Operational Risk Survey and Report 2020-21

Resilience Put to the Test

baringa.com

Contents

Executive Summary

Key Findings

1. Operational Risk Management and COVID-19

2. Trends in Operational Risk Identification and Assessment

3. Embedding Operational Risk Management

4. The Future for Operational Risk Management

Baringa
Brighter together

Executive Summary

Welcome to Baringa's third annual Operational Risk Survey and Report for the financial services sector, providing industry-led insight into best-practice and ongoing challenges in operational risk management.

Operational risk professionals have been thinking about resilience for some time, and so the pandemic-related shock of 2020 provides an opportunity to review the effectiveness of policies amid real-world disruption.

While the shifting and emerging risks will be closely watched, the ability of operational risk systems and processes to adapt and support organisational resilience is key. The evidence that follows is mixed.

Risk and Control Self-Assessments (RCSAs) are ubiquitous, but when a real crisis hit, many institutions didn't turn to them. Governance structures are considered robust, but the day-to-day oversight of committees can be unclear. Management information is improving, but many still find it burdensome and inefficient to produce. And while most institutions have a strong risk appetite setting process, their alignment with an organisation's actual strategy and risk profile can be weak.

If the goal is to create true organisational resilience, then embedding sound operational risk processes into a business must be the priority.

About this Report

This is the third annual Operational Risk Survey & Report conducted by Baringa Partners.

To inform the analysis, during the winter of 2020-2021, we contacted a diverse range of financial institutions.

The survey aggregates structured and qualitative responses from approximately 30 senior operational risk professionals. Respondents covered multiple jurisdictions, demonstrating the global challenge that effective operational risk management poses.

The survey contained around 50 questions and recorded detailed information on the composition and role of the operational risk team; the maturity of firms' risk and control frameworks; future challenges for operational risk management; and more.

Benchmarking

The survey data can be analysed by different attributes, including sector, geographic footprint and size of firm, allowing comparison versus peer organisations.
We can help you benchmark your own firm against this data. For more information, please contact us via OpRisk@baringa.com.

Respondent Profile

Respondents were broad in both the nature of their financial services and size of institution.

They covered multiple jurisdictions, and although almost all responses related to the UK and EMEA, almost a third of these also related to APAC, and a similar amount also related to the Americas. This illustrates the global challenge that effective operational risk management poses.

Business services offered by respondent firms

52% Investment banking and capital markets

38% Wealth and/or asset management

38% Retail/commercial bank

28% Insurer

Key Findings

1 Operational risk management and COVID-19

The pandemic and related responses have tested the systems, processes and resilience of financial services firms, while contributing to a growing list of top priorities for busy operational risk teams.

Key insights

- ▲ IT and cyber are top priorities. Almost 30% of respondents identified information security and cyber as their biggest operational risks arising from the COVID-19 crisis.
- ▲ Control environments. Over 70% reported a change in their control environment due to COVID-19.
- ▲ RCSAs split opinion. More than 40% did not leverage their Risk and Control Self-Assessments (RCSAs) during the COVID-19 crisis.
- ▲ Team sizes less affected, so far. Over 90% of respondents had not made any material changes to the size of their operational risk team due to COVID-19 at the point of responding.

2 Trends in operational risk identification and assessment

We asked senior operational risk professionals about their evolving priorities; the systems and tools they have in place to support effective risk management; and the maturity of their processes.

Key insights

- ▲ Data security gives ground. Data security is still the chief risk, but regulatory compliance, data management and business continuity are all catching up.
- ▲ Access to information. Over 60% of respondents had a single system in place for recording operational risk data and 55% have a standardised risk and control library in place.
- ▲ Control-testing a priority. Over 75% of respondents undertake control testing.
- ▲ RCSAs are universal. And yet there is little consistency around their level of detail or update mechanisms. The experience of 2020 also raises questions about how embedded and aligned they are with the business.

3 Embedding operational risk management

High-level confidence that operational risk is well-embedded in processes belies ongoing practical challenges, including alignment with the businesses' risk appetite, accessing the right data to inform management, and mechanisms to maintain quality.

Key insights

- ▲ Embedding risk. 86% of respondents reported that they have embedded operational risk within their change management process.
- ▲ Team changes ahead. Almost 40% of firms expect a material change in the size of their operational risk team in the next year.
- ▲ Information challenges. Just 31% of respondents reported that MI was easy and efficient to produce, leveraging system capabilities and data analytics.
- ▲ Risk appetite mismatch. In a majority of cases (85%), risk appetite statements are set by the board and reviewed at least annually. But challenges remain in aligning this with the business.
- ▲ Quality assurance overlooked. Only 45% of respondents reported that they have a quality-assurance programme in place to ensure consistent implementation of the operational risk framework.

4 The future for operational risk management

Some clear trends emerge from the survey, many of which are reinforced by existing regulatory focus. Particular challenges include aligning operational risk, operational resilience and third party risk frameworks.

Key insights

- ▲ Top priorities. The highest immediate priorities are improving and standardising RCSAs. The recent crisis has shown them to be static, business-as-usual tools.
- ▲ Third party risk. Operational outsourcing and third party risk management is a clear regulatory and firm focus for 2021.
- ▲ Resilience. Refining the relationship between risk and resilience is an ongoing challenge, from the perspective of management, governance and information.

1 Operational Risk Management and COVID-19

COVID-19 has had a tremendous impact on financial services providers across the world. The operational risk profile of institutions has therefore fundamentally altered, which, in turn, effects how risks are assessed, monitored and managed. It has also changed how operational risk teams work from a people perspective, including how they work with 1st line stakeholders.

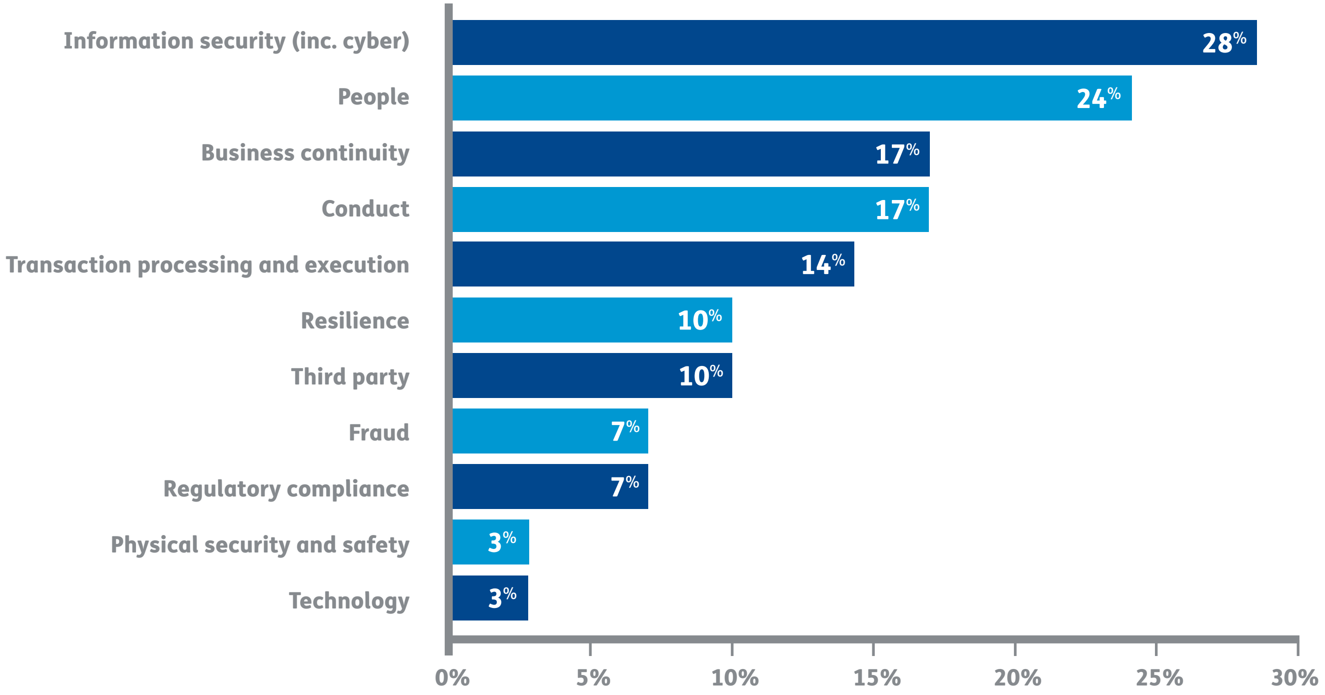
Operational risk teams remain stable… for now

Over 90% of respondents have not needed to make any material changes to the size of their operational risk teams as a response to COVID-19. However, some respondents reported that resources had been re-aligned within the team and non-key activities suspended to enable staff to focus on pandemic-response related activities.

Less than 10% of firms reported a reduction in team size, either as a result of job cuts across the firm or due to risk resources being re-deployed to support compliance or other activities.

COVID-19 has led to certain operational risks becoming more prevalent, with firms highlighting information security and people risk as being the two that have increased the most.

Fig. 1: Top risks due to COVID-19 highlighted by respondents



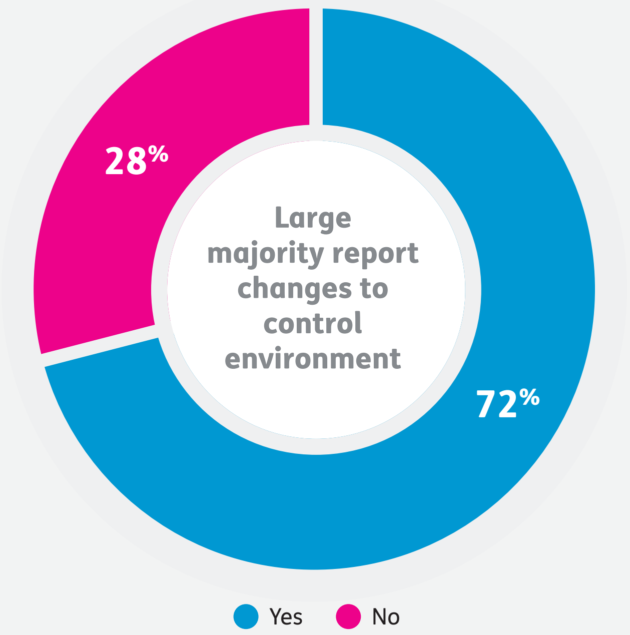
Changes to underlying risk profiles

Although the overall risk position for most institutions remained relatively static, COVID-19 resulted in a change in the level of certain risks.

Declining risks included those relating to money laundering, as a result of a reduction in the volume of transactions.

Rising risks were largely driven by changes in the ways of working, which consequently compromised the effectiveness of the control environment. Indeed, **more than 70%** of firms reported a change in their control environment as a result of COVID-19.

Fig. 2: Percentage of firms that reported a change in their control environment as a result of COVID-19



Remote-working challenges

In some instances, the move to remote-working meant that existing controls had to be relaxed or abandoned. For those firms with trading businesses, which have in recent years been subject to tight controls to address market abuse and conduct risks, restrictions on the ability to trade from home had to be lifted.

Controls over the use of mobile phones at the trading desk could not be enforced and firms also faced challenges with staff increasingly relying on collaboration technologies that were not fully integrated into monitoring and surveillance processes. Firms have had to adapt as a result and introduce new controls or amend existing controls.

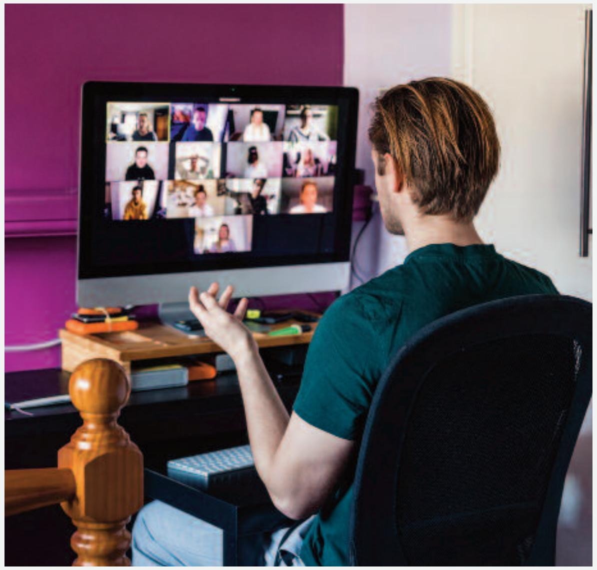
Insight: How some firms have adapted controls to remote-working

- Amending the approval process to enable remote printing.
- Introducing electronic signature processes and controls.
- Creating new control frameworks to enable the use of remote customer-contact centres.
- Relaxing mobile-phone-usage rules for trading teams.

Key challenge: evaluate the impact of changes to the control environment.

Consider:

- Those changes in the control environment that can and should be retained as we return to business as usual.
- Where further investment in the control environment may be needed to ensure a sustainable remote-working set-up going forward.
- Where controls could potentially be de-commissioned e.g. as a result of new technology or ways of working being introduced.

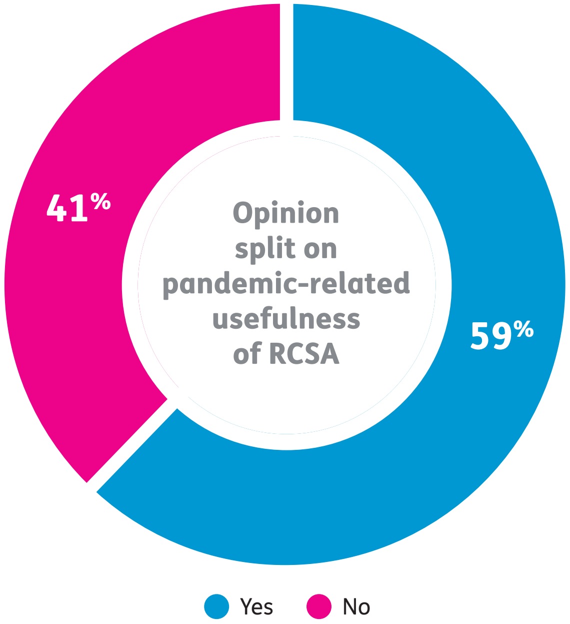


RCSAs overlooked by minority

Existing Risk and Control Self-Assessments (RCSAs) were used by **almost 60%** of respondents, in order to identify the key risks and relevant controls; the critical processes and functions that should be prioritised for IT support; and hotspots that may potentially need particular focus or consideration.

However, **more than 40%** chose not to leverage their RCSAs.

Fig. 3: Percentage of firms that have leveraged their RCSAs during the COVID-19 pandemic



A number of challenges were highlighted over the static and BAU nature of RCSAs that limited their value. As a result, a number of firms introduced offline logging and tracking of COVID-19-related changes to risks and controls, to enable timely review and decision-making. Indeed some firms created COVID-19-specific RCSAs to track risks, and performed light-touch testing of key controls identified.

COVID-19 RCSA learnings

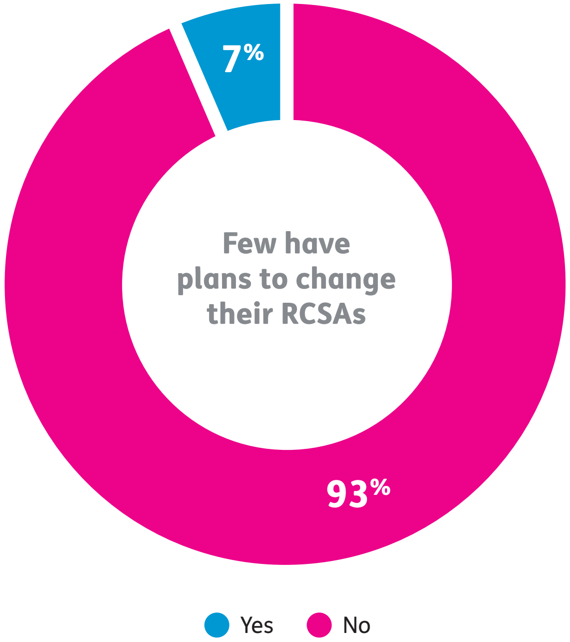
> *"[We are now] using the RCSA more real-time, rather than just on a frequent update cycle"*
>
> **Head of Operational Risk**
> UK Asset Manager

> *"Our RCSA process is due a refresh and will need to be flexed in response to Operational Resilience regulation. Learning points from COVID will be incorporated as part of this process"*
>
> **Head of Operational Risk & Resilience**
> UK Building Society

Our view: Embedding RCSAs

Whilst most firms do not anticipate any changes to their BAU RCSA process as a result of COVID-19, it is still important they take the time to integrate any risks and controls identified as part of these offline processes into the regular BAU RCSA going forward, and to assess any resulting changes in priorities.

Fig. 4: Percentage of firms planning to change their RCSA process as a result of COVID-19



COVID-19 control changes

> *"Around 200 specific changes were identified group-wide, following a consistent decision-making and monitoring process… these span technology; customer interaction; post-handling; third party oversight processes; and beyond"*
>
> **Head of Operational Risk**
> UK Asset Manager

2 Trends in Operational Risk Identification and Assessment

In this section, we considered the chief operational risks facing financial institutions; the tools and technology to support operational risk management; and the maturity of Risk and Control Self-Assessment (RCSA) processes, by drawing on data from previous years.

Operational risk: increasingly complex risk landscape

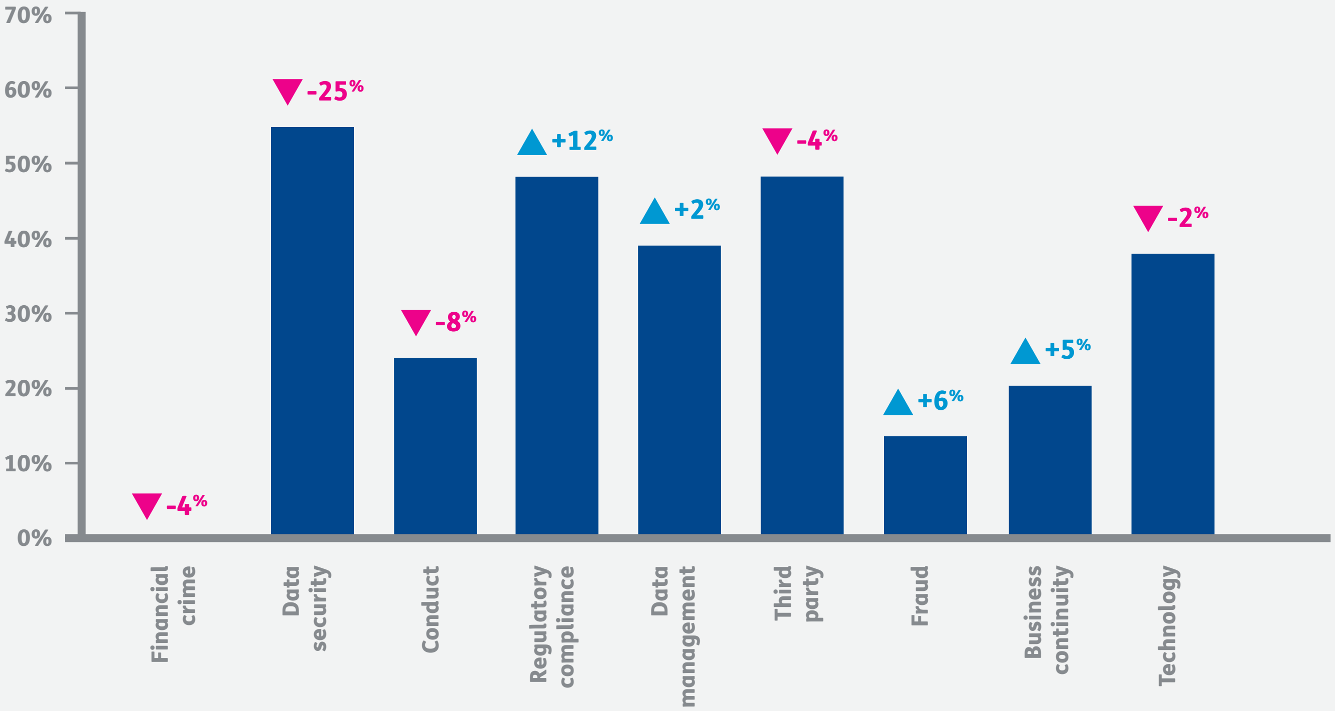
In previous surveys, data security has been a stand-out priority. This year, financial services providers have highlighted a multitude of rising risks that must be managed.

Data security remains a top priority but it is now accompanied by several other rapidly growing risk priorities.

A number of exogenous factors have added to the task of operational risk management.

COVID-19 working styles have introduced new pressures, while a number of developments in the regulatory landscape around third party, business continuity, technology and cyber risk, have sharpened attention across a variety of risks.

Fig. 5: Diversification of top risks - change vs. 2019-20



More risks: unprompted responses

A number of other key risks were proposed by respondents.

- Manual processes in the absence of automation
- Internal and external change management
- People risk and employee health and well-being in a post-COVID world.

Policy-driven priorities

Since the last survey was conducted, the UK regulators have published consultation papers on operational resilience and on outsourcing and third party risk management. The European Commission and the Canadian regulator, Office of the Superintendent of Financial Institutions (OSFI), have both published papers on digital resilience for the financial sector. The International Organization of Securities Commissions (IOSCO) published a consultation paper on proposals to update its outsourcing principles. While the Basel Committee on Banking Supervision (BCBS) published principles for operational resilience, which included principles on business continuity.

Operational risk management systems

62% of respondents had a single system in place for recording operational risk data. This is relatively consistent with the results from last year.

A rapidly declining and small minority of respondents have no system for recording operational risk data; meanwhile **31%** of respondents reported that they have multiple systems in place.

Of those respondents with systems in place, the majority use vendor systems, rather than in-house systems, with a handful of vendors dominating the respondent group. This result is consistent with previous years.

Ongoing challenge: data analysis

Despite the prevalence of systems to record data, challenges were still raised on the ease of data analysis.

Key risk indicators are not as integrated as other data elements, and analysis tends to involve dumping data into Excel. It is therefore unsurprising that a number of respondents highlighted that programmes were in-flight to replace existing systems to resolve this. Programmes include those to better integrate with other systems and to allow for easier linking of risks, events and KRIs.

Risk and control taxonomies

As with previous years, almost half (**45%**) of respondents do not have a standardised risk and control library or taxonomy in place. To understand the challenge better, this year we split the question, revealing that it is the control taxonomy/library that poses the biggest challenge, given that **28%** of those who responded stated that they don't have a taxonomy in place.

This is crucial as it provides firms with a mechanism to compare and aggregate risk profiles across the organisation, as well as enabling consistent monitoring and reporting on risks and events.

In addition to their risk-event taxonomy, **over 60%** of respondents this year reported the use of causal and impact taxonomies. This reflects an increase of **more than 15%** versus last year.

Fig. 6: Percentage of respondents who have a standardised risk and control library in place

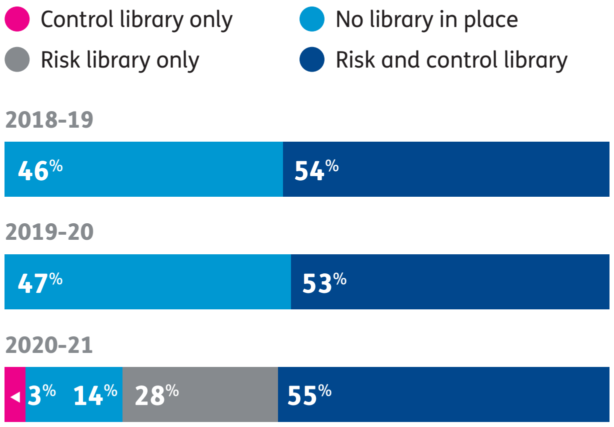
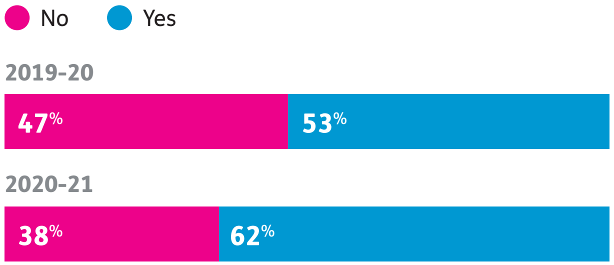


Fig. 7: Percentage of respondents who have a causal and impact taxonomy in place



Our view: The power of taxonomies

Following on from their work last year to define a risk-event taxonomy, the operational risk association ORX provided further guidance on the use of causal and impact taxonomies in 2020. As such, we can expect this trend of causal and impact taxonomies to continue.

Causal and impact taxonomies can help firms to better understand how to reduce the likelihood of risks crystallising, and to manage the fallout if they do. In the case of the causal taxonomy, it also provides a helpful way to root out any common drivers across different risks, and thus prioritise investment; for instance, if employees are a driver for many risk events, this can point to the need for further training to upskill employees and/or embed a culture of risk management.

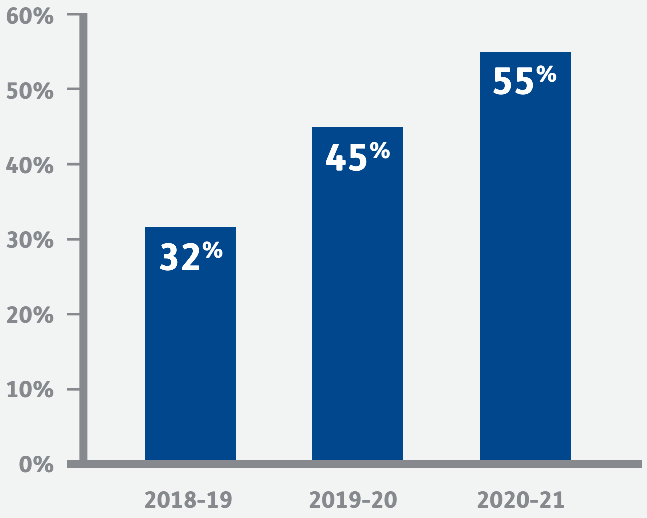
While the work by ORX has provided some suggestions of impact categories, a number of firms have taken the use of impact taxonomies further in order to explicitly make the connection between operational risk and resilience. Resilience is defined by the regulators as an outcome, which is supported by strong operational risk management. Regulatory requirements around operational resilience, and particularly around reporting to the Board and senior management, have increased the demand to be able to slice and dice existing operational risk MI in order to identify events with a resilience impact. As such, a number of firms have considered adding a resilience category to their impact taxonomy to assist with this.

Similarly, having a clear view of how processes, risks, controls and events fit together can help when it comes to tackling resilience requirements, and understanding what resources underpin critical business services.

The rise of risk mapping

The number of respondents who have a mapping of regulations, policies, processes, risks, controls and events in place, has risen consistently in the past three years, from **32%** to **43%** last year, to **55%** this year.

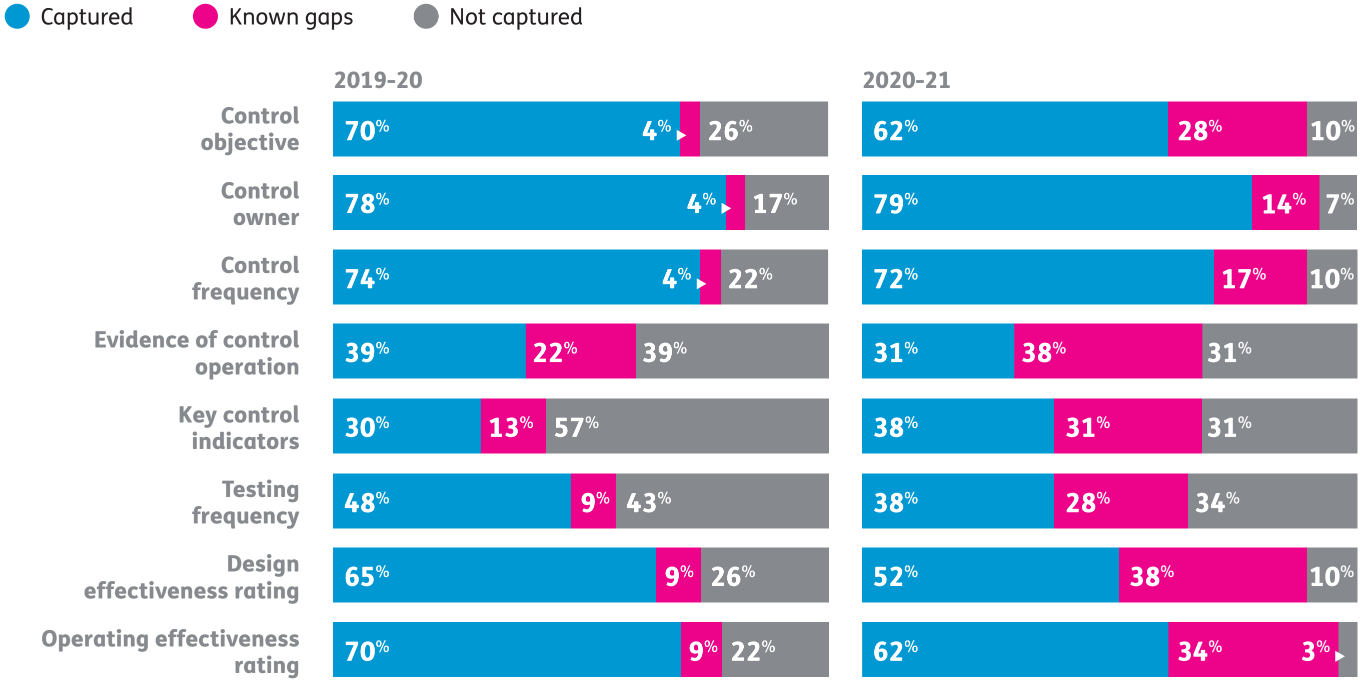
Fig. 8: Percentage of respondents who have a mapping of regulations, policies, processes, risks, controls and events in place



Control documentation

Fundamental attributes continue to be captured in control documentation, such as control objectives, control owners, control frequency and information on design and operating effectiveness. However, similar to last year, weaknesses remain in the capture of information around control operation, key control indicators and testing frequency. Given the earlier commentary around the control environment amid the COVID-19 pandemic, we might expect to see a change in this data going forward, as firms keep a better record of what their key controls are and how they are performing.

Fig. 9: Factors captured within respondents' controls documentation



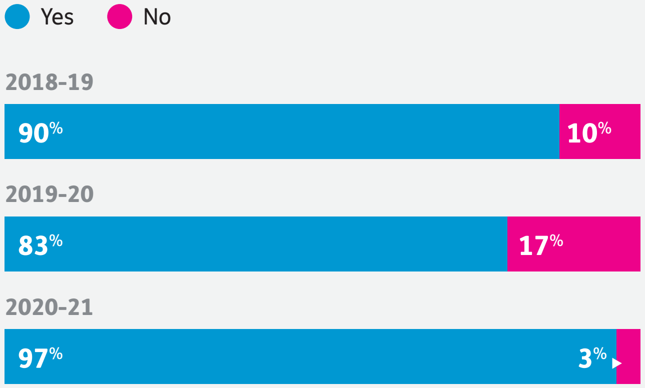
Control testing and monitoring

More than 75% of respondents have some form of testing in place, with others looking to incorporate testing going forward. There was variety in who the testing was performed by, with firms undertaking either 1st or 2nd line testing, or a combination of the two. Across both approaches, firms generally took the approach of sample testing key controls. However, not all firms have a defined mechanism for identifying their key controls or a test plan that specifies what should be tested, by whom and how often.

RCSAs: a variety of approaches

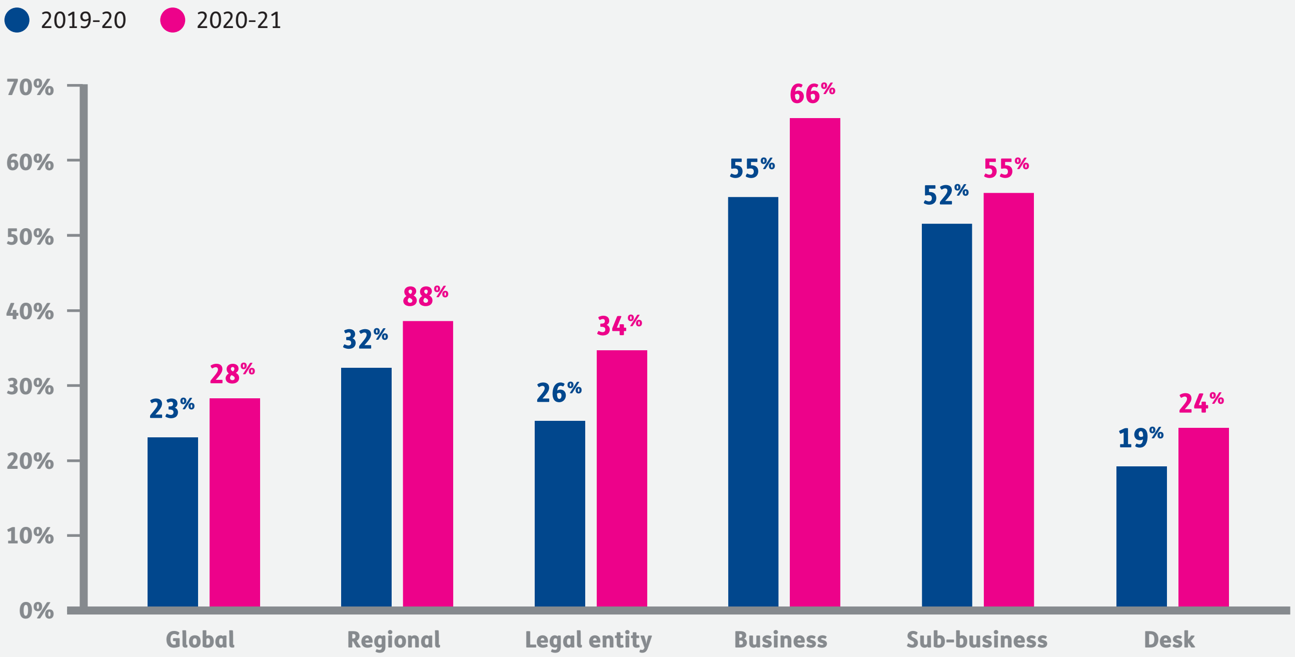
97% of respondents reported that they have a standardised Risk and Control Self-Assessment framework in place, which is an increase of **over 15%** on last year.

Fig. 10: Percentage of respondents who had a standardised RCSA framework in place



The majority of firms undertook RCSAs at business or sub-business level, which is consistent with the results from last year. Once again, the use of desk-based RCSAs was limited to **around 25%** of respondents, but there was an uptick in the use of legal entity RCSAs over the year. This may reflect the increased focus on legal entity restructuring, particularly in the light of Brexit.

Fig. 11: Level of granularity at which RCSAs are performed



As in previous years, the majority of firms employ an annual cycle for reviewing and refreshing their RCSAs. Looking at the trend over the last three years, it is interesting to see how the proportion of firms employing quarterly or bi-annual updates has declined, while the use of trigger-based updates by respondents has increased to **over 40%**.

RCSAs: tracking the changes

We continue to see widespread adoption of a workshop-based approach to RCSAs, albeit with a drop in prevalence versus last year, as some firms look to employ less formal discussions, bilateral meetings or utilise systems instead.

RCSA challenges

> *"[Despite our standardised framework] the granularity of assessment within each RCSA is inconsistent, the hierarchy which drives the requirement is inconsistent. Control assessment is free format and common risks across business lines are rated differently"*
>
> **EMEA Head of Operational Risk**
> Global Investment Bank

Our view: Calibration and collaboration

It will be interesting to see if this trend towards trigger-based updates accelerates in the aftermath of COVID-19. It is important to note that trigger-based updates are only as helpful as the triggers on which they are based. If triggers are calibrated at too low a level, this risks RCSAs not being updated until it is too late, and the RCSA becoming backward-looking, rather than forward-looking.

When it comes to drafting, more informal approaches may be preferred, as opposed to large workshops, as they may involve less prep work and be less time-consuming. This is important given some of the challenges firms face around the time-consuming nature of RCSAs, and around ensuring end-to-end ownership and business buy-in. Nonetheless, in adopting such approaches, it is important that firms ensure they still provide for an active discussion around risk.

A number of firms also noted that they are not doing enough with the output of their RCSAs, with automation being one mechanism for trying to improve this. They also reported challenges around ensuring consistency across the business in performance and quality.

This latter point is surprising given most firms reported that a standardised RCSA framework was in place, and suggests there is scope for further embedding. The role of 2nd line operational risk within the RCSA process is key to enabling this, and we see encouraging signs that the majority of respondents articulated the role of 2nd line as one of oversight, facilitation and challenge.

3 Embedding Operational Risk Management

This section looks at how well operational risk management is embedded within firms. This includes operational risk organisation, governance and reporting, the setting and cascading of risk appetite statements across the business, and the embedding of operational risk into change management processes.

Operational risk teams shrink

As in previous years, the wide range of organisation sizes within our sample means that the size of operational risk functions varies considerably. Even so, a trend of decreasing team sizes continued, with **86%** of respondents reporting an operational risk team of 20 or less personnel, versus **77%** in 2019 and **67%** in 2018.

This shift in the size of operational risk teams is consistent with the analysis from 2018, which forecast a material change in the size of operational risk teams for **over 40%** of firms. Changes are expected to continue to a certain degree, with **almost 40%** of firms still expecting a material change in the size of their operational risk team this year.

However, looking ahead, the overall decline in team size is likely to halt, given a roughly even split between those expecting to increase the size of their team and those expecting a decrease.

Fig. 12: Size of operational risk teams

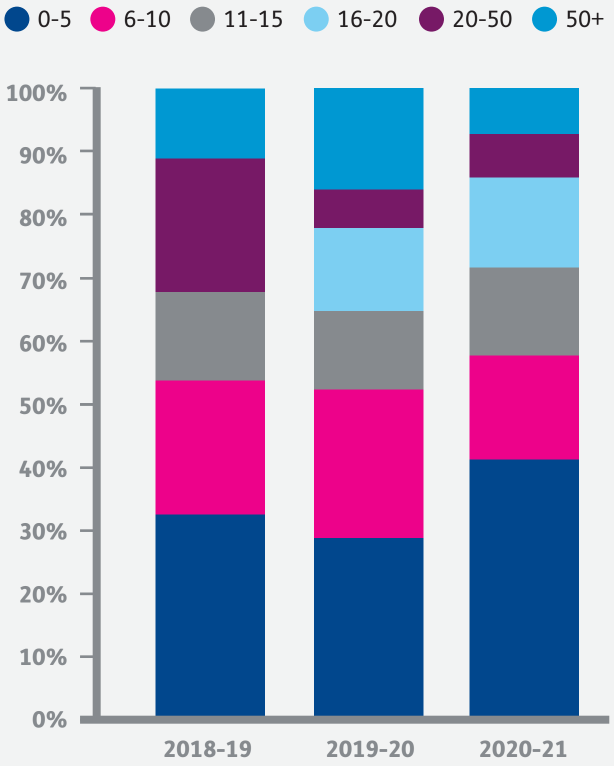
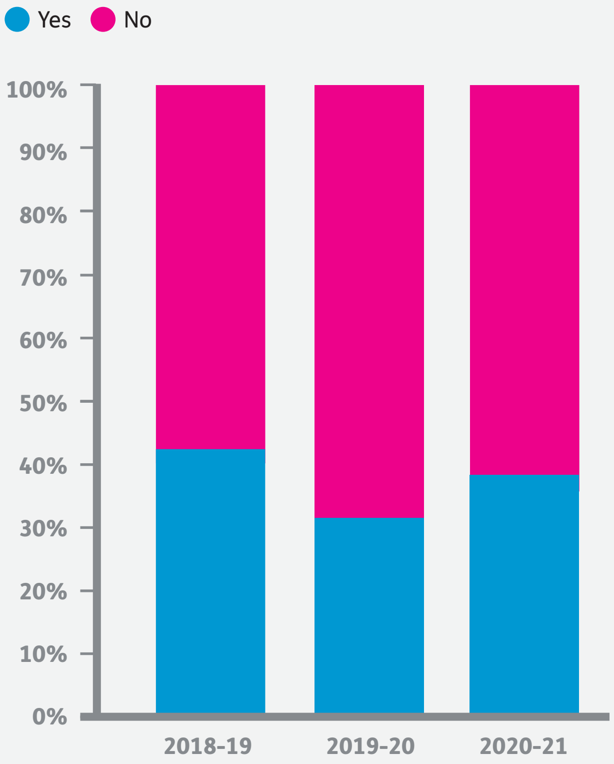


Fig. 13: Percentage of respondents expecting a material change to the size of their operational risk team over the next 12-18 months



Consistent with last year, **almost 80%** of firms reported that they have sufficient knowledge and skills in the team. As such, changes in team size are largely reflective of a need to cut costs, particularly post the COVID-19 pandemic, or conversely to bolster resource in light of an increase in focus on risk.

Ongoing challenge: governance roles

Previous reports have identified challenges in operational risk oversight in terms of the clarity of the role of various governance committees and how issues are escalated.

While a large majority (**90%**) of respondents report robust operational risk governance structures, with forums meeting at an appropriate frequency, challenges remain around membership and attendance at relevant governance committees. A fifth of respondents say that operational risk management responsibilities of various committees and forums could be improved.

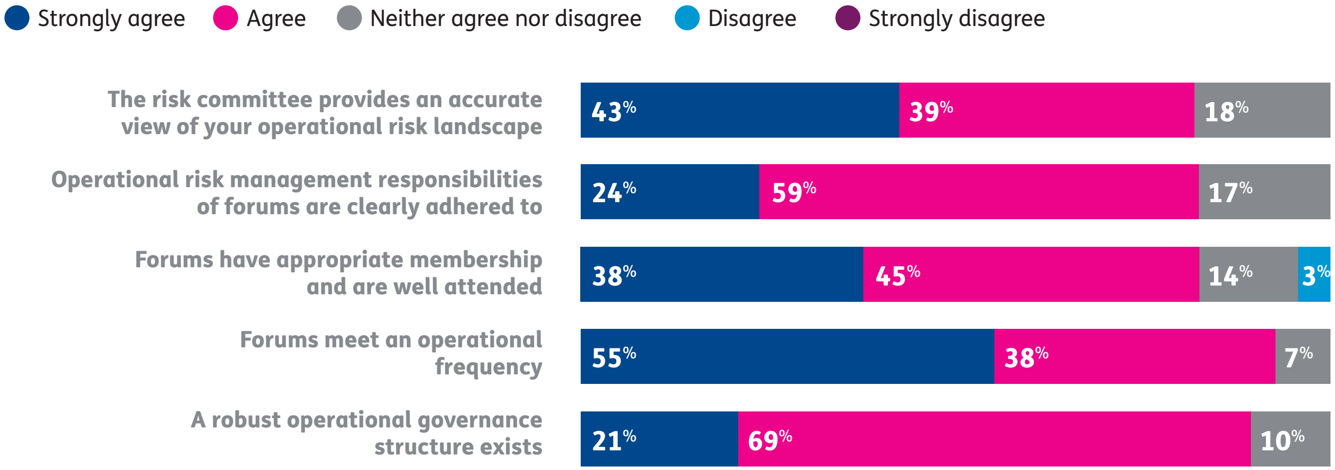
Our view: Define, assess, support

There are great benefits to defining clear roles and responsibilities at both individual and committee level for operational risk, in order to ensure accountability. For individuals, these roles could be included within personal objective-setting, the performance of which can then be assessed as part of performance-management processes.

At a group-level, committee-effectiveness testing can be helpful to assess whether the activities detailed in the terms of reference are being carried out in practice.

In addition, it is important that committees receive the right information to support them in performing their role effectively. Again, this is an area where we have seen firms historically face challenges, although this has been steadily improving over time.

Fig. 14: Respondents' views on their operational risk governance structures



Management information: good progress

More than 90% of respondents felt that management information was regularly received at business line, senior management and Board levels, tailored to the relevant forum it is presented to.

Last year, half of respondents identified enhancing operational risk Management information (MI) as a top area of focus over the next 24 months. The impact of such improvements is starting to come through in the data.

There is a slight deterioration in the prevalence of qualitative and quantitative information in MIs, but a significant increase in the number who reported that key issues are easily identifiable from the MI and that it is used to drive decision-making.

Fig. 15: Respondents' views on whether MI includes qualitative and quantitative information

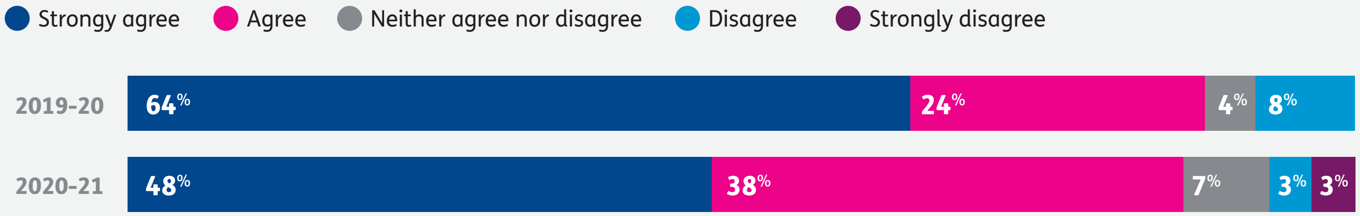
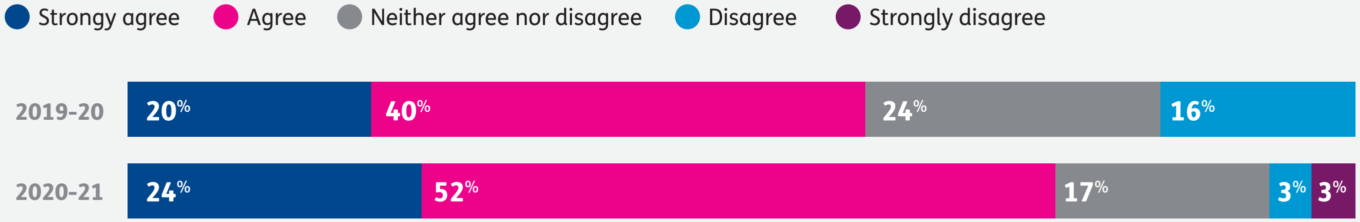


Fig. 16: Respondents' views on whether key issues are easily identifiable from the MI and used to drive decision-making, with escalation thresholds clearly defined and regularly reviewed



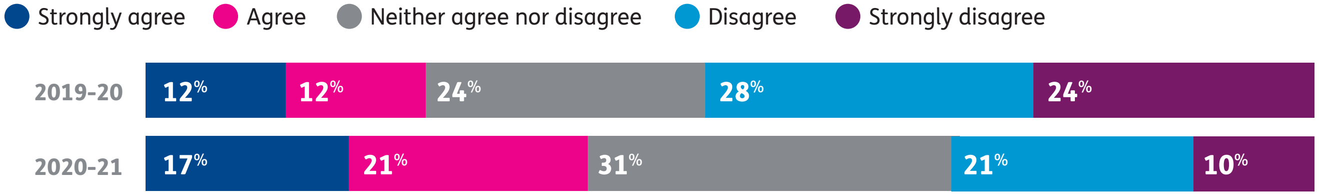
Ongoing challenges: data analytics for MI reports

As with last year, **around 45%** of respondents indicated that there was still some way to go in ensuring that MI encompasses both forward- and backward-looking indicators, which is key for operational risk management to move away from being reactive to proactive.

Furthermore, while improvements have been made, **31%** of respondents still disagreed or strongly disagreed with the statement that MI was easy and efficient to produce, leveraging system capabilities and data analytics, with a further **31%** of respondents neither agreeing nor disagreeing on this topic.

We expect to see ongoing improvements in this area over the coming year as the benefits from investment in analytics tools and system enhancements are realised.

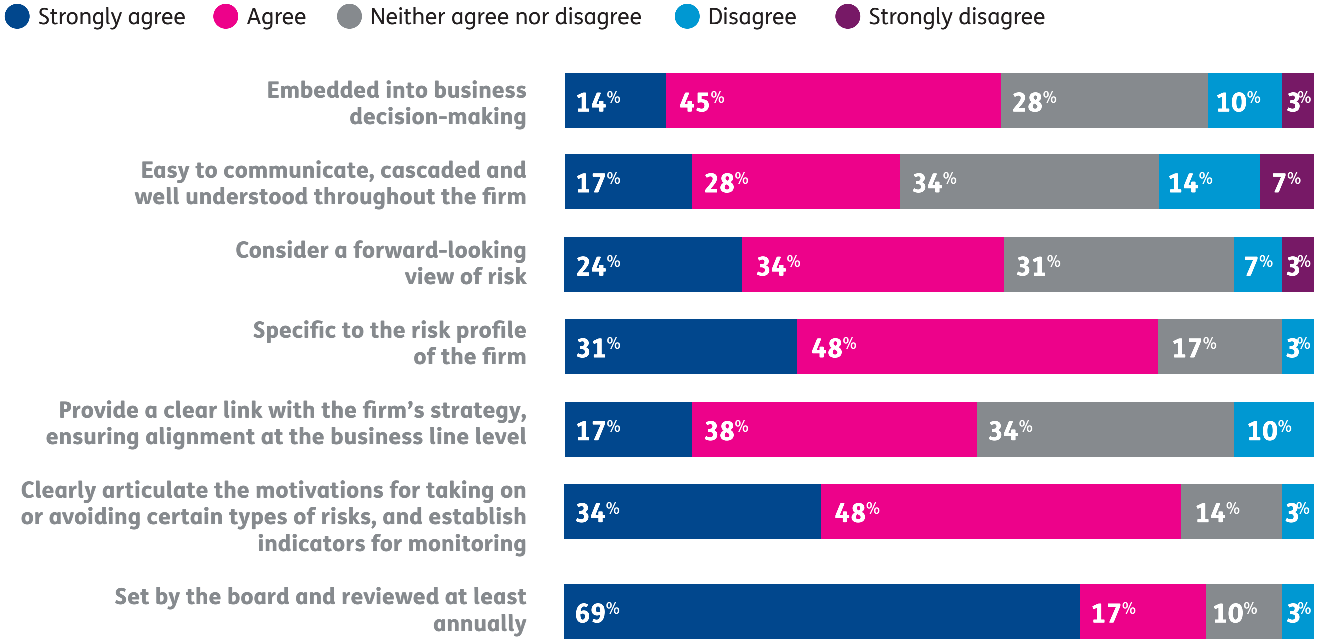
Fig. 17: Respondents’ views on whether MI is easy and efficient to produce, leveraging system capabilities and data analytics



Risk appetite statements

More than 85% of respondents agreed or strongly agreed that risk appetite statements are set by the board and reviewed at least annually. But **just 55%** of respondents agreed that risk appetite statements provide a clear link with the firm’s strategy, suggesting there is still some way to go in ensuring alignment between strategy and risk.

Fig. 18: Respondents’ views on their operational risk appetite statements



Our view: The importance of risk appetite frameworks

The risk appetite framework is key to the embedding of operational risk within the organisation. A strong risk management culture starts at the top of an organisation, with a clear link between a firm's business strategy and its risk appetite, and both Board and senior management oversight. Risk needs to be baked into the way the business operates and into business decision-making, and that means translating high-level risk appetite statements into more granular business-level statements, against which monitoring thresholds and associated key risk indicators can be set.

The responses show that operational risk professionals continue to struggle in implementing their risk appetite framework, particularly when it comes to cascading risk appetite statements throughout the firm and embedding them into business decision-making.

This is perhaps unsurprising as several respondents reported that risk appetite statements are defined at a high level, with only a handful translating these high-level statements into risk appetite statements for specific operational risks, legal entities, departments or segments. This challenge will only increase as firms consider the inter-relationship between risk and resilience, and how risk appetite interplays with impact tolerance.

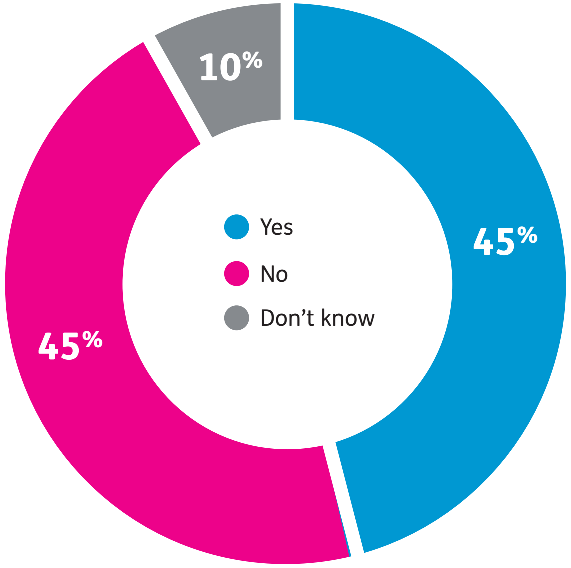
Consistency and quality: room for improvement

Just 45% of respondents reported that they have a quality-assurance programme in place to challenge the consistency of business-unit implementation of operational risk-management tools, measurement activities and reporting systems.

Where this is in place, firms reported the use of various mechanisms to ensure consistency, including the provision of regular feedback from 2nd-line to 1st-line stakeholders on their performance in implementing the risk framework. This may take the form of a more formal independent oversight or validation of operational risk framework compliance by 2nd line stakeholders.

A number of firms monitor and report on metrics around framework implementation, in order to hold business areas to account. These may include basic metrics around the number of RCSAs that are out-of-date or not yet completed. Other firms take a more active role when it comes to RCSAs, with all RCSAs reviewed and approved by 2nd line, in order to ensure they are held to the same standard, with cross-review to ensure issues identified by one business are highlighted to other businesses, where relevant.

Fig. 19: Percentage of respondents who have a quality-assurance programme in place

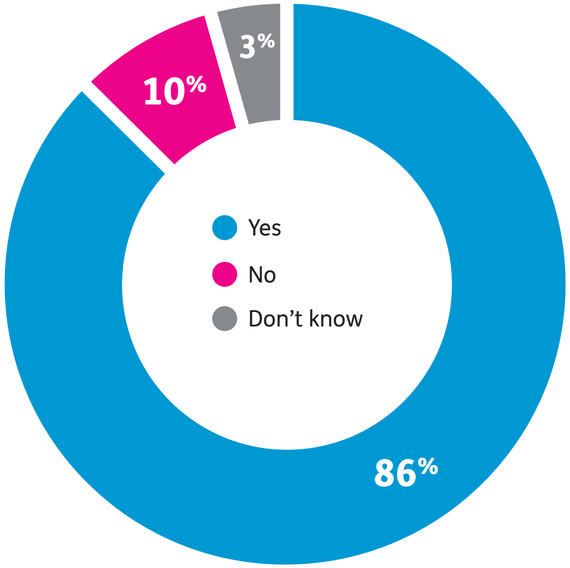


Operational risk and change

In spite of the challenges, **more than 86%** of respondents reported that they have embedded operational risk within their change-management process.

Firms reported undertaking risk assessments on material changes, with operational risks being considered before a change is approved and signed-off. However, some reported inconsistency here, and that further work is needed to embed risk fully into the BAU change framework. For more mature firms, operational risk has a defined role within BAU new product and new business initiative processes .

Fig. 20: Percentage of respondents who have operational risk embedded within their change management process



4 The Future for Operational Risk Management

We concluded the survey by asking which areas senior operational risk professionals will focus attention on in the future.

The highest priorities were standardisation and improvement of RCSAs, as well as operational risk MI, consistent with 2019. This corresponds to the reported challenges around COVID-19 and the "static and BAU nature of RCSAs".

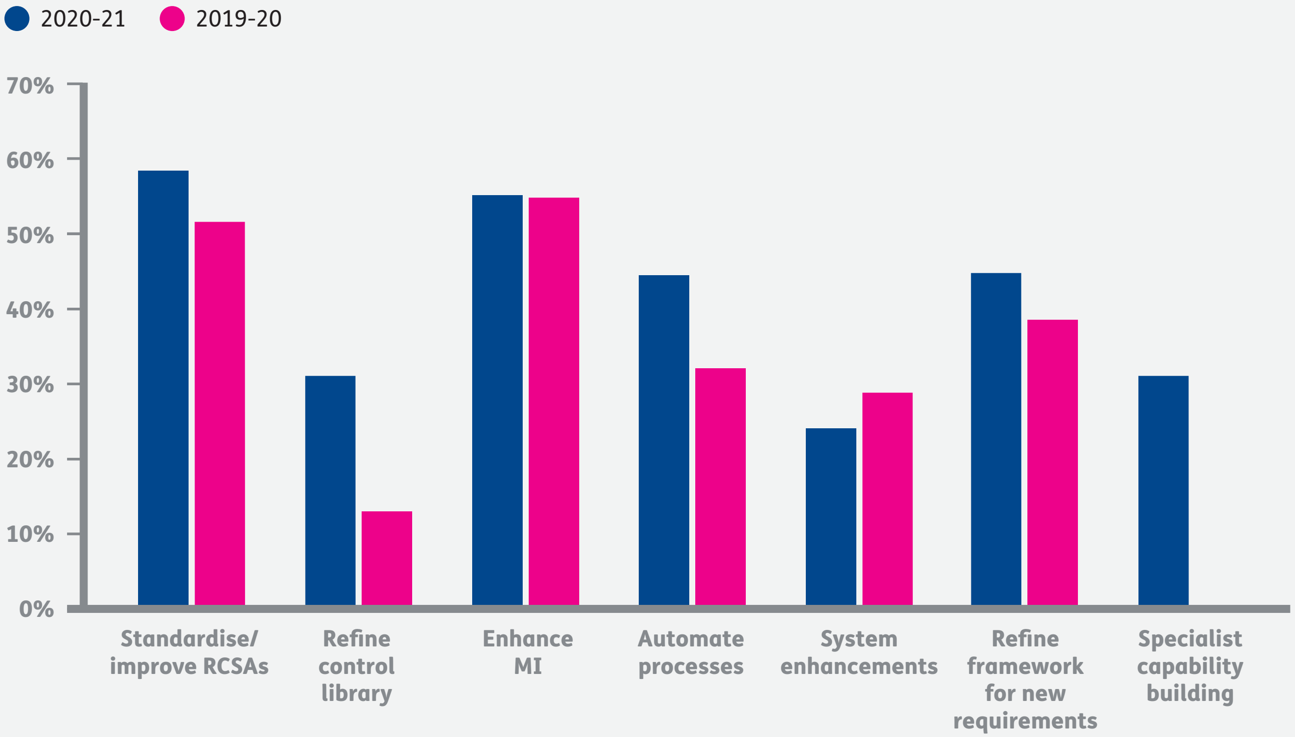
Meanwhile, this year, **the UK regulators have an increased focus on operational resilience and outsourcing and third party risk management.**

Resilience requirements

"Our operational risk framework will be a key tool used to demonstrate compliance with the regulator"

Global Head of Operational Risk
Global Investment Bank

Fig. 21: Top areas of focus for improvement over the next 24 months



The risk and resilience relationship

In 2019, **60%** of firms reported they were refining their operational risk framework in the context of resilience. Evolving regulatory guidance, combined with the COVID-19 real-life test of firms' resilience, means the relationship between operational risk and operational resilience continues to grow. We looked at three areas of interaction between the two concepts: organisational; governance and data inputs.

a. Organisational

In most instances, firms have stood up projects or programmes of work to address the incoming regulatory requirements on operational resilience.

When asked to define the role of operational risk in relation to operational resilience, a handful of firms (**21%**) stated that operational risk is leading or co-sponsoring this work. However, almost half of firms stated that the role of operational risk increasingly focuses on oversight, review and challenge responsibilities.

b. Governance

Many firms have also been grappling with how governance and oversight of operational resilience integrates with that of operational risk. Merging committees have been explored by some firms, especially in the case of smaller firms where attendees for relevant forums are similar.

c. Data

While different data points and MI will be required, firms can look to leverage existing operational risk MI in order to support operational resilience monitoring. Some firms have incorporated resilience into their operational risk framework by adding resilience to their impact taxonomy, in order to better facilitate this extraction of resilience-relevant MI. For firms that have a process view of their risks and controls, this has also provided an accelerator when it comes to mapping their important business services from a resilience perspective.

Risk & resilience working together

> *"Currently, operational risk offers a challenge to resilience [activity]. In the future, [we need] to ensure further alignment between the frameworks"*
>
> **Head of Operational Risk & Risk Appetite**
> Global Investment Bank

> *"We see operational resilience as an outcome of effective operational risk management... [however] at present operational risk's role has not been exactly determined, and there is an element of uncertainty"*
>
> **Head of Operational Risk & Resilience**
> UK Building Society

Our view: Risk and resilience

Defining the interaction between risk and resilience frameworks can be challenging. Operational resilience is an outcome that benefits from the effective management of operational risk – strong operational risk management should reduce the likeliness of resilience issues occurring. Things can still go wrong, however, and the respective framework can help firms better understand the impacts of their operational risk events on operational resilience, and how to deal with them.

There are different ways to handle this, partly dependent on the existing structure of relevant frameworks a firm has. We have seen a range of approaches adopted: most important is that firms do take steps to document and educate on how risk and resilience frameworks, and their key underlying processes, work together. Without this, efforts may appear duplicative or disconnected, causing confusion across the business and damaging overall risk ownership and service resilience.

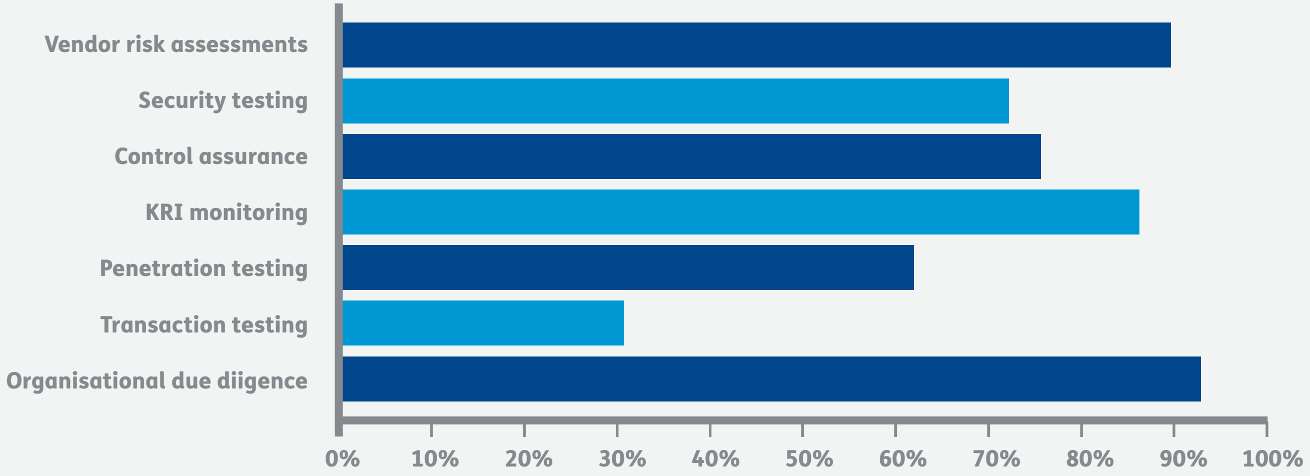
While there may be pragmatic synergies to be found at a governance level, firms must be cautious not to lose sight of the fact that these are related but separate topics, and sufficient airtime is needed for both, with distinct management responsibilities driving the need for different discussions and decisions. It is important that firms define and maintain delineated roles and responsibilities, to ensure clear accountability across these two topics.

Emerging challenge: outsourcing

Outsourcing is another key area of focus for firms, not least given the Prudential Regulation Authority (PRA)'s continuing focus on the theme.

This year, the majority of respondents have multiple processes in place to mitigate operational risk associated with outsourcing. Vendor risk assessments, operational due diligence and KRI monitoring were the most prevalent processes, with **around 90%** of respondents having these in place.

Fig. 22: Percentage of firms that had the following processes in place in relation to mitigating operational risk associated with outsourcing



While **76%** of firms reported that they have control-assurance processes in place, a key discussion point in our operational risk round-table discussion in November 2020 was how the COVID-19 environment has impacted on controls testing. Firms have had to rely on remote testing of controls relating to third party suppliers, rather than performing on-site visits, as well as placing a higher reliance on suppliers' own control testing.

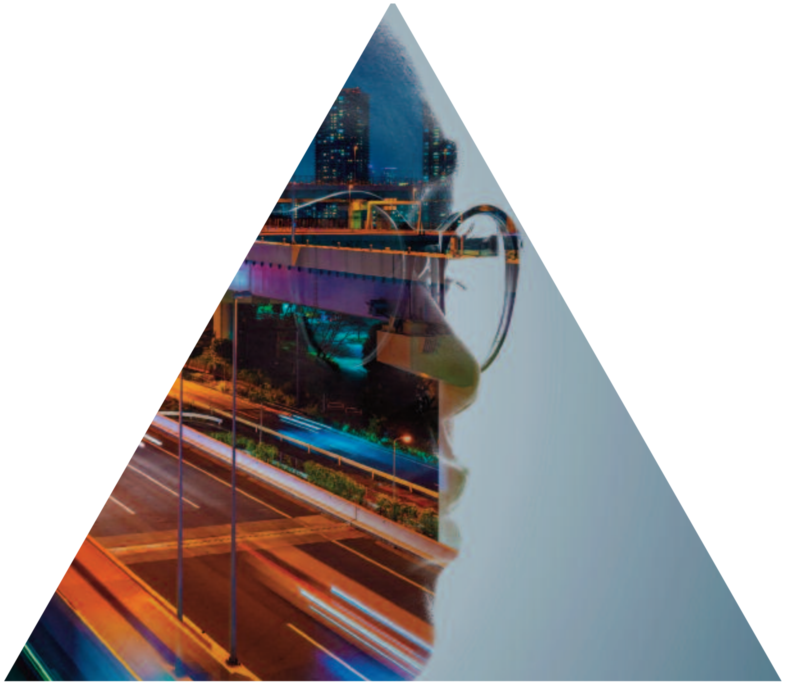
Our view: Embedding risk of outsourcing

Risk needs to be embedded across the engagement lifecycle of an outsourcing arrangement. This includes:

- Upfront processes to make sure there is a clear understanding of the risk and resilience implications of an outsourcing arrangement before the decision is made
- Thorough due diligence and background checks to verify the processes and controls that suppliers have in place to manage their risk
- Contracting provisions to hold suppliers to account and ensure that they provide suitable MI on their performance and enable monitoring of risk incidents
- Ongoing dialogue and engagement to remediate any risk issues and to identify and plan for potential risks on the horizon

We have also seen an increase in the data requests that firms are making of their suppliers, in order to gain a greater level of comfort around the processes and controls suppliers have in place to manage their risk. As firms also look to understand the resilience profile of their suppliers, we can only expect those data requests to continue going forward. Industry initiatives to develop a supplier certification or a standardised set of minimum data requirements that suppliers should provide are positive: however, firms need to make sure that they still ask the challenging questions and do their own due diligence, rather than taking such things at face value.

Baringa
Brighter together



Baringa Partners

Baringa Partners is an independent business and technology consultancy.

We help businesses run more effectively, navigate industry shifts and reach new markets. We use our industry insights, ideas and pragmatism to help each client improve their business. Collaboration is central to our strategy and culture ensuring we attract the brightest and the best. And it's why clients love working with us.

Baringa launched in 2000 and now has over 700 members of staff and more than 65 partners across our practice areas Energy and Resources, Financial Services, Products and Services, and Government and Public Sector. These practices are supported by cross-sector teams focused on Customer & Digital; Finance, Risk & Compliance; People Excellence; Supply Chain & Procurement; Data, Analytics & AI; Intelligent Automation & Operations Excellence; and Technology Transformation. We operate globally and have offices in the UK, Europe, Australia, US, Middle East and Asia.

Baringa Partners have been voted as the leading management consulting firm in the Financial Times' UK Leading Management Consultants 2020 in the categories energy, Utilities & the Environment, and Oil & Gas. We have been in the Top 10 for the last 13 years in the small, medium, as well as large category in the UK Best Workplaces™ list by Great Place to Work®. We are a Top 50 for Women employer, and are recognised by Best Employers for Race.

Baringa. Brighter Together.

For further information please contact:

Salina Ladha
Director – Finance, Risk and Compliance
salina.ladha@baringa.com

Guy Munton
Partner – Finance, Risk and Compliance
guy.munton@baringa.com

www.baringa.com/reframeresilience