Find out more
www.thebci.org

Thought Leadership

BCI Operational Resilience Report 2024

riskonnect
Integrated Risk Management Solutions™

Leading the way to resilience

Contents

Foreword

We are pleased to introduce the 2024 BCI Operational Resilience Report, sponsored by Riskonnect. This report was first published in 2022, driven by the spate of new operational resilience regulations being brought in across the globe for financial services (FS) organizations. At that point, the implementation deadlines for operational resilience regulations were three years away, and professionals were confident that, with the length of time available, they would be able to meet those deadlines.

Two years on from the first report, the deadline to meet the requirements of the Monetary Authority of Singapore (MAS)'s Business Continuity Management Guidelines has already passed, and the UK's Operational Resilience Framework, the EU's Digital Operational Resilience Act (DORA), and adherence to Australasia's CPS 230 standard are all looming. Although confidence in meeting the requirements remains high, it has dipped slightly. This is somewhat attributable to natural concerns of time running out, but participants in the research for this report also criticise the regulators for not providing enough guidance or feedback on current arrangements made, as well as additional areas being added to regulation (such as third-party requirements) which require additional work and resource.

It is encouraging to note in this report that while 'definition confusion' is still very much present when it comes to business continuity, operational resilience, organizational resilience, and operational risk, the key principles of operational resilience are now extending beyond the financial services sector due to the perceived value in protecting both customers, reputation, and, ultimately, their balance sheets. While regulation is the primary driver to building an operational resilience programme, it is refreshing to see that nearly 60% of respondents have an operational resilience programme for 'good practice purposes'.

This year's report has also seen significant steps forward in how operational resilience is led, managed, and implemented in organizations. With the c-suite (normally the CEO) taking overall charge, this year has seen another leap in the number of organizations creating the role of Chief Resilience Officer or Head of Resilience to manage the implementation of the programme, as well as providing a voice directly to board level. This year, nearly a fifth of respondents report such a role in their organization (18.8%), a seven-percentage point increase on 2023 (11.8%), and more than doubling since 2022 (9.2%). Furthermore, the report shows that operational resilience is now more regularly on the agenda of board meetings, as well other committees.

A notable concern of respondents this year is ensuring critical third-party suppliers meet the requirements of the regulations. While this has always been an intrinsic part of DORA regulation, the new requirements were introduced into UK legislation only last year. For smaller suppliers, the cost of meeting the requirements may prohibit them in continuing as a supplier, whereas practitioners report that larger suppliers can be reluctant — or very slow — in providing information proving compliance.

Overall, this report provides a window in the exciting and fast-moving sphere that operational resilience has become in 2024. We would like to thank Riskonnect for their sponsorship of this report, and also those who gave their time to answer the survey or take part in interviews as part of the research. We hope you find this report useful, and provides a useful benchmark and guide for operational resilience activities within your own organizations.

Rachael Elliott
Knowledge Strategist
The BCI

Foreword

Riskonnect is proud to once again sponsor the BCI Operational Resilience Report 2024.

In today's fast-paced environment, operational resilience has become a cornerstone for organizations across various sectors. This report delves into the changing contours of resilience in the face of regulatory mandates and practical realities.

The financial services industry stands as a prime example, facing imminent deadlines for compliance with regulations like the EU Digital Operational Resilience Act (DORA) and the Australian APRA CPS 230 standard. The findings revealed in this report detail widespread adoption of operational resilience initiatives, reflecting the growing recognition of its importance.

Regulatory pressure serves as a catalyst for many organizations, driving them to establish resilience programmes. Yet, alongside compliance, there's a growing understanding of the broader benefits these programmes offer, from bolstering customer trust to enhancing commercial viability.

In the UK financial sector, confidence in meeting regulatory targets is high, but as deadlines approach, concerns arise about aligning investments and mapping exercises with predefined impact tolerances.

Operational resilience isn't confined to the financial sector; its influence extends across all sectors, underscoring its universal relevance. Definitions may vary, but there's consensus on key elements: identifying critical services, mitigating vulnerabilities, and setting impact tolerances.

The line between business continuity and operational resilience remains blurred, with overlapping responsibilities. Nevertheless, there's a shift towards proactive approaches in preventing disruptions and safeguarding customer interests.

At the helm of these efforts, senior management plays a crucial role, driving resilience agendas and fostering a culture of adaptability. But challenges persist, from organizational adoption to resource constraints, highlighting the need for ongoing support and innovation.

I hope that you enjoy reading this report and trust it will provide insights that help shape your thinking on how operational resilience concepts can introduce value to your organisation in 2024 and beyond.

Jim Wetekamp
CEO
Riskonnect

Executive summary

Operational resilience is now an intrinsic part of most organizations' operating structures.

In the financial services industry, with deadlines looming in January, March and July 2025 for the EU Digital Operational Resilience Act (DORA), the UK FCA/PRA/Bank of England operational resilience requirements, and the Australian APRA CPS 230 standard respectively, implementation is now at a critical stage. With the regulation cutting through related sectors (e.g. critical third-parties such as datacentres) and operational resilience regulations rising in other sectors, the vast majority of organizations either have an operational resilience programme, or are in the process of developing one.

Does your organization have an operational resilience programme or project?

✓ **64.8%** Yes

16.0% We are in the process of developing one

✗ **8.8%** No

Regulation is the primary driver for building an operational resilience programme, although a statistically significant percentage do so for good practice purposes.

Regulation is the primary driver for developing an operational resilience programme for the first time since the inception of this report. However, a high number of respondents are still developing operational resilience programmes for good practice purposes. This further demonstrates the cross-sectoral recognition of the importance of an operational resilience programme and, with organizations also building a programme for commercial and/or customer benefit, an appreciation of the cost and reputational benefits a programme can deliver.

Top five reasons for the development of an operational resilience programme.

1	67.0%	Regulatory requirement
2	58.5%	For good practice purposes
3	32.1%	Commercial and/or customer benefit
4	32.1%	Industry requirement
5	27.4%	To be prepared for incoming regulation

There has been an increase of operational resilience regulations around the world. As new countries and sectors introduce new guidelines, many organizations are now having to comply with multiple regulations simultaneously.

There has been a surge of legislation worldwide. Two-thirds of organizations comply to between one and five different regulatory schemes, with nearly a fifth (18.4%) having to meet the requirements of more than five. A minority of respondents do not adhere to any scheme or legislation. The definitions outlined in these documents often vary, leading to potential confusion. Interviewees also report that compliance to an increasing number of global regulatory schemes was requiring additional staff time and investment, creating challenging operating conditions.

Number of operational resilience regulatory compliance requirements.

66.2%	1-5
18.4%	More than 5
15.4%	Unsure

Although a set definition of operational resilience across all sectors and countries still has yet to be clearly defined, there is a growing agreement of the key elements that should be part of an operational resilience programme.

Although financial services organizations are sometimes deemed to be the forerunners for operational resilience, the concept has existed in the sectors such as aviation and emergency services for decades. Despite these different settings, there are common factors across the different components of operational resilience programmes. The identification of important business services (IBS) has near universal agreement as being an essential activity when building an operational resilience programme, while the identification of critical suppliers, the prioritisation of establishing the vulnerabilities that threaten impact tolerances, and establishing impact tolerances are all seen as vital by more than 80% of respondents.

Top four critically essential processes/tools within operational resilience

95.8%
Identifying Important Business Services (IBS)

88.3%
Identifying critical suppliers

83.2%
Prioritising and working vulnerabilities that threaten impact tolerances

81.7%
Establishing impact tolerances

Support by senior management for operational resilience programmes is high. Furthermore, as implementation deadlines approach, operational resilience is now typically on the agenda of risk and technology risk committees more frequently than ever before.

This year has seen an increase in the frequency of discussions around operational resilience especially within the technology function, incentivised by the digital components of regulations such as DORA, third-party technology risk management.

How often is operational resilience on the agenda of the following committees or their nearest equivalent in your organization? Those answering quarterly or more often:

	2023	2024	Percentage change year-on-year
Risk Committee	59.1%	68.4%	+9.3%
Technology Risk Committee	47.9%	65.4%	+17.5%

The role accountable for operational resilience tends to sit within the c-suite. However, newly created 'heads of resilience' have become more prominent than ever before in running the day-to-day activities of the operational resilience function.

The responsibility for operational resilience should — and does, to the most extent — lie within the c-suite. In terms of operational management, the last three years has seen an acceleration in the creation of the head of resilience role, which typically takes ownership of the daily management of operational resilience programmes. The head of resilience is now responsible for operational resilience in almost a fifth of organizations, an increase of over 100% since 2022.

What is the job title of the person with **overall** responsibility for operational resilience in your organization? Top three responses.	What is the job title of the person with **day-to-day** responsibility for operational resilience in your organization? Top three responses
16.7% Chief executive officer (CEO)	**22.9%** Business continuity manager
14.8% Chief operations officer (COO)	**18.8%** Head of resilience
14.8% Chief risk officer (CRO)	**12.5%** More than one person accountable (shared accountability)

The UK financial services regulators were one of the first to launch a discussion paper on operational resilience. With the deadline almost upon us, most organizations are now confident that they will reach the implementation deadline of 31 March 2025.

The confidence shown by organizations in the UK finance and banking sector regarding meeting regulatory targets indicates that most will meet the March deadline. However, confidence has waned slightly compared to last year, just as the deadline approaches. This could be due to the additional third-party demands being added late into the regulation, but also last-minute concerns that requirements would not be met — a discussion point in the 2022 edition of this report[1].

Confidence levels in **mapping and testing** to remain within impact tolerances for each important business service by 31 March 2025

23.8%
Very confident

38.1%
Confident

23.8%
Somewhat confident

Confidence levels in the **necessary investments** being made to enable important business services to operate consistently within impact tolerances by 31 March 2025

23.8%
Very confident

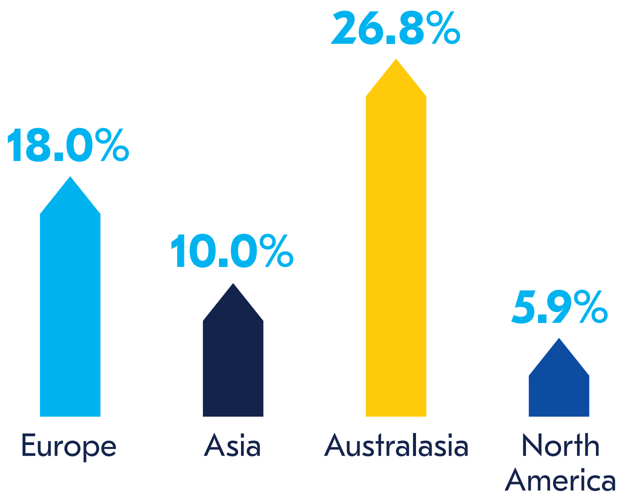
31.0%
Confident

28.6%
Somewhat confident

Professionals still believe that the regulators are not doing enough to facilitate the implementation of operational resilience.

Respondents' have expressed dissatisfaction with regulators' support in helping organizations implement operational resilience since the first edition of this report in 2022, with only 18.6% believing regulators have provided enough support. Satisfaction levels vary geographically and some of this could be due to different approaches taken by the regulators. Australian respondents, for example, reported that APRA was very open to feedback and supported change (albeit not always taken on board), while a frequent ask from global practitioner community is for more case studies showing what 'good' looks like. Interestingly, satisfaction levels tend to increase as deadlines approach, signalling a need for regulators to offer more guidance and assistance when the implementation process starts.

Do you feel the regulators/government in your country/region have done enough to help organizations to implement operational resilience? **Those answering 'yes'**



Organizational adoption of operational resilience remains the primary challenge to those implementing programmes, with some management teams still reluctant to invest in a programme which, in their eyes, offers little financial return.

This issue is particularly relevant as organizations struggle to recruit and retain qualified personnel to build and maintain operational resilience programmes, particularly within a context of budget restraints. However, for many practitioners, educating management of the importance of an operational resilience programme, together with the reputational and financial benefits it can bring, is still the challenging first stage in winning the crucial support it needs from the top of the organization.

Top 5 major challenges of implementing operational resilience

58.2% Embedding operational resilience into the fabric of the organization

50.5% Not having the headcount and/or staff time to implement a realistic policy

50.5% Addressing legacy infrastructure

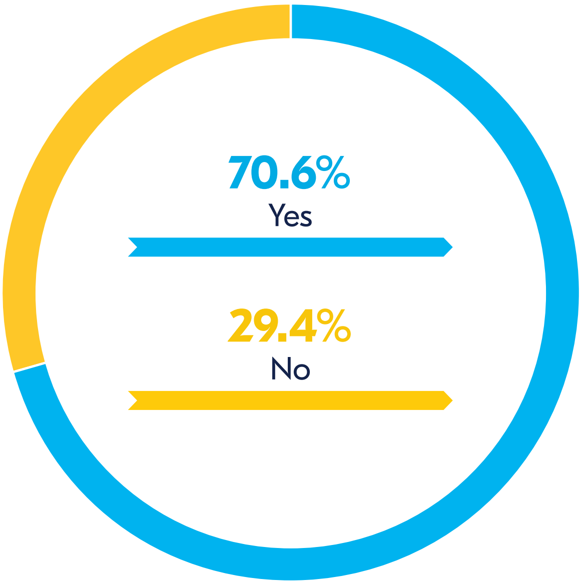
45.9% Getting critical third-party suppliers to comply with regulations

42.4% Understanding, monitoring and managing supply chain risks

Concerns persist this year regarding the possibility of operational resilience regulation becoming a mere tick-box exercise, particularly as organizations race to meet 2025 deadlines.

As a byproduct of the challenge of embedding operational resilience within organizations, a high percentage of respondents still warn over the possibility that resilience regulation could become a tick box exercise, with senior executives supporting the minimal compliance in order to meet the requirements of the regulators. This is particularly the case in Australia where the timelines for implementation are very tight.

Do you have concerns that meeting regulatory requirements/laws will become a tick box exercise?



1 Defining Operational Resilience

Defining Operational Resilience

Providing a universal definition of operational resilience is difficult due to the varying requirements, regulations, and understanding in different regions and sectors. However, there are some tools and processes which are universally recognised as being critical components of an effective operational resilience programme.

The identification of important business services (IBS) is now considered critical to an operational resilience programme by more than 19 in 20 respondents (95.8%). This is up substantially on last year's figure (82.4%) and suggests that the principles behind operational resilience — even if it is not identified with that term — are becoming more universally accepted. The identification of critical suppliers, which is a primary focal point for the incoming DORA regulation as well as the critical third-party addendum to the UK regulations, is rated as 'critical' by 88.3% of respondents, with no respondents considering them non-essential. Indeed, the concept of the identification of critical suppliers is something which has been an intrinsic part of many business continuity (BC) managers' roles for many years, so the high position here is not surprising.

Prioritising and working vulnerabilities that may threaten impact tolerances are also highly ranked this year (83.2% rank as critical), with the establishment of the tolerances themselves also still perceived as a critical part of operational resilience (81.7%). As noted last year, the interchangeability between 'business continuity' and 'operational resilience' is very much in evidence in here, with maximum tolerable period of disruption (MTPD) being used interchangeably with the term impact tolerance.

An area where there is a more of an interest this year is that of identifying and using plausible scenarios; perhaps because implementation deadlines are approaching, and regulators are increasingly requiring demonstration that organizations are able to meet their impact tolerances in the face of significant disruption.

Identifying plausible scenarios has been a concern for practitioners over the lifetime of the report; particularly those that meet the often-strict demands of the regulator. Some practitioners are now looking towards AI to help develop such scenarios which can prove an effective approach. However, while AI's use is rapidly increasing in resilience settings, information bias can — and is — occurring with this kind of method. A recent study by Cornell University in the United States showed that AI-generated scenarios tend to choose aggressive, and often violent scenarios. Indeed, nuclear war was the scenario that was generated more than any other[2].

As organizations worldwide seek to define operational resilience within their sectors/industries and gear up towards full compliance with a diverse range of operational resilience regulations, this report shows the challenges that are standing in their way, and the opportunities that achieving true operational resilience can bring.

> **"Operational resiliency is an outcome and is the umbrella that sits across good business continuity, good operational risk management, good supplier management, good cyber strategy and making sure that all your technology is up to date and works as expected."**
>
> Resilience & continuity manager, banking and finance, UK

What, if any, of the following processes/tools you consider key within operational resilience.

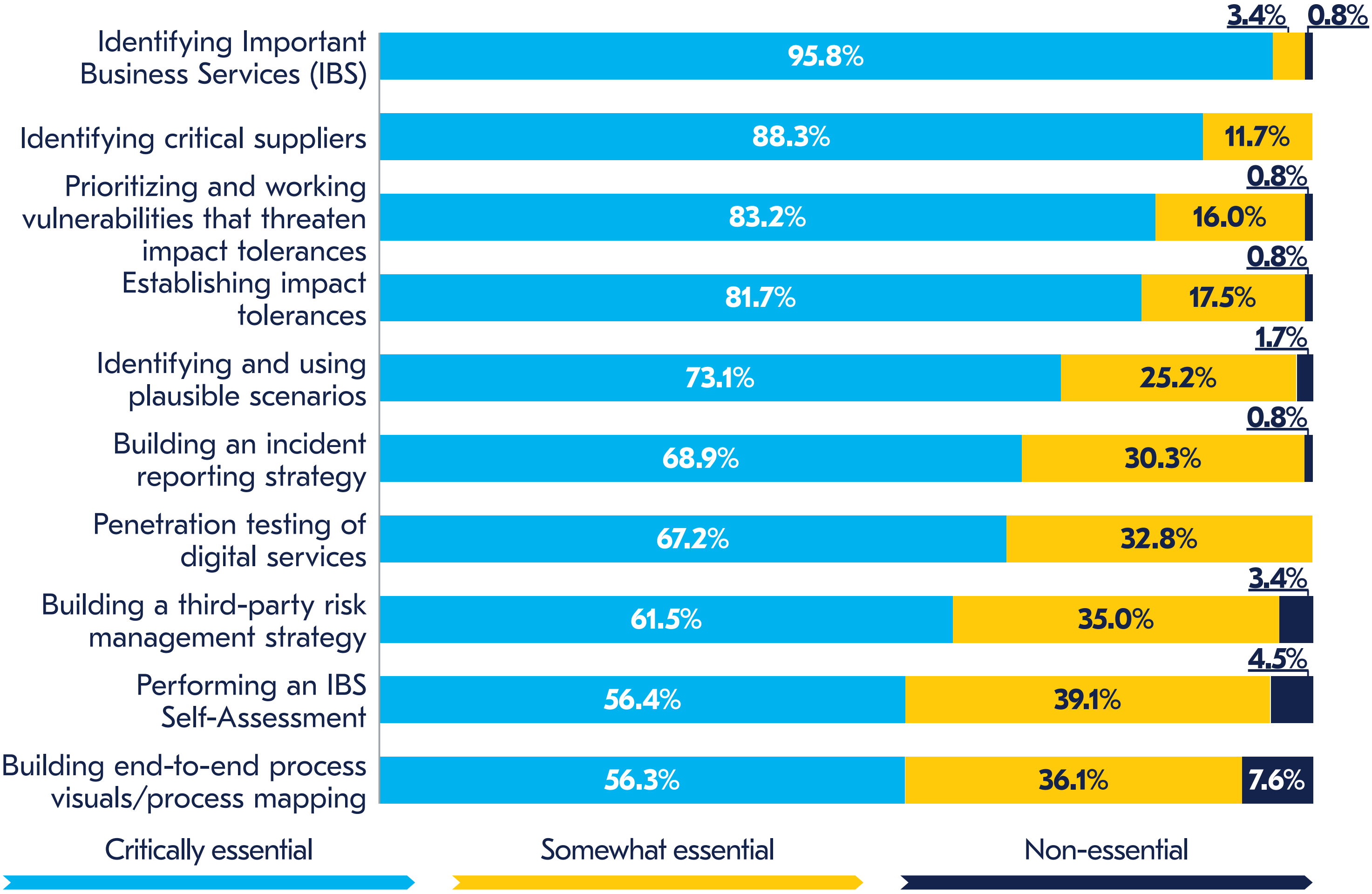


Figure 1. What, if any, of the following processes/tools you consider key within operational resilience. Please rate on the following scale (0=Non-essential; 5=Critically essential)

Business continuity and operational resilience – the perceived differences

The view that operational resilience is more proactive, and BC is more reactive has grown this year. 74.6% of respondents 'very strongly' or 'strongly' believe that 'op res is proactive', compared to 69.2% in last year's report. Meanwhile, 45.8% of respondees believe 'strongly' or 'very strongly' that BC is reactive (2023: 38.5%). This might come as be a surprise to some, particularly when some BC programmes and BC manager roles have broadened. Activities such as risk mapping, the external PR response in a disaster, social media monitoring, and coordinating with external parties to ensure a more holistic response to an incident are all examples of some of the activities which BC managers have highlighted as being intrinsic parts of their role now. Such diversity in job roles also goes some way to explaining why 73.1% of respondents believe that BC supports both the internal and external impacts to an organization.

Some of the reasoning behind this is because resilience has been defined in organizations and, particularly in financial services environments, now BC has a more defined remit. In many instances, is a more operational, internal-facing role. This is perhaps a reason why 76.4% of respondents believed 'strongly' or 'very strongly' that 'BC is part of op res' and 'supports resilience'. To compound this blurred definition even further, Figure 3 shows that more than a third (37.7%) of respondents believe organizational and operational resilience to be exactly the same.

> **"Business continuity is a distinct thing and a distinct component. It is our ability to be able to recover from disruption, whereas operational resilience is broader."**
>
> Resilience manager, financial services, UK

> **"Business continuity can be very narrow in its focus when you deploy it in a large organisation because people just look down the prism of the activities that they undertake, and they look at recovery and impact within that section. While you can do some sort of stretching activity through scenario analysis, which you always did within business continuity, what we lacked was a primary focus. An important business services brings a focal point, enabling a much more holistic view of what your recovery would look like."**
>
> Resilience manager, financial services, UK

> **"Within the financial sector the expectation has always been to have continuity plans in place to make sure we are ready and prepared for disruption events. However, when the operational resiliency regulations came out it was about that wider, more strategic approach. It wasn't just about having a plan for when disruptions happen. Operational resilience was taking everything else into account and considering all impacts from a disruption: the customer impact, the market impact and the impact on the business' safety and soundness. Operational resilience is about the ability to prevent, to adapt, to respond, to recover and then learning from operational disruption."**
>
> Resilience & continuity manager,
> banking and finance, UK

"Business continuity is an integral part of operational resilience. Operational resilience has sort of two phases: One is the anticipation and identification, to make sure we never get to a disruption. It includes identifying your CBS, scenario test them on a regular basis, fix your vulnerabilities, invest towards them and make them resilient. The second bit of it is BCM. You also prepare for disruptions: you prepare for worst case scenario, should all the resilience building measures fail, you still need to respond effectively. You put all sorts of continuity plans on key dependencies. Operational resilience is both sides covered, preparing to make sure you never reach a disruption, and also preparing in case you do."

Global Head of Resilience & Continuity, Banking sector, Netherlands

"Operational resilience is rolled out into our most important services, those that we provide to the customers and our clients. However, business continuity is everything else. It is looking after the people, the buildings, all the pillars that underpin operational resilience. I think without business continuity you would have a very hard time implementing operational resilience because operational resilience is just that next step. It's just making sure you have that end-to-end process and more strategic look of operations."

Resilience manager, financial services, UK

An interviewee in the public sector highlighted how operational resilience to them is very much on the external side, and ensuring the community can endure significant impacts.

"It is only recently because of the Federal Act of the security of Critical Infrastructure Act, that we are being brought into the 21st century, because there are requirements under that to implement operational resilience within the organization."

Business Resilience Specialist, public sector, Australia

"Our technical definition of operational resilience within the organizations is 'the capability to maintain services so that our community can endure any event and proactively anticipate or build redundancy to withstand by adapting to changing conditions and recover, adapt and learn from disruptions, shocks and stresses."

Business Resilience Specialist, public sector, Australia

The overall story this graph portrays is one where, once again, there cannot be a universally agreed crossover point for operational resilience and BC, how one is linked to the other, and which duties should be performed by each part of the business. While it might be more straightforward for financial services to have assigned structures for each due to defined regulations in place; for other organizations it is likely that they will exhibit fluidity in terminology for the short- to mid-term future.

How are business continuity (BC) and operational resilience (Op Res) distinguished within your organization (if at all)?

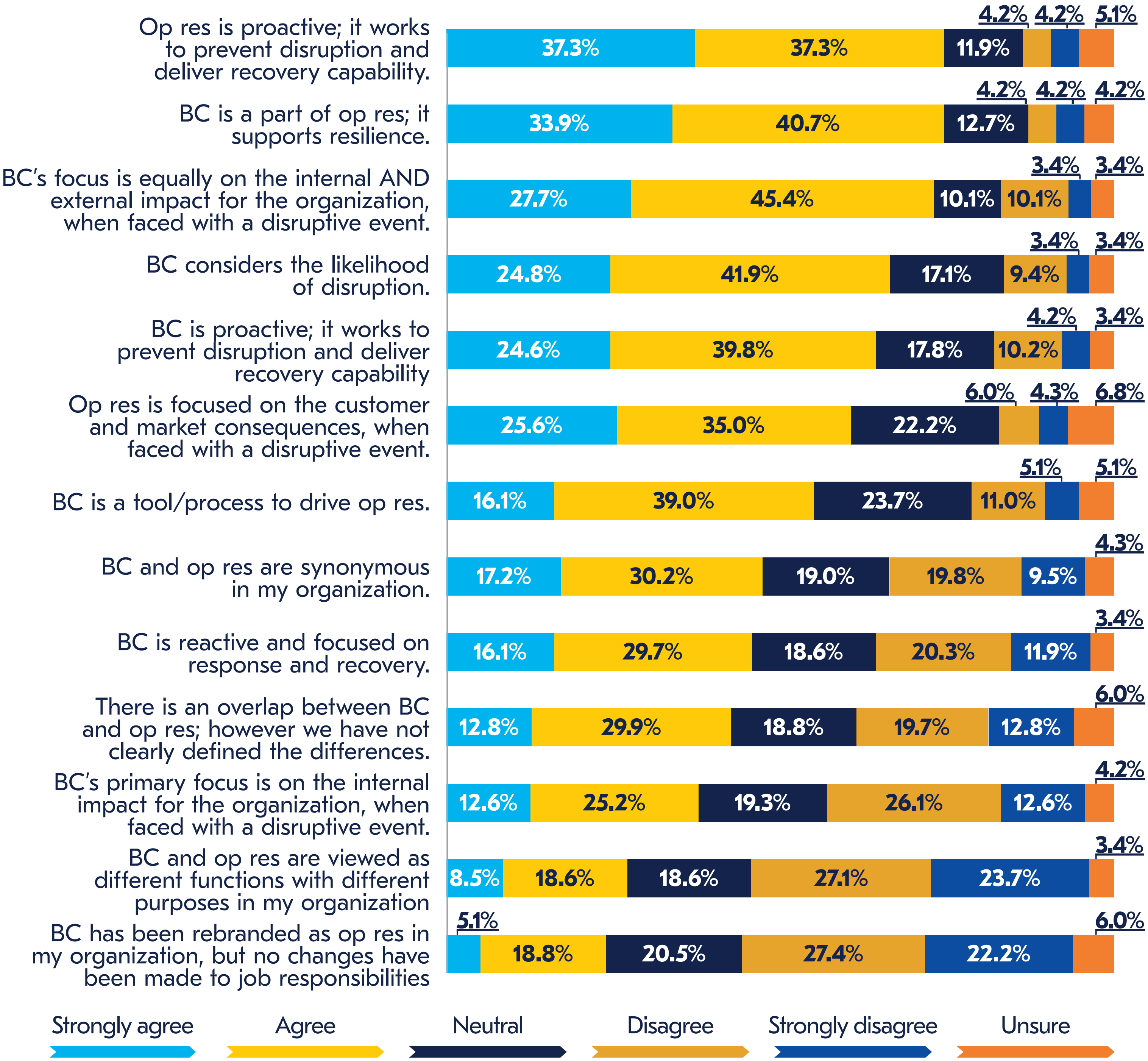


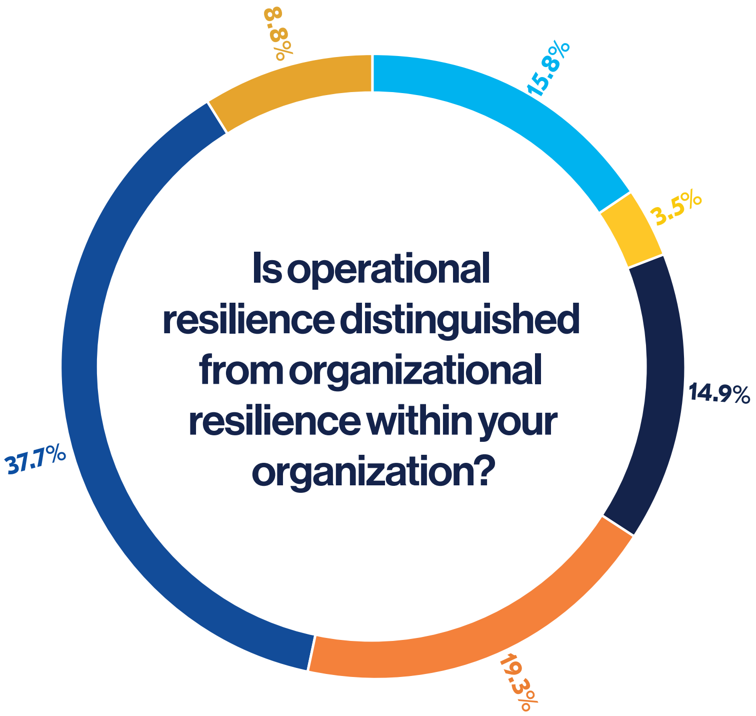
Figure 2. How are business continuity (BC) and operational resilience (Op Res) distinguished within your organization (if at all)? Please select if you agree/disagree with the following statements

Operational vs organizational resilience

As analysed previously, there are different definitions of operational resilience depending on the sector/country, albeit with similar attributes and characteristics. According to ISO 22316:2017, organizational resilience is defined as “the ability of an organization to absorb and adapt in a changing environment”[3].

When it comes to organizational resilience and its difference with operational resilience, this year’s survey shows that 53.5% of organizations do indeed distinguish between the two terms/concepts. 15.8% of survey respondents report having separate functions for operational and organizational resilience within their working structure, whereas others have adopted just one of the two functions within their structure: 3.5% have an organizational resilience without an operational resilience function and 14.9% have an operational resilience function without an organizational resilience department. A further 19.3% of organizations acknowledge the existence of differences between the two concepts of organizational and operational resilience, however it is not reflected at all in their working structure as there are no dedicated structures for either of these functions.

A growing number of organizations (31% in 2023 vs 37.7% in 2024) concede that organizational and operational resilience are the same, with no difference between the two. These types of organization tend to have a one general resilience function where they develop activities pertaining all ‘resilience-orientated’ activities (e.g. operational resilience, crisis management, business continuity, cyber security).



15.8%
Yes, we have operational resilience and organizational resilience functions within my organization.

3.5%
Yes, we have an organizational resilience function within my organization, but not an operational resilience function.

14.9%
Yes, we have an operational resilience function within my organization, but not an organizational resilience function.

19.3%
Yes, however there are no dedicated specific functions within my organization.

37.7%
No difference, they are the same to us.

8.8%
Unsure

Figure 3. Is operational resilience distinguished from organizational resilience within your organization?

Operational resilience and organizational resilience may have blurred lines – but operational risk?

Respondents were also asked about how they perceive the relationship between operational risk and operational resilience. The figures were on a par with those noted in last year's survey with four-fifths of respondents believing the two concepts to be different, albeit with a slightly higher percentage of respondents saying the two phrases were the same (2024: 20.8%; 2023: 18.6%). The general consensus is that the two were heavily related, with some believing that operational resilience could not be achieved without good operational risk. Some of the responses received in the survey that echo this are as follows:

> **"Operational risk management is one of the pillars of operational resilience."**

> **"They are linked but not the same: operational risk is just one component in establishing resilience."**

> **"Operational resilience is an outcome of good operational risk management."**

> **"If done correctly, they complement each other."**

For others, there was a view that was similar to those encountered earlier in the report when comparing operational and organizational resilience, or operational resilience and BC. One considers the external risks of the organization, whereas the other features the internal:

> **"Operational risk focuses on identifying and mitigating specific risks from failed processes, systems, people, or external events while operational resilience is about the broader ability to maintain critical operations and withstand and recover from disruptions."**

> **"Operational risk is a risk associated with the organization's operations while operational resilience is the organization's ability to recover from operational disruptions either caused from internal or external reasons."**

> **"Different elements - operational risk is about identifying operational risks and controls, and mitigating those, whereas operational resilience is about putting more options in place to be resilient against those risks."**

An interviewee, meanwhile, stated that operational resilience was not the 'outcome' of effective risk management, as it does not go far enough to ensure the full resilience of an organization.

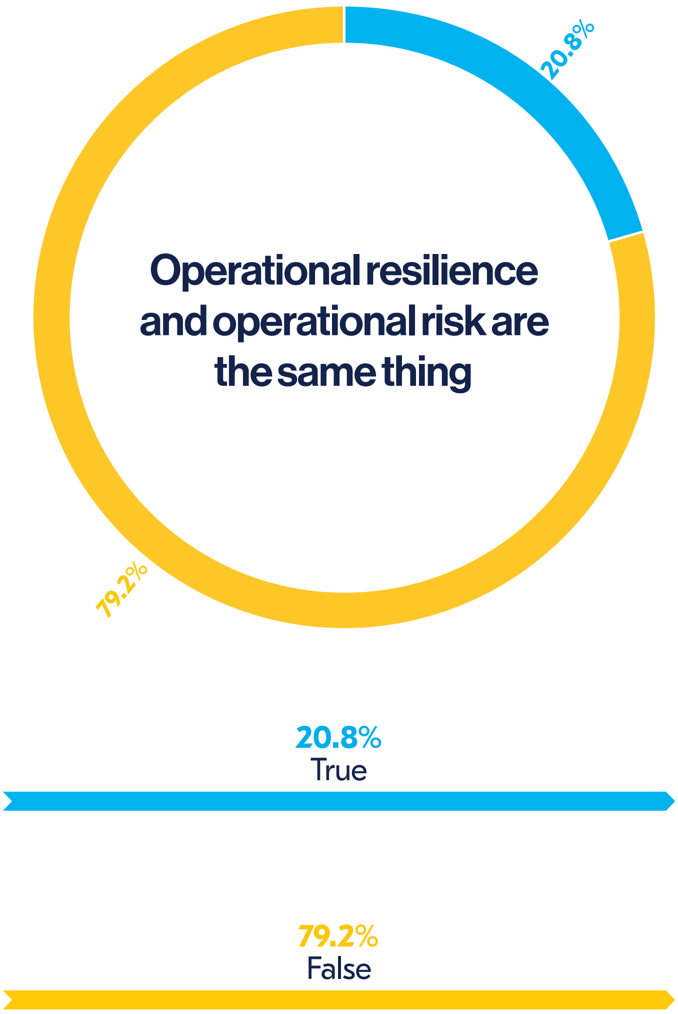


Figure 4. Operational resilience and operational risk are the same thing

2

Compliance With Operational Resilience Regulations

Compliance With Operational Resilience Regulations

2023 was a year of preparation for many financial services organizations, as implementation deadlines loom for some of the forerunner nations in building new operational resilience regulations/frameworks. While there are broad similarities between the different regulations, there are subtle differences to each, as reported by interviewees.

> **"We had adopted the FCA definition of operation resilience across the group, but the way that we measure that definition is probably different from other countries. This is because the artefacts to enable operational resilience for us in the UK are very specific to ensuring that we have the mapping, the scenario testing, and the vulnerability analysis."**
>
> Resilience manager, financial services, UK

The Monetary Authority of Singapore (MAS) has arguably been at the forefront of operational resilience regulation, with its revised Business Continuity Management Guidelines being released in June 2022 aligning to international standards. Financial institutions were required to have a plan for regulatory compliance and an audit regime in place by June 2023, with the first audit due to happen just one month after the publication of this year's report (June 2025). Also in Asia, the Hong Kong Monetary Authority (HKMA) launched its circular on operational resilience (OR-2 Supervisory Policy Manual) at the same time, although full compliance is not due until May 2026.

Outside Asia, the European Union (EU)'s Digital Operational Resilience Act, effective from 16 January 2023, and the United Kingdom (UK)'s Operational Resilience Framework, first milestone effective from 31 March 2022, will both require full compliance early 2025, on 17 January and 31 March respectively. Although professionals who took part in this year's research were feeling more confident than a year ago, there is an acknowledgement that a significant amount of work still needs to take place between now and then in order to reach full compliance.

Meanwhile, in Australia, the Australian Prudential Regulation Authority (APRA) finalised both the CPS 230 (operational risk management) and the CPS 234 (information security) standards in July 2023, with APRA-regulated entities having to prove that they can effectively manage operational risks and maintain operations by 1 July 2025. The roadmap is short for Australia and, whilst some have applauded APRA for being proactive with detailing what they require financial services organizations to provide, the timescale for implementation is the shortest of any of those regulations currently being introduced. Others have found that the complexity of the standard, combining operational risk, BC, and material service provision, has resulted in greater-than-anticipated work both for organizations — and the practitioners themselves. This has ultimately extended out the timescales and, what appeared to be sound regulation at the start, has become overly complex for many.

> **"I think in APAC they are both lucky and unlucky, because the regulator has very clear requirements of what they need. However, they have very tight deadlines."**
>
> Resilience manager, financial services, UK

Outside these regions, other countries continue to build their own operational resilience programmes and regimes. Canada, for example, is revising operational risk management guidelines from the Office of the Superintendent of Financial Institutions (OSFI), and Dubai and South Africa are also finalising their own policies.

For those who supply the financial services sector, particularly cloud or other providers of digital services, they too will be required to meet the same requirements as the organizations they service. As this report reveals, the cost for some suppliers to comply is prohibitive meaning which could mean financial services organizations scrabbling to source additional suppliers when the deadline clock is ticking.

Outside financial services, other organizations, governments, and sector regulators/governing bodies are also having to comply with increasing regulations and guidance regarding their operational resilience programmes. The top five sectors having to comply with several operational resilience regulations outside banking and finance are information technology, public services, government and administration, professional services and energy and utilities.

Healthcare is one the top ten sectors that has to comply with operational resilience regulations. Healthcare organizations, for example, are reporting an ever-increasing numbers of data breaches. In 2023, 112 million people were impacted by healthcare data breaches, compared to 48.6 million in 2022. The HCA Healthcare breach in the UK affected 11,270,000 individuals, while the Perry Johnson & Associates incident resulted in 8,952,212 being impacted[4]. With increasing global tensions and climate change threatening the resilience of energy companies, service resilience failures are becoming commonplace in the retail sector[5], and unregulated AI is potentially bringing additional threats to data security. Indeed, a recent survey of Chief Information Security Officers showed that 70% believe that AI provides an advantage to attackers over defenders[6].

Highlighting the attention that operational resilience is receiving from a wide range of organizations, almost 85% of surveyed organizations are now required to comply with one or more operational resilience regulations. This number is likely to keep rising as operational resilience rules and regulations extend from financial services organizations to critical entities deep in supply chains, other sectors, and smaller organization. BC and resilience professionals of all sectors and regions should be aware of the scope and implementation of operational resilience concepts, and be able to adapt them to their organizations.

While smaller organizations typically have to comply with regulations from a single regulator, for large multinational organizations, compliance with multiple regimes is necessary. This typically means a significant amount of resource is required to ensure all regulatory demands are met, with the list growing as more regulations are introduced. 84.6% of respondents stated that they have to comply with one or multiple operational resilience regulations.

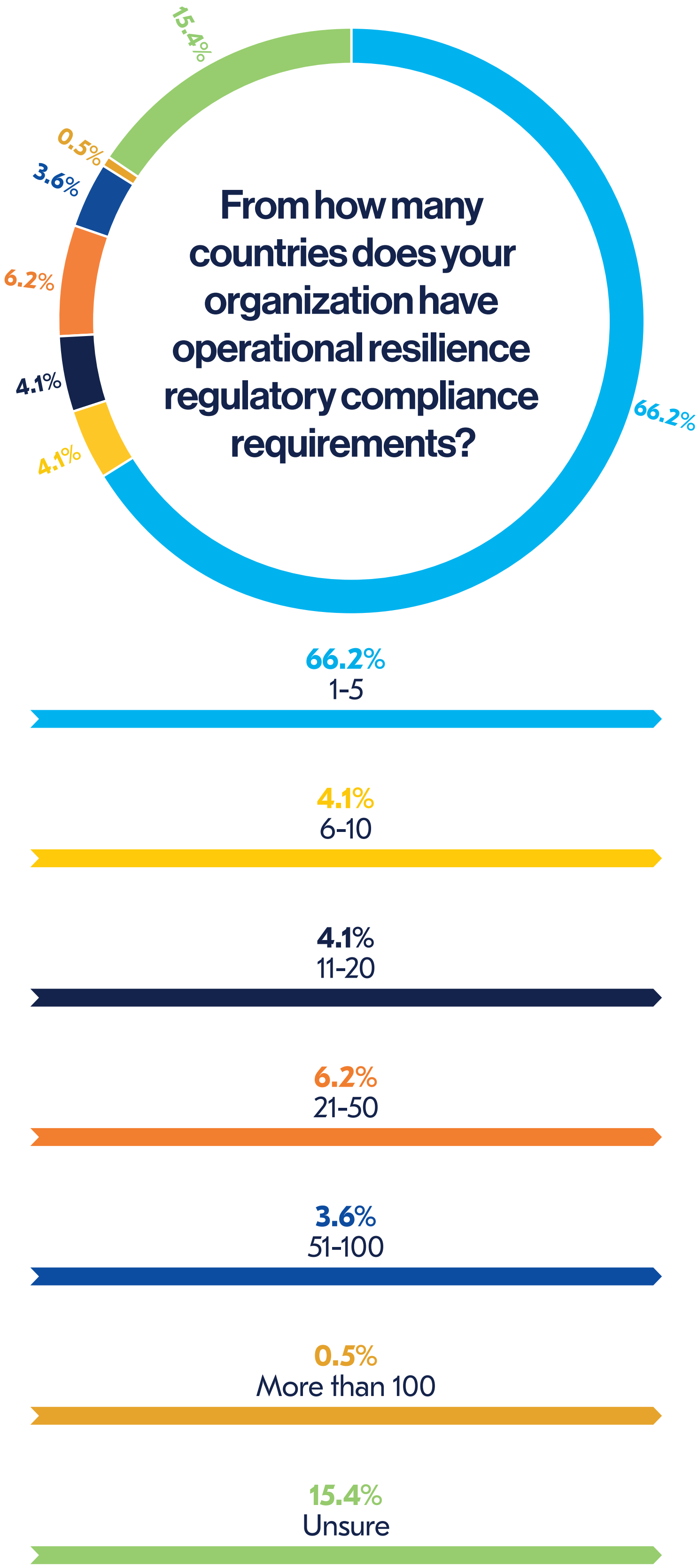


Figure 5. From how many countries does your organization have operational resilience regulatory compliance requirements?

Most organizations now have, or are considering, an operational resilience programme or project.

Nearly two-thirds (64.8%) of organizations say they have an operational resilience project or programme, a figure on a par with last year's results (64.6%). However, with more organizations now considering implementing a programme (16.0%), up from last year's figure of 12.0%, adoption rates are growing. Furthermore, of those organizations that have any kind of operational resilience compliance requirement, almost 90% of them have an operational resilience programme in place or are in the process of developing one.

When additional countries push out regulation to financial services organizations, or when regulation further expands into other sectors, it is likely that this figure will rise further. In this year's survey, no respondents from the charity, not-for-profit, creative industries, and retail industries reported having an operational resilience programme in place, whereas 84.3% of those in the financial services sector and 66.7% from the IT/telecommunications sector did. However, even in countries where regulation does exist, operational resilience programmes are still a long way from maturity.

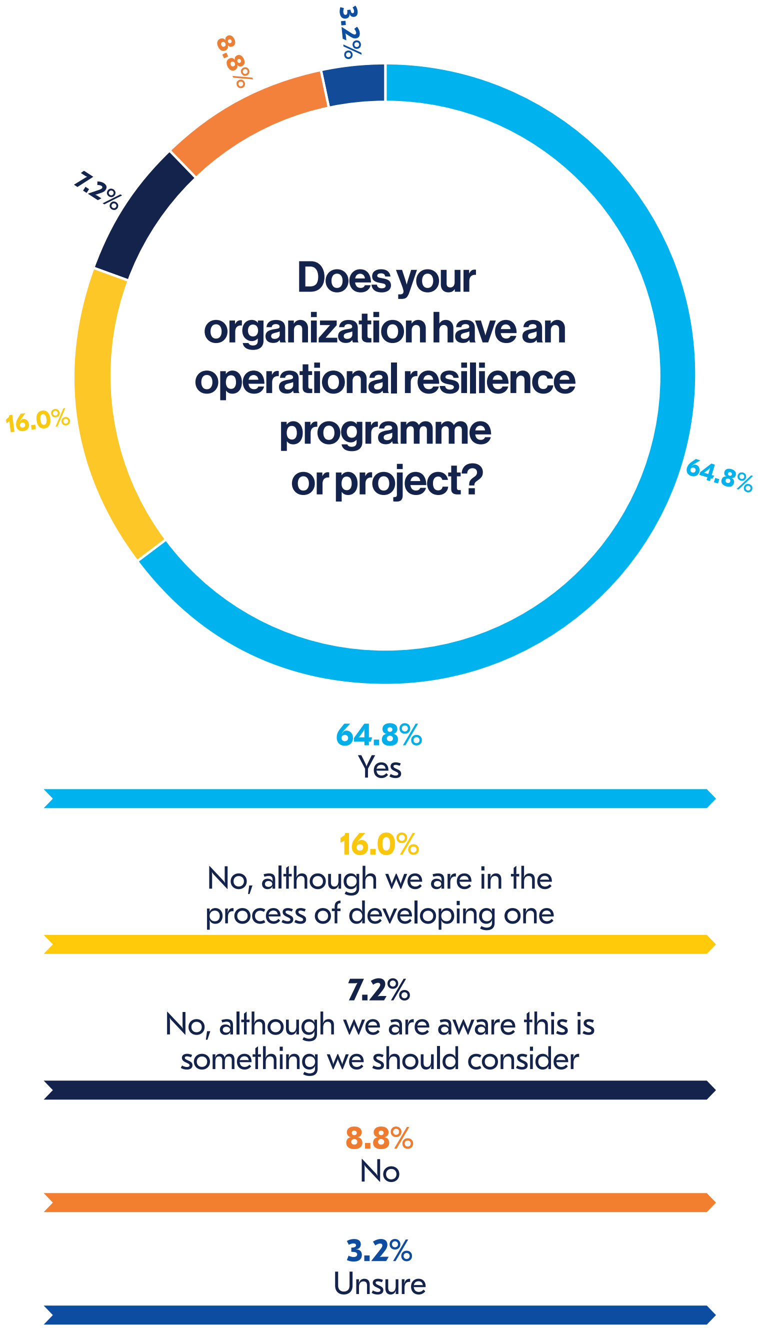


Figure 6. Does your organization have an operational resilience programme or project?

> **"There are some things like infrastructure and procedures that my organization has been doing for a long time to provide operational resilience, but it's never been defined as that, and it hasn't been thoroughly documented. There's a lot of processes from operational resilience that exist due to that structure, but I think the challenge for us is getting that formalised and put into a living document so it can be scalable for different types of incidents and disruptions."**
>
> Business continuity specialist, insurance services, Canada

No regulatory requirement does not mean no operational resilience programme.

79.5% of respondents whose organizations are not bound by regulation to have an operational resilience programme, still report that they practice operational resilience either to a certain extent (48.0%) or fully (31.5%). The cumulative figure (79.5%) has increased slightly on last year's 75.2%.

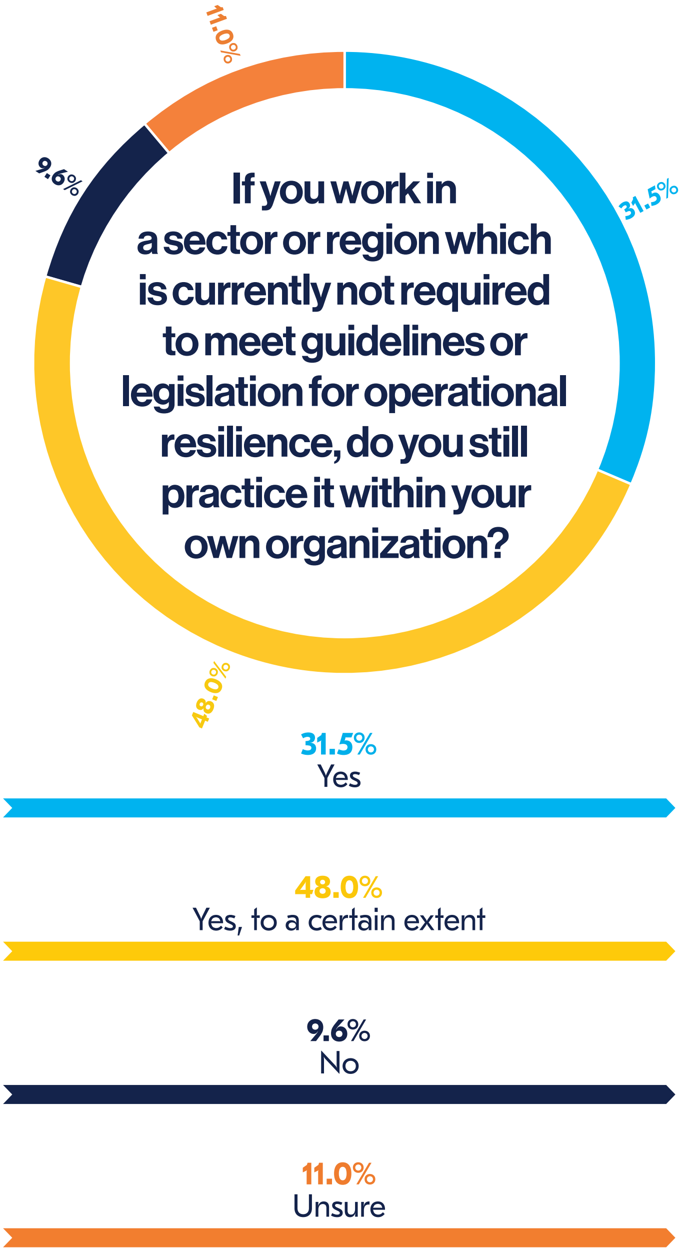


Figure 7. If you work in a sector or region which is currently not required to meet guidelines or legislation for operational resilience, do you still practice it within your own organization?

Regulations have helped to bring the subject of operational resilience to the fore, with other global incidents (such as the pandemic) highlighting the risk to customer-facing operations if they are not correctly considered in planning. The rise in the number of organizations that are following an operational resilience programme, even if they are not regulated, is testament to this.

To further corroborate this statement, nearly two-thirds of respondents (59.5%) report that an operational resilience programme helps them to better meet their customer needs. For more than a third, adding an operational resilience programme was a natural step to make the organization more resilient when a mature BC programme was already in place (37.5%). For others, they felt it aided them in the supplier procurement process or in the bidding process for new work (13.5%). With a renewed focus on operational resilience and supplier due diligence as a result of global supply chain issues recently (e.g. COVID-19, severe weather incidents, global conflicts, or one-off episodes such as the Evergreen Suez Canal blockage), BCI members report that more questions are now being asked at the early stage of a new business partnership. By adhering to an operational resilience programme, they are more able to demonstrate the requirements expected from them by a customer or supplier.

> **"As a business, what is most important for us is protecting our customers. Using operational resilience and going through the process with that lens is very useful. We are a relatively simple operation, so it's a very good way of focusing the business on what's important. Operational resilience is becoming more helpful because business continuity tends to sit in the silos of the department, whereas operational resilience starts to make people think outside the box and connect all the dots."**
>
> Operational resilience manager, financial services, UK

However, the area which has seen the greatest change this year is in organizations having to adhere to regulation because they interact with stakeholders, typically financial services organizations, which have stringent arrangements in place for third-party suppliers. Last year, 40.3% of organizations reported this was a reason for having a programme in place. This year, the figure has risen to almost half (47.3%). This is an intrinsic part of DORA regulation and, in the UK, the third-party requirements for organizations regulated under the FCA/PRA have been released only in more recent stages, which could be partly to blame for some of this increase. These new third-party rules are discussed in the *Looking ahead: key challenges* section of this document.

If you have drawn up your own guidance, what has been your motivation for doing this?

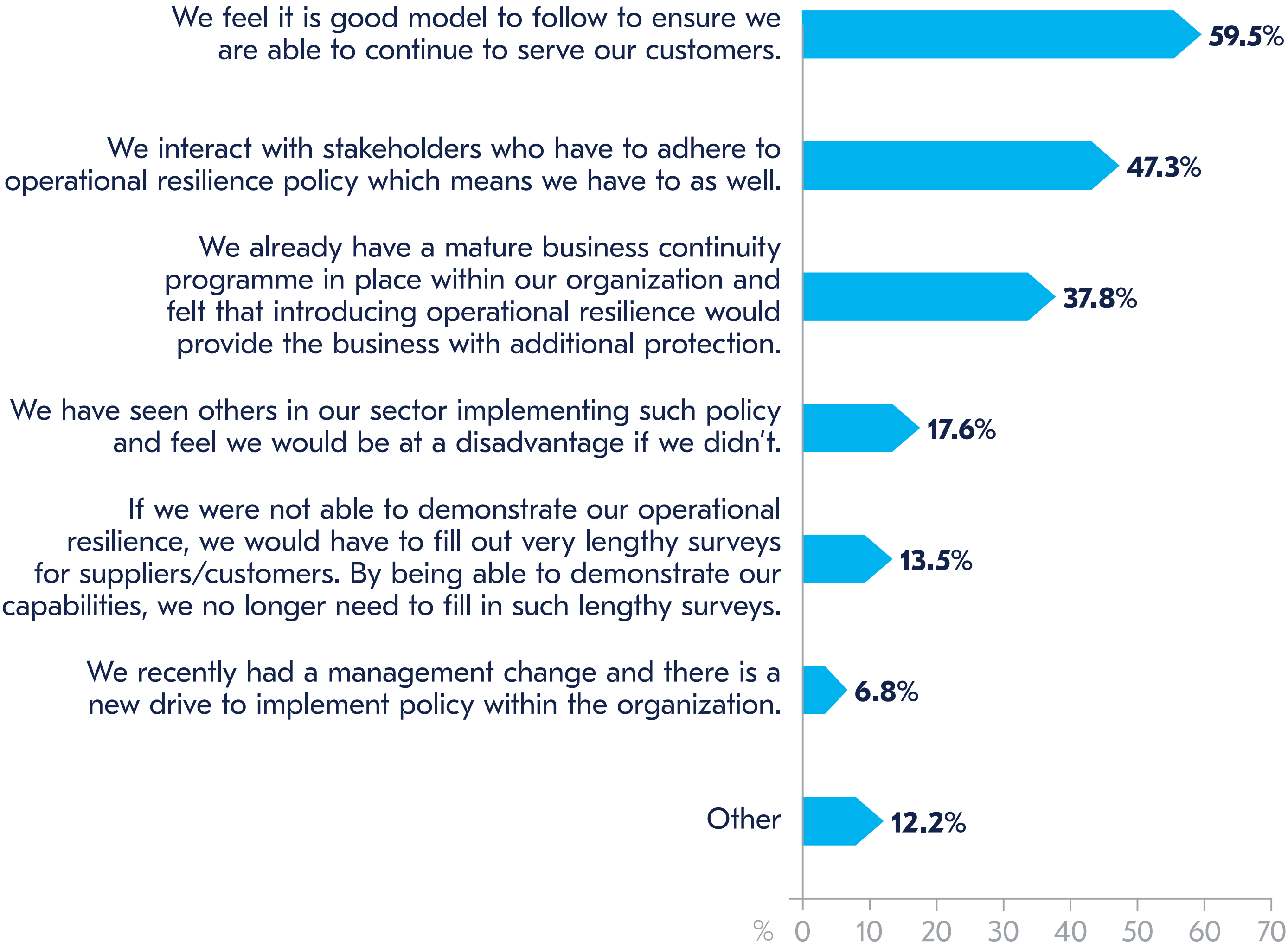


Figure 8. If you have drawn up your own guidance, what has been your motivation for doing this?

Regulation becomes the primary driver for operational resilience.

Two-thirds of respondents (67.0%) in this year's survey said their reason for having or developing an operational resilience programme was because it was now a regulatory requirement. This option has risen to the top of the table this year, climbing above last year's favoured option of good practice being the primary driver for a programme which has dropped by a similar amount (2024: 58.5%; 2023: 68.3%). While regulation might be expected to be the top option in a global survey, having more organizations complying for good practice purposes is very welcome, particularly given the number of consumers that were hit by outages in 2023. In the UK in March this year, for example, likely issues with payment systems meant that two of the UK's largest supermarket chains (Tesco and Sainsbury's) were unable to process payments, in addition to McDonald's restaurants, and Greggs bakery outlets[7]. Although organizations are normally keen to blame a third-party IT outage for a problem, could some of these outages been mitigated if the retailers had contingency plans in place? It seems likely: in a recent report by Splunky, half of respondents to a recent survey admitted they did not have a resilient infrastructure in place to mitigate or prevent significant impact on the business in the event of a network outage[8].

Certain groups (including a joint project between the BCI and the BCS[9]) are working to highlight the importance of service resilience to governments, but legislation may be a long time coming. Merely following good practice is unlikely to drive the measures needed to ensure customers — and the organizations themselves — are protected in the event of an outage.

Continuing on the best practice theme, some organizations report that they have introduced operational resilience into a particular geography because it is a regulatory requirement, but they have then pushed the regulation out into other regions to ensure all benefit from the protection that the regulation offers.

> **"We started implementing operational resilience in the UK because of legislation. However, in other parts of the world we implement it because it is good practice and benefits our customers. For example, in Singapore, although it's called business continuity enhancements, it is very much operational resilience with a different name and some different terminology. We're seeing it in Dublin as well. We're finding that operational resilience beginning to get rolled out across the globe. We're executing it because our clients are beginning to ask if we are operationally resilient. Before, it used to be business continuity."**
>
> Resilience manager, financial services, UK

> **"The reason why we have an operational resilience programme is in part because it is a regulatory requirement, as we have to comply with DORA. However, as a bank we have applied operational resilience in a generic way. This was a natural progression in the state of maturity of our programme. It was very evident that there needs to be a move towards operational resilience as a concept."**
>
> Operational resilience manager, financial services, Malta

As already mentioned, third-party guidance is fast becoming an integral part of most operational resilience guidelines and regulations. Indeed, it forms the backbone of DORA, and it is now a focus for the UK regulators after initially being omitted from the document. These changes are reflected in the survey results, with 20.8% of respondents saying they have an operational resilience programme as the result of being a critical supplier to a regulated entity: a figure which is only likely to increase as more organizations become aware of the need to comply.

Over the course of the following year, it will be a useful exercise to monitor incoming regulation or guidance, particularly new guidance for non-financial services entities.

If you do have an operational resilience programme or are in the process of developing one, why is this?

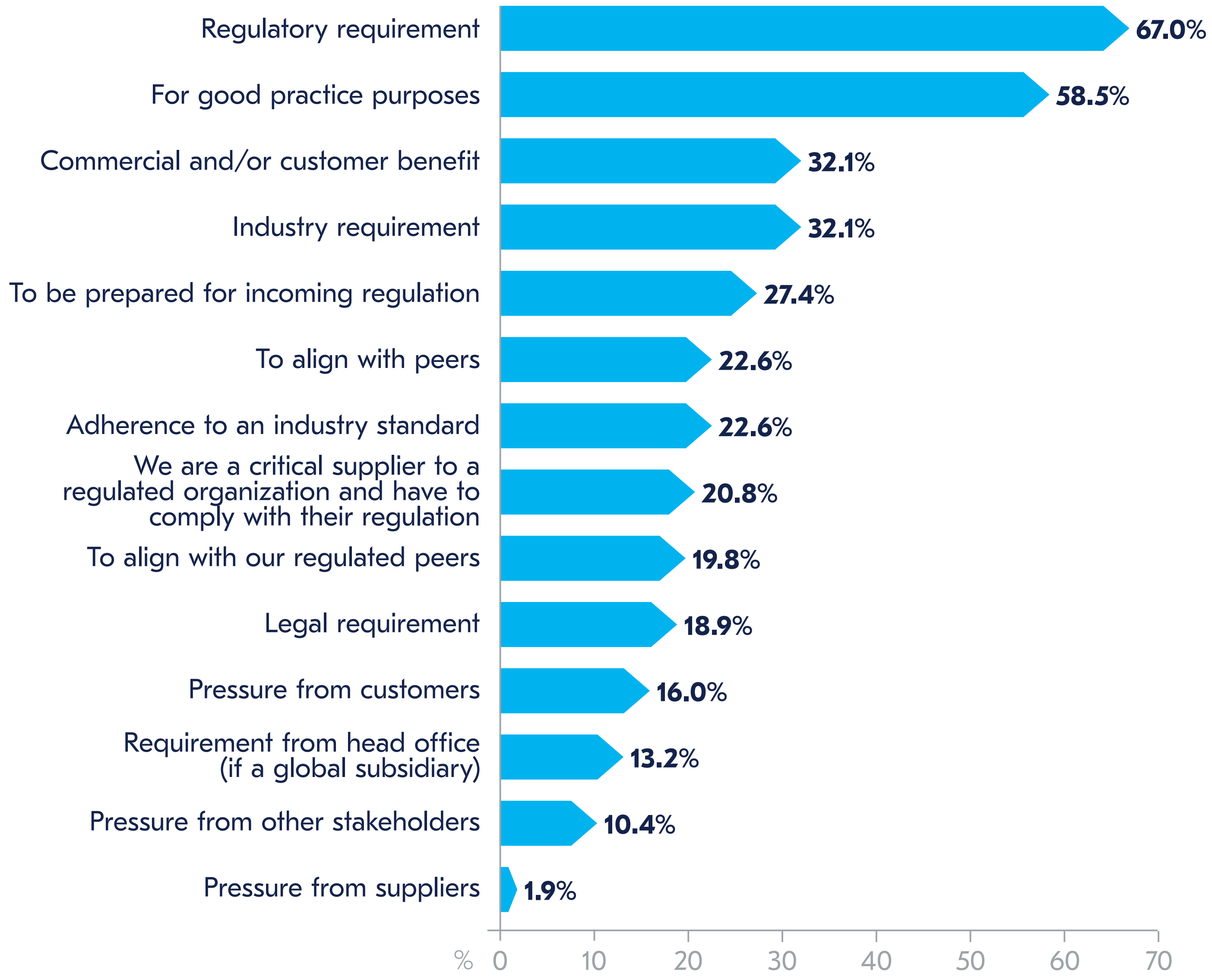


Figure 9. If you do have an operational resilience programme or are in the process of developing one, why is this?

The absence of laws and regulations also dominate the reasons for not having a programme in place.

While operational resilience has become part of business-as-usual (BAU) for many organizations, for some, it has not yet even entered into conversations. For those which do not have a programme, 60.8% do not because it is either not a legal (39.1%) or regulatory (21.7%) requirement. Interviewees from such organizations spoke about how they wanted operational resilience regulation to be introduced so they could create more buy-in from senior management and the board.

"We are going through a very large corporate transformation, and part of our challenge is that the business continuity area is not being included into any of those transformation projects. We're kind of existing separately and we're trying to create our own awareness. From my perspective, additional regulations and additional legislation would just create some more awareness from the board and from the executive level to help us to drive some of the changes that we're trying to implement."

Business continuity specialist, insurance services, Canada

"I'm struggling to get my upline, to understand resilience and operational resilience. If there was a guideline from a recognized institution, a standardized definition, then top management would fall into step because they have an authority providing a definition. This would be really helpful."

Business resilience manager, information technology, USA

"In the region regulation is geared toward business continuity or crisis management. Operational resilience is not yet fully embraced by regulators. There is mention of operational resilience within the outsourcing regulations in Rwanda. However, there is no other regulation in East Africa that speaks of operational resilience."

Head of internal controls, banking & finance, Kenya

Just under a third (30.4%) do not have the time and/or resources to implement a programme, and the same amount have not event considered it. Interestingly, the option of 'business continuity is all we need' has fallen to the bottom of the table with 8.7% selecting it as an answer, compared to 24.2% in last year's survey. Although discussions are still rife in the sector about the definition of operational resilience, the reduction suggests a shift away from the 'definition challenge' that has dominated conversations since the pandemic.

For some countries, it should be noted that 'resilience' is still interchangeable with the term 'business continuity'. Indeed, the Monetary Authority of Singapore (MAS) guidelines are titled Guidelines on Business Continuity Management, despite the guidelines having identical roots to 'operational resilience' guidelines in other jurisdictions. In south and central America, it is BC, rather than resilience, is the term that dominates many countries' legislation[10].

Comment from the BCI Operational Resilience Special Interest Group (SIG):

bci Special Interest Groups

It would be safe to assume that the COVID pandemic, together with the fragile and complex threat environment globally, has convinced leadership across sectors that effective risk mitigation and management is no longer enough. Pivoting to operational resilience is not an easy journey in terms of costs, effort and time, and unless mandated, organizations that do not have a legal or regulatory mandate are often still choosing to run their risk management in a fragmented and siloed model, as is evidenced in the table. The economic environment further pressurises the leadership in non-regulated organizations to spend from their tightening purse strings only on costs that will generate further revenue, or is an Industry or regulatory mandate.

Reasons for not having an operational resilience programme

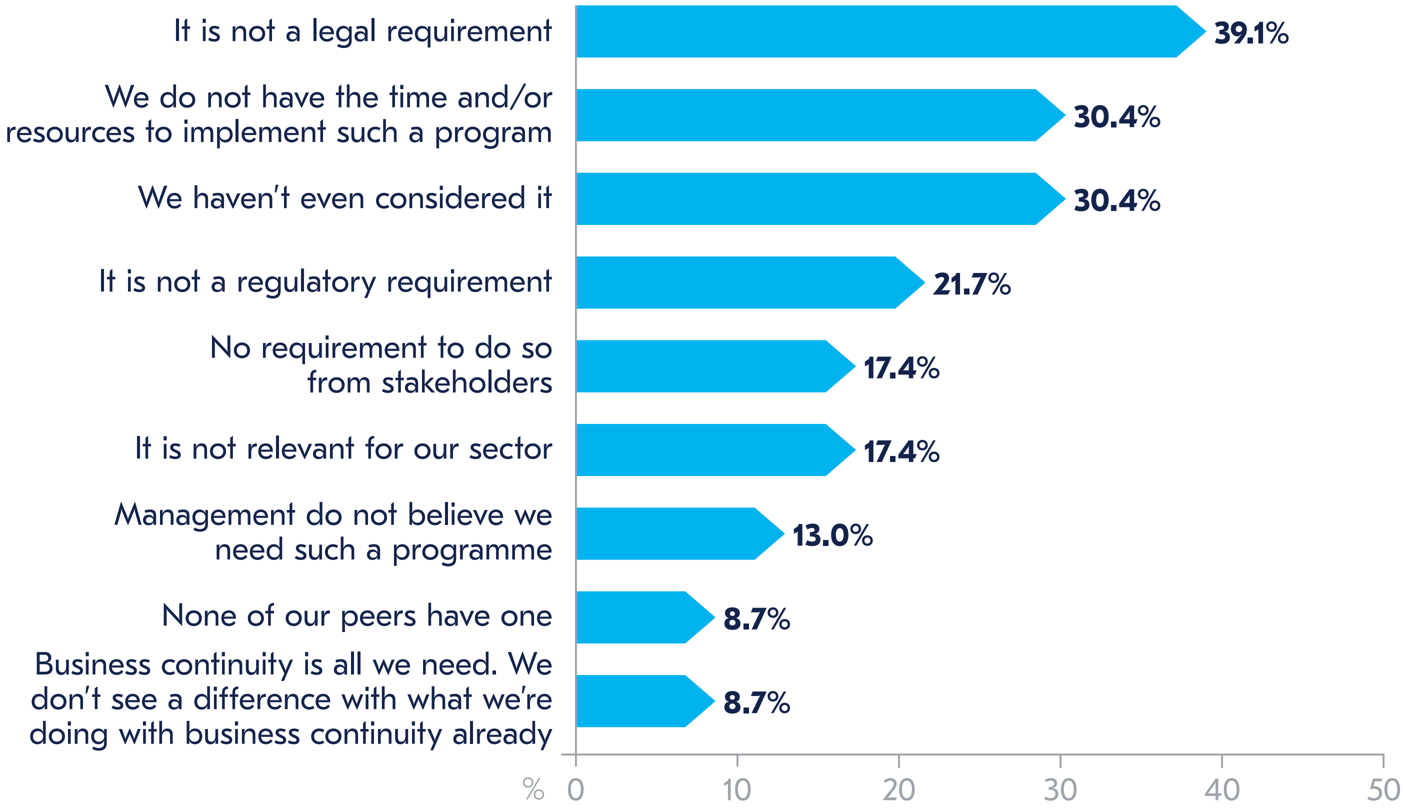


Figure 10. Reasons for not having an operational resilience programme

3

Commitment to Operational Resilience

Who is accountable? Are we seeing a shift to more devolved responsibility?

For an organization to achieve resilience, every person in the organization has some part to play in ensuring getting to that point. From knowing how to respond in a crisis, to putting plans in place to ensure customers face minimal disruption if an incident occurs, everyone should have an awareness of how their own role fits into the overall resilience of the organization.

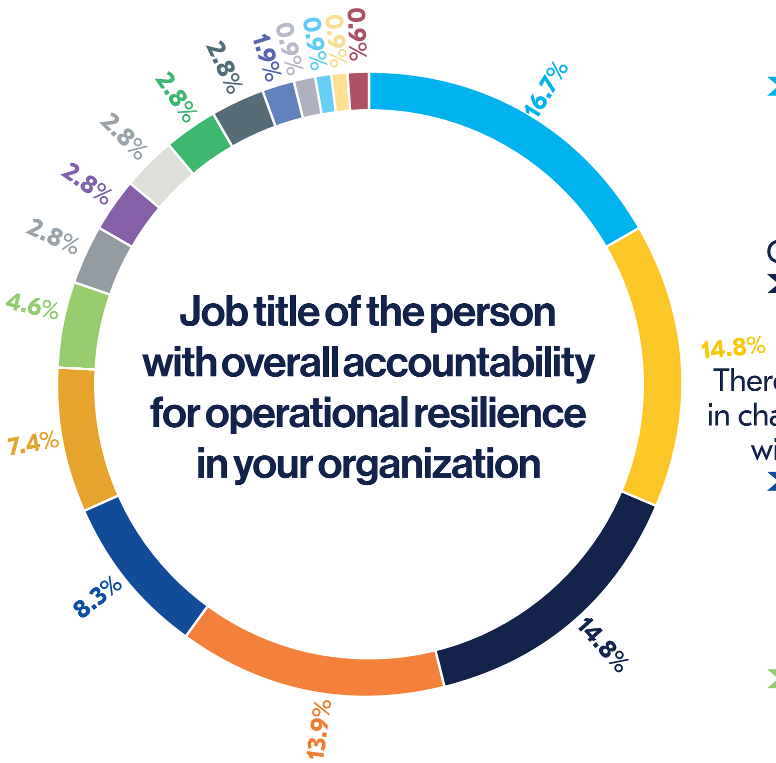
However, when it comes to overall responsibility, the widely adhered to phrase that 'the buck stops with the CEO' tends to also be the case when it comes to operational resilience. The 'CEO' has been consistently identified as the person most likely to be in charge of operational resilience since this report was first published four years ago. However, this year is the first time where overall accountability has seen a more event split amongst other members of the c-suite: while the CEO still does have overall accountability for 16.7% of respondent organizations (2023: 22.6%), 14.8% now say that the Chief Operations Officer takes responsibility (2023: 12.7%), while 14.8% report it being the Chief Risk Officer (2023: 8.8%).

In financial services, the UK FCA/PRA/Bank of England regulations specify that it should be the COO (SMF24) who takes responsibility for the operational resilience programme. However, for the more ICT-focused DORA it is typically the CEO, but with the Chief Information Officer (CIO) and the Chief Information Security Officer (CISO) sharing some of the key responsibilities in terms of ICT risk management, vendor management, cyber security, and annual testing. Other regulations may not specify who should be in charge, and other sectors may have a different person (such as the Chief Constable in the Police in the UK) who assumes the role.

However, regardless of who is in charge, responsibility should be at the top of the organization, and, for most, this is where it lies. For non-listed organizations, the Executive Director typically takes on the same role as the CEO, which explains why this role takes fourth place in terms of popularity (13.9%).

"I think organizations need to have a top-down accountability for resilience, and there also needs to be a defined organisational structure because the pillars that support operational resilience have crossovers of a complex areas and complex risk types. Unless you're bringing those areas together and gain a holistic view as to where you are as an organization, you're focusing too much on one lens or a singular pillar, without being able to stand back and see the bigger picture."

Resilience manager,
financial services, UK



16.7%	Chief Executive Officer (CEO)
14.8%	Chief Operating Officer (COO)
14.8%	Chief Risk Officer (CRO)
13.9%	Executive Director
8.3%	There is no dedicated person in charge of this accountability within my organization.
7.4%	More than one person accountable (shared accountability)
4.6%	Operations Director
2.8%	Chief Security Officer (CSO)
2.8%	Chief Information Security Officer (CISO)
2.8%	Chair and/or board of directors
2.8%	Business Continuity Manager
2.8%	Compliance Director
1.9%	Head of Resilience
0.9%	Chief Financial and Operations Officer (CFRO)
0.9%	Operations Manager
0.9%	Global Security Officer
0.9%	Other

Figure 11. What is the job title of the person with overall accountability for operational resilience in your organization?

The rise of the Chief Resilience Officer

In terms of day-to-day responsibilities, it is the business continuity manager which obtained the most responses in the survey (22.9%). Given this report's survey sample containing a large number of BCI members, this is not a surprising result. However, what is noticeable is the number of respondents who report the Head of Resilience or Chief Resilience Officer is now responsible for operational resilience within organizations. With nearly a fifth of respondents selecting this option (18.8%), the creation of this role in organizations is increasing. This is a rise of seven percentage points from last year's report (11.8%), and more than double that noted in 2022 (9.2%). The BCI Future of Business Continuity and Resilience Report 2021 discussed the idea of such a role being introduced into organizations as a direct result of the COVID-19 pandemic and the increased awareness of resilience and, at that point, 23.3% of respondents wanted such a role to be created (although believed there was little chance of it happening), 8.4% of participants already had the role created during the pandemic, while 4.8% were actively looking to create such a role[11]. This report shows that these requests, at least for some organizations, have now been realised.

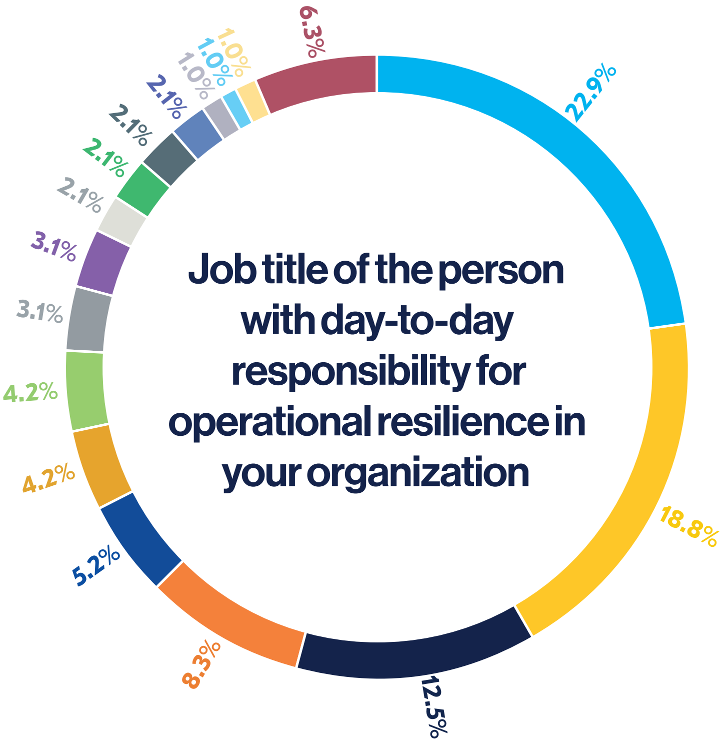
With these step-changes year-on-year, it seems that practitioners and management alike have now built a greater awareness of the importance of resilience, and the role is now becoming more widespread. Mainstream business journalism has regularly picked up the topic this year, with Bloomberg describing Chief Resilience Officers as 'working across all business units in the organization', and 'coordinating across silos'. It suggests they look 'beyond the boundaries of traditional risk mitigation and instead build resilience systems, ensuring that their organizations are equipped to thrive when faced with adverse circumstances."[12] Forbes also published an article at a similar time this year, reporting how such a role was needed in organizations to help ensure a coordinated response by engaging all parts of the organization, but to also help ensure resilience as a concept is considered, separate from the well-versed 'planning' and 'response'.[13]

"We have a Chief Resilience Officer who is a driving force for resilience in general across the board, which is really helpful for us because it means when we are having issues, we can go to him and get support. I think that the role of Chief Resilience Officer is useful not only for driving resilience within the organizations, but for the CEO as they are accountable for operational resilience as per regulations, however in many cases they don't have the time to prioritise this."

Resilience manager, financial services, UK

"The Operational resilience regulations have really put it in the forefront of people's minds the fact that if we get this outcome right, we're doing what's best for the customers, for our business and the marketplace. I think what operational resiliency has also done is really created that extra focus for the Board, giving me an opportunity to reinforce the idea that good business continuity is part of operational resilience. So it's uplifting business continuity as well."

Resilience & continuity manager, banking and finance, UK



22.9% Business Continuity Manager	18.8% Head of Resilience
12.5% More than one person accountable (shared accountability)	8.3% Operational Resilience Manager
5.2% Chief Operating Officer (COO)	4.2% Operations Manager
4.2% Business Continuity Officer	3.1% Risk Manager
3.1% There is no dedicated person in charge of this accountability within my organization.	2.1% Chief Risk Officer (CRO)
2.1% Chief Security Officer (CSO)	2.1% Chief Information Security Officer (CISO)
2.1% Executive Director	1.0% Operations Director
1.0% Chair and/or board of directors	1.0% Security Officer
6.3% Other	

Figure 12. Job title of the person with day-to-day responsibility for operational resilience in your organization?

Organizational attention to operational resilience

As determined already, operational resilience is now generating board room and executive level discussions, and staff awareness of its importance is starting to filter down to all levels. Notably, this is now becoming more commonplace in organizations which do not have any formalised rules or regulations in place.

However, outcomes from conversations can only be derived if discussions are documented, points discussed in the right meetings, actions are written, and progress is documented. This year's survey shows that the cadence of discussions at board and executive level has risen this year in line with the findings that greater consideration is being given to resilience programmes, as well as Chief Resilience Officers becoming more commonplace. At 36.0%, the percentage of respondents who say resilience is discussed at board meetings at least once every quarter remains similar to last year (2023: 36.4%), while 50.5% report the same for executive level meetings (2023: 49.3%). However, it is at the technology risk committee where there has been the greatest rise in the frequency of meetings, with 65.4% reporting meetings at least every quarter (2023: 47.9%), with 33.3% saying these meetings happen every month (2022: 27.2%). This is likely to be due to the fast-approaching digital-focused DORA deadline, as well as new guidance from the UK regulators about the consideration of third-party risk, primarily from digital service providers.

"Now we are definitely seeing much more engagement in committees within the organization, more involvement, much more challenges, and better challenges from all the way up to board level. Particularly as we approach that March 2025 deadline, it's been a maturing landscape. Pre-regulations, the visibility was there but it was difficult to understand how the pillars interplay off one another, and how we inadvertently may have put more weight on one pillar than another. Now we are making sure that we bring them all together as they are equally important in in terms of the delivery of the service."

Resilience manager, financial services, UK

Having these discussions at the top level of organizations is encouraging and, for some organizations, is vital to ensuring regulatory compliance. However, at least for the executive level discussions, tangible actions need to come out of those in order to ensure the resilience agenda is driven in day-to-day operations. For some organizations however, the conversations are still failing to happen at all. An interviewee highlighted how siloed working practices were stifling any chance of developing an operational resilience programme.

"We do not have somebody with overall look for resilience because we've got different pillars, and they are siloed; they don't work together. We don't even have anybody that meets quarterly, annually to analyse the overall state of resiliency of the organization."

Business resilience manager,
information technology, USA

How often is operational resilience on the agenda of the following committees or their nearest equivalent in your organization?

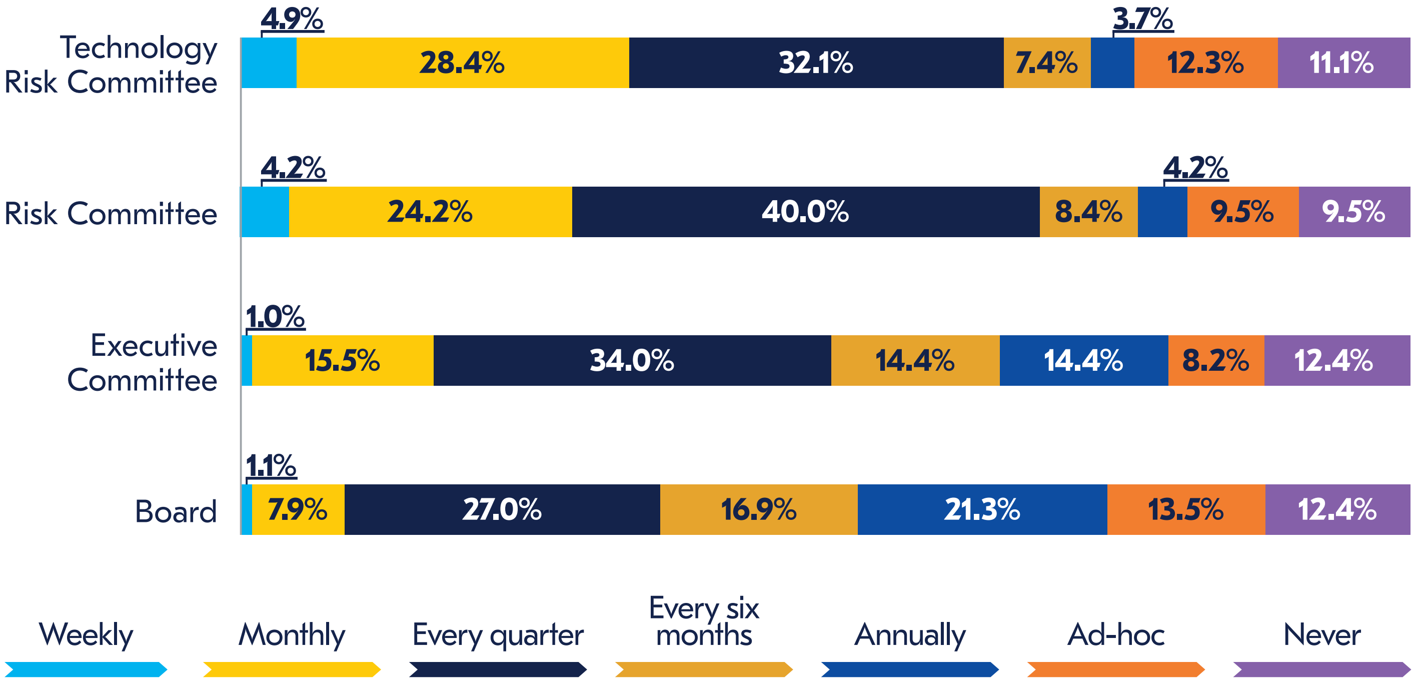


Figure 13. How often is operational resilience on the agenda of the following committees or their nearest equivalent in your organization?

In addition to attention from senior management, organizations also have groups which bring together personnel from across the organization to help ascertain the tactical and operational steps required for an organization to realise its resilience goal. Although nearly a third of organization do not have any such body set-up (30.4%), half of organizations do now have a steering committee (50.0%), 30.4% a working party, and 26.8% a project team. The 'other' responses typically focus on similar groups with different names, although some say groups have been set-up to focus on the IT/third-party supplier aspect, as well as others that are focused on cyber-security. Two respondents noted they have specific teams set-up to examine how they can exploit AI within their operational resilience programme, while another detailed that they have people within different departments all around the business who are operational resilience 'champions' for their particular areas.

Of course, all these groups help to break down the internal silos and ensure cross-functional conversations take place. While two-thirds (65.6%) do so through these internal working committees described in the previous paragraph, 21.2% report that key people 'all report to the same person' (often the head of resilience or chief resilience officer), and a further fifth (19.5%) have dual/cross reporting.

Does your organization have any of the following operational resilience related bodies?

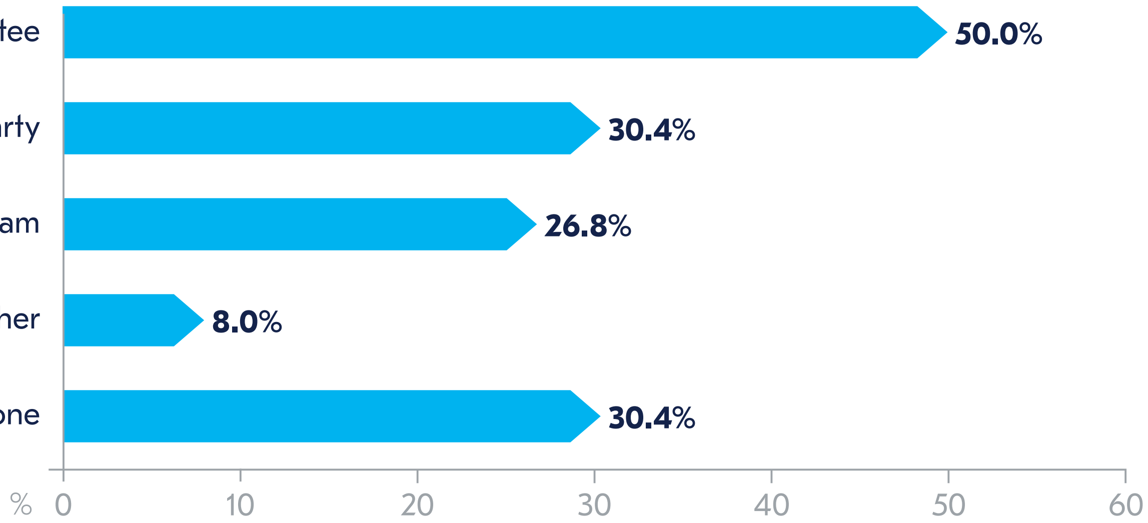


Figure 14. Does your organization have any of the following operational resilience related bodies?

What has your organization done to bring together operational resilience and other related functions such as cyber or risk?

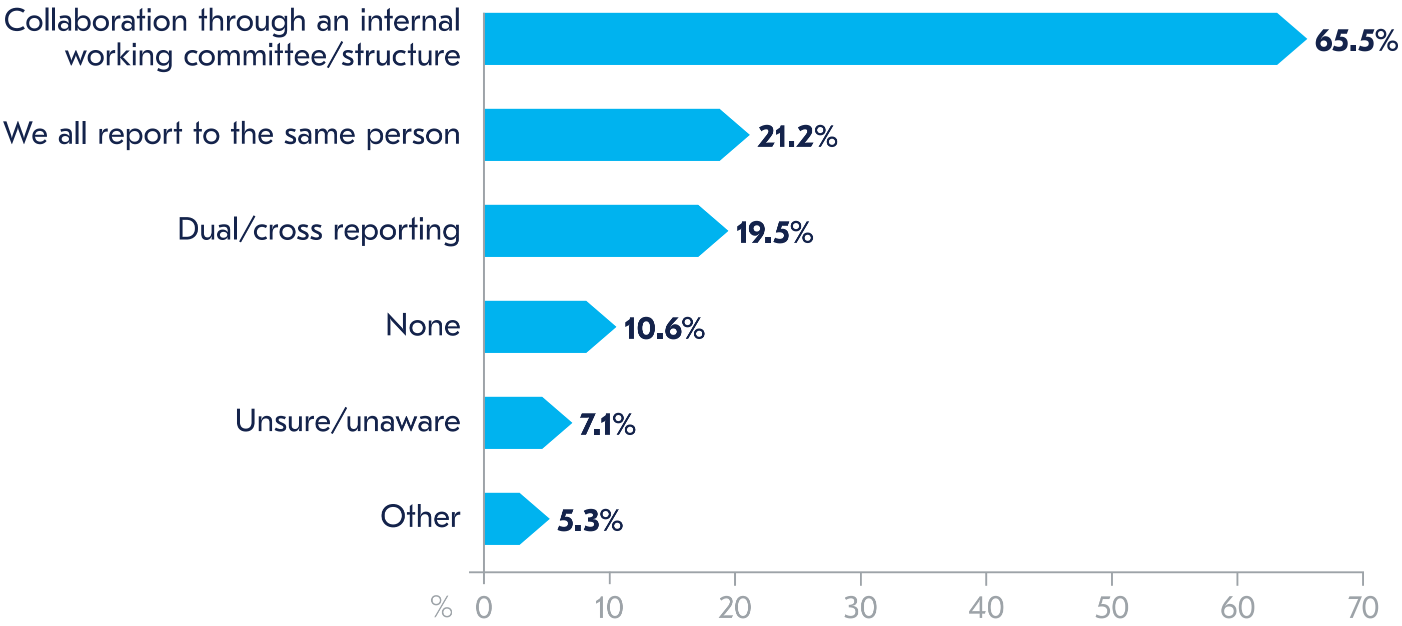


Figure 15. What has your organization done to bring together operational resilience and other related functions such as cyber or risk?

4 Global Operational Resilience Regulation in Financial Services

Global Operational Resilience Regulation in Financial Services

For many countries, 2024 is the final year of preparation before implementation deadlines approach in 2025. DORA is the regulation which is at the forefront of many practitioners' minds with full compliance required by 17 January 2025. The scale of the new regulation might only be EU-wide, but due to the breadth of the regulation and attention to digital third-parties, its reach is global. Meanwhile, the UK's Operational Resilience Framework also requires full compliance by 31 March 2025, and APRA-related entities in Australia must prove that they can effectively manage operational risks and maintain operations by 1 July 2025, as per the CPS 230 (operational risk management) and the CPS 234 (information security) standards (finalised in July 2023).

Does your organization adhere/will adhere when regulation comes into force to any of the following supervisory schemes or legislation?

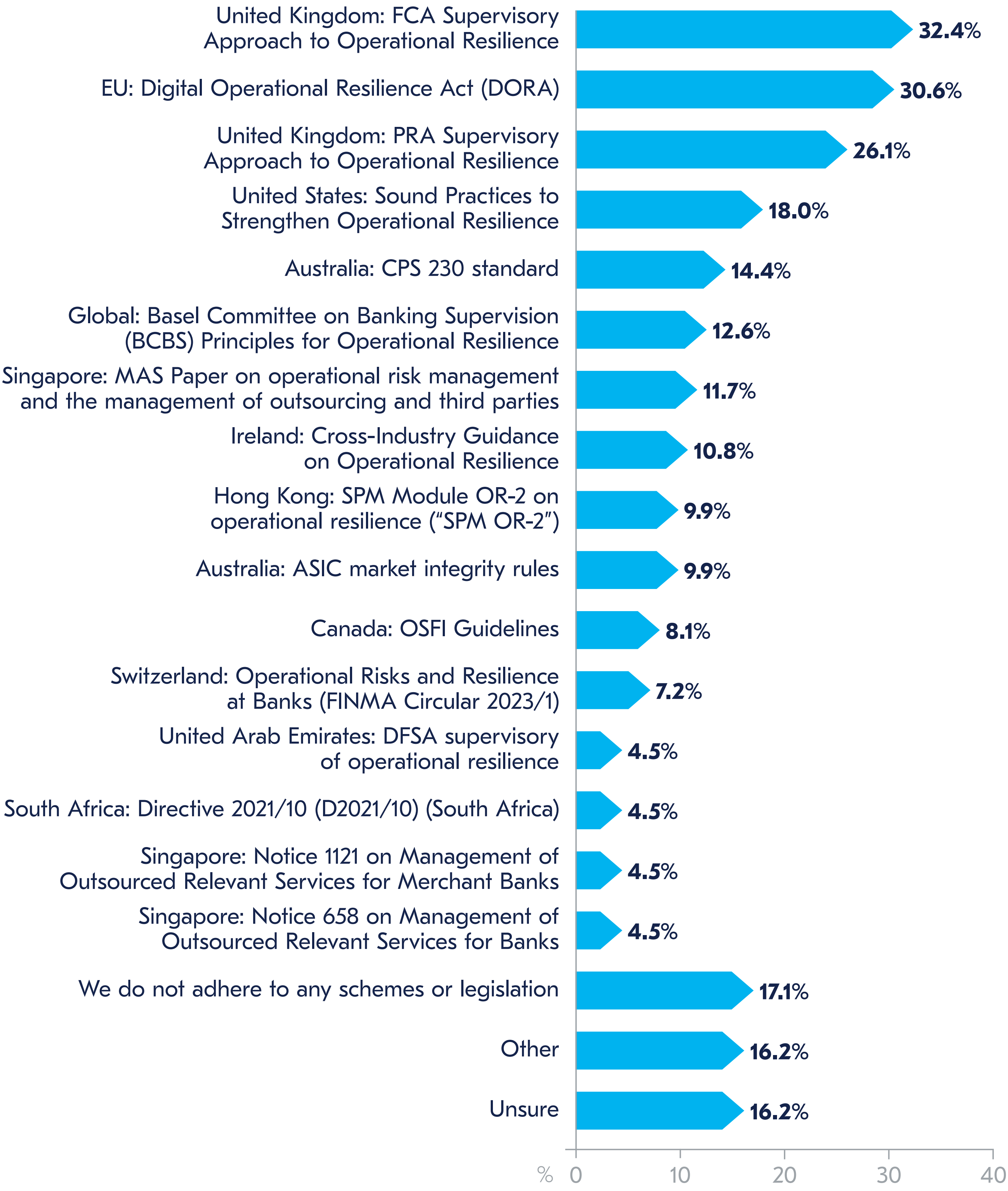


Figure 16. Does your organization adhere/will adhere when regulation comes into force to any of the following supervisory schemes or legislation?

Table 1 shows the level of adherence to operational resilience regulations globally from respondents to this survey. This particular graph should be viewed with caution, however. The picture will be skewed by the number of respondents who answered the survey from each country. As per last year's report, where there were more than 10 respondents from a specific country covered by regulation, the data was analysed further to see just how many organizations complied to their 'local' regulation. This shows that where regulation is coming towards its implementation deadline, compliance is 100%. Australia, where the deadline falls in the second half of 2024, has near universal compliance at 83.3%. The United States, meanwhile, where no deadline for its regulation has been set, sees much lower compliance at 66.7%.

Country/Region	Body	Title of paper	Adoption rate
United Kingdom	FCA/PRA	Supervisory Approach to Operational Resilience	**100.0%**
European Union	EU	Digital Operational Resilience Act (DORA)	**100.0%**
Australia	CPS 230	Operational Risk Management	**83.3%**
Australia	ASIC	Market Integrity Rules	**66.7%**
United States	OCC	Sound Practices to Strengthen Operational Resilience	**66.7%**

Table 1. Level of adoption of regional operational resilience regulation by survey participants in the financial services sector (financial services organizations; country sample size <10)

The overriding view is that regulators are not doing enough to aid implementation of operational resilience.

Fewer than a fifth of respondents (18.6%) believe the regulators have done enough to help organizations to implement operational resilience. With 28.3% still reserving judgement, more than half (53.1%) say that they have not done enough. Generally, satisfaction levels increase the nearer the deadline is. In the UK, for example, exactly a third of respondents are happy with the information provided, although there is some criticism that the FCA has been 'particularly quiet' recently. However, in the United States, where regulatory processes have been behind those of European and Asian counterparts, zero percent have given a 'yes' response, with 57.2% offering a resounding 'no'.

The fact that satisfaction grows as the deadline approaches sends a clear message to regulators that more guidance and help needs to be provided at the start of the regulatory process. While United States professionals might be feeling somewhat lost in terms of information, these feelings may soon cease: on 12 March 2024, the Acting Comptroller of the Currency, Michael Hsu, indicated in a speech that operational resilience regulations may be forthcoming by the end of 2024 and, like other international regulation, would be designed to bolster financial organizations' ability to withstand disruption to critical operations. Furthermore, the statement also said that third-party service providers would be a core consideration in this new regulation[14].

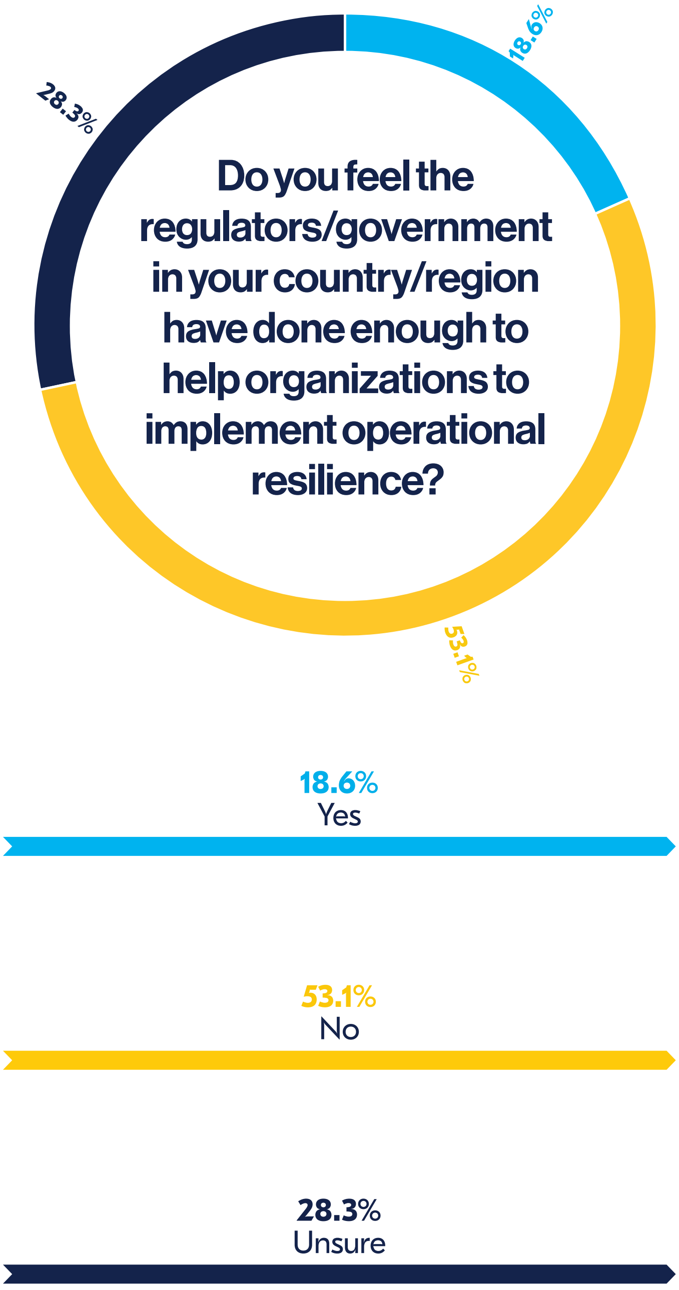


Figure 17. Do you feel the regulators/ government in your country/region have done enough to help organizations to implement operational resilience?

In the general comments to this question, a number of themes emerged. Many called for publication of 'best practices', with case studies also something that practitioners were calling for. Furthermore, although the conversations about the correct definition of operational resilience might be becoming tiresome for some, they are something that many practitioners believe the regulators should be doing; ideally through a collective approach. Some of the comments made are as follows:

"[We need a] basic, broadly understandable definition and explanation of what operational resilience is. Currently, there is virtually no official information similar to this in Japan."

"[We need] all the regulators to get together and come up with universal definitions. All the regulations have good points, but terminology differs dramatically, and content does too."

"[There's a] lack of alignment between various regulators in expectations. And regulatory responses have asked for items and formats that are not included in their existing policy statements."

"The awareness on the importance of operational resilience is still lacking thus not many companies are willing to invest on it".

Others wanted greater guidance on particular parts of the regulation, such as defining impact tolerances, or more help on severe but plausible scenarios.

"More direction on impact tolerance requirements (how to define activities within that time frame), more guidance on severe but plausible scenarios, more alignment of industry and definition of critical operations, and more flexibility on exceptions for valid reasons."

"[More help is needed on] defining tolerance levels and specific plausible disruption scenarios."

"Impact tolerance should be defined by the regulator for industry-specific participants to avoid systemic risk."

"[We] need a better definition of proportionality and more examples."

"Additional guidance on integration across risk types would help."

"More supporting details on the requirements. Often, they are very vague. Also impacts on global companies and how/when/where things are to be reported."

Others continued to be critical of the regulators, saying they were being asked for information, which was not mentioned in the regulation, or continued to be unresponsive when questions were fielded to them. Others still mooted the lack of regulation available in different countries and different sectors.

“Guidance has not yet been finalised. APRA have not responded to requests for them to attend finance industry forum to discuss and provide further details.”

“PRA have been very good. FCA have been quiet although assuming this will change as they now mature their resilience team.”

“Have they done anything for non-profits?”

“[There’s a] lack of alignment between various regulators in expectations. And regulatory responses have asked for items and formats that are not included in their existing policy statements.”

“There is no specific government organisation that is totally responsible for this function, predominately for business continuity to get any guidance or support from.”

“I think the main issue with the regulator is the issue of clear deliverables. I understand why they’ve not given them because every organization is quite different, but for operational resilience it was quite unclear on what was required. For example, we provided a yearly self-assessment. The regulator came back to us and said that our self-assessment didn’t have what they need it to have, but the year before they said it was fine. There was lack of consistency, no clear parameters, no willingness to tell us what they’re actually looking for, no specifics. I know a lot of my peers are feeling that way as well. It’s like the government’s telling us to do something but without telling us what that something looks like, which is not helpful at all.

The regulators in the UK are very slow at giving feedback. It can be that they come back with feedback from a 12 month old document. They need to give us a lot faster responses so that we can meet that deadline of March 2025.”

Resilience manager, financial services, UK

“The regulator will hold webinars, summits and conferences. These are done locally, and they give an explanation of what the requirements are. However, the problem still remains when specific questions are asked. Then we receive a roundabout answer, very often quoting the regulation a verbatim and we are still not able to fully implement or fully understand what needs to be implemented. We want their perspective, their interpretation of the regulation.”

Operational resilience manager. financial services, Malta

Overall, the specific requests for information do decline as implementation deadlines are approaching. For future regulation, regulators have the advantage of seeing what other regulators were missing when they were in the consultation stage. One would therefore hope that when the US regulation is finalised, hopefully towards the end of 2024, there is more consideration made to the comments other regulators have received, as well as taking on board feedback from around the world about additional detail that should be included from the start (e.g. in the UK, the lack of third-party consideration in the initial guidance was one such omission).

> **"Regulators could have done more in terms of third-party regulation. It feels like that there's a bit of a lag in that instance: if our disruption happens through one of those third-parties, then we're at a disadvantage because that's where we are maybe getting into the difference between severe but extreme scenarios and severe but plausible scenarios, scenarios that that we can practically run.**
>
> **It's very difficult to get suppliers to comply with the regulation if they're not a regulated entity themselves. Once you've already contracted them, unless you're coming up for renewal, is hard to demand them to comply with regulation. Outsourcing is something that we're doing more of as an industry, not less. That trend will probably continue, hence the importance for suppliers to be compliant and to have that end-to-end visibility."**
>
> Resilience manager,
> financial services, UK

> **"Operational resilience is an integral part of our operations, as are our third-party suppliers. It's not just a question of how resilient the bank is to an attack or an issue, but also about the ecosystem of our suppliers. The risk resides with us, and outsourcing could bring additional risk which we have to take this into consideration."**
>
> Operational resilience manager,
> financial services, Malta

> **"One of one of the things I think we struggle with as an organisation of our size is getting the required information from suppliers and testing participation. We use some suppliers that are used by other big firms within the industry. So, we're asking that same firm the same questions as everybody else around resiliency. It would be really helpful if there was one document or one set of documents, a place, where we could all go and get the information. One of the things the regulators can do is where we've identified those multi use suppliers, they could support with a centralised test, whether it's one test or two tests or multiple. All the bigger suppliers can get together with us as smaller organisations and do one test."**
>
> Resilience & continuity manager,
> banking and finance, UK

Not everyone was of the same view, however. An interviewee felt that it was more up to the financial institutions themselves to be more in control of their operational resilience programmes.

> **"I don't think the banks should look to get more guidance from the regulators. The banks need to be more in control of their destiny and write down their Operational Resilience ambitions. The regulators are also as new to the field as the banks, and we should work in a collaborative fashion to learn about Operational Resilience together, the end goal being the same."**
>
> Global Head of Resilience & Continuity, Banking sector, Netherlands

Comment from the BCI Operational Resilience Special Interest Group (SIG):

bci Special Interest Groups

Operational resilience regulations and standards have been introduced primarily in the financial services sector in the past few years, with clear and detailed regulatory mandates driving its adoption & implementation. The BCI Operational Resilience Report 2023 showed how important regulation was for driving operational resilience programmes, a trend that has continued in this year's report, indicating that most organizations without a programme did not have one due to not having to comply to regulation.

But only financial services regulators in mature markets/countries have specific mandates, driving uniform standards of adoption. Unfortunately, not all regulators across markets see the need to drive operational resilience or even if they do, lack prescriptive mandates, thereby leaving a lot to interpretation.

Also, as this survey suggests, there is a glaring gap of incorporating operational resilience in non-regulated sectors. This could potentially be where governments have an opportunity to step in and drive operational resilience across public and private sectors, especially in the context of today's complex and uncertain environment.

The UK financial sector

Operational resilience in the UK financial sector has been featured in this report since its inception. At the time, the UK regulations were considered to be one of the primary forerunners in regulation, so it has retained this space in the report each year. However, with other regulations having more concertina'd compliance deadlines for 2025, more in-depth research will be produced from this point forward.

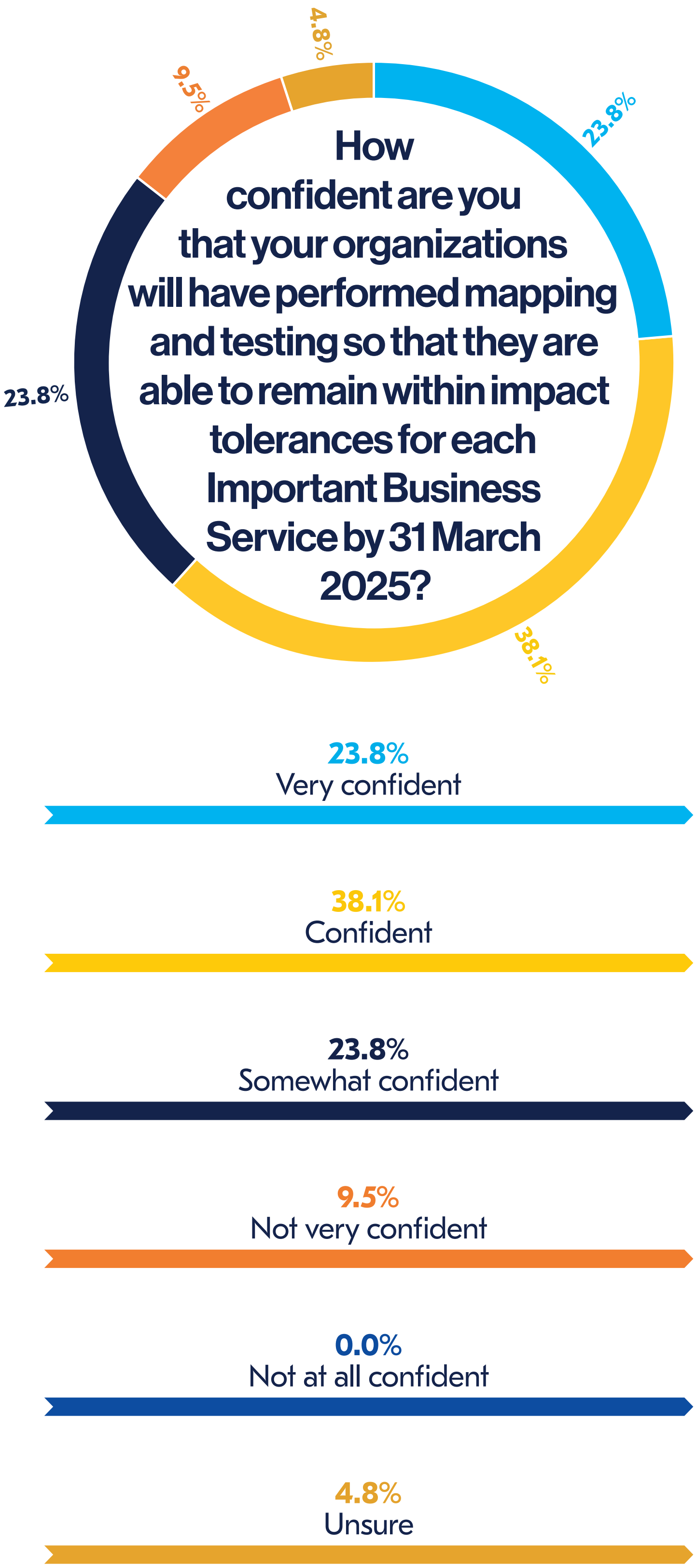
As the 31 March 2025 deadline approaches for implementation of the UK FCA/PRA/Bank of England regulations, confidence amongst regulated financial services organizations that they will be able to meet the deadlines has fallen in the past year.

Part of the reason for this could be due to the imminence of the deadline: it is now almost 10 months' away, and time is running out to ensure everything is in place. Furthermore, with the response deadline closing only recently (15 March 2024) on the CP23/30: Operational resilience: Critical third-parties to the UK financial sector consultation paper[15], the extra requirements for suppliers could be providing additional complexities to those responsible for those responsible for implementation in their own organizations.

Last year, confidence had grown amongst respondents that they would be able to meet the deadline to perform mapping and testing to prove they could remain within impact tolerances for each Important Business Service by 31 March 2025. At this point, the deadline was still two years' away, and professionals felt there was still sufficient time to ensure everything was in place. As such, 78.1% were either 'very confident' (42.7%) or 'confident' (35.3%) that they would be able to meet the deadline. Just twelve months later, in confidence has fallen: less than a quarter (23.8%) now report being very confident, and 38.1% are 'confident'. An interviewee went one step further, expressing surprise that anyone could be very confident staying within their impact tolerances due to unknown unknowns.

> **"I would be surprised by anybody who says that they are very confident that they can remain within impact tolerances because I think the opportunity for disruption, particularly for what we don't know, always exists. We can map and we can test to our level of maturity using the information from the regulations, but I just wouldn't be confident in saying that we'll have thought of everything or will have thought of most things."**
>
> Resilience manager,
> financial services, UK

Part of the reason for the lack of confidence may be down to a lack of funding in this area to allow an organization to make the necessary investments to ensure it can meet the deadline. When the regulation was first introduced, practitioners were hopeful that management would invest in order to ensure their organization would comfortably meet the deadlines. Our research has shown that they did – at the start. However, with changes being made to requirements, particularly on the third-party side, investment was not as forthcoming.



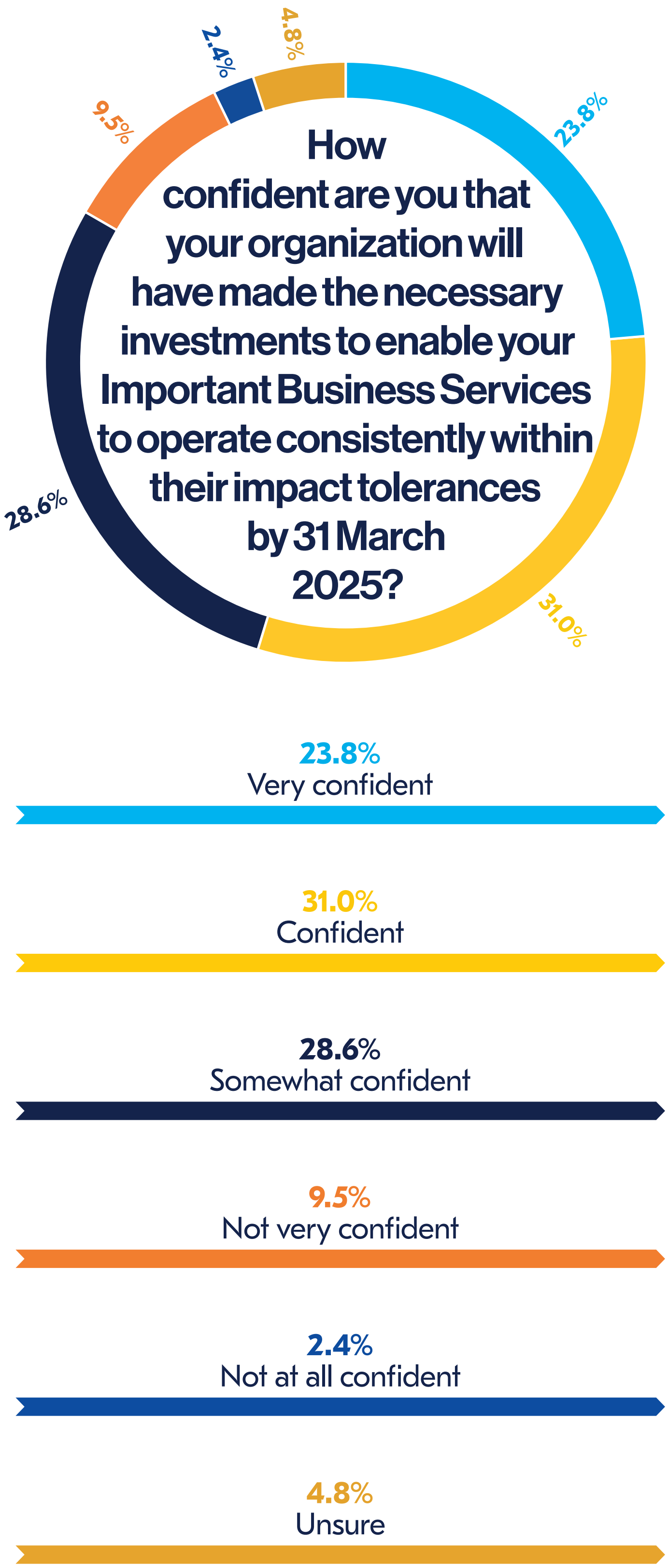


Figure 18. How confident are you that your organizations will have performed mapping and testing so that they are able to remain within impact tolerances for each Important Business Service by 31 March 2025?

Figure 19. From how many countries does your organization have operational resilience regulatory compliance requirements?

Operational resilience programmes

One of the reasons for not being able to retain the right level of funding may, in some cases, be because those in charge of building and running the programme still have some degree of confusion themselves about the requirements. Last year's report discussed how 13.5% of respondents reported their organization had more than 100 IBSs. Although the regulators are keen to point out that there is no "ideal" number of IBS, most financial services organization will have a maximum of 20. Some expect significantly lower numbers, too.

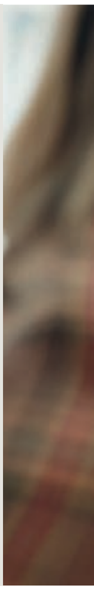
> **"Certainly, in our industry, we're not expecting firms to have any more than 10 IBSs."**
>
> Head of business operations, insurance services, United Kingdom

This year, however, the figures are higher than last year. Only just over half of respondents (57.6%) reported having fewer than 25 IBSs (2023: 74.6%), while a quarter of respondents (25.2%) say their organization has more than 100 IBSs (2023: 13.5%). The reason for some organizations having a greater number of IBSs directly correlates with whether the organization has to comply with operational resilience regulations. If the data is cut to only include financial services organizations in the European Union and the United Kingdom, 95.2% have fewer than 25 IBSs, and the remaining 4.8% still have under 50. If the same analysis is done for the United States where regulation still has to be defined, 83.3% have more than 26 IBSs, with 41.7% reporting over 100. Indeed, some organizations continue to struggle to differentiate between critical activities and IBSs.

> **"I think some misunderstanding within the organization about the definition of a critical activity. Our list of critical activities is so big, all-encompassing, that I don't think that we have really defined what it means."**
>
> Business continuity specialist, insurance services, Canada

The differences are likely to be down to the approach taken in defining these IBSs, as well as the staff in charge of carrying out the role. BC professionals are well-versed in identifying a fairly contained number of prioritised processes or services by conducting activities such as the BIA. However, while these processes and services can be referred to as guidance when looking to define IBSs, they should certainly not be used as a blueprint. Typically, a BIA will contain lower-level operational processes, whereas IBSs are those which typically provide an output for the consumer. A common example is that of payroll: while important to internal 'customers' (i.e. the staff), it is not something that affects external customers. Therefore, this should be included in the BIA, but not as an IBS. The Bank of England/FCA/BIA provide the following guidance in response to questions asked about the identification of IBSs:

> **"In the final policy, the supervisory authorities have set out that internal services such as human resources or payroll should not be identified as an important business service. These services constitute enablers of the important business service. The policy is focused on delivery of specific outcomes or services to external end users. The supervisory authorities are therefore requiring firms to prioritise work to build the operational resilience of those important business services."[16]**



However, it should be noted that different industries will have their own definitions of an IBS. In the aviation industry where safety is the greatest concern, there is different terminology used such as ‘critical parts’, and the industry is likely to have a much longer list of activities which are critical to the safety of its customers.

How many Important Business Services/critical activities/critical operations* does your organization have?

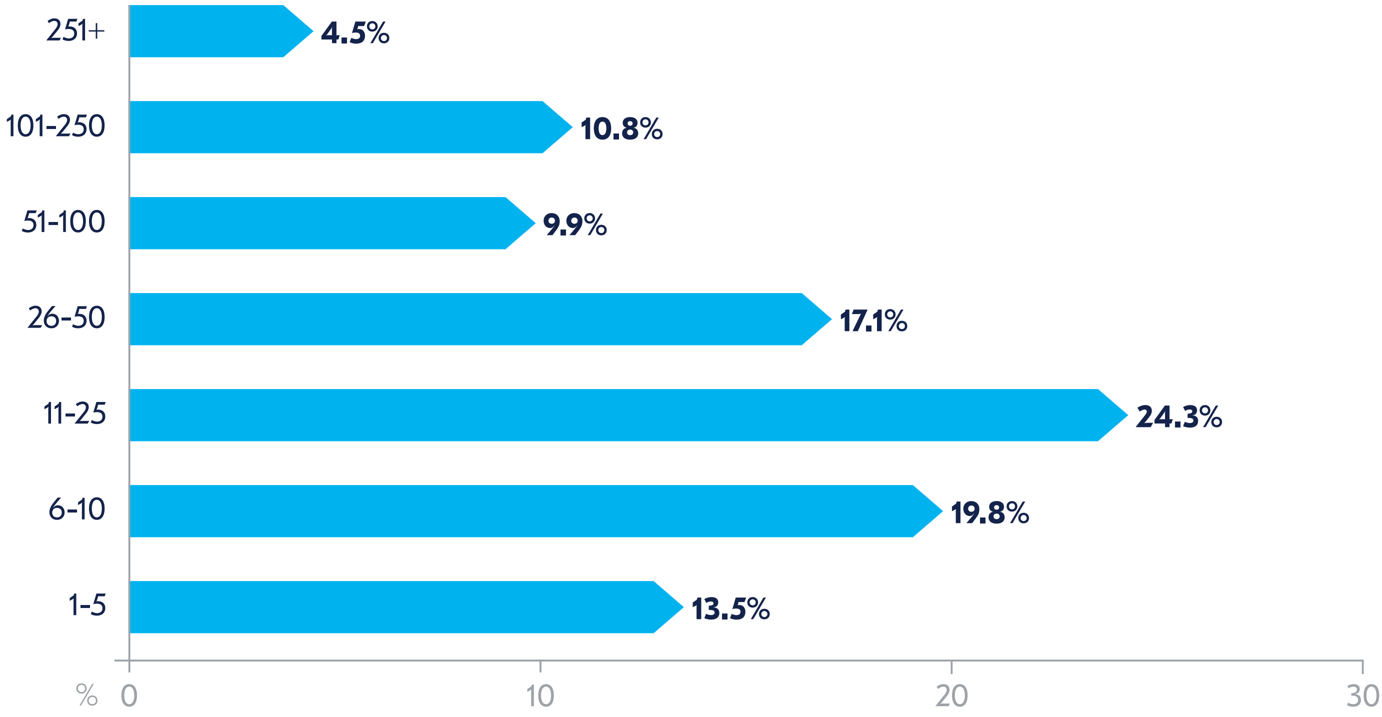


Figure 20. How many Important Business Services/critical activities/critical operations* does your organization have? *The definition depends on the region you are located.

Cross-organizational working

A sound organizational resilience programme will require the input from multiple parts of the organization in order to be effective. Such groups are vital for knowledge sharing, helping to unpick new regulatory demands, and ensuring a cross-organizational view can be obtained for any decision-making processes. Most committees will typically include senior management, as well as dedicated operational resilience staff and departments such as business continuity, IT, risk, compliance, legal, HR, and facilities management. Some organizations will have a very large 'base group' for their working group, enabling them to pull on individuals in different departments if required, but not necessarily having everyone attend every meeting.

Nearly two-thirds of organizations (62.7%) have a committee/working party in place to ensure operational resilience is implemented and managed correctly, and a further 11.8% are working to get such a group in place.

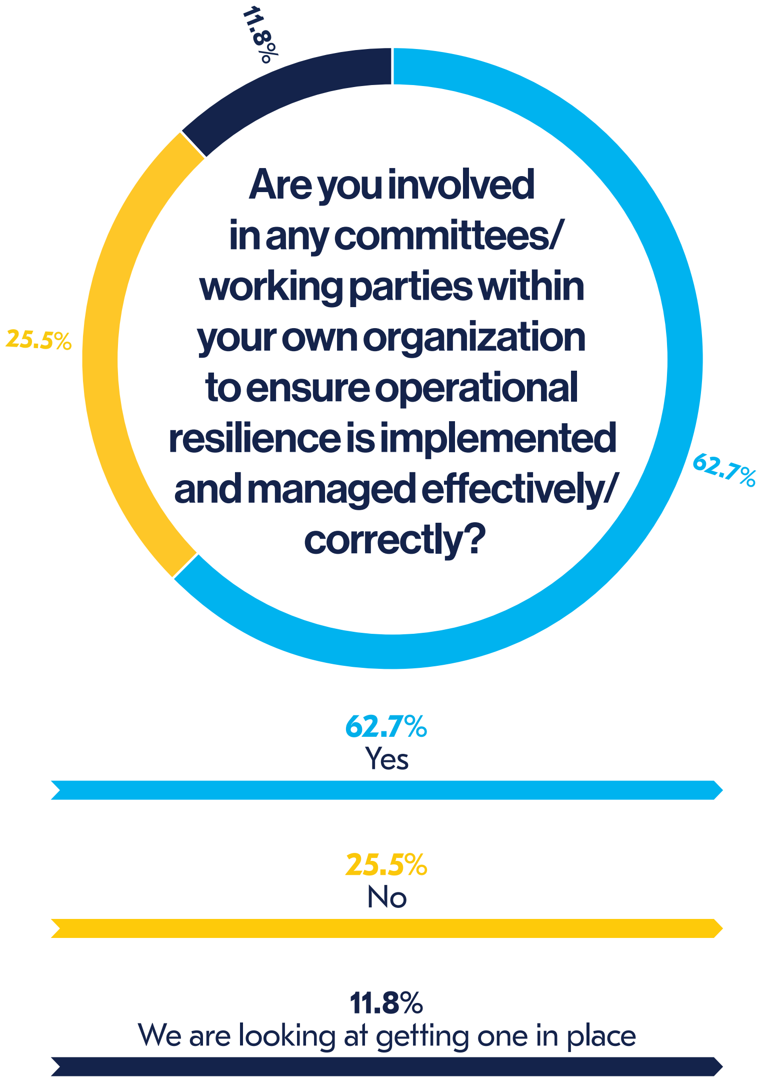


Figure 21. Do you feel the regulators/ government in your country/region have done enough to help organizations to implement operational resilience?

Intra-industry groups

For some professionals, taking part in external groups can be critical to building a successful programme. These types of groups can offer a number of advantages to those who are setting up a programme. For example, experts in the group could help guide others with ideas for implementation, concerns can be shared — along with possible solutions from others, new industry guidance can be unpicked, and ideas bounced off each other. Some groups are self-formed by a group of professionals known to each other, others may be facilitated by advisory firms or banks, and additional groups could be established through channels within industry bodies (such as the BCI chapters or the BCI Operational Resilience Special Interest Group).

Although participation in intra-industry groups is not as high as it is for internal groups, nearly two-thirds (59.5%) say they are involved in such a group. The figure is higher than last year's 53.2% which shows a concerted effort to join such groups as regulatory deadlines approach.

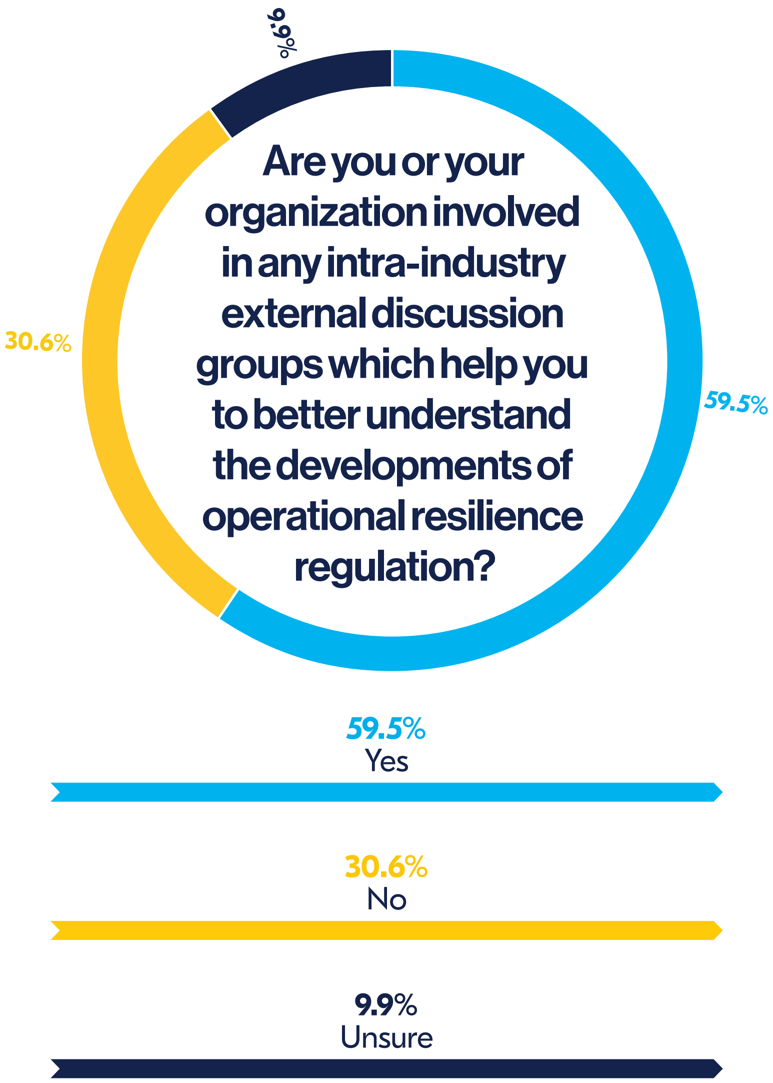
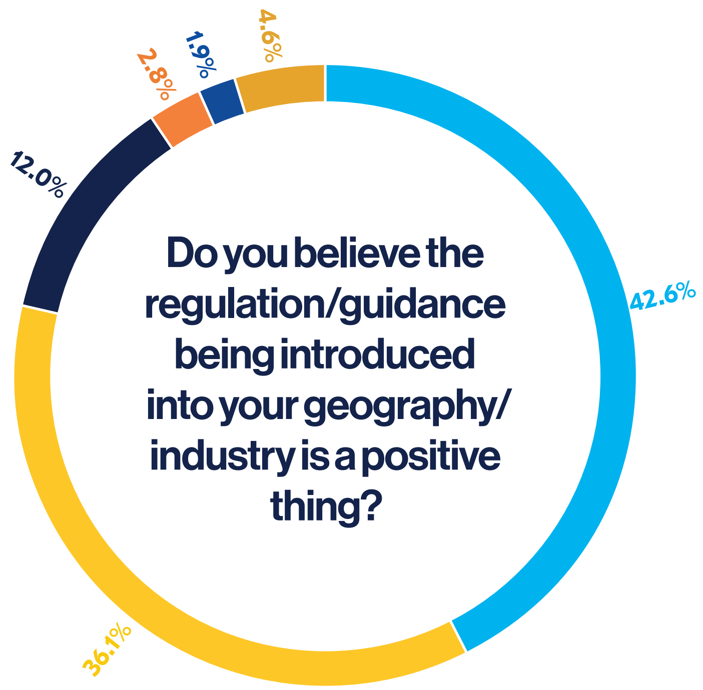


Figure 22. Are you or your organization involved in any intra-industry external discussion groups which help you to better understand the developments of operational resilience regulation?

Although there might be concerns about how the regulators are delivering guidance, the overall sector-agnostic consensus remains that operational resilience regulation is a good thing for organizations: nearly four out of five respondents (78.7%) are either 'very much in agreement' or 'in agreement' that regulation is positive. Only 4.7% have say they are 'not really' or 'not at all' positive about the regulation. Interestingly, the majority of negative views were harboured from small organizations which are likely to struggle more with the fees involved in compliance, as well as not having the depth of staff knowledge to know how to put such a programme in place.



42.6%
Yes, very much so

36.1%
Yes, somewhat

12.0%
Neutral

2.8%
No, not really

1.9%
No, not at all

4.6%
Unsure

Figure 23. Do you believe the regulation/guidance being introduced into your geography/industry is a positive thing?

5 Looking Ahead: Key Challenges

Looking Ahead: Key Challenges

In a story similar to last year, the primary challenges to implementing operational resilience # have two principal themes: that of embedding operational resilience into the organization, and also have the resources, both from a monetary and people perspective, to build and run the programme effectively.

Embedding an operational resilience programme

This year, 92.9% said that 'embedding operational resilience into the fabric of their organization' was either a 'major' or 'minor' problem. This is up from 85.9% in last year's report. Embedding operational resilience into an organization is dependent on a number of factors: 1) whether the organization falls under regulation, or is mandated to follow sectoral or government guidelines; 2) whether management are aware of the importance of an operational resilience programme; 3) if there is an industry acceptance of resilience as a concept; 4) if the organization already has a business continuity programme in place.

People challenges

Having enough people with the right skillset is a continuing problem for those developing operational resilience programmes. With different parts of organizations contesting for extra funds and extra staff, sourcing of the right expertise can provide difficult. Therefore, it is not a surprise to see that not having enough headcount/staff time to implement a realistic operational resilience programme is the second greatest challenge to professionals: 88.9% report it being a 'major' or 'minor' challenge, with a further 80.7% saying that having the right people providing guidance and oversight in their organization was a challenge. With an additional two-thirds (66.3%) saying that there was a lack of knowledge to understand how to implement policy, there is clearly a need for more organizations to upskill their staff with the knowledge they require.

Although the regulators may not be so forthcoming with the practical information that practitioners would use, there are knowledge sharing opportunities that professionals could explore to enable them to increase their knowledge: the BCI, for example, has an operational resilience Special Interest Group for members to engage and share best practice, while many accountancy firms provide free webinars and papers about building and managing operational resilience programmes.

Technical detail

Enhancing resilience involves updating outdated systems that may fail during disruptions, with legacy infrastructure noted as the third main challenge in operational resilience implementation, highlighted by over half of respondents as a major challenge within their organizations. This often pertains to digital equipment that becomes obsolete or fails to integrate with new technology or updates, despite its crucial role in operations. DORA, for example, reflects a specific focus on this issue, mandating the inclusion of legacy infrastructure in the regulation. Whenever regulation is adopted, the technical detail of that regulation needs to be carefully picked apart and understood, and there are particular elements of operational resilience, especially in regard to technology, which practitioners find challenging with operational resilience regulation. An interviewee explained how an additional complication was the detail required from the European Central Bank (ECB) and national supervisors within 48 hours of an incident — at a point when it should be all-hands on solving the crisis.

The importance of third-party suppliers

Third-party suppliers related issues are a main challenge for organizations. Understanding, monitoring, and managing supply chain risks, together with ensuring regulatory compliance from third-party suppliers are the primary issues.

Ensuring third-party suppliers' compliance with regulations poses a significant challenge for 45.9% of surveyed organizations, placing it as the fourth biggest challenge to the implementation of operational resilience. As regulations mandate a certain level of supply chain management, achieving compliance from third-party suppliers becomes imperative. While larger organizations typically anticipate regulatory requirements and align their structures accordingly, smaller or medium-sized suppliers, located abroad in regions unaffected by regulations, may struggle with the associated economic burdens. For them, there is the potential loss of business due to perceived high costs which could be a barrier to compliance. For the organizations themselves, this could result in looking for different suppliers which, in turn, could lead to rising costs and other complications.

Meanwhile, suppliers to organizations that still have yet to fully address their critical third-party suppliers could face additional complications close to launch date, particularly — as an interviewee highlighted — that many are unaware of the incoming regulations. At the other end of the spectrum, an interviewee also spoke about how it is difficult to challenge large technology companies to address the requirements for third-party compliance as, for them, the business makes up only a small part of their wider customer base.

> **"DORA places a focus on ICT TPPs however we are faced with situations where third party providers have never heard of the Act. This is not an ideal situation, given that DORA is coming into play in January 2025."**
>
> Operational resilience manager, financial services, Malta

> **"Challenging big tech companies is also difficult. We believe that there isn't an even playing ground between us and these big organizations, especially when it comes to non-EU institutions. We end up between the regulator and these institutions and we have to find a compromise and assume risk."**
>
> Operational resilience manager, financial services, Malta

In 2024, a greater percentage of organizations (42.4% vs 37.9% in 2023) concede that the understanding, monitoring, and management of supply chain risks as a major challenge to implementing operational resilience. Managing third-party risk becomes particularly challenging when providers operate under different regulations. To address this issue, some regulators are considering the establishment of minimum resilience standards. This proactive approach aligns with practitioners' demands for additional regulatory clarity, as mentioned previously in this report.

What do you perceive as the major challenges to implementing operational resilience within your own organization?

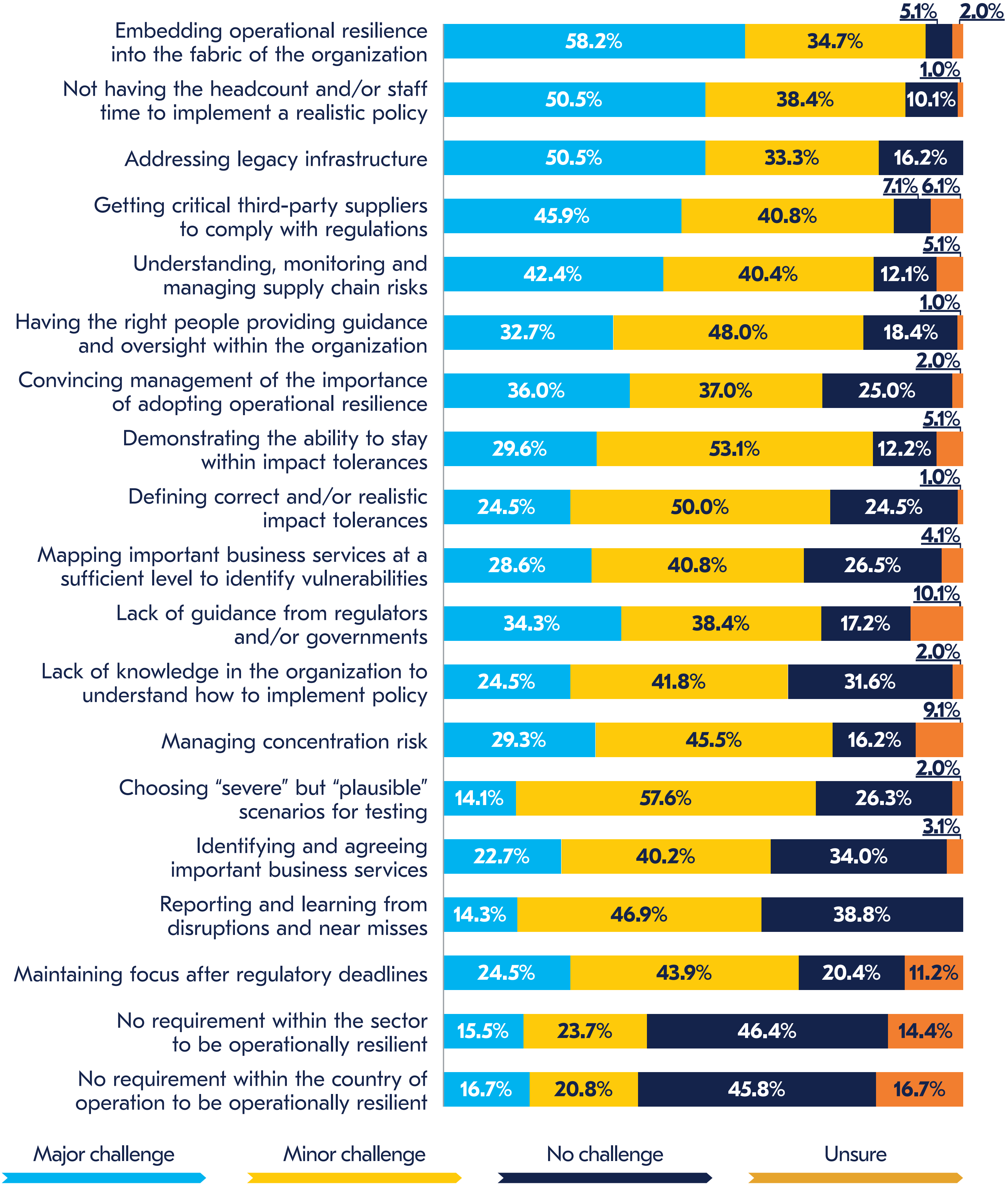


Figure 24. What do you perceive as the major challenges to implementing operational resilience within your own organization?

In regions where operational resilience regulation is minimal or non-existent, third-parties are not a consideration at all within existing governance. Although this obviously opens up the banking system to significant risk, some financial institutions are considering it regardless, and the general awareness of the subject hints that regulation is likely to be incoming.

> **"Most local organisations within the region haven't really embedded third party risk management into their processes. While the process for managing third parties exists in some organizations however, it's not being managed centrally so that you have a consistent and uniform third-party risk management process and framework."**
>
> Head of internal controls, banking & finance, Kenya

Finally, respondents were queried over their concerns that meeting regulatory requirements could become a tick box exercise — and concerns do persist. While management might be supportive of meeting regulatory requirements to avoid fines and reputational impact, those implementing the programmes voice concerns about regulations becoming a 'tick box exercise' and not going far enough. This year, slightly fewer respondents indicate concerns of a programmes becoming a tick-box exercise compared to last year. However, the proportion of organizations concerned about this point remains substantial. The danger is that organizations might focus solely on completing tasks or checking boxes to demonstrate compliance, rather than actively implementing effective practices to enhance resilience.

An interviewee from Australia hinted that organizations may complete only the necessary requirements for CPS 230 by July 2025, but was concerned that it would take much longer to fully embed this into organizations. With Australian financial services organizations under pressure with such a short timeline, it could be argued that the regulators themselves are forcing organizations down the tick-box route, albeit unintentionally.

> "Currently I am running the project and I get the resources that I need, but I believe once I have done this it will be a challenge for people: it's the embedding of processes that will be a challenge. I think people will still treat it as a bit of a tick box exercise, which is what they do with business continuity. I think it will be a major challenge."
>
> Operational resilience manager, financial services, UK

> "What we need to make sure is that resilience is embedded in the overarching framework of the organization. We could be very focused on the March 2025 date. We get to deliver by that date, but how is this model sustainable post March 2025? Needs to be a model that is continually assessing the threats, the resilience. If you don't have that infrastructure, that support, then there's a risk that resilience can kind of become a tick box exercise. It's difficult to assess how effective the model will be post-March 2025 until we're post March 2025."
>
> Resilience manager, financial services, UK

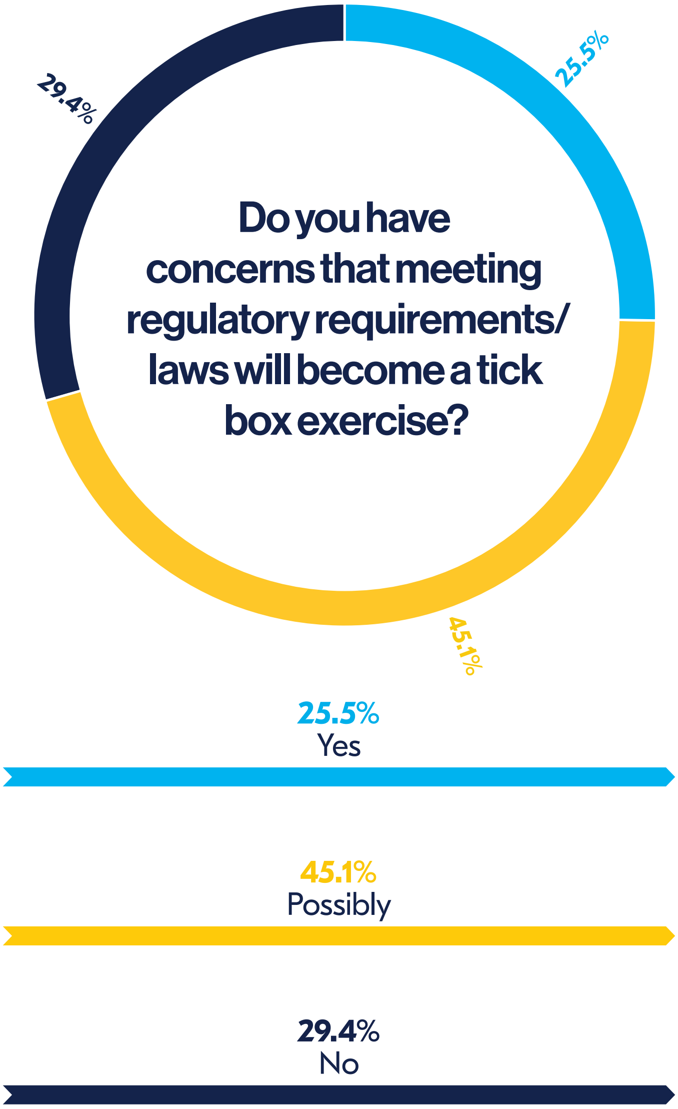


Figure 25. Do you have concerns that meeting regulatory requirements/laws will become a tick box exercise?

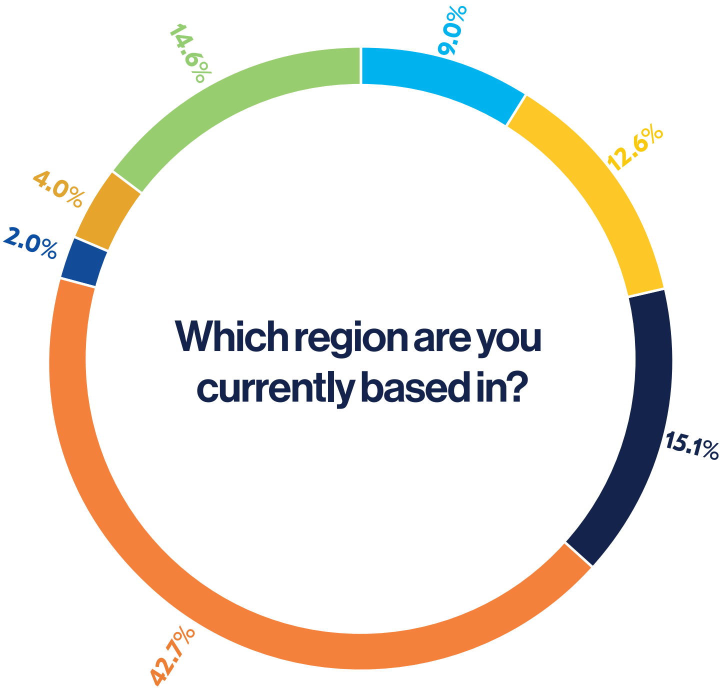
Annex

202 Respondents

46 Countries

17 Sectors

13 Respondent interviews



9.0%	Africa
12.6%	Asia
15.1%	Australasia
42.7%	Europe
2.0%	Latin America and The Caribbean
4.0%	Middle East
14.6%	North America

Figure 26. Which region are you currently based in?

How many other countries do you operate in?

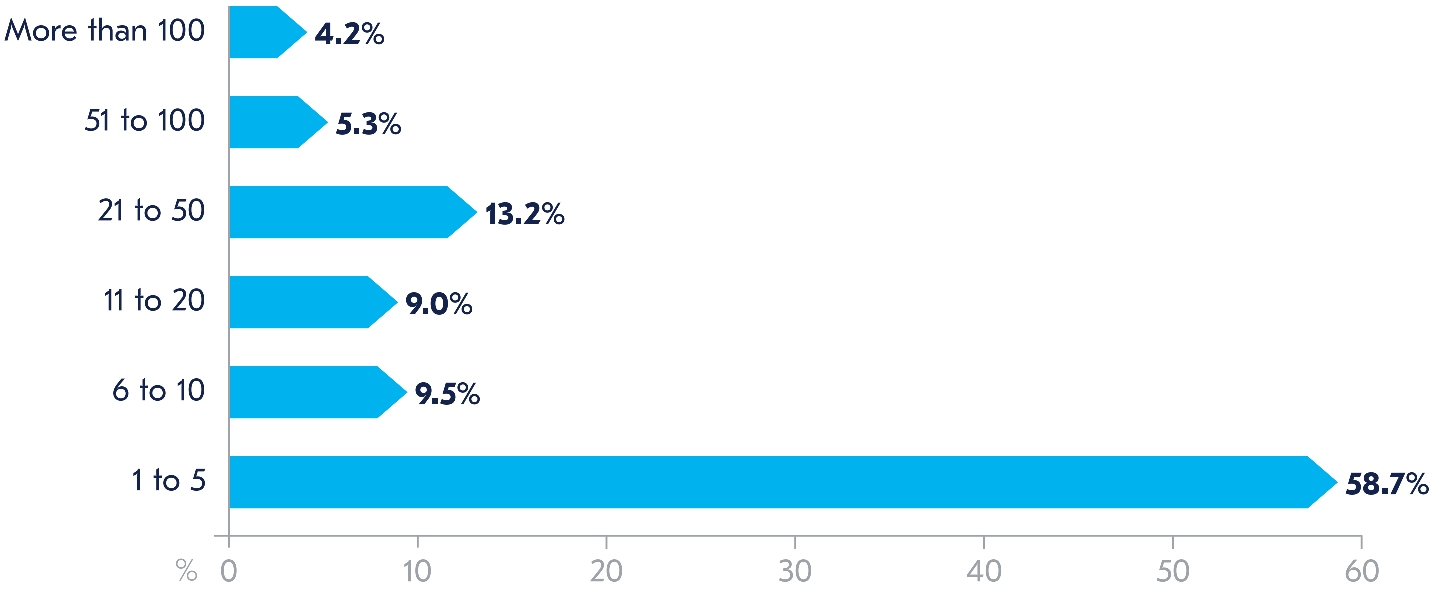
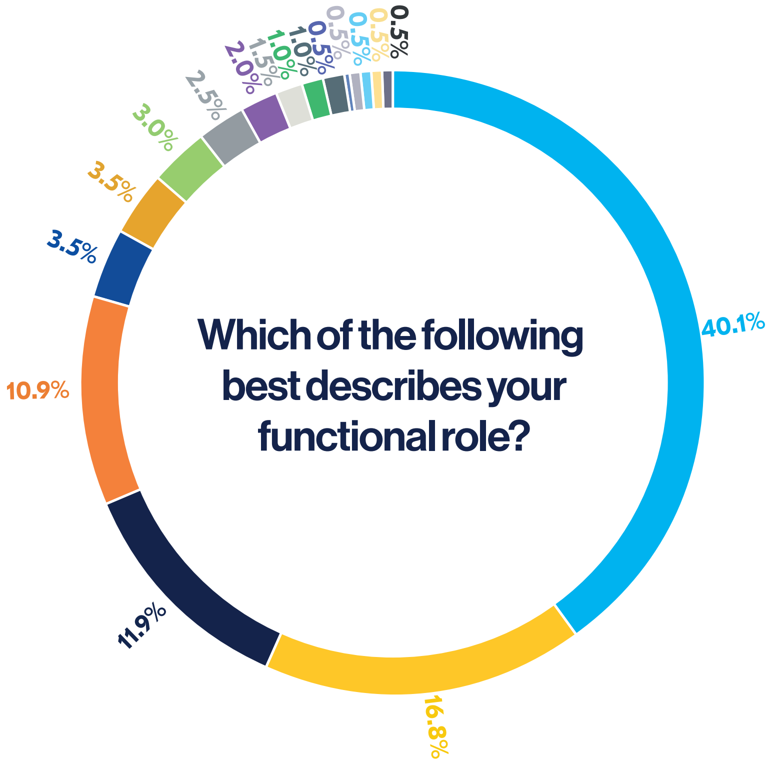


Figure 27. How many other countries do you operate in?



40.1%	Business continuity
16.8%	Operational Resilience
11.9%	Risk management
10.9%	Organizational Resilience
3.5%	IT disaster recovery/ IT service continuity
3.5%	Cyber and information security
3.0%	Quality/Business improvement
2.5%	Physical security
2.0%	Crisis management
1.5%	Supply chain and logistics
1.0%	Emergency planning
1.0%	Internal audit
0.5%	IT (other)
0.5%	Health & safety management
0.5%	Line of business or service directorate
0.5%	Operations management
0.5%	Executive leadership (CEO, COO, CFO)

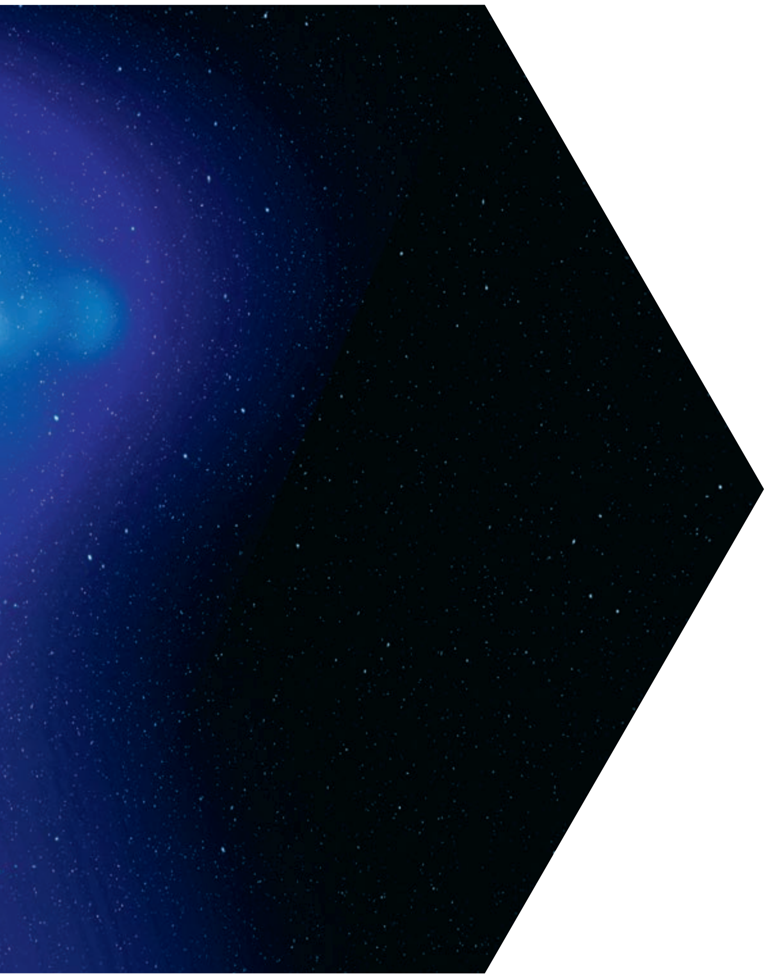
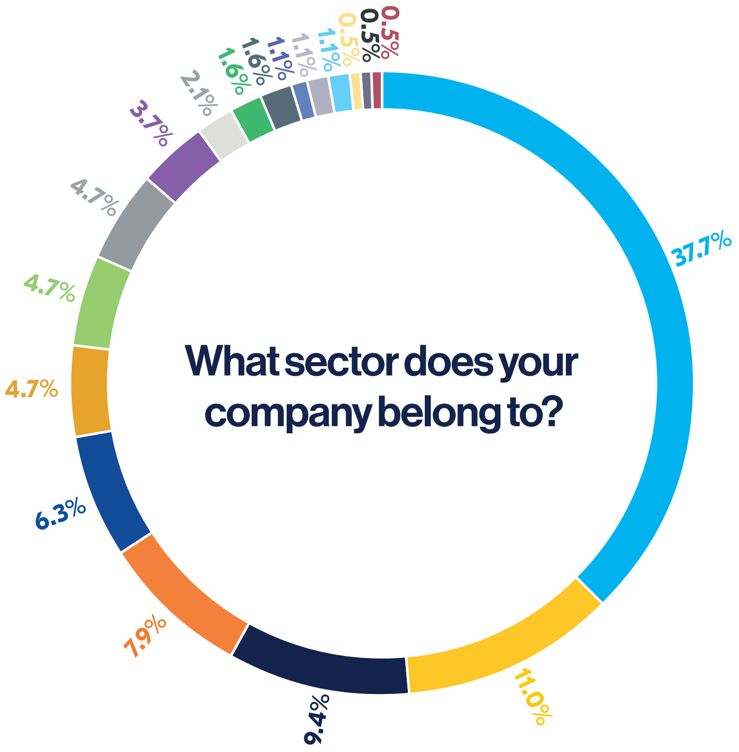


Figure 28. Which of the following best describes your functional role?



37.7%	Banking and finance
11.0%	Information technology
9.4%	Public services, government and administration
7.9%	Professional services
6.3%	Energy and utilities
4.7%	Education and training
4.7%	Manufacturing
4.7%	Transport and logistics
3.7%	Healthcare
2.1%	Telecommunications
1.6%	Charity/Not for profit
1.6%	Real estate and construction
1.1%	Environment and agriculture
1.1%	Leisure and hospitality
1.1%	Retail and wholesale
0.5%	Creative industries
0.5%	Engineering and infrastructure
0.5%	Law enforcement and security

Figure 29. What sector does your company belong to?

Approximately how many employees are there in your organization?

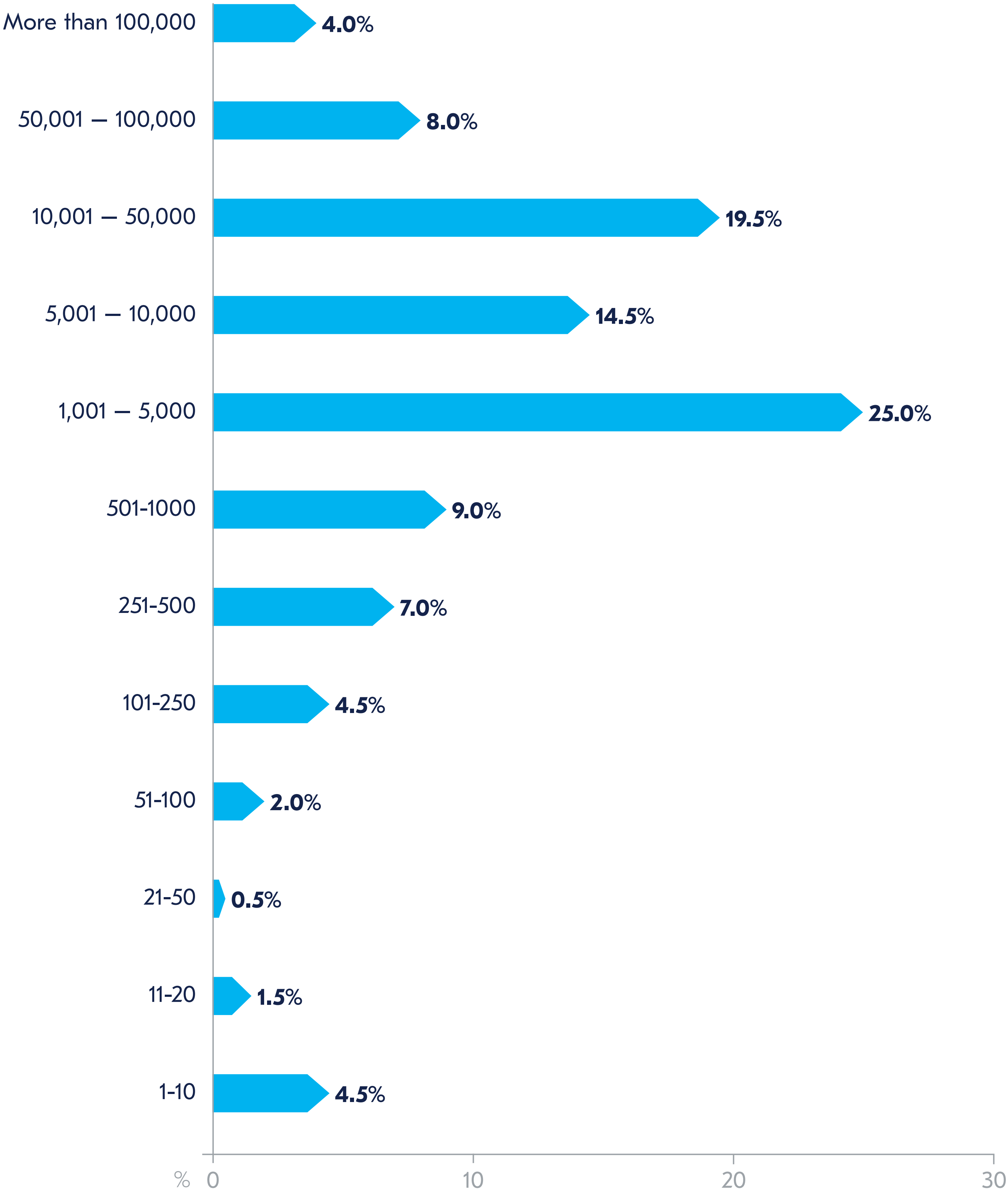


Figure 30. Approximately how many employees are there in your organization?

About the authors

Rachael Elliott

(Knowledge Strategist, The BCI)

Rachael has twenty years' experience leading commercial research within organizations such as HSBC, BDO LLP, Marakon Associates, CBRE, and BCMS. She has particular expertise in the technology and telecoms, retail, manufacturing, and real estate sectors. Her research has been used in Parliament to help develop government industrial strategy and the BDO High Street Sales Tracker, which Rachael was instrumental in developing, is still the UK's primary barometer for tracking high street sales performance. She maintains a keen interest in competitive intelligence and investigative research techniques.

She can be contacted at rachael.elliott@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 2,500 customers across six continents use our unique risk-correlation technology to gain previously unattainable insights that deliver better business outcomes. Riskonnect has more than 1,000 risk management experts in the Americas, Europe, and Asia.

To learn more, visit riskonnect.com

References

1. https://www.thebci.org/resource/bci-operational-resilience-report-2022.html
2. https://arxiv.org/abs/2401.03408
3. https://www.thebci.org/knowledge/bci-statement-on-organizational-resilience.html
4. https://healthitsecurity.com/features/this-years-largest-healthcare-data-breaches
5. https://www.independent.co.uk/tech/down-tesco-greggs-sainsburys-mcdonalds-shops-offline-not-working-b2515841.html
6. https://www.splunk.com/en_us/campaigns/ciso-report.html
7. https://www.bbc.co.uk/news/technology-68628348
8. https://www.splunk.com/en_us/campaigns/digital-resilience-pays-off.html
9. https://www.thebci.org/resource/service-resilience-and-software-risk.html
10. https://www.bcb.gov.br/content/about/legislation_norms_docs/CMN_Resolution_No_4,893_2021.pdf
11. https://www.thebci.org/news/bci-publishes-the-future-of-business-continuity-resilience-report-2021.html
12. Alam, S (2024). Chief Resilience Officers enter boardrooms as global risks climb.
    Bloomberg Law News. 29 February 2024. Available at: (last accessed 8 April 2024)
13. https://www.forbes.com/sites/hillennevins/2024/02/27/is-it-time-for-a-chief-resilience-officer/
14. https://www.jdsupra.com/legalnews/operational-resilience-requirements-may-9256861/
15. https://www.bankofengland.co.uk/prudential-regulation/publication/2023/december/operational-resilience-critical-third-parties-to-the-uk-financial-sector
16. https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/publication/2021/building-operational-resilience-impact-tolerances-for-important-business-services.pdf

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

bci@thebci.org / www.thebci.org

riskonnect
Integrated Risk Management Solutions™

bci Leading the way to resilience