

Find out more
www.thebci.org



BCI Horizon Scan Report 2025



Contents

- 05** Executive summary
- 12** Introduction
- 14** Risk and threat assessment
- 22** Consequences of disruptions
- 26** Risk and threat assessment:
next twelve months
- 30** Long-term trend analysis
- 38** Benchmarking business continuity
- 45** Looking ahead
- 51** Annex





Foreword

The BCI is pleased to introduce the Horizon Scan Report 2025. The report looks at the complexity of the operating environment, providing a well-established benchmarking tool for both expert practitioners and newcomers to the business continuity and resilience industry. The report examines threats ranging from digital challenges and the adoption of new technologies to geopolitical changes and natural hazards, trying to capture the levels of current impact and future concern for practitioners.

Furthermore, the results consider the effectiveness and the evolution of the techniques and tools that practitioners use to scan the risk and threat horizon. The rise of new technologies, such as artificial intelligence, is challenging traditional methodologies, but practitioners still see value in the interpersonal exchange of information.

Building on this theme, the value of human resources sits at the heart of this report. While threats may range in nature and impact, organizations must protect their most vital asset, their people. Attention towards health and safety has grown over the past five years and yet there are gaps in the risk perception that the report examines in detail to raise awareness among the community.

Overall, the report combines findings from both quantitative survey data and qualitative interviews with practitioners on the front lines of business continuity and resilience. Their insights highlight that efforts towards improved response measures and better compliance should be considerate of the health and safety of the workforce.

The report adopts a broader outlook on the way organizations perceive, prepare for, and respond to disruptions, considering multiple aspects. From the adoption of new technologies and the integration of trend analysis to the focus on staff capacity and wellbeing, the report captures the diverse nature of resilience practices. By combining evidence from surveys with rich firsthand experiences, this work offers valuable guidance for leaders seeking to navigate uncertainty, safeguard critical operations, and strengthen their organization's ability to adapt and thrive in a rapidly evolving risk landscape.

Maria Florencia Lombardero Garcia

Thought Leadership Manager
The BCI





Foreword

As a crisis exercise platform dedicated to helping organisations prepare for the unexpected, we are proud to support this year's BCI Horizon Scan Report 2025. The findings of this report underline what the community of practitioners has long understood: that resilience is ultimately a human story.

While the risk landscape continues to evolve with new digital, geopolitical, and environmental pressures, the report reveals a simple truth: people remain at the centre of every resilient system. Whether responding to extreme weather, managing cyber threats, or maintaining continuity amid disruption, it is the wellbeing, confidence and capability of individuals that define how organisations truly perform under pressure.

Yet human factors often receive less attention in forward-looking risk assessments. This gap between recognition and readiness highlights the vital importance of regular, realistic exercising. When teams train together in authentic scenarios, they strengthen not only procedures and coordination, but trust, empathy, and decision-making under stress.

At Conducttr, we believe that experience is everything. Technology can inform and enable, but it is practice that embeds preparedness. Reports like the Horizon Scan 2025 remind us that resilience cannot be automated: it must be lived, tested, and continually refined through human interaction.

Belén Santa-Olalla

Chief Creative Officer
Conducttr

Executive summary





Incidents concerning staff well-being have been the highest risk to organizations over the past twelve months.

Broadening the analysis to the last five years, respondents have consistently placed safety incidents at the top of this chart, with the exception of last year, when frauds ranked first. From the immediate aftermath of the pandemic until today, health and safety incidents as well as diseases have been the most disruptive event for organizations. Nevertheless, digital threats still remain a noticeable concern and should not be underestimated. Resilient organizations should ensure people's safety without neglecting the assets that allow them to carry out their work.

Top five most frequent and impactful events in the past 12 months:

1



Safety incidents

2



Cyberattacks

3



Fraud/attempted fraud

4



Security incidents

5

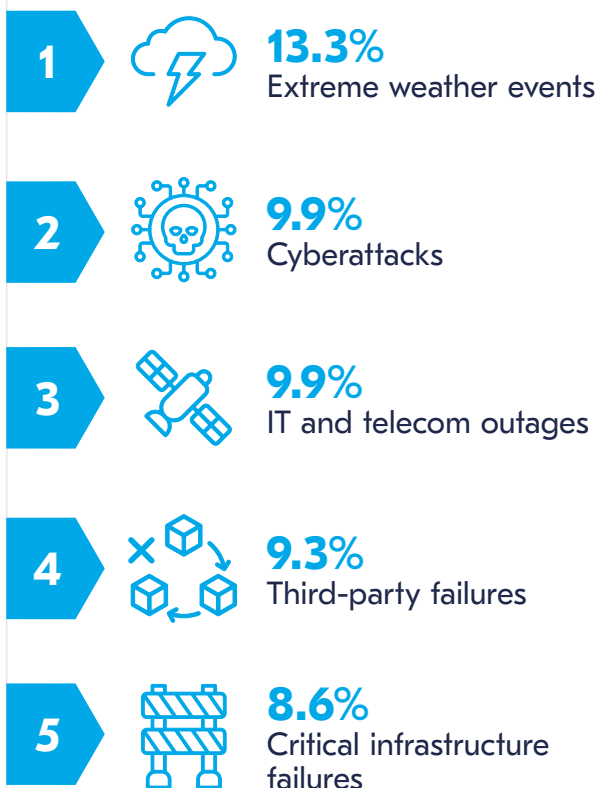


IT and telecom outages

Extreme weather is the single largest cause of disruption over the past 12 months for the first time since 2017.

In the previous five years, this chart was dominated by digital threats, which are still present in the top five but are now secondary to natural hazards. This trend is in line with major global events. The 2024 report reflected the sensation caused by the CrowdStrike outage, while in the past twelve months major extreme weather hazards such as the Valencia floods may have influenced the experiences reported by practitioners.

Top five single biggest causes of disruption in the past 12 months:



Disruptions have a broad impact, affecting operational performance, staff morale and customer experience.

Loss of productivity is not as prominent as it was last year but it is still among the main consequences of disruption, topped only by customer complaints. Respondents pointed out how disruptions can hinder productivity while internal expectations remain the same, which leads to increased stress and potential mental health issues. This introduces the theme of personal resilience among the workforce, which should entail collaboration among multiple departments.

Top five most common consequences of disruptions for organizations:

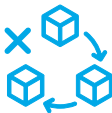


Top five risks for organizations

Practitioners perceive the future threat landscape as a complex combination of digital challenges, climate risk and geopolitical uncertainty. Dependencies are an additional major concern. Whether this is due to a supplier disruption or a critical infrastructure failure, external parties to the organization are a source of worry to practitioners, since complex interdependencies can quickly reduce visibility over risk. Interestingly, health and safety issues do not figure in either of the charts below, revealing a disconnect between disruptions that occurred recently and the risk perception of the future.

Risk index assessment next 12 months:

Top concerns for organizations over the next 5-10 years:

1  7.37 Cyberattacks	1  63.6% Cyber security
2  6.19 Extreme weather events	2  40.7% Climate risk
3  5.98 IT and telecom outages	3  30.5% The role of AI
4  5.34 Data breaches	4  28.8% Geopolitical changes
5  4.91 Third-party failure / Critical infrastructure failure	5  26.3% Supply chain issues

Trend analysis adoption

The majority of respondents conduct long-term trend analysis and they use its results as part of their business continuity programmes. However, this trend has sharply declined compared to the previous year, while discussions along agnostic plans and holistic planning are picking up. Respondents stated that they would rather focus on internal response capabilities without planning for every specific scenario. In this sense, understanding the threat landscape in the long term works more as an awareness tool, whereas real attention is dedicated to internal resources and their vulnerabilities.

Does your organization conduct longer-term trend analysis to better understand the threat landscape?

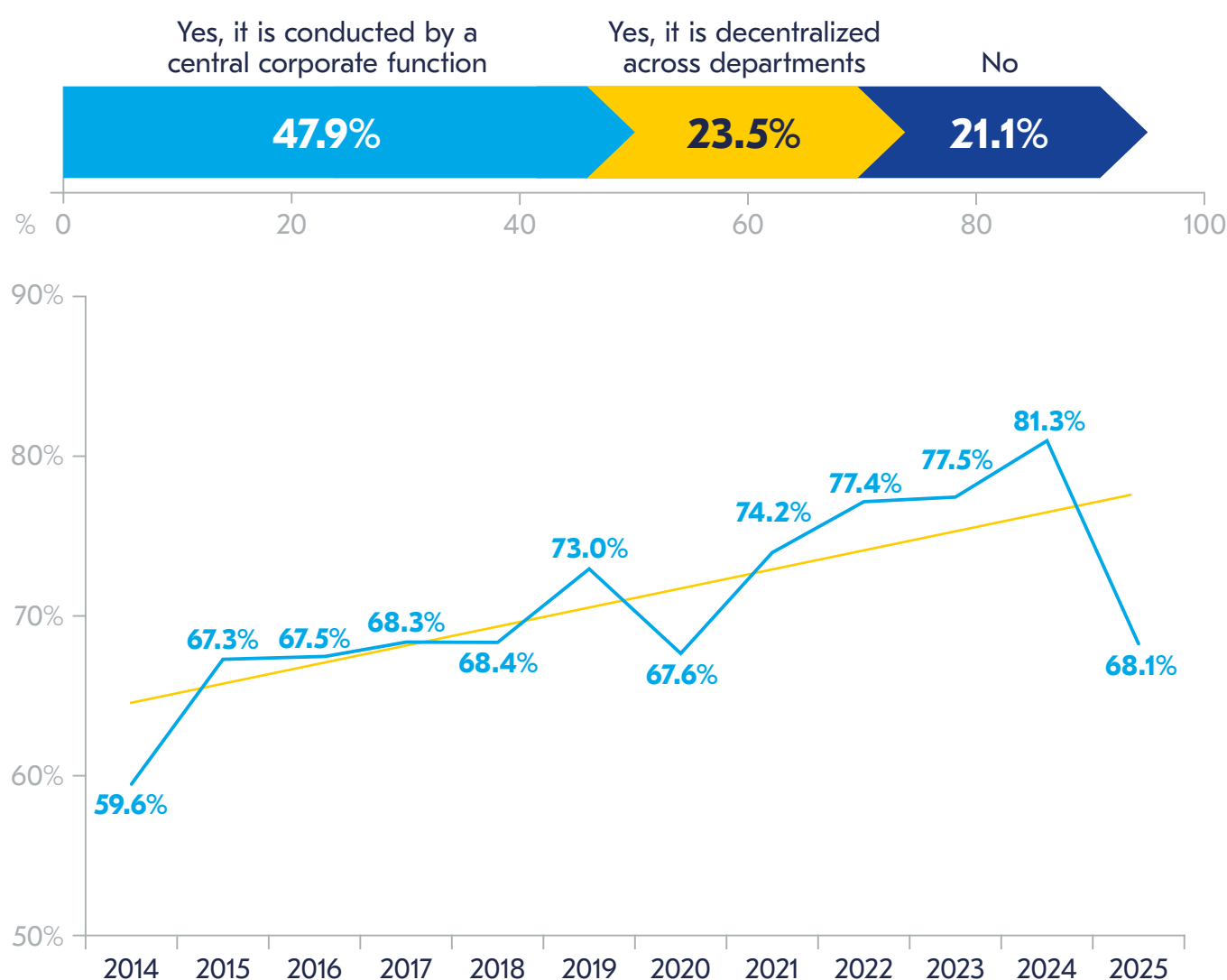


Figure 1. Usage of trend analysis outputs.

Organizations rely on a combination of internal assessments and external insights to inform their risk landscape understanding.

While advanced tools for risk analysis become increasingly popular, there is still a significant manual and human component to horizon scanning. Whether through interpersonal relationships or by consulting sources without the mediation of an advanced tool, practitioners are still scanning the future threat landscape trying to put together the pieces of the puzzle themselves.

Top five tools for conducting trend analysis:

- 1



87.2%

Internal risk and threat assessments
- 2



75.2%

External reports/industry insight (e.g., Horizon Scan)
- 3



55.6%

Participation in industry events and conferences
- 4



52.1%

Collaboration with peers
- 5



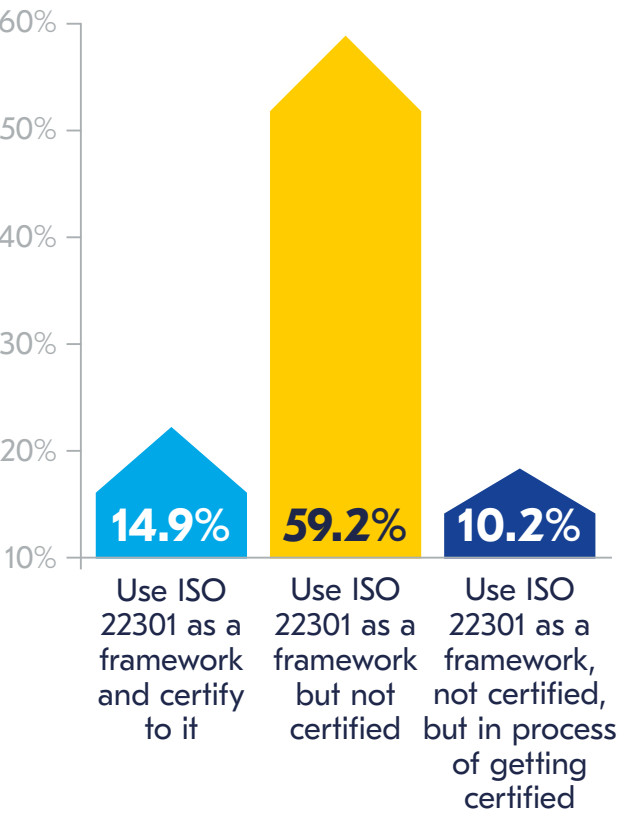
50.4%

Research reports

Relationship of BCM programmes to ISO 22301:

ISO 22301 remains the dominant framework, though full certification is less common than alignment with the standard. Most organizations that contribute to the Horizon Scan report each year tend have stuck to the standard, maintaining their investment levels stable or even increasing them. This year, those adopting ISO 22301 without certifying have nearly doubled, showing an increased interest. The emergence of new regulations such as the EU Digital Operational Resilience Act (DORA) could be a strong driver for this shift, since standards can help in the road to compliance.

If you have a formal business continuity management programme in place, how does it relate to ISO 22301?



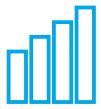
Investment strategies for 2026 reflect a focus on sustaining or enhancing programme capabilities in response to emerging threats.

Investment levels in business continuity & resilience programmes:



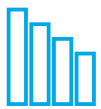
43.1%

Investment will be maintained at current appropriate levels



19.8%

Investment will be increased to meet growing programme needs



9.5%

Investment will be reduced, limiting scope or effectiveness



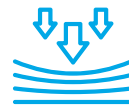
9.5%

No investment in a BC/resilience programme

Certification strengthens resilience and demonstrates program effectiveness to both internal and external stakeholders.

In the face of emerging regulations across the world, being able to demonstrate preparedness is valuable to organizations.

Top three benefits of ISO 22301 certification:



80.8%

Increases organizational resilience



76.9%

Demonstrates effectiveness of BCM programme to external stakeholders



57.7%

Improves customer satisfaction



Introduction

This year, the findings show that health and safety disruptions have had the most serious impacts, consolidating a trend that has been building since 2020. Meanwhile, external pressures from extreme weather events, supply chain failures, and failing infrastructure are also increasingly threatening organizations.

The digital space continues to offer new opportunities for strengthening resilience while broadening the attack surface for malicious actors. Organizations face constant choices to strike a balance between risk and innovation, as new technologies evolve at a very rapid pace.

In this operating environment, trend analysis remains a vital tool to evaluate risks and threats, although its use has slightly declined. There is a growing indication that practitioners are discussing agnostic planning. While this is not a new concept, particularly to business continuity practitioners, it is gaining traction, since many believe that keeping up with every single threat is an unrealistic ask.



The 2025 findings also highlight a disconnect between the disruptions occurred over the past twelve months and the events practitioners are concerned about when scanning the future threat landscape. Health and safety issues, including occupational diseases, have been the most recurring challenge for participants since 2020, and yet direct threats to the workforce often slip under the radar.

The goal of the Horizon Scan Report is not only to present the risks and threats that concern participants, but also to question current methodologies and risk perceptions. Currently, it seems as though the “people come first” principle might be overshadowed by disruptions that appear more sinister such as cyber-attacks. Still, it is important to not be misled and place the right amount of attention to each aspect of an organization.



1

Risk and threat assessment





Disruptions in the past twelve months

Organizations are facing a wide range of disruptions, with ramifications both in the digital and physical domain. Respondents evaluated the overall risk level of each event, by indicating the estimated impact and frequency. This report combines these two values to provide a general risk index for several disruptions that occurred in the past twelve months.

Safety incidents stand out with the highest risk index (14.64), especially due to their frequency. During follow-up interviews, respondents highlighted that while high-impact events may be rare, smaller-scale incidents still require sound risk assessments and mitigation measures.

A longitudinal analysis of risk and threat assessments from 2014 to 2025 reveals how the recurrence of health and safety incidents has increased with time. Before 2020, the main cause of disruptions was exclusively digital, in the form of either cyberattacks or IT and telecom outages. However, from 2021, the chart has predominantly been headed by health and safety issues or non-occupational diseases.

“Health and safety incidents have probably been our biggest disruption over the past 12 months. Even minor accidents carry an operational impact. When someone with specialist skills is injured, the work doesn’t stop, but resources have to be redeployed.”

Business Continuity Manager, Energy Sector, UK.

Top 3 cumulative disruptions to organizations 2014-2025



Figure 2. Top three cumulative disruptions 2014-2025

Cyberattacks (13.33) and fraud attempts (13.11) rank second and third in the chart. Respondents emphasized that these threats are largely operational and require mitigation measures to prevent their escalation into major incidents. Hence, preparedness is key, since these incidents can lead to both operational and reputational consequences if left unmanaged.

“As cyber threat actors become more sophisticated, even the amateur ones, our defences have to rise just to stand still. That’s the challenge, you are spending more, and it looks like nothing has changed, when in reality the threat landscape is constantly evolving.”

Business Continuity Manager,
Energy Sector, UK.

Security incidents (12.38) and IT and telecom outages (11.9) round up the top five, revealing the complexity of a threat landscape that blends physical and digital challenges. Interestingly, shortages of natural resources (11.69) also figure among the most relevant disruptions. Further qualitative insights reveal that even short-term shortages can generate significant impacts on productivity, data centres, and customer service, due to the interconnectedness of technical infrastructure and supply chains.

“The number of third parties has increased drastically, from IT and cloud services to cleaning and facilities. Not all contracts are up-to-date or include resilience clauses, so building a resilient supply chain is still a work in progress.”

Business Continuity Officer, Technology
and Electronics Sector, Europe.

On a different note, health-related incidents (11.61), including stress and mental health challenges, highlight the need for organizations to maintain employee capacity and manage workload pressures, particularly when teams are small and operational demands are high. In this regard, it is important not to neglect that professionals working in the protective disciplines, such as business continuity and risk management, are often on the frontline when it comes to disruptions and crises, which can take a heavy toll on their mental health in the medium and longer term.

“The biggest disruption was caused by a sole-source blood supplier going down. It created shortages that impacted patient care, required reallocating supplies, and lowered staff morale because people couldn’t do their work as they should.”

Director of Enterprise Risk Management,
Healthcare Sector, US.

Looking at the wider operating environment, extreme weather events (11.59) and trade wars (11.26) demonstrate that organizations remain vulnerable to macro-level disruptions outside their direct control. Interviewees highlighted that infrastructure not originally designed for extreme weather, combined with energy or cooling constraints, can amplify the operational impact of such events. Both rank lower than others in frequency but carry high impact, since sudden shocks from geopolitical or environmental events are becoming increasing drivers for disruptions. On a similar note, activist campaigns (10.83) complete the top ten, as they intensify as a response to growing international and societal tensions.

Cumulative disruptions 2025

Rank	Event	Frequency	Impact	Risk Index
1	Safety incident	7.59	1.93	14.64
2	Cyber attacks	6.52	2.04	13.33
3	Fraud/attempted fraud	7.03	1.86	13.11
4	Security incident	6.70	1.85	12.38
5	IT and telecom outage	5.46	2.18	11.90
6	Natural resources shortage	5.86	2.00	11.69
7	Health incident	6.37	1.82	11.61
8	Extreme weather events	5.27	2.20	11.59
9	Trade wars	5.07	2.22	11.26
10	Activist campaigns	5.51	1.97	10.83
11	Third party failure	4.99	2.16	10.77
12	Increased cost of living	4.92	2.10	10.32
13	Introduction of new technology	5.16	1.97	10.19
14	Data breaches	5.29	1.90	10.07
15	Travel restrictions	5.39	1.83	9.85
16	Interruption to energy supply	4.68	2.11	9.85
17	Tariff changes	4.73	2.06	9.72
18	Issues arising from remote/hybrid working	5.22	1.82	9.48
19	Mis/disinformation	4.86	1.91	9.29
20	Natural disasters	4.33	2.14	9.28
21	Critical Infrastructure failure	4.10	2.22	9.11
22	Supply chain disruption	4.44	1.99	8.84
23	Non-occupational disease	4.79	1.83	8.76
24	Hybrid attacks	4.05	2.15	8.69
25	Regulatory changes	4.25	2.04	8.68
26	Product safety recall	4.67	1.85	8.62
27	War/conflict	4.01	2.13	8.53
28	Political violence/civil unrest	4.26	1.98	8.42
29	Energy price shock	3.91	2.13	8.31
30	Higher interest rates	3.72	2.15	7.99
31	Political change(s)	3.88	2.05	7.93
32	Enforcement by regulator	3.79	2.05	7.75
33	Exchange rate volatility	3.65	2.10	7.68
34	Industrial action (strikes)	3.75	1.96	7.36
35	Lone attacker/active shooter incident	3.00	2.33	6.99
36	Insider threat	3.38	1.96	6.62

Main disruption drivers

Extreme weather events represent the greatest concern (13.3%), as they are the largest single driver for disruption this year. Looking at a multi-year trend that includes past Horizon Scan reports, it is interesting to observe that extreme weather makes the top of the chart for the first time since 2017, while in the past, practitioners were mainly concerned with digital challenges such as cyberattacks or IT and telecom outages.

In-depth interviews with respondents showed different levels of exposure to natural hazards. Some experienced events, such as floods but were unaffected due to their geographical location, while in other cases production plants were disrupted due to droughts as well as freezing temperatures.

"I tell people that any conversation about disaster recovery eventually becomes a conversation about tornadoes. Just because it's visual and people think it's cool. But your response to a labour shortage, pandemic, or weather event can all have similar aspects, and my team looks at it holistically, tweaking emergency response plans, contingency plans, and disaster recovery plans based on those scenarios."

Senior Resilience Manager,
Transport Sector, Canada.

"Our infrastructure was never designed for the extremes we're seeing now. A few years ago, cold winters caused the concrete bases of our stations to crack, and in hot summers, data centre cooling becomes a critical vulnerability. If the cooling fails, things escalate very quickly. So, climate risk isn't abstract for us, it's a direct operational challenge that will require real investment."

Business Continuity Manager,
IT and Telecom Sector, Europe.



In joint second position, cyberattacks (9.9%) and IT and telecom outages (9.9%) are equally pressing and possibly interconnected. Practitioners from multinational organizations emphasized that even well-protected systems require continuous monitoring, rapid incident response, and contingency planning to maintain continuity. A successful cyberattack or prolonged outage can halt operations, compromise sensitive data, and trigger regulatory scrutiny or reputational damage.

Third-party failures (9.3%) also stand out, due to growing vulnerabilities through suppliers, contractors, and service providers. Respondents overseeing supplier risk in regulated industries explained the practical challenges of working with smaller or legacy vendors who may struggle to meet compliance and security expectations, requiring risk exceptions or additional oversight. Disruptions in this area can quickly cascade into operational bottlenecks, particularly in highly interconnected or regulated sectors. Critical infrastructure failure (8.6%) rounds out the list, stressing the inherent risk carried by providers of essential services such as energy, water, and transport, where breakdowns can spread rapidly across operations.

"Suppliers are a major risk vector, and regulations like NIS2 are forcing us to focus more on third-party management. The difficulty is that we don't just deal with large firms; we have small legacy vendors with only a handful of staff. Expecting them to comply with GDPR, NIS2, and all our requirements is unrealistic, but because of vendor lock-in, we often have no choice but to grant risk exceptions."

Business Continuity Manager,
IT and Telecom Sector, Europe.

"We investigate our suppliers' business continuity plans. A few years ago, you might have said, 'Yes, we have a plan,' and that would have been enough. Now companies want to see your plan, evidence of testing and audits. It's no longer just trust; we need guarantees because we're so reliant on different suppliers, and that scrutiny is only going to increase."

Senior Resilience Manager,
Transport Sector, Canada.



Causes of disruption to organizations in the past 12 months

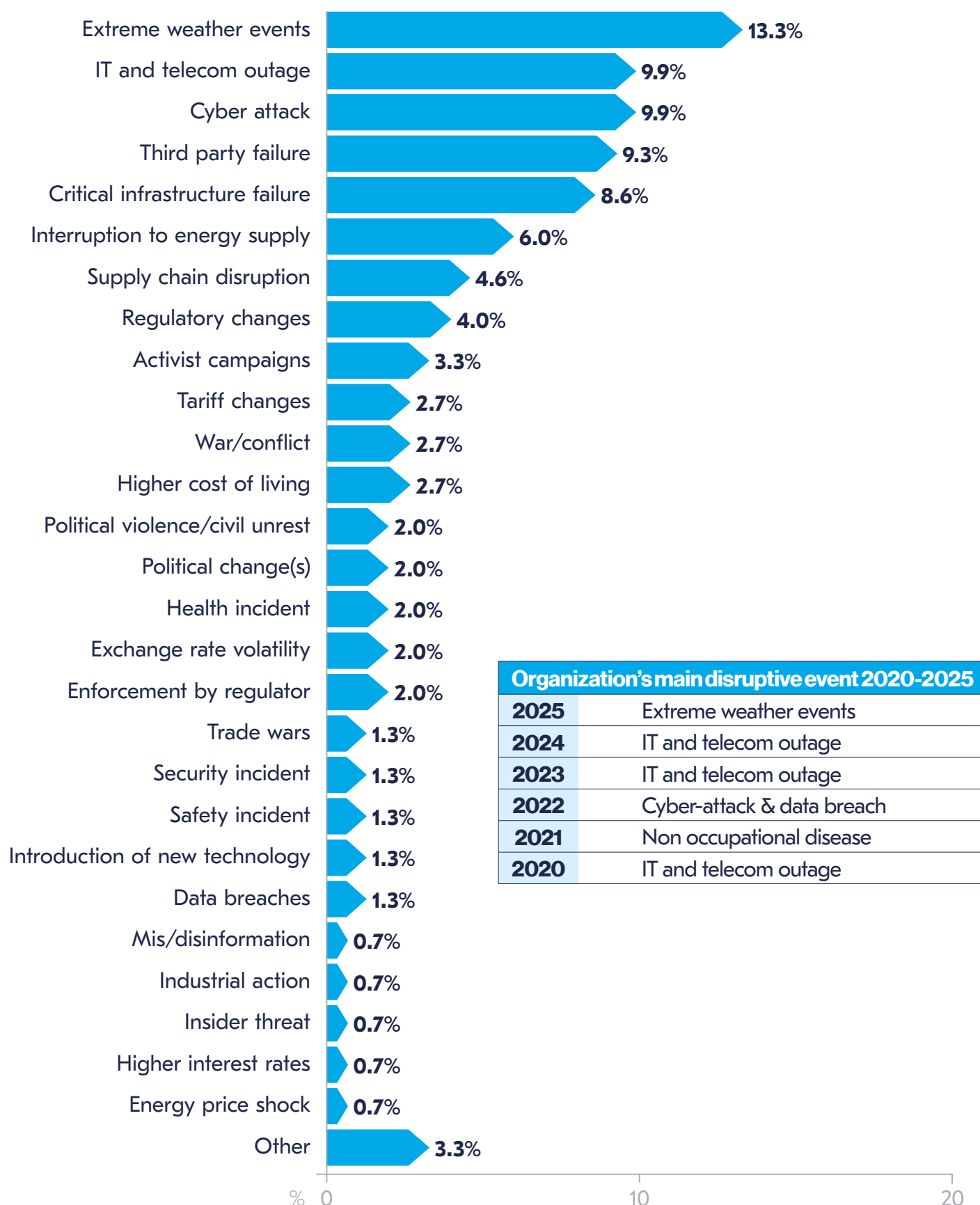


Figure 3. Causes of disruption to organizations in the past 12 months

2

Consequences of disruptions





Impacts and cascading effects

Customer complaints emerge as the most common consequence of disruptions (43.2%). A respondent further elaborated on this point, describing how even minor IT or telecom outages can quickly trigger complaints from retail branches and clients. Closely linked, loss of productivity (41.9%) reflects the internal strain organizations face, which may affect staff morale. Interviewees overseeing European operations noted that regulatory-driven audits, such as those required under NIS2, also divert staff time and resources, leading to productivity loss.

"As the context becomes more complex, it's easy for critical information to be missed or for the wrong people to be in charge of important areas. These issues may not seem critical initially, but they can become significant. This is a concern for large, medium, and small organizations alike, especially due to reputational risk. Reputational issues are increasingly connected to many aspects of the organization, not just product quality or management effectiveness."

Business Continuity Officer,
Technology and Electronics Sector, Europe.

On a similar note, negative impacts on staff morale, wellbeing, and mental health (35.8%) should not be underestimated, due to the physical and mental cost of ongoing instability. A participant from Central Europe shared that the rush to meet audit requirements, while simultaneously responding to cyber threats and integrating new AI tools, created high stress levels among the team, affecting engagement and resilience.

"Workplace violence and stress are already challenges in healthcare, so these disruptions amplify them. When repeated events occur, like another infrastructure failure days later, it further lowers morale. Staff question why the organization hasn't invested more or improved systems, which adds to the frustration. It's not just the workflow; it's the awareness of patient impact and the constant reassessment required."

Director of Enterprise Risk Management,
Healthcare Sector, US.

Further down the chart, impaired service outcomes (33.1%) represent the type of consequence that directly impacts customer trust and can even complicate contractual obligations. For example, small suppliers struggling to comply with new regulatory or security requirements can inadvertently create service gaps.

As a result of the complex disruption dynamics highlighted in this top five, loss of revenue (31.8%) shows how disruptions can easily turn into tangible economic costs. Interviewees emphasized that while financial loss is often the most visible consequence, reputational damage, operational inefficiencies, and workforce challenges are equally demanding, requiring proactive investment in both technology and human resources to mitigate long-term risks.



Impacts or consequences of disruptions in the last 12 months

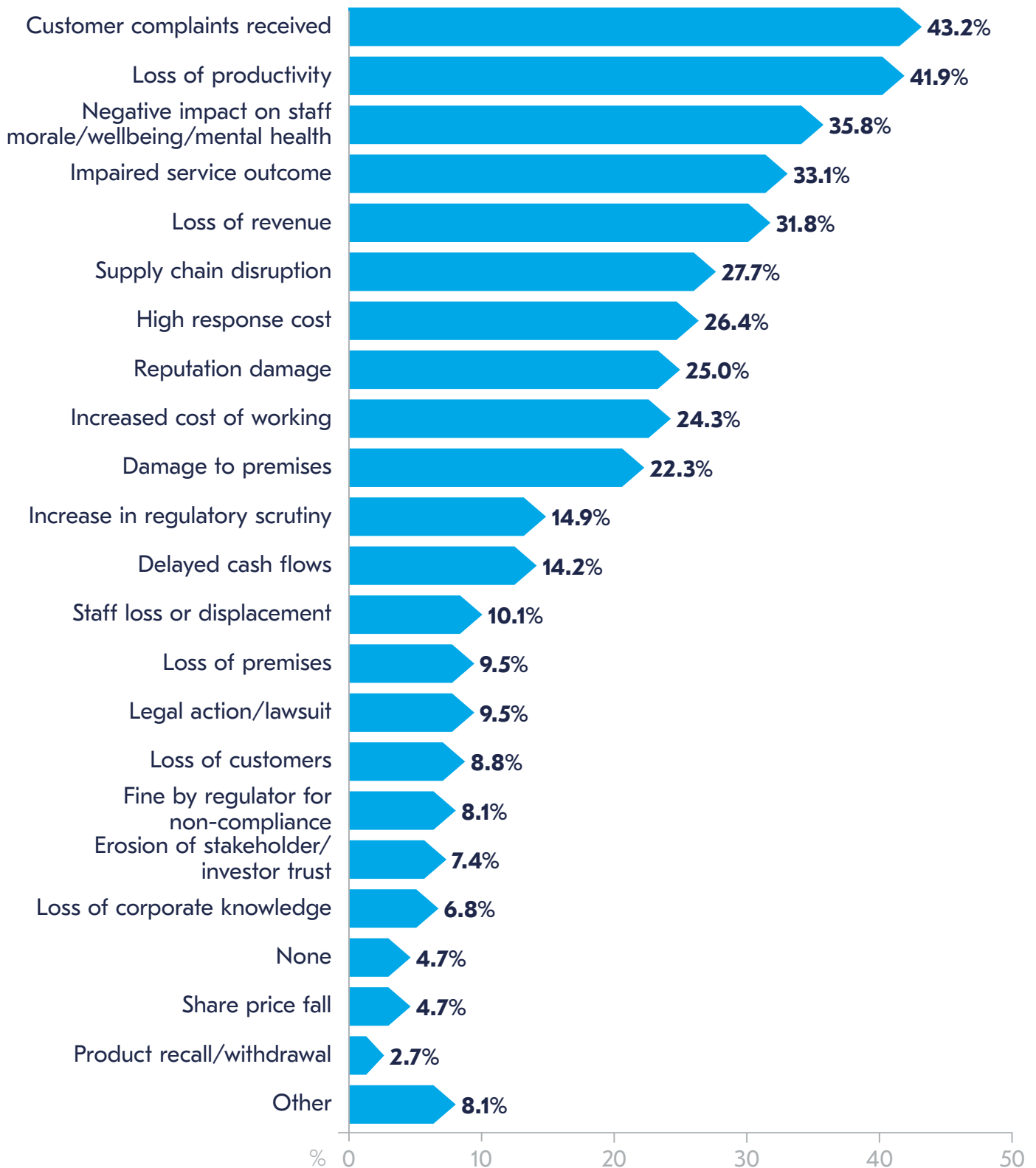


Figure 4. Impacts or consequences of disruptions in the last 12 months.

Risk and threat assessment: next twelve months





The threat landscape in the near future

The outlook for the next twelve months indicates that organizations expect a diverse range of threats across digital, environmental, and operational domains. Similarly to the risk and threat assessment for the past twelve months, participants indicated both frequency and impact of disruptions, which were combined to form a risk index.

"I'm always doing horizon scanning, looking at what's happening in healthcare globally, from wildfires in Canada to outages in Spain and Portugal, and asking if it could affect us here, and what lessons we can learn."

Director of Enterprise Risk Management,
Healthcare Sector, US.

"The information is all there, from government briefings, LRFS, and the BCI, but it's a bit disjointed. One of our priorities over the next 12 months is to pull that together into a more consistent approach to risk assessment and horizon scanning."

Business Continuity Manager, Energy Sector, UK.

Cyber attacks top the list (7.37), with ongoing concerns that even if digital systems are well-prepared for containment, the increasing sophistication of cyber threats keeps response teams on high alert, as one respondent pointed out. On a similar note, IT and telecom outages (5.98), along with data breaches (5.34), are among the top five future concerns. In the interviews, business continuity managers noted that IT system interruptions, regardless of their cause, can lead to multiple delays due to the interdependencies that constitute modern organizations. To meet present and future cyber-related challenges, practitioners are taking different approaches, including aligning to multiple standards such as ISO 27001, ISO 27005 and ISO 22301. Additionally, some are devoting large parts of their budget to increase defences over their attack surface, which includes third parties. Cyber attacks also headed this chart in 2024, a sign that they remain the greatest concern to practitioners despite the fact that other disruptions – perhaps those regarding health and safety – might have greater impact over the course of the entire year.

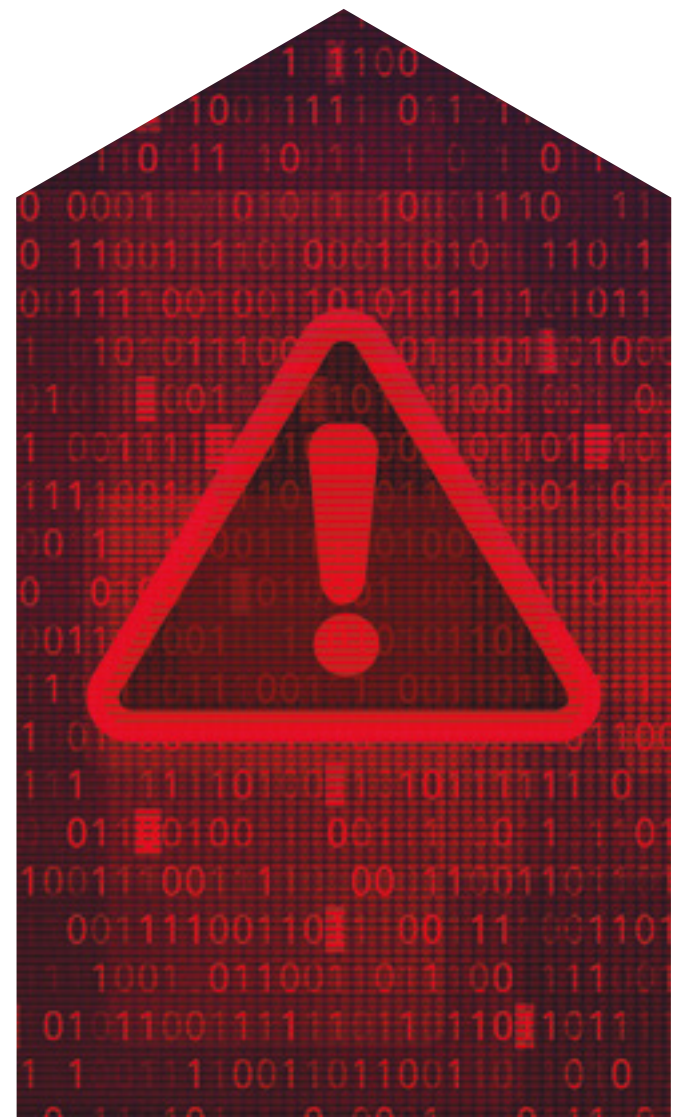
Extreme weather events (6.19) are also expected to be a significant challenge. It is worth stressing that the impact of natural hazards changes not only according to exposure, but also to vulnerability. Depending on factors such as geographical position and mitigation measures, organizations might be more or less, vulnerable to the same event.

A respondent from Japan cited the example of a large earthquake in Russia's Kamchatka Peninsula, which caused a 1.5-metre tsunami in their region. Their factories had to stop operations to prepare in case of an even bigger wave. While this did not happen, the factory still had to close for a day as a preventative measure. The respondent went on to explain that they are located in the middle of an earthquake-prone region, known as the Ring of Fire, where there is an 80% probability of a magnitude 9 class earthquake within the next 30 years.

Therefore, they need to prepare as if it could happen any year, rehearsing scenarios and building preparedness measures accordingly.

Third-party failures (4.91) and critical infrastructure failures (4.91) highlight the importance of dependency risks beyond organizational boundaries. This trend is also confirmed by the indicators for supply chain disruptions (4.59) and energy supply interruptions (4.48), as concerns over global instability and resource reliability mount.

Looking at technology hazards, emerging risks such as the introduction of new solutions, including IoT, AI, and big data (4.64), also feature in the top ten. A risk manager described how internal AI adoption is accelerating, creating both opportunities for efficiency and new exposure if governance and security measures lag.



Cumulative disruptions in the next 12 months

Rank	Event	Likelihood	Impact	Risk Index
1	Cyber attacks	2.4	3.1	7.37
2	Extreme weather events	2.5	2.5	6.19
3	IT and telecom outage	2.2	2.8	5.98
4	Data breaches	1.9	2.8	5.34
5	Third party failure	2.0	2.5	4.91
6	Critical Infrastructure failure	1.8	2.7	4.91
7	Introduction of new technology	2.2	2.1	4.64
8	Supply chain disruption	1.9	2.4	4.59
9	Interruption to energy supply	1.8	2.5	4.48
10	Security incident	1.9	2.2	4.23
11	Increased cost of living	1.9	2.2	4.21
12	Regulatory changes	1.8	2.2	3.96
13	Political change(s)	1.7	2.2	3.86
14	Natural disasters	1.4	2.8	3.76
15	Hybrid attacks	1.4	2.6	3.62
16	Safety incident	1.7	2.1	3.61
17	Fraud/attempted fraud	1.6	2.1	3.38
18	War/conflict	1.3	2.6	3.27
19	Health incident	1.6	2.0	3.18
20	Mis/disinformation	1.5	2.0	3.12
21	Enforcement by regulator	1.4	2.2	3.04
22	Higher interest rates	1.5	2.0	2.97
23	Non-occupational disease	1.2	2.4	2.96
24	Tariff changes	1.5	2.0	2.96
25	Trade wars	1.3	2.1	2.75
26	Insider threat	1.2	2.3	2.68
27	Political violence/civil unrest	1.2	2.2	2.65
28	Activist campaigns	1.3	2.1	2.64
29	Energy price shock	1.2	2.1	2.53
30	Exchange rate volatility	1.2	1.9	2.22
31	Industrial action (strikes)	1.1	2.1	2.21
32	Travel restrictions	1.1	1.8	2.08
33	Natural resources shortage	0.9	2.2	2.06
34	Lone attacker/active shooter incident	0.6	2.9	1.75
35	Issues arising from remote/hybrid working	0.9	1.8	1.54
36	Product safety recall	0.7	1.9	1.40

A man with a beard, wearing a white shirt, is seen from the side, looking out a large window. The scene is bathed in the warm, golden light of a sunset or sunrise, with a city skyline visible in the background. A large, semi-transparent blue arrow points from the left towards the man, and a large, semi-transparent blue number '4' is overlaid on the left side of the image.

Long-term trend analysis



Adoption levels through the years

The results show that nearly half of organizations (47.9%) take a structured approach to long-term trend analysis, with a central function such as business continuity, resilience, or enterprise risk leading the effort. This centralized model allows for consistency, alignment with strategic objectives and a clearer enterprise-wide view of emerging threats. Departing from the main trend, a smaller but notable proportion (23.5%) adopts a decentralized approach, where individual departments conduct their own analyses.

Combining the different organizational structures, more than two-thirds of practitioners regularly develop long-term trend analysis (71.4%). While this is rather encouraging, the larger picture is not quite as comforting. As the longitudinal analysis shows, interest in long-term horizon scanning activities peaked in the immediate aftermath of the Covid-19 pandemic, only to slowly return to pre-2020 levels. Last year, there seemed to be some renewed attention to this practice, but in 2025, this indicator has decreased again to 2018 levels.

“I’m a very active sponsor for building a control tower because integrating all inputs can be tricky. The major benefit is having outcomes that drive decisions and investments while enabling trend monitoring in a fast-changing environment.”

Business Continuity Officer,
Technology and Electronics Sector,
Europe.

“That is one of the challenges I’ve noticed recently. Broadly, the business has a good resilience posture, but it’s fragmented. Each division (electricity, gas, fibre, water, etc.) works differently, partly due to differing regulatory requirements. The result is that the trend analysis, and resilience more generally, is handled in silos.”

Business Continuity Manager,
Energy Sector, UK.

“We work to break down silos through strong interdepartmental relationships. Over the past 18–24 months, we’ve built a close working relationship with Information Security, collaborating on exercises and evaluations. Emergency Management was integrated into my function about 18 months ago, so our hazard vulnerability analyses now feed into the same BCMS platform. We’re aggregating critical risk information from other functions, like patient safety and risk management, and discussing trends weekly with communications. This integrated approach allows us to identify emerging threats quickly.”

Director of Enterprise Risk Management, Healthcare Sector, US.

Organizations developing long-term trend analysis 2014-2025

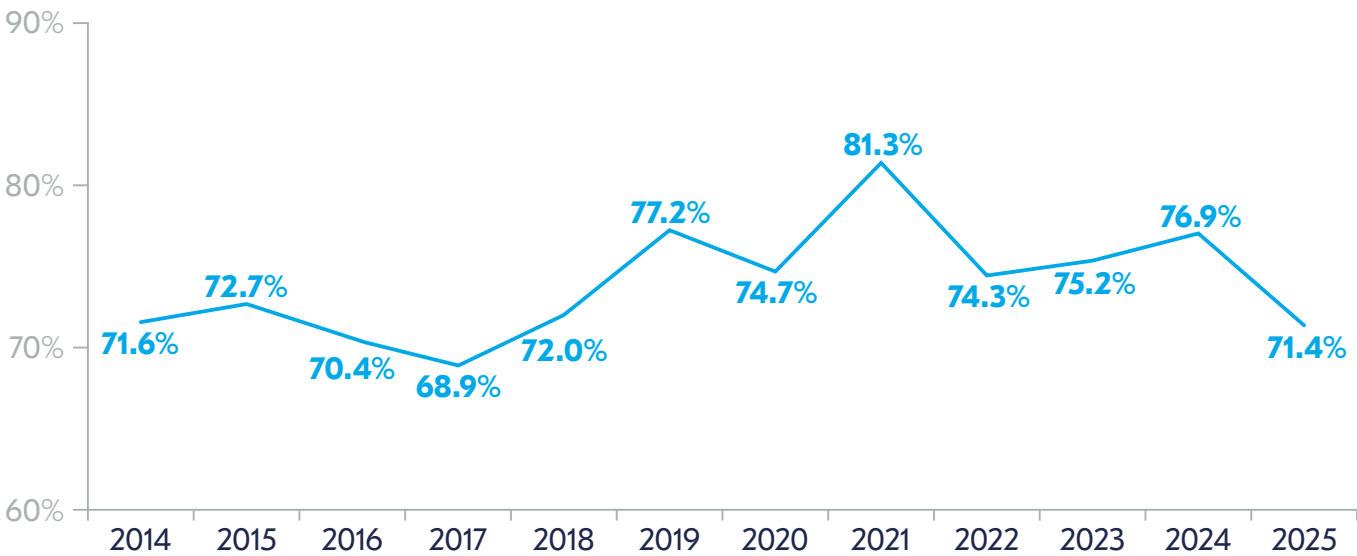
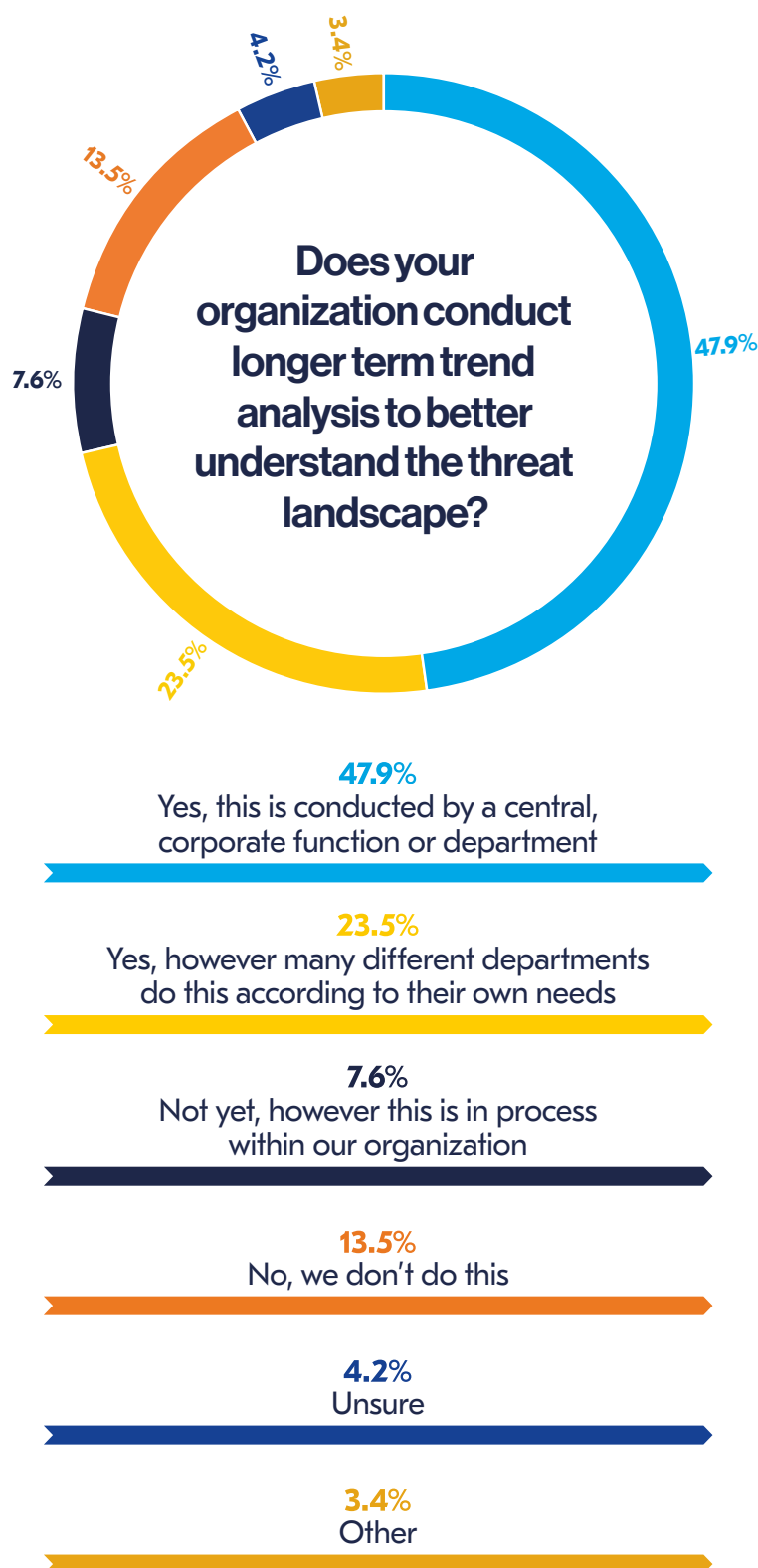


Figure 5. Organizations developing long-term trend analysis (2014-2025).



Leveraging the results of trend analyses

The majority of business continuity and resilience practitioners recognize the value of trend analysis in shaping their programmes. Over one-third (37%) report that they actively use the outputs to inform scenario planning and capability development, while a further 31.1% are directly involved in developing the analysis itself. A senior resilience manager highlighted in a follow-up interview that integrating long-term threat intelligence can strengthen preparedness and support more realistic exercises.

“Running full BCP and RPO exercises takes a lot of time to plan and deliver, so one of my priorities is to get better tooling. We’re exploring more gamified platforms where staff can complete an exercise in 25–30 minutes. Alongside that, I’m asking for an analyst-level colleague to help with documentation and dashboards, because right now everyone is overloaded with meetings and reporting, and we need more capacity to keep things moving.”

Business Continuity Manager, IT and Telecom Sector, Europe.

Figure 6. Does your organization conduct longer term trend analysis to better understand the threat landscape?

“It’s testing, that’s recovery testing, and that’s every organization I’ve been on. That’s definitely the core of my reporting on resilience. I think the place I want to be in any organization is to have the evidence and the security of knowledge that yes, we’ve done certain activities that can show that we’re ready, not perfectly everywhere, but we have a certain level of assurance.”

Senior Resilience Manager, Transport Sector, Canada.

However, more than a quarter (26%) state that they do not have access to this information, reflecting limitations in organizational infrastructure and resource allocation. Practitioners noted that legacy systems, budget constraints, and the sheer volume of external reports often make it challenging to extract actionable insights in a timely manner. Without clear visibility over trends, practitioners may be limited in their ability to prepare for emerging threats, such as supply chain vulnerabilities or climate-related disruptions.

Building on the trend highlighted through this section of the report, interest towards the results of trend analyses is shrinking. The number of participants using their outputs for business continuity purposes has now fallen to its lowest in the past five years. The majority of respondents remain committed to this practice, but this year the figures show a significant decrease (from 81.3% to 68.1%).

Usage of the outputs of trend analysis on practitioner’s business continuity programmes 2014-2025

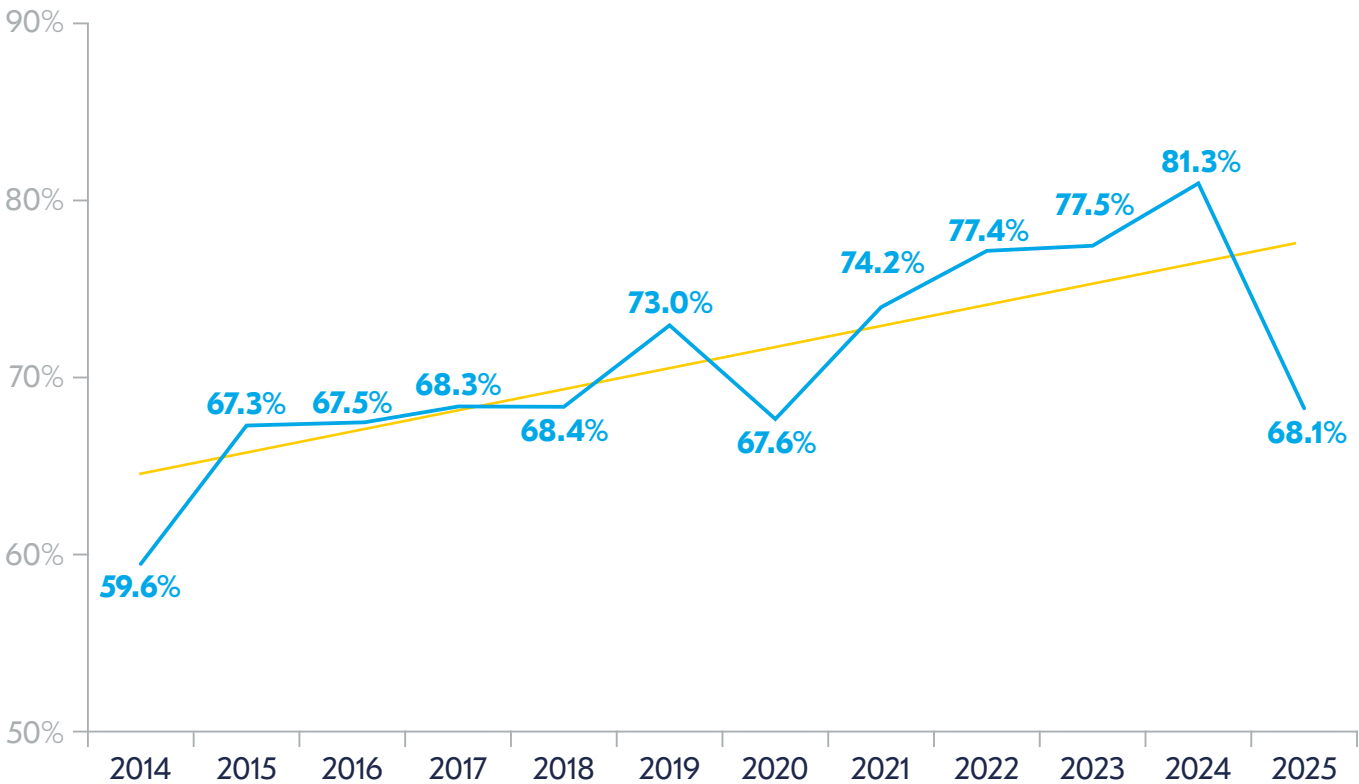


Figure 7. Organizations using the output of trend analysis (2014-2025).

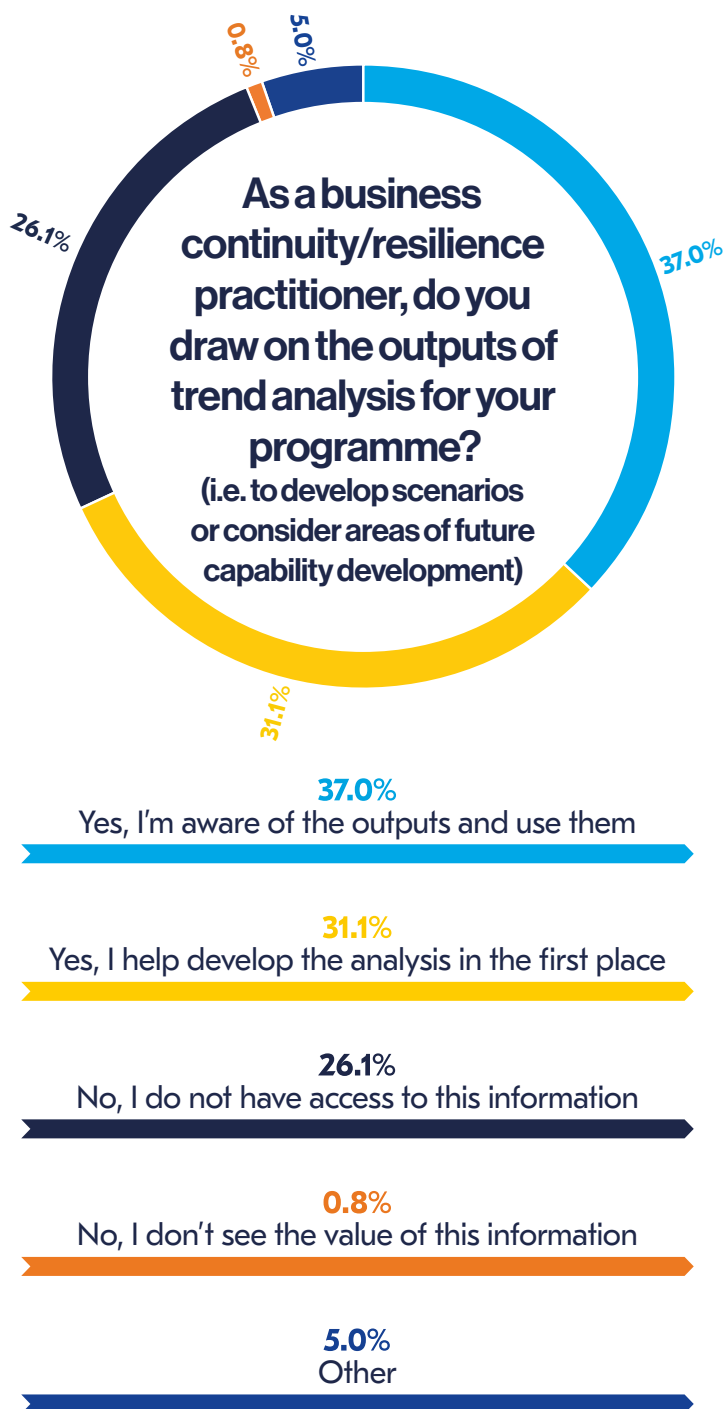


Figure 8. As a business continuity/resilience practitioner, do you draw on the outputs of trend analysis for your programme? (i.e. to develop scenarios or consider areas of future capability development)

Tools and techniques

Organizations draw on a combination of internal and external resources to conduct trend analysis, with a clear preference for insights grounded in their own operations. Internal risk and threat assessments are the most widely used tool (87.2%), as they allow for a tailored analysis to specific organizational contexts and vulnerabilities. Further qualitative insights reveal that internally generated intelligence, such as operational data and exercise results, is critical for anticipating risks that are unique to an organization's facilities, workforce, and regional infrastructure.

External reports and industry insights, including horizon scanning, are also highly used (75.2%) to gain a broader view of emerging risks and benchmark performances against sector-wide trends. Practitioners highlighted the value of regional risk registers and industry reports, though they also noted challenges in processing the volume and complexity of this information without additional tools or AI support.

Participation in industry events (55.6%) and collaboration with peers (52.1%) also play a role in facilitating shared learning and a comprehensive understanding of the threat landscape. Practitioners noted that informal peer exchanges often supplement formal reporting, helping to interpret regulatory expectations and regional operational nuances.

Research reports (50.4%) are slightly less common but still make the top five, due to their structured, evidence-based perspectives that can complement internal and peer-derived insights. Further qualitative insights revealed that these sources are particularly useful for horizon scanning around technological innovations, such as AI and IoT, and for monitoring macro trends such as climate events or geopolitical instability, which may not yet be fully reflected in internal operational data.

It is interesting to observe that the top five tools practitioners use for trend analysis all rely on human inputs. Despite growing talk around new technology, particularly artificial intelligence, reading reports, collaborating with peers and exchanging views with other professionals at conferences remain vital activities to better understand the risk and threat landscape. Even internal assessments, which are increasingly relying on new solutions, are still in many cases a predominantly human-based task, where information is extracted through interviews and meetings.

Which tools do you use to conduct trend analysis/horizon scanning of the risks/threats to your organization?



Figure 9. Which tools do you use to conduct trend analysis/horizon scanning of the risks/threats to your organization?

Over half (55%) of the organizations in the sample have strengthened their use of technology to varying degrees over the past two years. In-depth interviews suggest that where adoption has increased, it often involves leveraging AI and automated tools to process large volumes of internal and external data, such as incident logs, regulatory updates, and horizon scanning reports. While these tools are valuable for a faster identification of emerging risks, they are usually adopted alongside other solutions. Still, the largest single group (34.2%) indicates no increase in technology at all. Barriers include high costs, lack of in-house expertise, and uncertainty over the tangible benefits of advanced analytics.

"We're already seeing that processes are becoming heavily dependent on AI models. People use them for everything, from writing emails to analysing data, and if there's an outage, I think many would really struggle. In the future, we'll need to build workarounds into our continuity planning, because as useful as AI is, these models can and will fail."

Business Continuity Manager,
IT and Telecom Sector, Europe.



Figure 10. Has the use of technology to analyse your organization's threat landscape and its potential impact increased over the last two years?

Benchmarking business continuity





ISO 22301 adoption and alignment

The findings highlight that ISO 22301 continues to serve as the leading reference for business continuity management programmes, though certification levels remain relatively low. A small proportion of organizations (14.9%) use both the framework and certify to it, whereas the largest group (59.2%) apply ISO 22301 as a framework without pursuing certification. This is a noticeable increase from the 2024 report, where only a third of respondents (36.8%) aligned towards the standard. This trend matches the decrease in the number of those who are planning to align towards ISO 22301 compared to last year (26.3%). Therefore, it appears that at least some of those organizations who were looking for greater alignment have in fact moved closer to international good practices this year. This shows that organizations are recognizing the value of the standard in structuring their programmes, but certification is not always considered essential due to cost, resource considerations, or customer requirements.

“We align closely to ISO 22301, but we’re not certified. For me, alignment means if you applied tomorrow, you’d pass. In reality, most organisations aren’t quite there, alignment gives you flexibility that certification doesn’t.”

Business Continuity Manager, Energy Sector, UK.



Those respondents who certify perceive several key benefits associated with ISO 22301. The most widely recognized advantage is its contribution to organizational resilience (80.8%). Closely aligned, 76.9% note that certification allows them to demonstrate the effectiveness of their BCM programme to external stakeholders, reinforcing trust with regulators, clients, and partners.

Certification also supports operational improvements. Over half of the respondents report that it enables consistent BCM measurement and monitoring (57.7%), improves customer satisfaction (57.7%) and strengthens communications and employee engagement (53.9%). These outcomes extend beyond the organizational value of structured BCM processes, with a positive impact on regulatory or reputational benefits. As for specific business continuity objectives, the standard supports faster recovery after a disruption (50%), which is in line with the overall purpose of the document.

"We use ISO 22301 as a framework, but are not certified. It's very useful to reference for best practice, but it would be quite alien to our organization, which focuses on Joint Commission and CMS standards for compliance."

Director of Enterprise Risk Management,
Healthcare Sector, US.

"ISO certification reduces insurance costs, opens doors to certain contracts, and ensures a level of implementation that helps optimize day-to-day management and operational efficiency."

Business Continuity Officer,
Technology and Electronics Sector, Europe.

Figure 11. If you have a formal business continuity management programme in place, how does it relate to ISO 22301?

What benefits does certification provide to you and your organization?

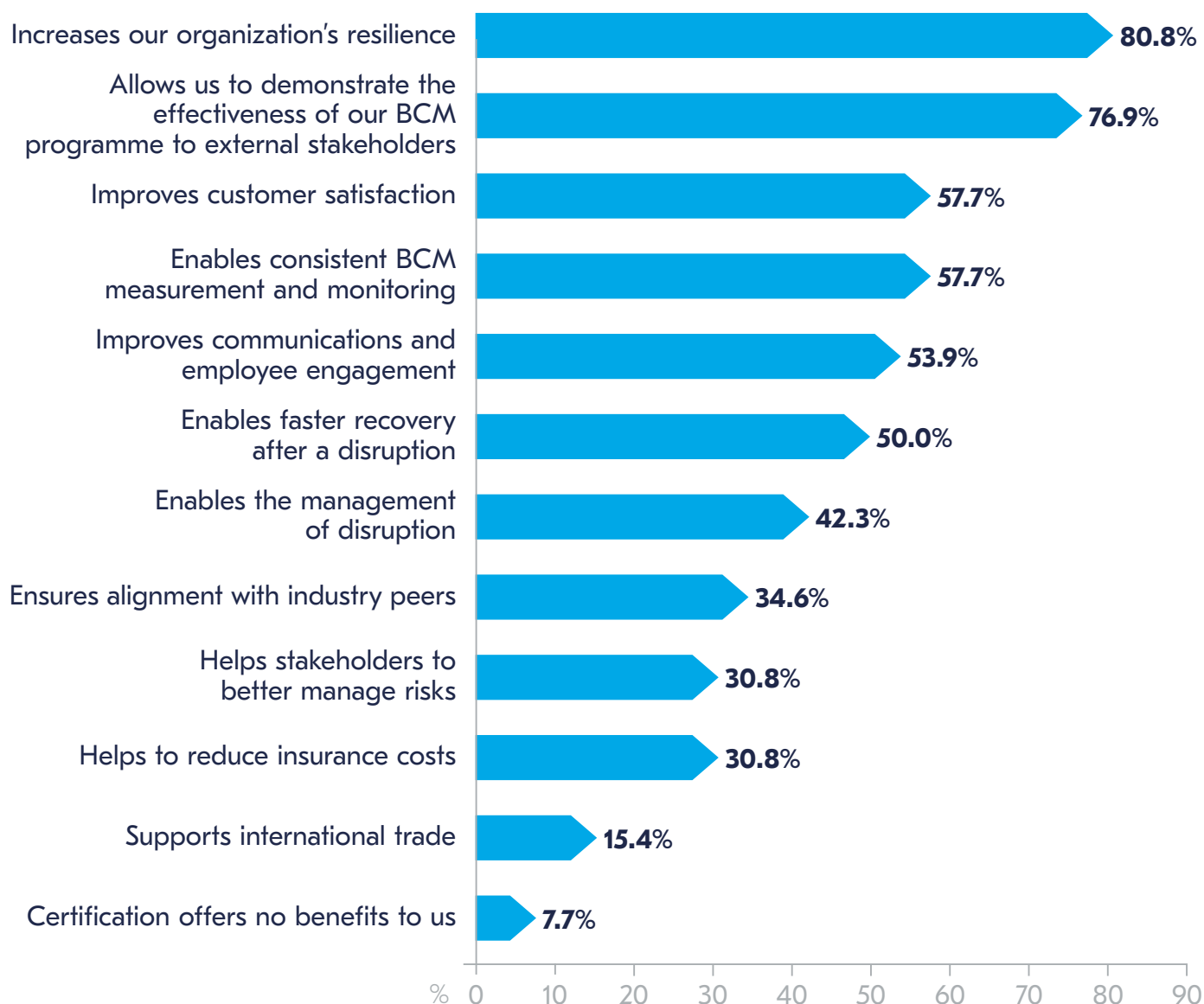


Figure 12. What benefits does certification provide to you and your organization?



Alignment over time

The results show that the vast majority of organizations (92.4%) have continued to use ISO 22301 over the past two years, indicating strong ongoing reliance on this standard for structuring their business continuity and resilience programmes. Only a small minority (5.1%) report moving away from ISO 22301 in favour of another resilience standard.

“If regulation did come to manufacturing, the simplest and most understandable model would be to follow ISO standards. ISO is clear, internationally recognized, and would give us a framework to work with.”

Business Continuity and Risk Management Specialist,
Technology Sector, Japan

“Certification is increasingly valuable. With regulations like DORA, banks and financial institutions are sending us detailed questionnaires about business continuity. Being able to show ISO 22301 certification demonstrates maturity and makes those conversations easier. We had hoped to finish certification this year, but with delays around NIS2 and the audit, it will likely be pushed into early next year.”

Business Continuity Manager,
IT and Telecom Sector, Europe.



Figure 13. Have you moved away from using ISO 22301 in place of another resilience standard over the past two years?



On the other hand, respondents who chose not to certify did so for a variety of reasons. The most commonly cited factor is the absence of a business requirement (58.8%), followed closely by organizations that already align to the standard but do not see the need for formal certification (55%). These responses suggest that, for many, certification is viewed as optional rather than essential, particularly when internal processes already reflect good practices. Resource constraints also play a significant role; in particular, lack of staff time (40%) and budget limitations (38.8%) are frequent barriers, while 33.8% point to insufficient management commitment.

Several qualitative comments provide further context on why organizations may choose not to pursue ISO 22301 certification. Some note that the standard can be overkill, especially for a small or medium enterprise, since formal certification may be disproportionate to organizational size or complexity. Others report regulatory compliance as the primary driver, rather than certification itself, suggesting that meeting external obligations can suffice without formal ISO alignment.

Several organizations are still in early stages of maturity, stating that they are still in the preliminary stages of BCM implementation, and it is not the right time for them to consider certification. Similarly, some are actively exploring the requirements and potential benefits of certification, but they need to investigate the effective need and requirements for being certified. On a concluding note, a subset of participants emphasized alternative approaches to resilience and continuity, including a focus on operational resilience or adherence to other documents, such as the BCI Good Practice Guidelines.

What are your reasons for not being certified or having no plans to be certified to ISO 22301?

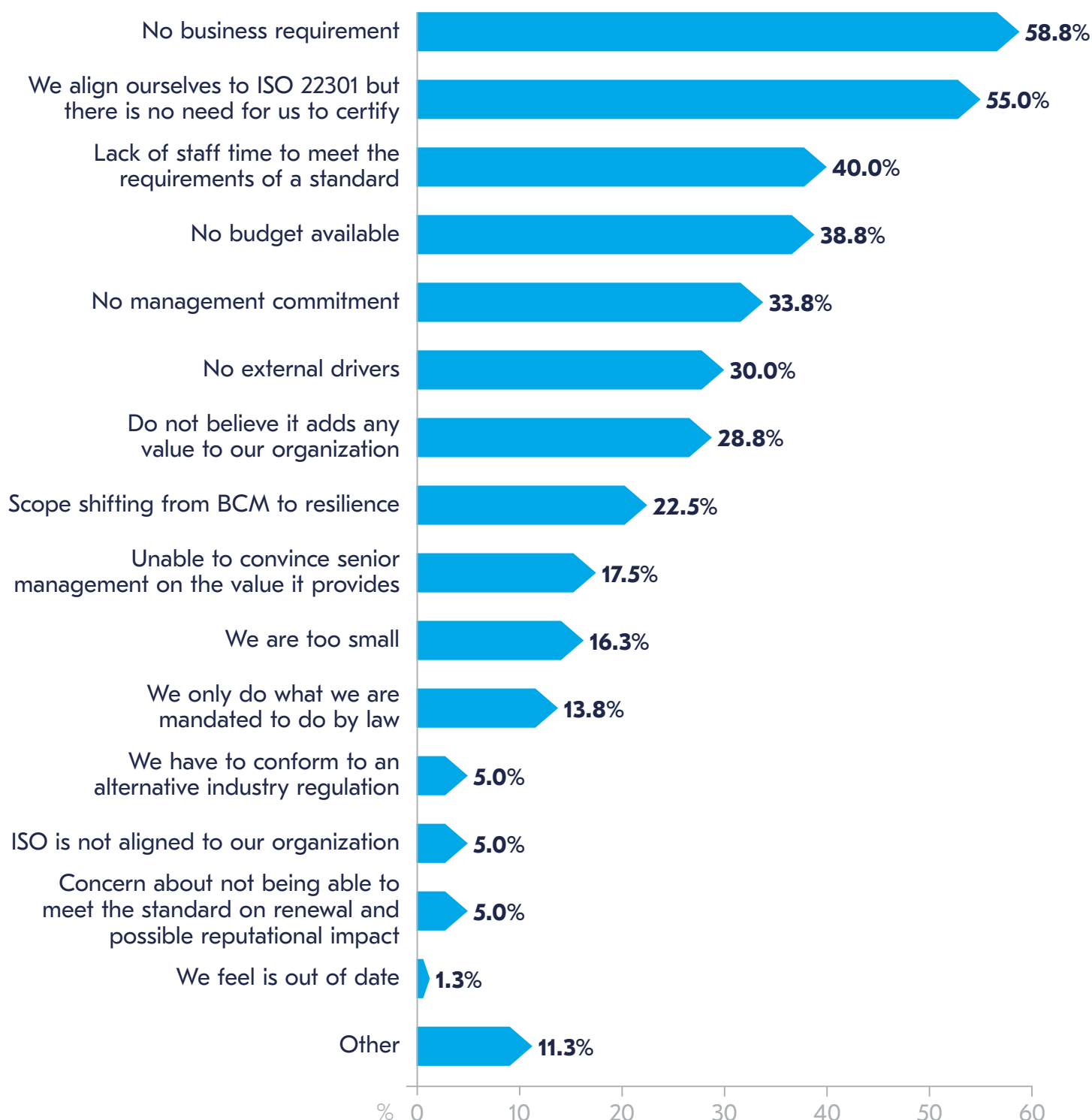


Figure 14. What are your reasons for not being certified or having no plans to be certified to ISO 22301?

6 Looking ahead



The future threat landscape

The survey highlights a broad spectrum of concerns for organizations over the next five to ten years. At the top of the chart, cybersecurity proves to be at the top of the agenda (63.6%), consistently with last year. Interviewees from different sectors echoed this urgency. A UK resilience director described boards' growing focus on reputational and regulatory fallout from breaches, while a US healthcare professional warned that cyber incidents can cascade into both patient care and compliance crises.

Climate risk follows in second place (40.7%), as practitioners consistently described extreme weather and changing environmental conditions as an immediate operational threat. The theme of extreme weather resonates with natural hazards being the most disruptive event for practitioner this year and it is also consistent with last year's figures for future concerns. Respondents warned about the impact of phenomena such as hurricanes, floods and heatwaves on facilities and supply routes. On this note, a global manufacturing risk director flagged droughts and resource scarcity as drivers of rapid cost escalation and production risk.

"Looking ahead 5 to 10 years, my top concerns are clear: first, natural disasters like earthquakes and tsunamis; second, cyberattacks, which keep rising in number and sophistication; and third, geopolitical tensions, particularly between the US and China, which could change the situation for Japanese companies in unpredictable ways."

Business Continuity and Risk Management Specialist,
Technology Sector, Japan.

The role of AI (30.5%) was raised repeatedly as both an enabler and a new source of exposure. This is the first time AI is expressed as a clear concern over the future threat landscape, although emerging technology (21.1%) was part of the top five last year. Respondents noted that efficiency gains may lead to rapid adoption without strong governance, possibly creating single points of failure and broadening attack surfaces. On this note, ISO has published an AI and information security bundle that includes ISO 27001 as well as ISO 42001, which is specific for AI management.

Geopolitical change (28.8%) was also part of the future risk picture, from tariffs and trade-policy shifts to changing regulatory priorities. Practitioners pointed out that shifts and tensions at the geopolitical level intersect with other attack vectors such as cyber incidents and supplier failure. Recent years have shown that while hybrid war is now a widespread practice and in many cases organizations are caught in the crossfire between state-sponsored actions. To meet these challenges, it is important to review both internal vulnerabilities and external dependencies that might hide risks to the organization.

“Cybersecurity is moving so fast, especially with AI. I can’t predict what will happen next month. Political change is uncertain too. We need scenario planning for major ‘what ifs’ to prepare for potential impacts.”

Director of Enterprise Risk Management,
Healthcare Sector, US.

Consistently, operational dependencies remain front of mind, with supply chain disruptions (26.3%), technology and telecom issues (24.6%), and third-party failure (22.9%) all cited as future risks. Across the interviews, smaller vendors and legacy suppliers were repeatedly identified as weak links that complicate compliance and resilience, sometimes forcing larger organisations to adopt risk exceptions or invest in remediation.

“Enterprises have a certain misunderstanding that trucks will always deliver, boats will always arrive on time, and staff will always be available. These networks are being strained, and organizations need to account for that. Something happening in one part of the world can ripple through the entire network, and corporations need contingency plans to deal with strikes, power outages, or other disruptions that affect the supply chain.”

Senior Resilience Manager,
Transport Sector, Canada.

Regulatory changes (18.6%) were seen as particularly consequential for organizations operating in critical sectors, where compliance requirements and government oversight strongly influence resilience investment. Several interviewees noted that regulation often acts as the main lever for securing board-level commitment, with one senior leader explaining that funding for continuity and resilience programmes is far more easily justified when tied to legal or sectoral obligations. At the same time, geopolitical instability, in the form of war or conflict (16.9%), was described as a persistent uncertainty, shaping supplier strategies and influencing long-term planning for international operations.

Looking further ahead, practitioners also pointed to challenges that may not dominate immediate risk registers but nonetheless accumulate over time. Talent shortages (13.6%) were a recurring concern, with interviewees linking them to both demographic shifts and the growing competition for specialist skills in areas such as IT security and crisis management. Practitioners cautioned that without sustained investment in people and expertise, even well-structured resilience frameworks risk becoming unsustainable in the face of rising digital, environmental, and geopolitical challenges.

"Talent concerns and misinformation are key risks. Critical information can be missed or managed by the wrong people, and reputational risk is increasingly connected to many aspects of the organization, not just product quality."

Business Continuity Officer,
Technology and Electronics Sector,
Europe.



Looking ahead over the next 5-10 years, what are your top three concerns for mid-term risks?

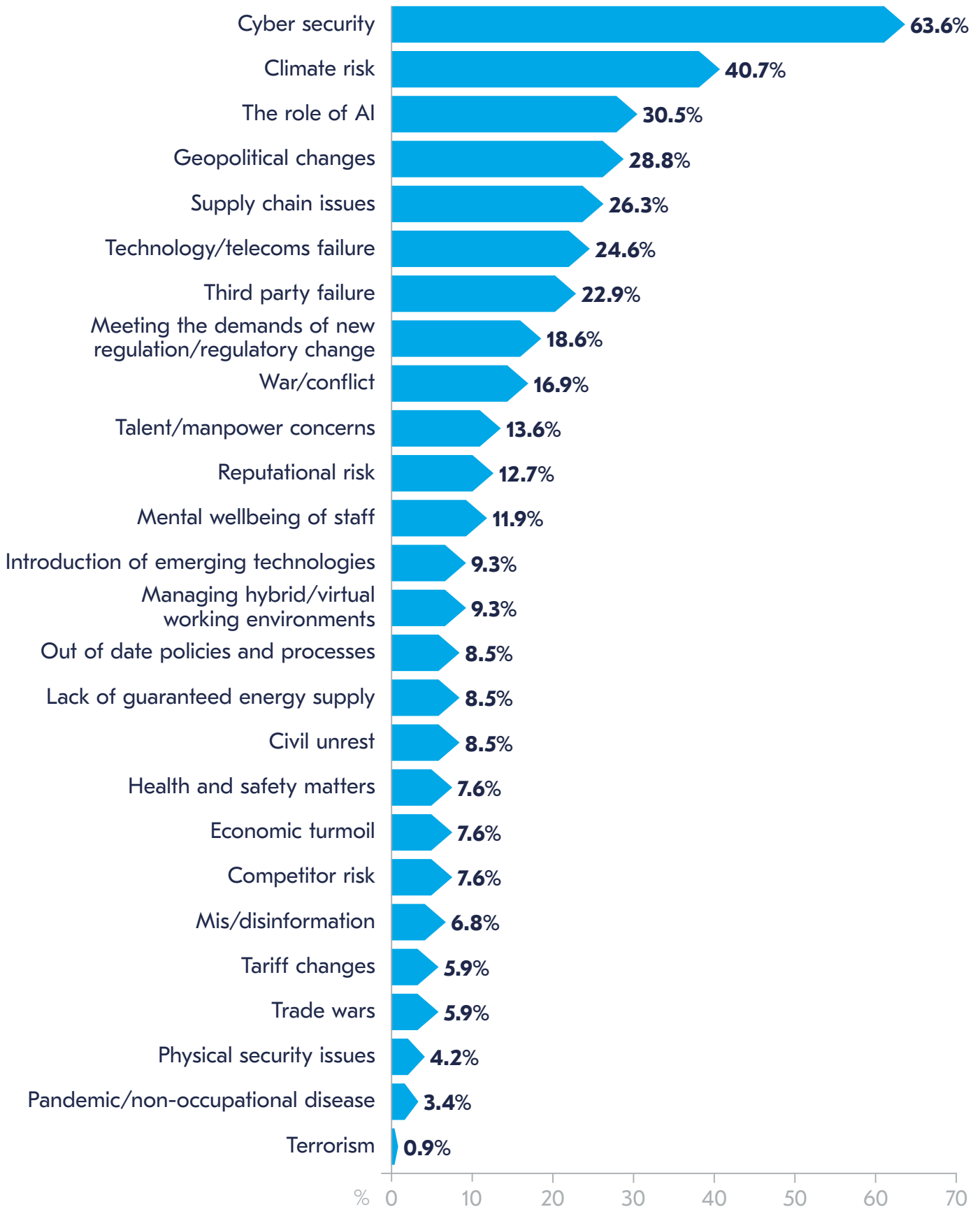


Figure 15. Looking ahead over the next 5-10 years, what are your top three concerns for mid-term risks?

Support for business continuity and resilience

The survey shows that most organizations plan to maintain or modestly increase investment in business continuity and resilience programmes in 2026. A significant proportion (43.1%) intend to maintain investment at levels appropriate to the programme’s scope and current lifecycle stage, reflecting a focus on sustaining existing capabilities.

Differently, nearly one-fifth (19.8%) plan to increase investment to address growing programme needs or emerging requirements identified through horizon scanning, indicating proactive efforts to strengthen resilience in response to evolving threats. Overall, the figures are rather consistent with last year’s results, when 73.9% stated they would maintain or increase investment levels, similarly to the 2025 percentage (62.9%).

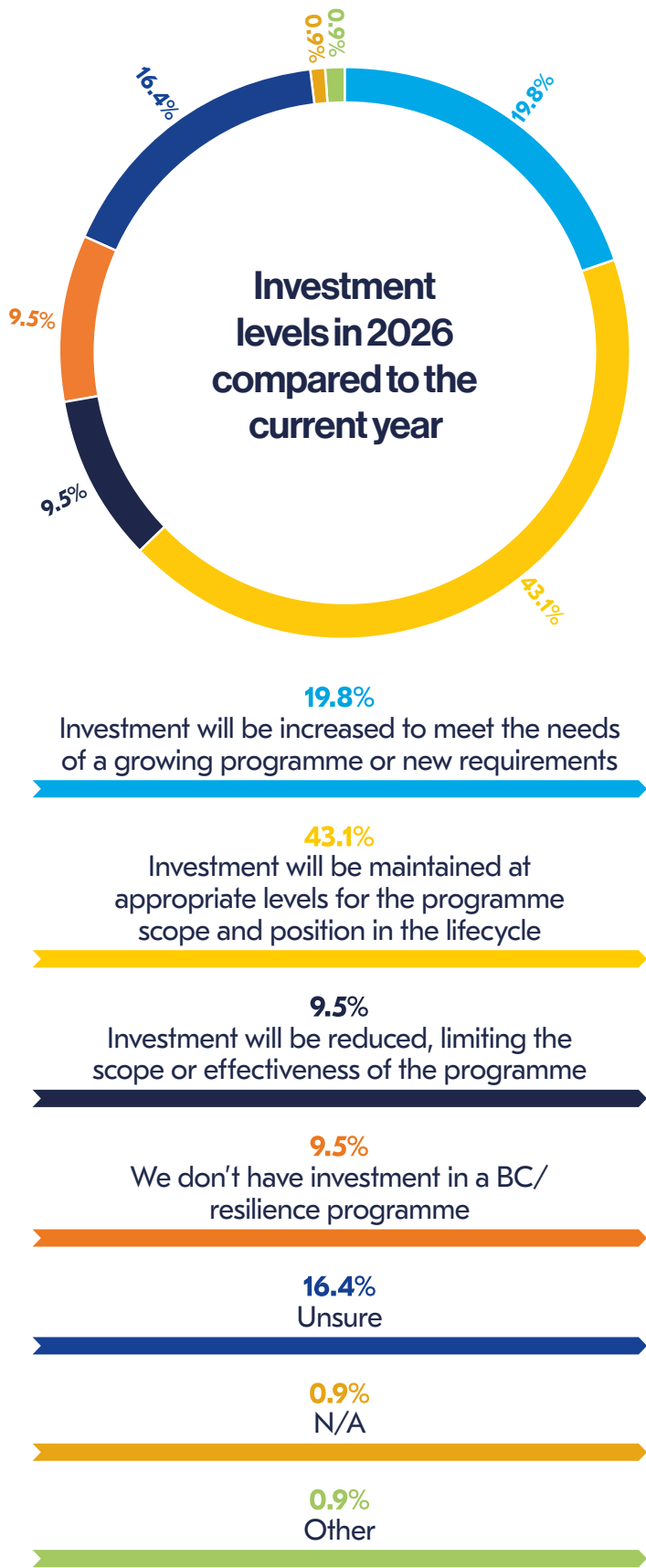


Figure 16. Investment levels in 2026 compared to the current year.

Annex



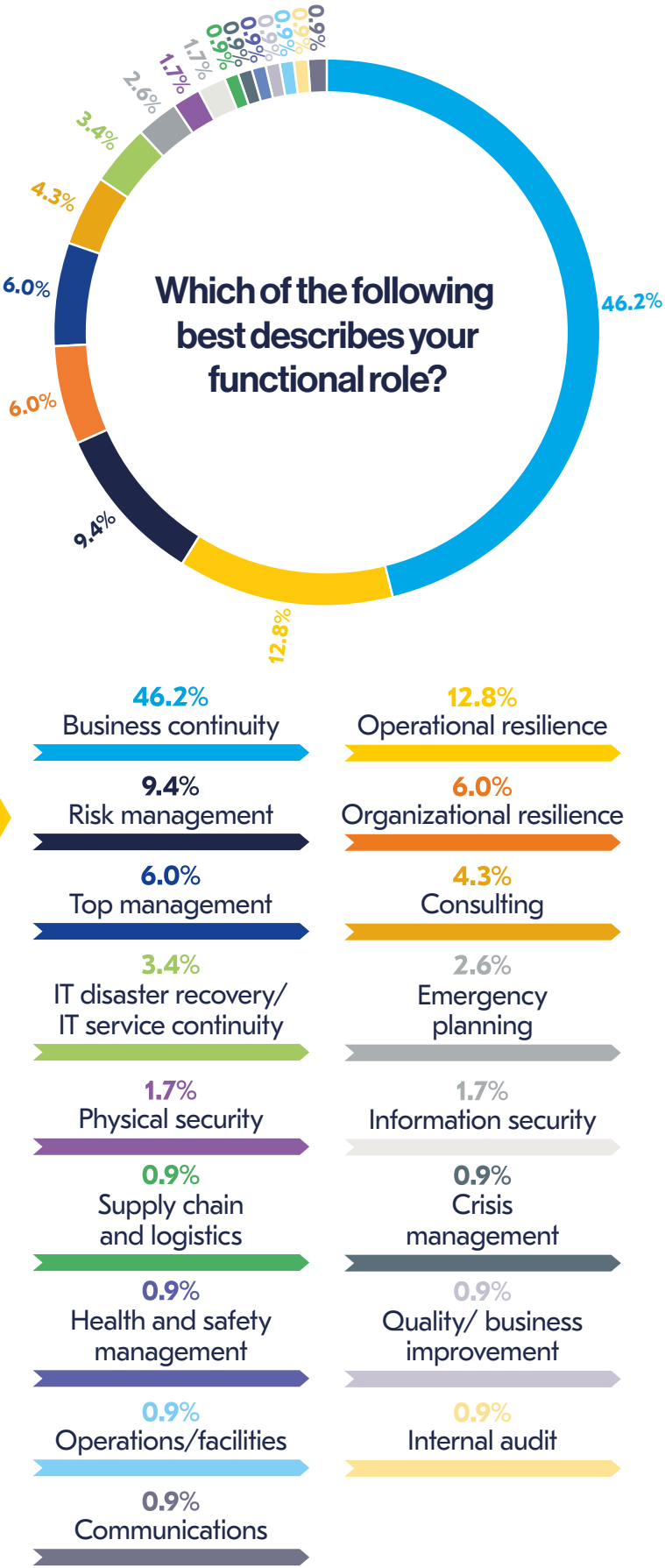


Figure 17. Which of the following best describes your functional role?

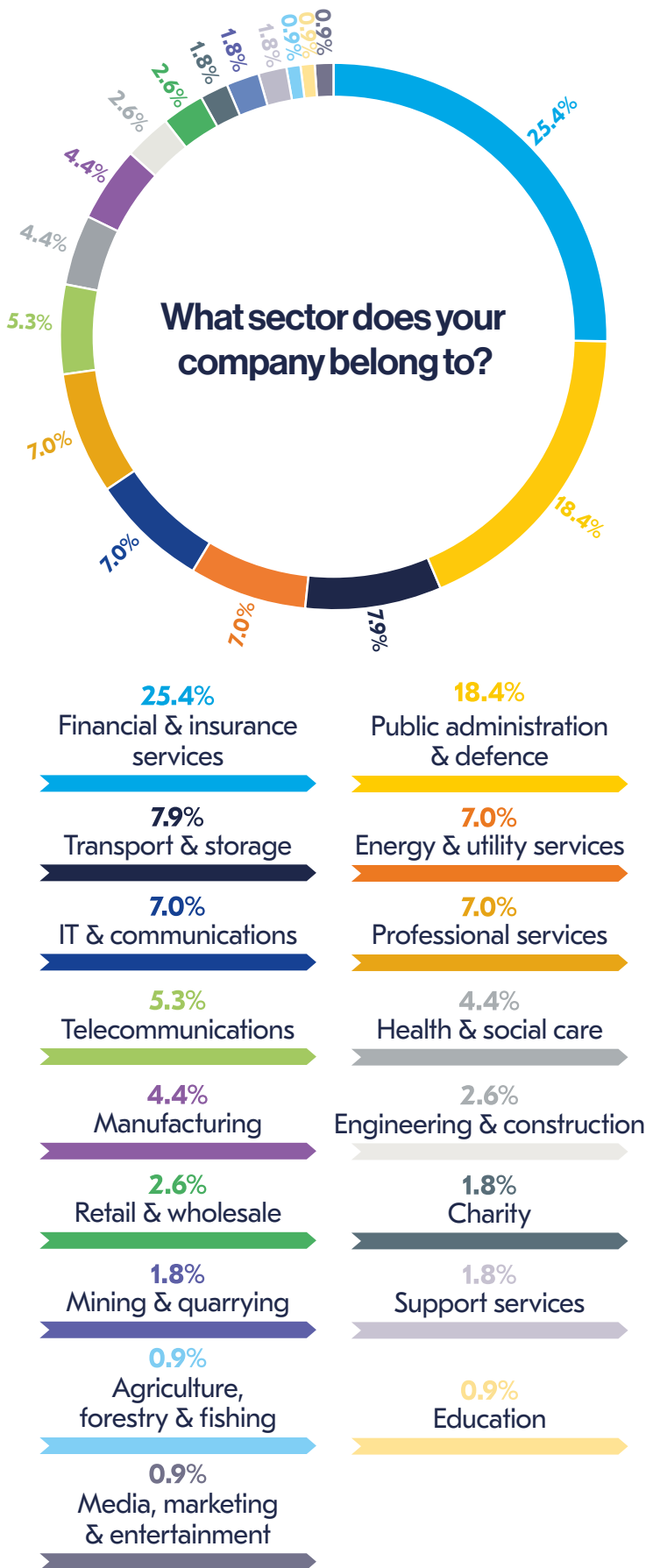


Figure 18. What sector does your company belong to?

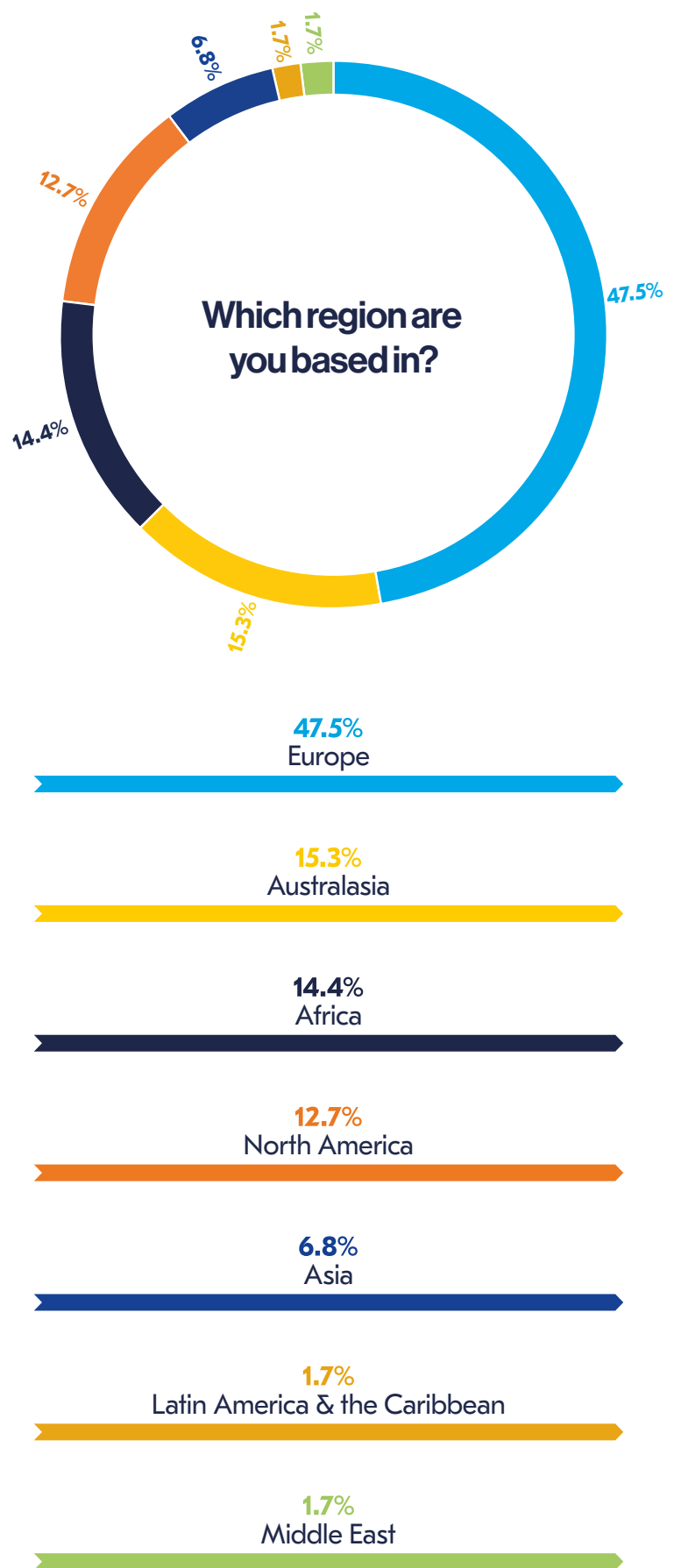


Figure 19. Which region are you based in?

Approximately how many employees are there in your organization globally?

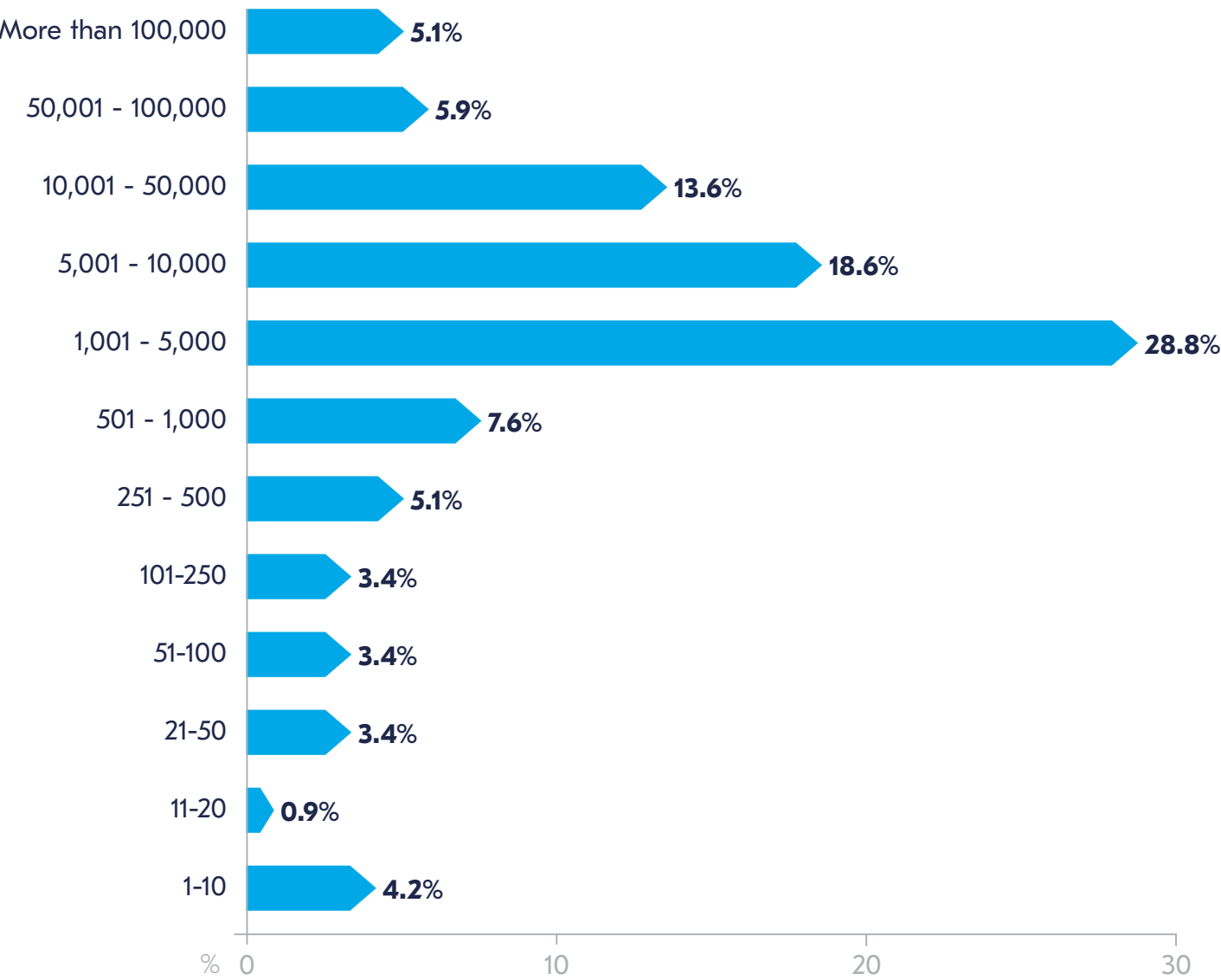


Figure 20. Approximately how many employees are there in your organization globally?

About the authors



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



Gianluca Riglietti

(Content Specialist in Business Continuity and Resilience)

Gianluca is a researcher and a freelance content creator interested in the development of resilient and safe societies. He has experience managing international research projects for companies such as BSI, Zurich, Everbridge, and SAP. He works regularly with a number of organizations in the field of organizational resilience, such as the BCI. In his publications he has addressed a wealth of topics, such as climate change, cyber security, supply chain management, and business continuity. He is also a PhD candidate at Politecnico di Milano, where he investigates the impact of business continuity management on supply chain resilience.

He can be contacted at SCWF@protonmail.com.

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 10,000 members in more than 120 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, is 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 180 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 Conducttr



Conducttr is a realistic crisis exercise platform that helps organizations prepare for the day they hope never comes. Risks and crises are growing, and when the unexpected hits, slides and checklists won't be enough.

Our platform lets you safely replicate crises as they would unfold in real life, capturing the stress, confusion, and urgency of true events. Through realistic, emotionally engaging exercises, teams build muscle memory to stay calm and perform under pressure when it counts most.

Conducttr supports every stage of the process, from scenario design to delivery and after-action review, with integrated AI to make creating and managing lifelike exercises faster and more efficient. Exercises can be run in person or remotely and hosted securely on your own hub for clients or business units.

Built for every business continuity, risk, and resilience scenario, Conducttr turns training into confidence.

Experience it yourself in our next live simulation: **www.conducttr.com/live-sim**

Bibliography

1. European Commission. "NIS2 Directive: securing network and information systems." Digital Strategy — Shaping Europe's digital future, [ec.europa.eu, digital-strategy.ec.europa.eu/en/policies/nis2-directive](https://ec.europa.eu/digital-strategy/ec.europa.eu/en/policies/nis2-directive).
2. European Insurance and Occupational Pensions Authority. "Digital Operational Resilience Act (DORA)." EIOPA, www.eiopa.europa.eu/digital-operational-resilience-act-dora_en.
3. International Organization for Standardization. ISO 22301:2019 — Security and resilience — Business continuity management systems — Requirements. ISO, www.iso.org/standard/75106.html.
4. International Organization for Standardization. ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO, www.iso.org/standard/27001.
5. International Organization for Standardization. ISO/IEC 27005:2022 — Information security, cybersecurity and privacy protection — Guidance on managing information security risks. ISO, www.iso.org/standard/80585.html.
6. International Organization for Standardization. AI and information security management bundle. ISO, www.iso.org/publication/PUB200427.html.



BCI 9 Greyfriars Road, Reading, Berkshire, RG1 1NU, UK

bci@thebci.org / www.thebci.org

