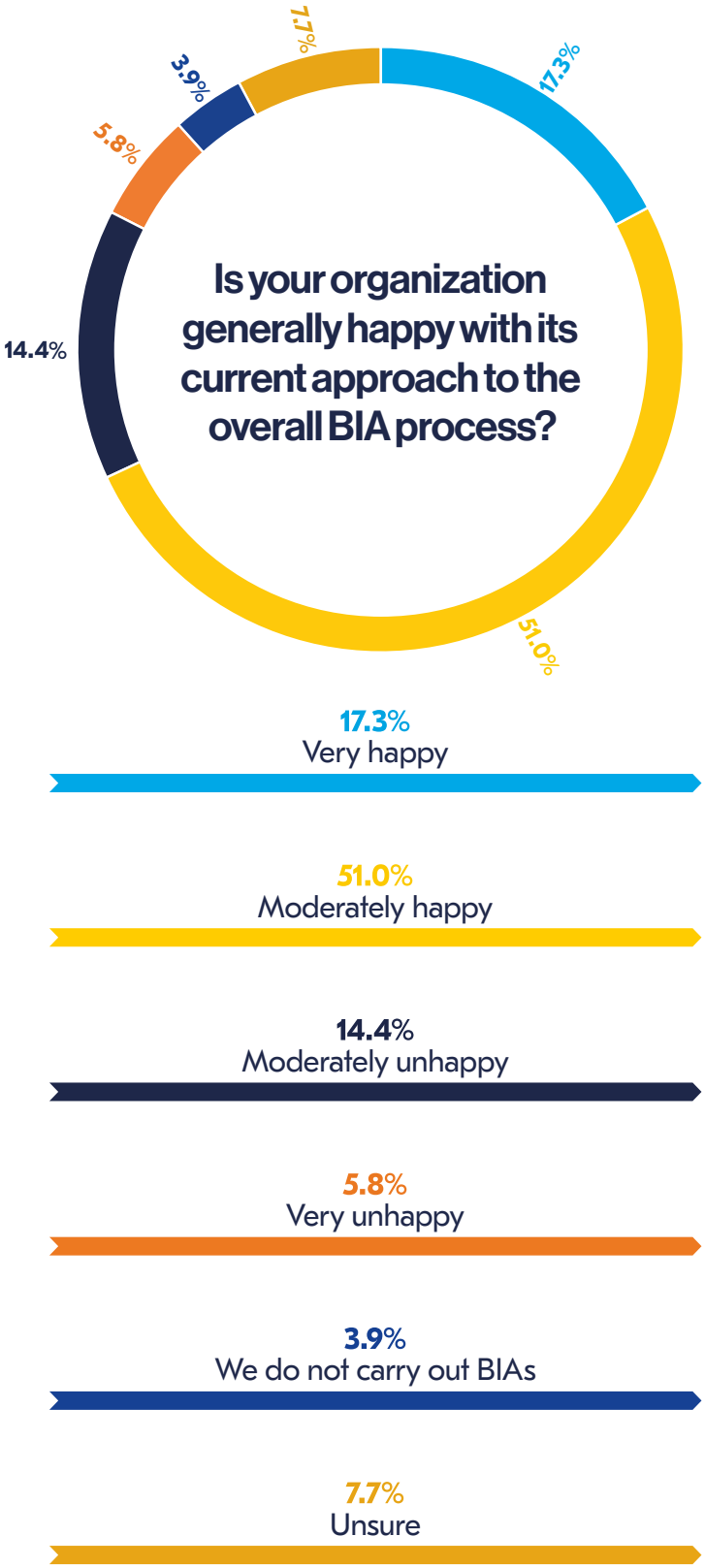


Figure 9. Is your organization generally happy with its current approach to the overall BIA process?

Most organizations use of technology to perform their BIA's

Over 70% of organizations rely on technology to conduct their BIAs. In 2024, there has been a slight increase in the use of standard business software like Excel, a minor decline in the use of specialised purchased or custom-developed software. However one in five organizations are still not leveraging technology for the creation of their BIAs.

Many interviewees who are not currently using specialist software say they are considering, or are already undertaking, a move to third-party software in the future, indicating a potential shift in priorities over the coming year. Organizations not currently considering BIA technology cited reasons such as the small size of their organization, which they feel does not necessitate technological tools, while others reported having no budget allocated for software.

22.9%
We use specialist software from a third party company to manage the BIA process

7.6%
We use specialist software that we have written to manage the BIA process

40.0%
We use standard business software to manage the BIA process

21.0%
We do not use software to manage the BIA process

4.8%
We do not carry out BIAs

3.8%
Unsure

Figure 10. What is your organization's attitude to using technology to help with the BIA?

Use of AI in the BIA

As mentioned in the earlier AI section, practitioners are slowly forming opinions on implementation of AI across organizations. Similar views emerged when respondents were asked if they would use a software tool to automate the BIA process, should one become available.

Emerging AI technology offers the potential to automate much of the BIA, and last year's response (58.8%) suggested practitioners would use AI to automate part of the BIA process, but would still retain human control. This year, there is a slight decrease in this response (53.3%). However, the number of practitioners who would fully embrace such technology rose from 15.0% to 20.0%.

Additionally, a small but considerable subset of respondents indicated they would not use such a tool at all (16.2%). Just a tenth of respondents remain unsure about an AI automation solution to the BIA process. This reinforces the above findings that more practitioners have made a decision about AI benefits and current challenges.

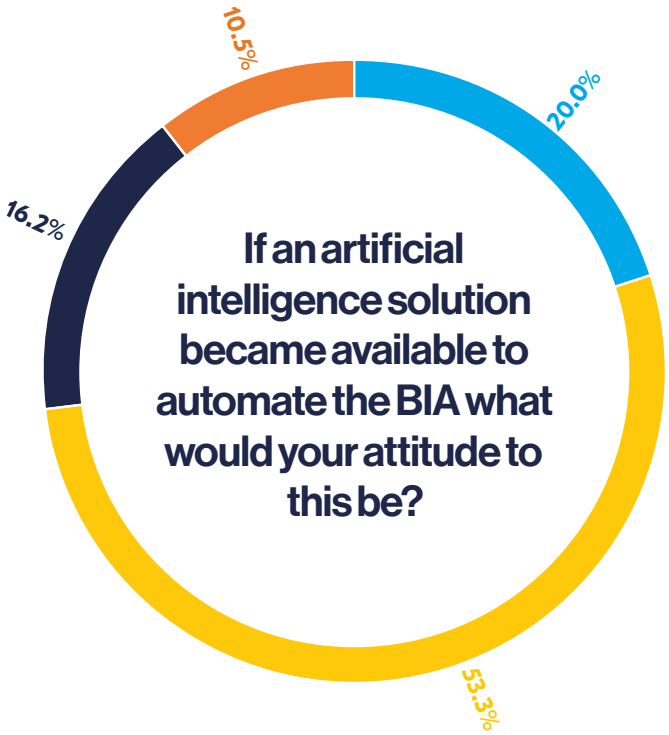
Most interviewees showed reluctance to let AI take complete control of what they considered to be a crucial resilience activity, and most pointed to the technology's early stage of development. Sharing their organization's sensitive and critical data with AI solutions was also seen as very risky. Despite this, interviewees were interested in what the future holds and, for the most part, they accepted that AI would eventually automate the BIA process.

"To use AI to create something like a BIA is risky, because firstly we would need to give our information, including detailed information about our supply chain and manufacturing processes, to an AI cloud, and then information security issues arise."

Risk management and BC specialist, manufacturing, Japan

"I'm open to using AI to support our BIAs. First, we'd look at the processes to see if any could be automated and then we'd have conversations around it, but I'd still check every step and conduct audits to retain the accuracy and the human element. I am not sure it is developed enough for high end finance decisions, taking minutes of meetings or for board meetings."

Business continuity and governance consultant, social services, Australia



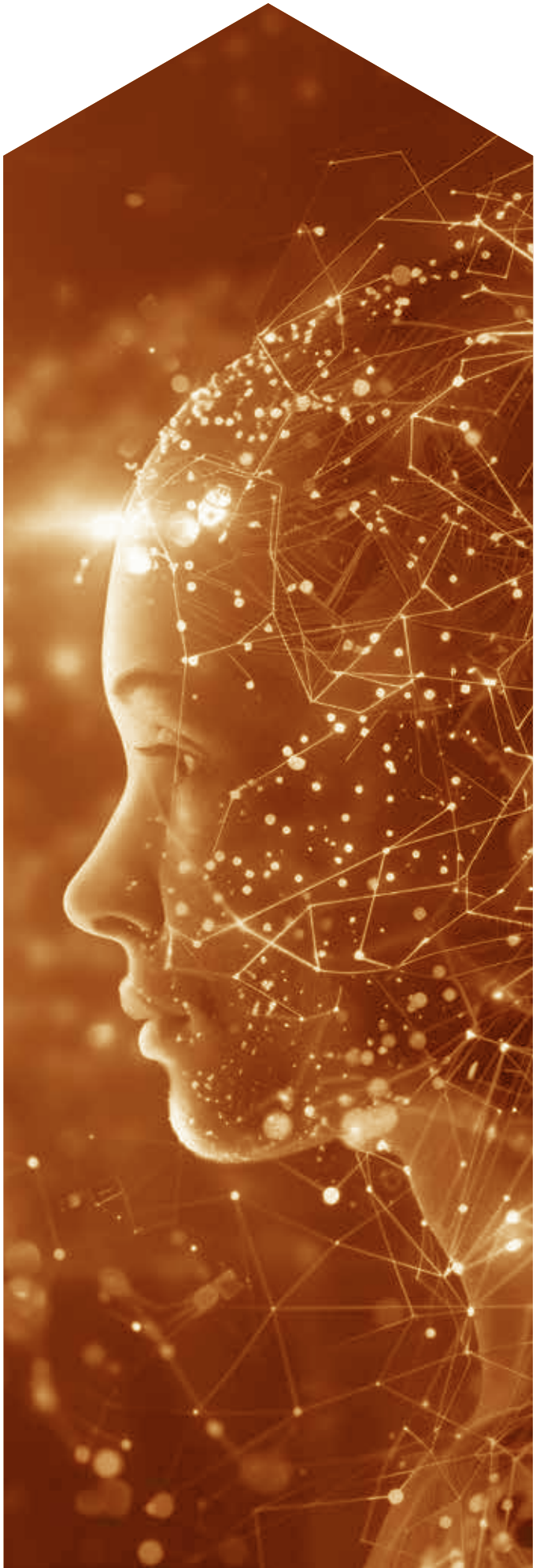
20.0%
I would fully embrace it — the more the BIA can be automated, the better

53.3%
I would use it to automate parts of the BIA process but would want to retain human input into the process as well

16.2%
I would not use it — AI cannot be trusted to develop an effective BIA

10.5%
Unsure

Figure 11. If an artificial intelligence solution became available to automate the BIA what would your attitude to this be?



6 Challenges

Challenges

- Regulations have been one of practitioners' greatest concerns in 2024.
- Multiple geopolitical developments pose risks to organizations this year, with economic uncertainty topping the list of threats.
- Climate threats continue to pose risks to organizations' operations and long-term stability, particularly on the supply chain.

In this chapter, we explore 2024's trending topics: regulations, geopolitical challenges, and climate risks, and examine what threats they posed to organizations over past 12 months.

As we have seen, regulations are a hot topic this year, especially in the realm of digital resilience. Last year's report suggested regulations were one of senior leadership's top concerns and this was expected to roll into 2024. This has certainly been the case as the majority of respondents (63.8%) report more regulatory pressures this year compared to last. Over a quarter of respondents feel that regulatory pressures have remained the same, and just 7.6% of respondents feel regulations have not increased for their organization. This mirrors abovementioned findings that regulations are one of the top concerns for senior management this year.

For many practitioners, new regulatory requirements of 2024 have created time, resource, and skill pressures, however a multitude of benefits have emerged too. Some organizations feel they have become more resilient as a result of it, such as the improvements made to supply chains where regulations have extended to third-party suppliers and outsourced providers. The downside is that some companies have been forced to stop working with certain suppliers who remain unaware of, or who cannot meet, the new requirements placed on them.

While some interviewees are satisfied that they have done enough to meet incoming legislation, with some having completed necessary activities months in advance, others are sceptical of their ability to meet upcoming regulations, and feel that other organizations are in the same boat, leading to concerns around increased pressures and potential fines months after implementation deadlines.

"We're based in Europe, so NIS2 is applicable. Due to recent regulatory changes, there is less time pressure, but meeting all the requirements will be a huge challenge. We've had some recent developments from the legislator; I think they realized as well that no one will be able to comply in time — so the deadline has been extended to EOY 2026. There is, of course, still quite a lot of pressure on us, but now it's more about meeting the requirements, rather than the deadline."

Business continuity manager, Telecoms, Hungary

33.3%
Yes, very much so

30.5%
Yes, somewhat

26.7%
About the same as last year

7.6%
No

1.9%
There are fewer regulatory pressures

Figure 12. Do you feel there are more regulatory pressures on your organization this year compared to 2023?

Geopolitical trends affecting resilience in 2024

Practitioners view global economic uncertainty as the most significant geographic threat in 2024, with nearly 70% of respondents indicating it poses a risk to their organization's operations and long-term stability.

The persistence of inflation and recession, and the consequences of higher prices, are imposing a significant toll on organizations across the globe this year, and it looks set to continue in the future.

The BCI Horizon Scan Report 2024 identifies the increased cost of living crisis as a leading threat for organizations this year, making it the only risk to rank in the top five in 2023 and 2024. Rising costs are creating significant challenges, with nearly a third of respondents seeking additional financing to cope with inflationary pressures.

The cost of living has a substantial impact on organizations and their workforce. Research from the Lancet Inflation and Health: A Global Scoping Review[15] found that high levels of economic inflation can adversely affect societies and individuals in many ways, such as their life expectancy and mental health, with specific socioeconomic groups facing greater risks. In addition, the Gallup State of the Global Workplace Report 2024[16] that found global employee engagement has stagnated, and overall employee wellbeing has declined, a trend that has increased for multiple consecutive years. This low engagement costs the global economy an estimated US$8.9 trillion, or 9% of global GDP, so it is no surprise that practitioners rate economic uncertainly as one of their top geopolitical risks.

The second greatest threat reported by respondents are regulatory changes with nearly half of organisations reporting they posed a risk to their organization. This will come as no surprise given the number of respondents reporting a rise in regulatory pressures during 2024.

There has been an increase in operational resilience regulations around the world, and many organizations face compliance with multiple regulations and standards. The BCI Operational Resilience Report 2024 illustrated that two-thirds of organizations comply with between one and five different regulatory schemes, and nearly a fifth (18.4%) have to meet the requirements of more than five. Some may argue that as a result, regulations have increased the risk of error, along with the need for additional staff time and investments to comply with new requirements, ultimately producing the opposite effect intended by regulatory bodies.

Political stability is affecting key markets

Political stability in key markets is recognised as a top geopolitical threat in 2024, with under half of respondents (45.6%) reporting it is a concern. This is mirrored by the BCI Horizon Scan Report 2024[17] which highlights the negative effects of geopolitical event on global supply chains and energy markets, and introduces political violence/civil unrest and war/conflict as new concerns, indicating that political stability and its resulting tensions now pose increasingly significant challenges for organizations. In addition, findings from The BCI Supply Chain Report 2024 indicate a potential shortage of materials and the possibility of major trade route closures due to politically motivated violence, such as the Houthi pirate attacks on shipping in the Red Sea, that has forced shipping companies to re-route journeys, creating longer transit times and higher costs for customers.

This year, political risk and violence is at its highest position since 2017 on the Allianz Risk Barometer[18], indicating global concerns over the threat of violent outbreaks and politically motivated disruption. This is partly due to the increased number of back-to-back elections. 2024 has been dubbed the Year of Elections with over 60 countries heading to the polls, all resulting in varying degrees of change and conflicts. Protests broke out across Europe, Mexico, and South America as a result of political change or rhetoric, and the United States' highly anticipated election resulted in clashes on and off the political stage. This disruption has influenced global economies and policies, and stirred violence against certain ethic groups — all topics that pose substantial risks for resilience professionals.

Other geopolitical threats reported by respondents this year include ungoverned AI, cross border conflicts, international security, strikes and trade/domestic conflicts, trade and tariffs, and energy security, all of which indicate the current instability of global politics and the long-lasting consequences that will emerge from it in the coming years.

"In terms of geopolitical risks, we have already stopped trade with Russia. We're also concerned with the relationship between China and Taiwan. We are heavily dependent on China for manufacturing and getting supplies. Conflicts in the Middle East is a concern too, because our supply chain and sales will be affected by it."

Risk management and BC specialist, manufacturing, Japan

"Energy security is always a concern especially around supply and demand. Right now, there's a concern that electric vehicles and charging stations and demand for new data centres to support AI present a bigger pull on the bulk electric grid than before and we're going to have to find ways address that. If the supply doesn't meet the demand, you're going to see geopolitical response to it."

Resilience manager, group business resilience and crisis management, USA

"The EU is putting a lot of pressure on Chinese suppliers and our infrastructure is quite heavily reliant on Chinese infrastructure, so that's a risk for many telecom providers."

Business continuity manager, telecoms, Hungary

"Instability in Europe is a particular geopolitical trend that's worrying us. I'm concerned about major regulatory changes coming in under emergency powers and possible changes to the energy distribution networks in the future."

Head of risk and resilience, education, UK

Which top three specific geopolitical trends do you believe pose the greatest threat to your organization's operations and long-term stability in 2024?

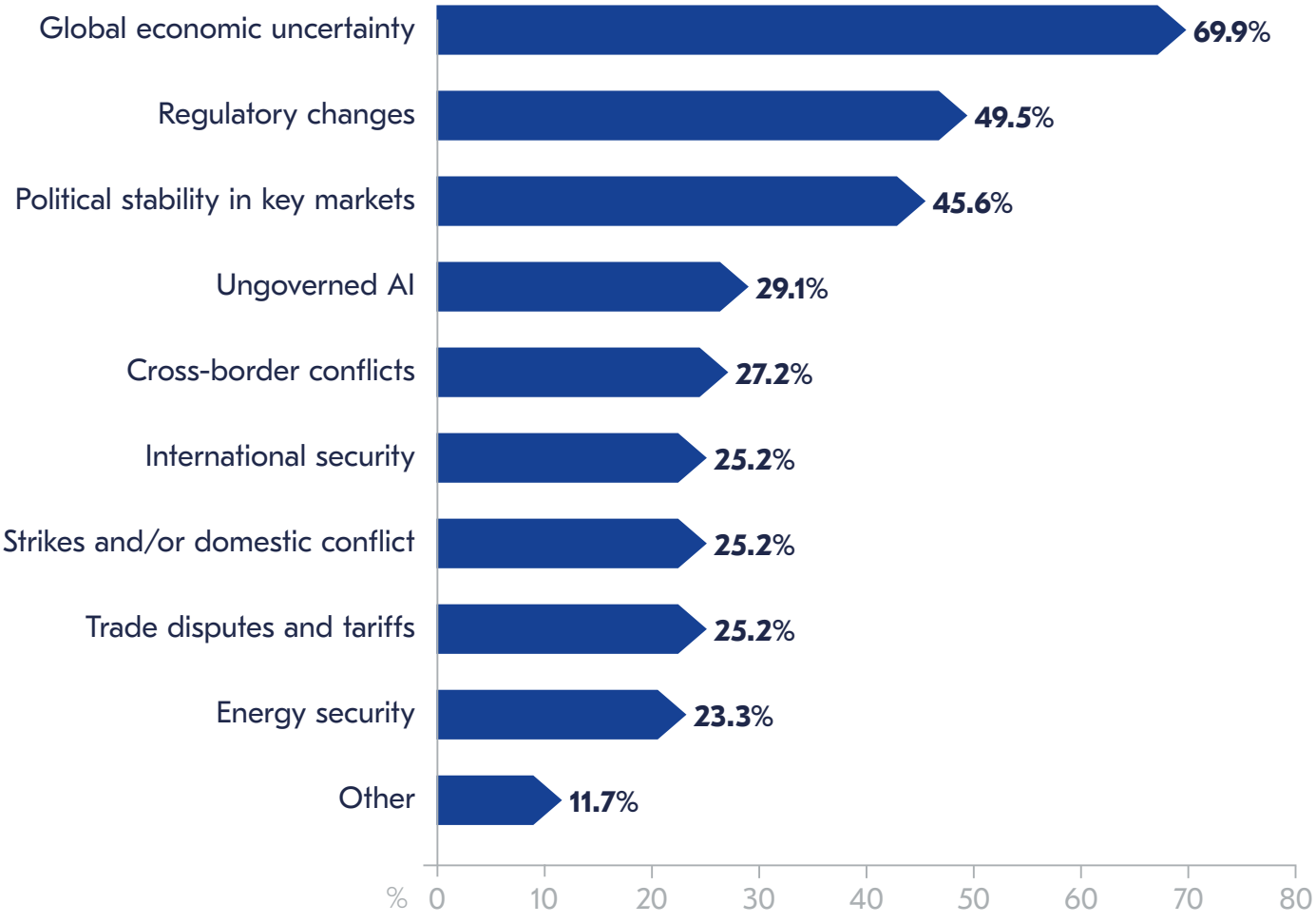


Figure 13. Which top three specific geopolitical trends do you believe pose the greatest threat to your organization's operations and long-term stability in 2024?

The effects of a changing climate

2024 has seen coverage of weather-related events dominating the media, from wildfires across Europe and the USA, to heatwaves in Asia, from devastating floods in Africa, to destructive hurricanes in the Americas. This widespread reporting has highlighted the impacts of a changing climate.

When respondents were asked to rank the top three climate-related risks to their organization, the top place resulted in a tie between supply chain disruptions and the physical impacts of climate-related events.

These results are not surprising as The BCI Extreme Weather and Climate Change Report 2023[19] found that 44.4% of respondents had experienced a moderate or significant impact from climate-related events over the past five years, and supply chain disruption was the most experienced disruptive effect. Underlining this are the findings from this year's BCI Horizon Scan Report that highlights extreme weather events have reached a risk index of 8.4, rising from last year's score of 6.3, indicating an ever-rising tide of climate events and disruptions.

Interviewees revealed climate related events that impacted their organizations over 2024 included floods, extreme heat, wildfires, and heavy snowfall. Weather related events are now happening in places that have previously been untouched by serious weather phenomenon's before (such as Spain) and therefore organizations have been sorely unprepared for them.

"We've got to provide some really fundamental services such as power, water, electricity, hospitals and sewage works. It's environmental events that create change outside the capability of what we're able to do and that presents a threat to us. The world is getting more unsettled weather and our challenge is we're an island with limited resources. We can't call in more resources quickly, we have to manage on our own for a period of time. We've got to be self-sufficient, and that does need focus and preparation."

Continuity and resilience director, public sector, UK

"The climate is changing here. In October the temperature is still 30 degrees, and we've had many massive typhoons and dealt with the heavy rain they bring. This year for the first time one of our main factories was affected by flooding. The surrounding city was flooded so badly that workers couldn't commute."

Risk management and BC specialist, manufacturing, Japan

"We don't have huge hurricanes or earthquakes, but we are definitely starting to see the impact of heatwaves, such as spending on cooling our data centres. If there's a power outage it's a problem, so we are developing a specific switch off plan that prioritises which systems can be turned off. People are realising it's a trend that will keep happening."

Business continuity manager, telecoms, Hungary

"Currently, our company is conducting a deep dive to assess our exposure and determine the necessary actions in light of the rapidly changing climate. We have many miles of electric transmission and distribution lines running through forest areas and open fields and things like that which are subject to bush or even larger wild fires due to a changing environment. These heat-related aspects worry us as we have seen them occur more frequently and with greater risk in other geographies all exacerbated by Climate Change."

Resilience manager, group business resilience and crisis management, USA

Although the BCI Extreme Weather & Climate Change Report 2023 highlights that many organizations have felt the effects of weather-related events, many still treat extreme weather as isolated occurrences and fail to move to a proactive mindset. However, the shifting climate's severe effects on supply chains has contributed to increased action this year. According to the BCI Supply Chain 2024 report, an encouraging majority of organizations now assess their supply chain's vulnerability to weather events and natural disasters. Although just over a third of respondents do not yet analyse climate risk, many intend to so in the future, and robust supply chain mapping and intelligence on all tier levels has risen over 2024, highlighting the growing recognition of climate threat to supply chains.

As severe weather events increase, the risks they pose to organizations grow significantly. The World Meteorological Organization (WMO) reports that extreme weather events have surged by a factor of five over the last 50 years and they are still on the rise. Keeping this issue on corporate agendas is essential for long-term resilience.

Which top three specific climate-related risks do you believe pose the greatest threat to your organization's operations and long-term stability in 2024?

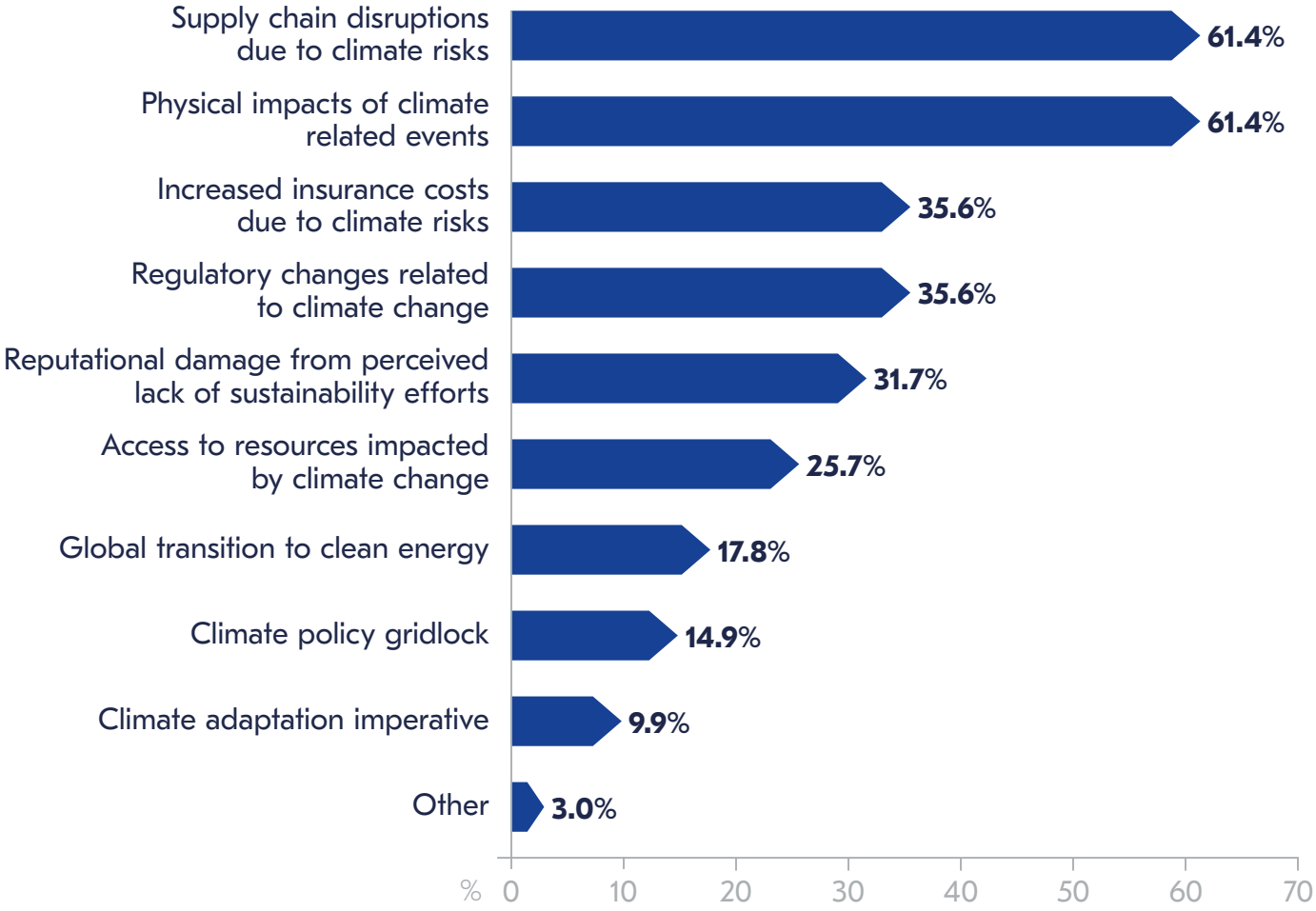


Figure 14. Which top three specific climate-related risks do you believe pose the greatest threat to your organization's operations and long-term stability in 2024?

7

Spending in 2025

Spending in 2025

- Despite global financial pressures, the majority of respondents anticipate that their business continuity and resilience budgets will either remain the same or will increase in 2024
- Cyber resilience is the area where most respondents anticipate a budget increase in 2024, reflecting the additional resources needed to address the growing complexity of cyber-attacks and other digital demands.
- More organizations than last year now anticipate reduced budgets over the next twelve months, indicating that economic instability is impacting resilience funding for some organizations.

This chapter explores spending priorities in 2025, the potential implications for resilience initiatives, and whether the priorities outlined by senior leadership in the first section of this report translate into increased investment.

Practitioners were questioned on their expected budget changes in 2025 compared to 2024. It is positive to see that, despite global financial pressures, most respondents expect their business continuity and resilience budgets to either stay the same or rise next year.

Over half of respondents expect their overall BC and resilience budgets to remain the same, suggesting organizations will focus on maintaining their existing capabilities and absorbing the cost of inflation, rather than expanding.

> **"A lot of increased spending is due to inflationary costs, but budgets have been cut and we have to be really careful about where we spend the money. The focus for us is on cyber, penetration testing and other cyber essentials."**
>
> Chief Officer, Public Service, UK

An encouraging 38.46% expect a much higher, or somewhat higher, budget despite the current challenging economic situations. This indicates the importance of driving resilience activities forward by leadership teams and an active ongoing interest in the sector, perhaps intensified by the increase in crisis management team activations and viral global news stories reporting incidents such as cybercrimes, extreme weather, floods and wildfires, and increasing political tensions.

"Government regulations on visa requirements have created a lot of pressure in the higher education sector. Some redundancies will occur across the sector due to budget constraints, but expenditure overall is increasing."

Head of risk and resilience, education, UK

"Our budget will be higher next year as we must do detailed gap assessments for all our systems to find what's missing, including disaster recovery plans and contingency plan for example. Then we'll have to spend to develop those to meet regulations."

Business continuity manager, telecoms, Hungary

However, for some organizations, budget cuts loom large. Last year, only 6.3% of respondents expected a decrease in funding, whereas this has now risen to 10.2%. Overall, this financial outlook points towards some belt tightening, perhaps partly due to outlay on imminent regulations having already taken place, and a gloomy future economic outlook. The Economic Intelligence Unit's 2025 Look Ahead Report[20] expects US economic growth to slow going into 2025, predominantly driven by a cooling labour market and high interest rates, and the International Monetary Fund's October 2024 World Economic Outlook Report[21] predicts the global economy will grow, but geopolitical risks will remain threats to global stability and growth — all predictions likely to stifle senior management spending.

Figure 15. How will your organization's overall business continuity and resilience budget change in 2025 compared to 2024?

Spending priorities for 2025: Cyber resilience

The top area for next year's spending is cyber resilience with almost 60% expecting income for cyber to increase in the next twelve months. Of those expecting more income, a quarter of them expect much higher budgets.

Cyber resilience spending leading the chart is unsurprising given top management's strategic and direct management interest in the subject. These numbers reflect last year's research, where the majority of organizations also expected cyber to account for the biggest rise in resilience expenditure. Reasons for this focus ongoing focus on cyber resilience, despite a challenging economy, is likely to be incoming digital regulations, coupled with the ever-increasing rise in complexity of cyber-attacks. The BCI Horizon Scan Report 2024 found that as technology becomes an ever-intrinsic part of organizations' day-to-day operation, they become more vulnerable to cybercriminals targeting sensitive data, customer information, and financial systems. This necessitates the need for more robust cybersecurity measures to protect digital assets and requires budgets to achieve it.

15.4%
It will be much higher in 2025 than in 2024

44.4%
It will be somewhat higher in 2025 than in 2024

30.8%
It will be the same

6.0%
It will be somewhat less in 2025 than in 2024

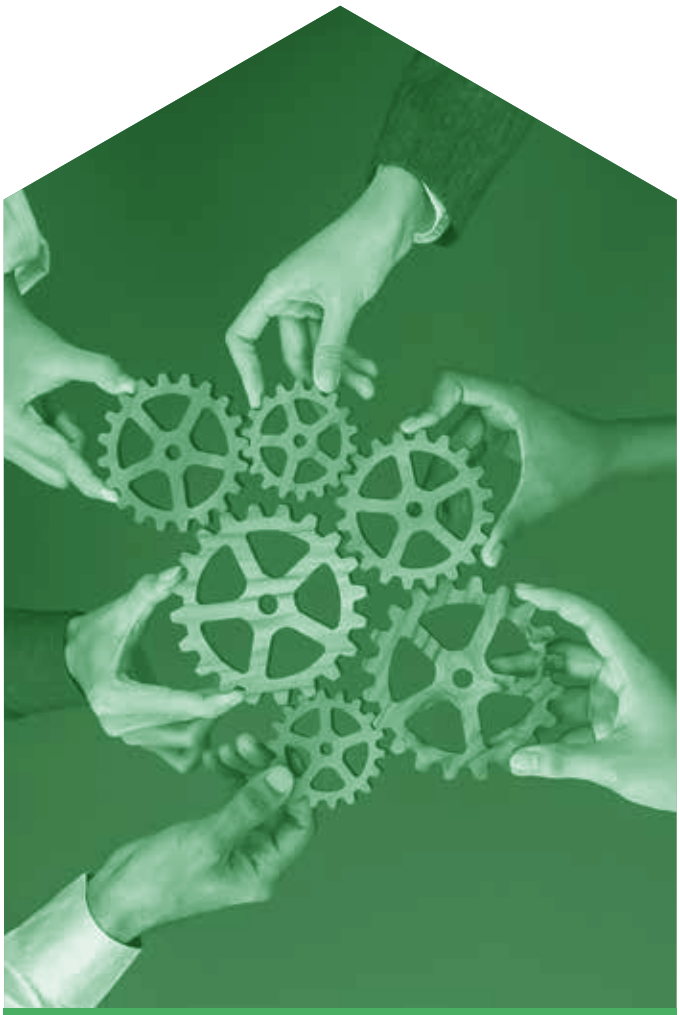
0.9%
It will be much lower in 2025 than in 2024

2.6%
We won't spend any money on this area in 2025

Figure 16. How will your organization's spending on cyber resilience change in 2025?

Business continuity management (BCM)

Looking at the upcoming year, the most popular response to spending on BCM is that it will remain the same, with just under half of organizations expecting stable levels of investment. This is a dip from the previous year and indicates that other areas are taking leadership priority, such as cyber security and meeting regulatory requirements.



"We do not expect to allocate additional funds to crisis management next year, as we have recently updated our plans to encompass our entire enterprise in the US and UK."

Resilience manager, group business resilience and crisis management, USA

7.7%
It will be much higher in 2025 than in 2024

30.8%
It will be somewhat higher in 2025 than in 2024

47.9%
It will be the same

6.8%
It will be somewhat less in 2025 than in 2024

2.6%
It will be much lower in 2025 than in 2024

4.3%
We won't spend any money on this area in 2025

Figure 17. How will your organization's spending on business continuity management change in 2025?

Operational resilience

In 2025, a significant portion of organizations are preparing for higher operational resilience budgets, with 42.2% expecting increases and a further 4.0% anticipating budgets to remain steady. This anticipated rise in funding is largely driven by the upcoming implementation of new regulations, such as the Digital Operational Resilience Act (DORA), CPS 230 Operational Risk Management, the UK's FCA/PRA/Bank of England operational resilience regulation and the Security of Critical Infrastructure (SOCI) Act . Although the NIS2 directive has been postponed until 2026, many organizations have already finalised their 2025 budgets, reflecting a proactive approach to meeting regulatory demands and reinforcing resilience capabilities well in advance.

8.6%
It will be much higher in 2025 than in 2024

33.6%
It will be somewhat higher in 2025 than in 2024

44.0%
It will be the same

5.2%
It will be somewhat less in 2025 than in 2024

3.5%
It will be much lower in 2025 than in 2024

5.2%
We won't spend any money on this area in 2025

Figure 18. How will your organization's spending on operational resilience change in 2025?

Crisis management

The majority of respondents (54.6%) expect their crisis management budgets to remain steady, while 34.5% anticipate increased spending next year. This marks a rise from last year, when only 31.8% forecasted higher crisis management expenditures, suggesting an increase in recent incidents may be driving up investment in this area.

This increase in incidents is highlighted in the BCI Crisis Management Report 2024, where 75.1% of organizations activated their crisis management teams in the past twelve months in response to a variety of threats, including severe weather events and third-party failures.

5.9%
It will be much higher in 2025 than in 2024

28.6%
It will be somewhat higher in 2025 than in 2024

54.6%
It will be the same

4.2%
It will be somewhat less in 2025 than in 2024

2.5%
It will be much lower in 2025 than in 2024

4.2%
We won't spend any money on this area in 2025

Figure 19. How will your organization's spending on crisis management change in 2025?

8 Key Takeaways

Cyber risks remain high

Cybersecurity has remained the primary concern for senior management in 2024. The frequency of cyber-attacks has continued to increase, and the rise of AI has offered cybercriminals new attack vectors. This risk will continue to pose a threat into 2025 and beyond.

What resilience professionals need to do:

Regular, monthly training for staff to recognize malicious emails, combined with ongoing penetration testing, plays a critical role in safeguarding an organization against attacks. Consistent training helps ensure that employees are equipped to detect potential threats early, reducing the risk of breaches. Paired with penetration testing to identify and address vulnerabilities, such measures strengthen the organization's defences against increasing complex and difficult-to-detect cyber threats.

Regulations have increased pressures

This year, regulatory requirements have added pressure to many organizations' resilience programmes, and they feature on senior management's priority list as a result. With operational resilience regulations now extending beyond the finance sector, compliance requirements are increasingly affecting IT providers, cloud solution providers, and other outsourcing partners. Most resilience professionals anticipate their budgets will remain steady or increase next year, and the additional obligation to comply with new regulations may result in extra funding for resilience departments.

What resilience professionals need to do:

It is important to remember that compliance should not be reduced to a mere tick-box exercise. Instead, management should engage the entire organization to ensure that a resilient mindset is embedded across all levels and every member of staff knows the part they play in ensuring the resilience of their organization. The majority of operational resilience regulations have been positively received by professionals, and there are more emerging in many industries and regions.

Economic difficulties will continue to create risks

Inflationary pressures and the rising cost of living have created pressures for organizations' finances and staff wellbeing this year. With a gloomy economic forecast and political upheaval still to come, this looks set to continue.

What resilience professionals need to do:

To foster personnel resilience, practitioners should collaborate closely with HR and management to develop and implement strategies that support employees facing mental health challenges due to the pressures of rising inflation. Additionally, organizations should seek to renegotiate terms with suppliers, ensuring that suppliers are not experiencing financial hardship. This comprehensive approach helps create a more adaptable and resilient workforce while safeguarding the organization's financial stability.

Supply chain awareness

Management awareness of supply chain vulnerabilities has increased this year. However, geopolitical threats, coupled with an increase in weather related events, ensure they remain vulnerable.

What resilience professionals need to do:

Over the coming year, it is important to ensure supply chain management does not fall far from leadership's radar. It is essential to maintain a strong focus on supply chain management, keeping senior management informed of emerging risks while continuing to prioritise horizon scanning. Organizations should invest in technology where possible to aid in supply chain mapping, enabling a comprehensive understanding of vulnerabilities, such as backup suppliers sourcing from the same primary supplier . Regular meetings with critical suppliers should be held to gain firsthand insight into potential disruptions, and organizations must ensure that due diligence processes are thoroughly completed before contracts are signed. It is also key not to overlooks specific areas such as climate-related vulnerabilities or rising political tensions within the supply chain as these are crucial factors to evaluate, as they significantly impact operations.

AI is one to watch

Although more practitioners have made decisions over AI, the field is increasing in complexity and more technologies will become available in 2025. With many practitioners currently 'watching and waiting' AI is highly likely to remain a subject of interest and regulatory action.

What resilience professionals need to do:

Resilience professionals should closely monitor the effectiveness of AI in transforming resilience practices. As AI capabilities continue to advance, ignoring its potential could result in a competitive disadvantage. It is advisable to experiment with AI tools and technologies that have already been tested by other resilience professionals and ensuring the organization has a clear AI-policy developed around its usage. Additionally, engaging with peers in special interest groups can provide valuable insights and help ensure that you remain at the forefront of industry developments, leveraging the latest innovations to strengthen your resilience strategies.

Collaboration is improving but there's still work to be done

Although the increase in regulations is helping to drive enhanced collaboration between departments there is still much work to be done to break down silos and ensure and fostering more integrated efforts across departments.

What resilience professionals need to do:

To strengthen overall organizational resilience, professionals should continue to promote cross-functional collaboration, ensure clear communication channels, and work towards aligning strategies across teams. Resilience professionals can lead this effort by facilitating regular coordination between departments, advocating for shared goals, and driving initiatives that support a unified, organization-wide resilience approach. BCI's recently launched Resilience Framework provides clear guidance on how to implement resilience within organizations, with collaboration between departments being a key part of it.

Annex


2126548
4395792
4567356
4395792
1312658
3852575
4637457
3852575
8674424

2nd - 20th September 2024.

Survey dates

119

Respondents

35

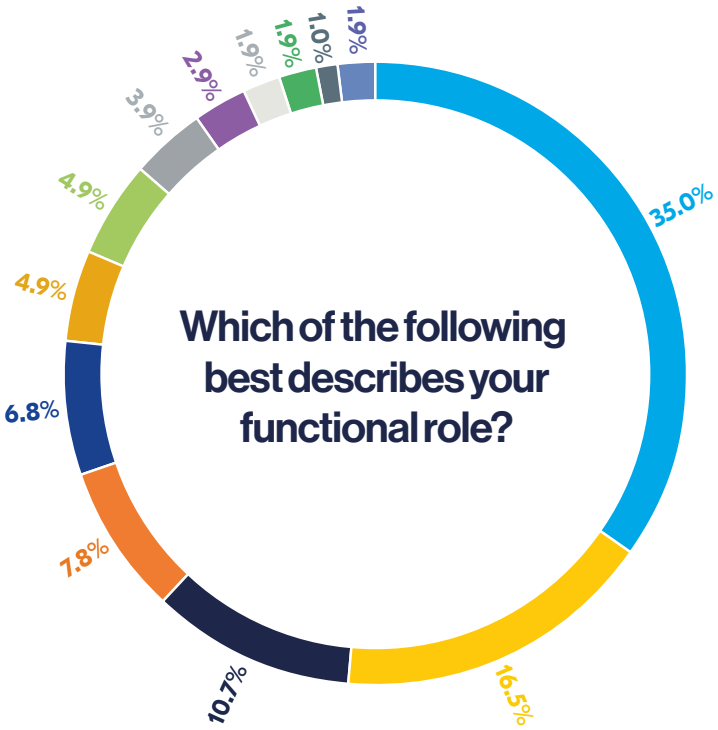
Countries

15

Sectors

10

Respondent interviews



35.0% Business continuity

16.5% Operational resilience

10.7% Risk management

7.8% Organizational resilience

6.8% Consulting

4.9% Emergency planning

4.9% Top management

3.9% IT disaster recovery/ IT service continuity

2.9% Supply chain and logistics

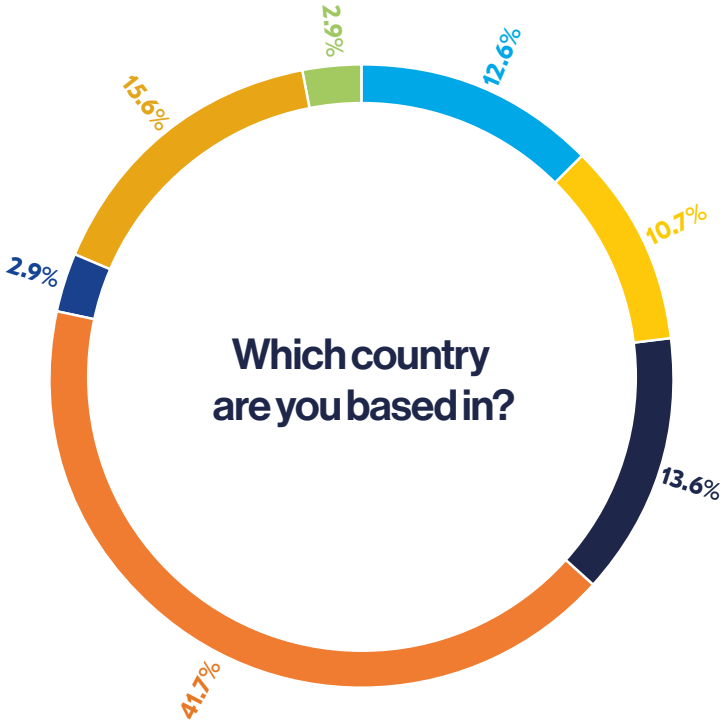
1.9% Crisis management

1.9% Quality/ business improvement

1.0% Information security

1.9% Other (please specify)

Figure 20. Which of the following best describes your functional role?



19.4% Financial & insurance services

17.5% Professional services

13.6% Public administration & defence

10.7% Health & social care

7.8% Education

7.8% Energy & utility services

4.9% IT & communications

4.9% Telecommunications

4.9% Transport & storage

2.9% Manufacturing

1.9% Engineering & construction

1.0% Agriculture, forestry & fishing

1.0% Charity

1.0% Retail & wholesale

1.0% Support services

Figure 21. What sector does your company belong to?

12.6% Africa

10.7% Asia

13.6% Australasia

41.7% Europe

2.9% Middle East

15.6% North America

2.9% South America and The Caribbean

Figure 22. Which country are you based in?

How many countries does your organization operate in?

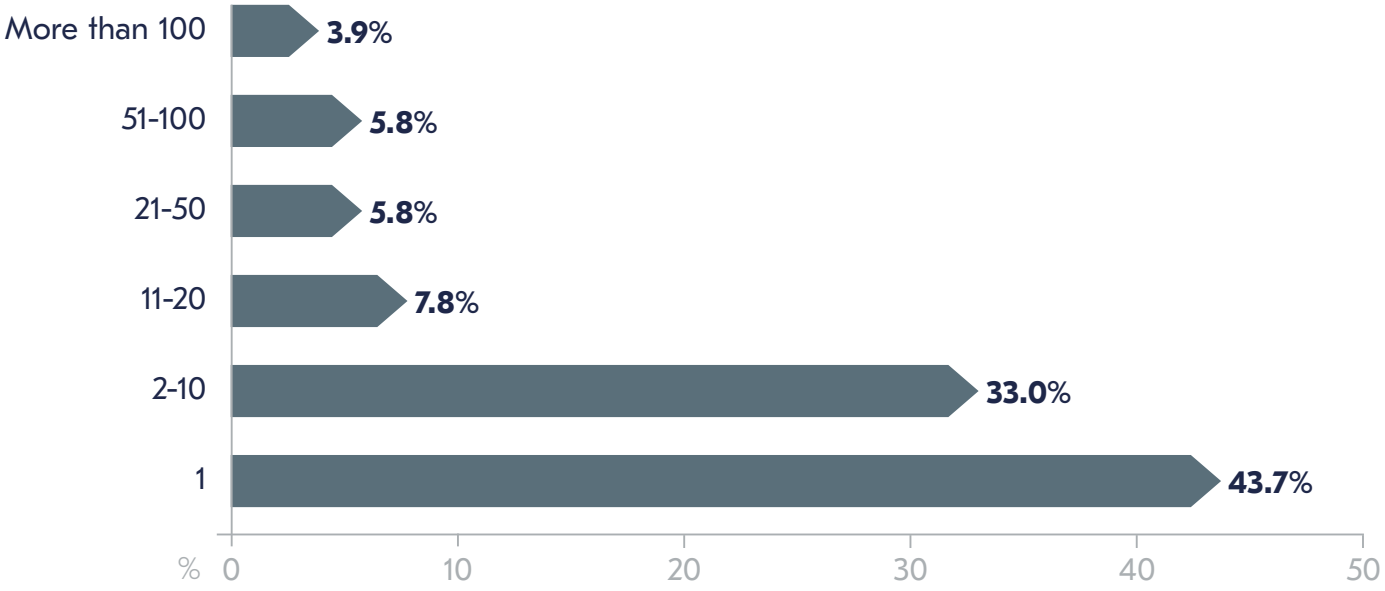


Figure 23. How many countries does your organization operate in?

Approximately how many employees are there in your organization globally?

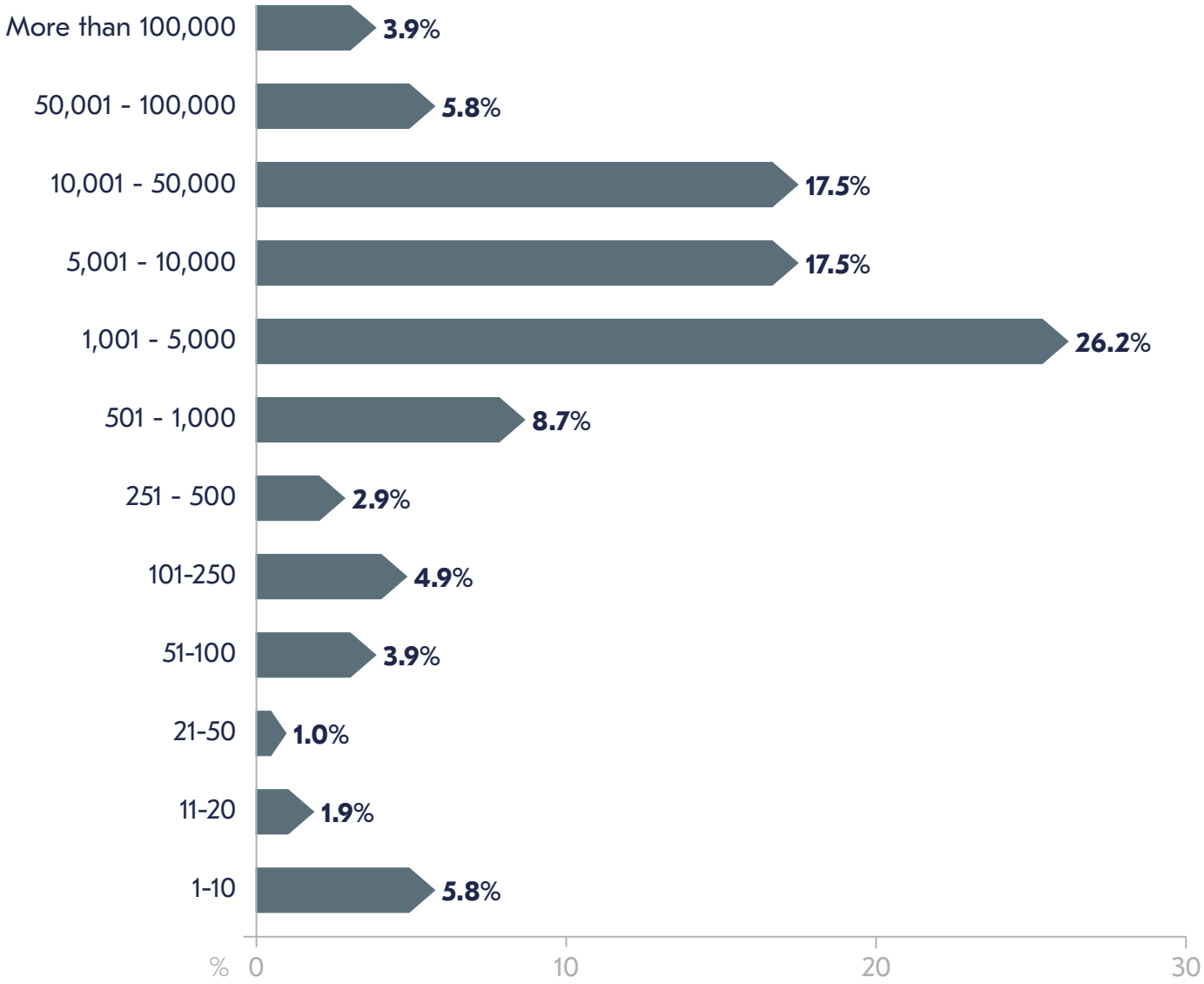


Figure 24. Approximately how many employees are there in your organization globally?

About the authors

Rebecca Matthews

Content Manager, The BCI

Rebecca has 10 years of experience in researching and delivering national and international publications across both print and digital platforms. She was a Cat 1 emergency planner for 8 years, specialising in governance of local resilience forums (LRFs) and civil contingency humanitarian aid where her work was used as beacon examples for national emergency planning frameworks. Through her work with the BCI she has used various research techniques to engage with topics such as climate risk, supply chain resilience, and emerging legislation. Rebecca's areas of interest include how critical national infrastructure impacts resilience, and the future issues that our changing climate presents.

She can be contacted at rebecca.matthews@thebci.org

Maria Florencia Lombardero Garcia

Thought Leadership Manager, The BCI

Maria has over 15 years of experience in academic and market research and has been responsible for the design and implementation of a wide range of policies within public and private organizations such as the Argentine Ministry of Defence, RESDAL, and BMI (Fitch Group). She has served as a policy advisor and political analyst at the Argentine Ministry of Defence and coordinated the Argentine National Security Council's Office. She has particular expertise in geopolitical risk, defence, and intelligence and her work has been applied to develop government defence strategies and draft legislation on the matter. Her areas of interest relate to open-source research and how geopolitics impacts resilience within organizations.

She can be contacted at maria.garcia@thebci.org

About the BCI

Founded in 1994 with the aim of promoting a more resilient world, the BCI has established itself as the world's leading institute for business continuity and resilience. The BCI has become the membership and certifying organization of choice for business continuity and resilience professionals globally with over 9,000 members in more than 100 countries, working in an estimated 3,000 organizations in the private, public, and third sectors. The vast experience of the Institute's broad membership and partner network is built into its world class education, continuing professional development, and networking activities. Every year, more than 1,500 people choose BCI training, with options ranging from short awareness raising tools to a full academic qualification, available online and in a classroom. The Institute stands for excellence in the resilience profession and its globally recognised Certified grades provide assurance of technical and professional competency. The BCI offers a wide range of resources for professionals seeking to raise their organization's level of resilience and its extensive thought leadership and research programme helps drive the industry forward. With approximately 120 partners worldwide, the BCI Corporate Membership offers organizations the opportunity to work with the BCI in promoting best practice in business continuity and resilience.

The BCI welcomes everyone with an interest in building resilient organizations from newcomers, experienced professionals, and organizations. Further information about The BCI is available at **www.thebci.org**.

Contact The BCI
+44 118 947 8215 | bci@thebci.org
9 Greyfriars Road, Reading, Berkshire, RG1 1NU, UK

About Riskonnect

Riskonnect is the leading integrated risk management software solution provider. Our technology empowers organizations with the ability to anticipate, manage, and respond in real-time to strategic and operational risks across the extended enterprise.

More than 2,000 customers across six continents use our unique risk-correlation technology to gain previously unattainable insights that deliver better business outcomes. Riskonnect has more than 800 risk management experts in the Americas, Europe, and Asia.

To learn more, visit riskonnect.com.

References

1. www.thebci.org/resource/bci-a-year-in-the-world-of-resilience-report-2023.html
2. dig.watch/updates/forrester-cybercrime-to-cost-12-trillion-in-2025
3. www.thebci.org/resource/bci-horizon-scan-report-2024.html
4. www.thebci.org/resource/the-bci-update-series--cyber-resilience-report-2024.html
5. www.thebci.org/resource/bci-crisis-management-report-2024.html
6. Ibid
7. www.thebci.org/resource/bci-operational-resilience-report-2024.html
8. www.gov.uk/government/publications/uk-covid-19-inquiry-resilience-and-preparedness-module-1-report
9. www.thebci.org/resource/bci-continuity-and-resilience-report-2023.html
10. www.thebci.org/resource/bci-emergency---crisis-communications-report-2024.html
11. www.thebci.org/resource/bci-technology-in-resilience-report-2023.html
12. www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence
13. There are a number of guidance, regulations or legislation on AI in place worldwide such as: AI Liability Directive, SAFE Innovation AI Framework, Montana, Oregon, Tennessee, New Hampshire, Delaware — Enacted legislation, Digital Information and Smart Data Bill, International Guiding Principles for Organizations Developing Advanced AI Systems, International Code of Conduct for Organizations Developing Advanced AI Systems.
14. www.technologyreview.com/2024/01/17/1086704/china-ai-regulation-changes-2024/
15. www.thelancet.com/journals/langlo/article/PIIS2214-109X(24)00133-5/fulltext?dgcid=raven_jbs_etoc_feature_langlo
16. www.gallup.com/workplace/349484/state-of-the-global-workplace.aspx
17. www.thebci.org/resource/bci-supply-chain-resilience-report-2024.html
18. commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/commercial-political-violence-civil-unrest-trends-2024.pdf
19. www.thebci.org/resource/bci-extreme-weather---climate-change-report-2023.html
20. https://www.eiu.com/n/global-outlook-looking-ahead-to-2025/
21. www.forbes.com/sites/jasonschenker/2024/10/22/imf-forecasts-global-economy-to-grow-32-in-2025

BCI 9 Greyfriars Road, Reading, Berkshire, RG1 1NU, UK bci@thebci.org / www.thebci.org