THE INSTITUTE OF OPERATIONAL RISK

Center for Financial Professionals

GLOBAL PERSPECTIVES ON OPERATIONAL RISK MANAGEMENT AND PRACTICE

A survey by the Institute of Operational Risk (IOR) and the Center for Financial Professionals (CeFPro)

March 2018

WHO WE ARE

THE INSTITUTE OF OPERATIONAL RISK

The Institute of Operational Risk is an international body focused solely on the discipline of operational risk. The Institute seeks to support those who have an interest in operational risk by developing research, discussion and sound practice guidance. The Institute offers webinars, events and access to publications while supporting education via their accredited programme, The Certificate in Operational Risk Management.

Full details can be found at www.ior-institute.org

Center for Financial Professionals

The Center for Financial Professionals (CeFPro) is an international research organization and the focal point for financial risk professionals to advance through renowned thought-leadership, unparalleled networking, industry solutions and lead generation. CeFPro is driven by and dedicated to high quality and reliable primary market research; helping us provide our audience with invaluable peer-to-peer conferences and knowledge sharing Risk Insights platforms, such as: Webinars, research reports, articles and also, a quarterly financial risk and regulation magazine.

Full details can be found at www.cefpro.com

CONTENTS

PREFACE & RESEARCH METHODOLOGY

The Operational risk practice is going through a process of continual change. The significance of operational risk losses continues to grow in importance as large losses are experienced by institutions across the globe. Furthermore, the risk types and categories of most significance to operational risk modeling and capital management are also evolving, especially with the onset of cyber risk and cyber-related crimes.

The objective of the survey was to develop an understanding of the dynamic and evolving nature of the operational risk management practice from industry practitioners. In this regard, we focused on developing a survey that would target the following core aspects of operational risk, both at present, as well as possible directions in the future:

- Current best practices and approaches to operational risk;
- tools and skills being applied in practice; and
- the directions the discipline may go in the future.

The survey was designed by members of the Institute of Operational Risk (IOR) and facilitated and collated by the Center for Financial Professionals (CeFPro), with basic analysis primarily undertaken jointly by IOR and CeFPro members.

We believe the survey represents the most comprehensive analysis of its kind, assessing the current status and future development of the operational risk discipline.

SUMMARY OF THE SURVEYED POPULATION

The survey comprised respondents drawn from IOR members, CeFPro Risk Insights subscribers and attendees of CeFPro events. It was completed as an online questionnaire, as well as with attendees at events in Europe and America, between October and December 2017.

While the majority of responses came from the USA and UK, responses were also received from over 600 respondents, spread across 58, countries including some as diverse as: Albania, Australia, Sudan, Singapore, India and China. Most major European centers were also included - the spread of countries makes this a truly diverse international survey.

What industry do you work in?

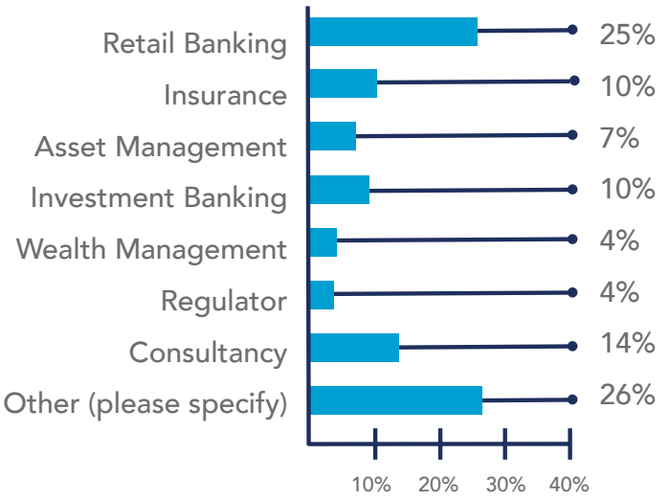

Figure 1

Figure 1 shows the breakdown by industry of responses received. Within the significant number of "Others" (26%), there were also responses from financial services and related areas such as FinTech, payment and services, microfinance, central banks, mutual funds, legal, pensions, clearing and settlement, tax, audit groups, software and IT, and ratings agencies. Outside financial services, a relatively small number of respondents came from travel and hospitality, education, manufacturing, medical and not-for-profit organizations. Respondents therefore represented a wide cross-section of industries, the great majority from financial services.

Figure 2 demonstrates that we also captured a broad spectrum of experience ranging from those relatively new to the area of operational risk, through to established career professionals in senior roles. Given the discipline really only started just over 20 years ago, it is impressive that a third of respondents have been in operational risk for more than 15 years and that a further third have been in operational risk for more than 8 years.

Respondents were asked to classify their role by practice area. The great majority of respondents (67%) were risk management professionals, followed a long way behind by business-oriented roles.

Given the importance for operational risk professionals to understand regulatory requirements, it is not unsurprising that, when asked about their familiarity with regulatory guidelines, approximately half the sample of respondents were very familiar with operational risk regulations and requirements and the other half at least basic familiarity. Only a very minor number of respondents answered non-familiarity or non-relevance of such regulations to their role.

Given such a significant cross-section of experienced operational risk practitioners, we believe these research findings offer valuable and valid insight on the discipline.

How many years of experience have you had in similar or related roles to the current role you are performing?

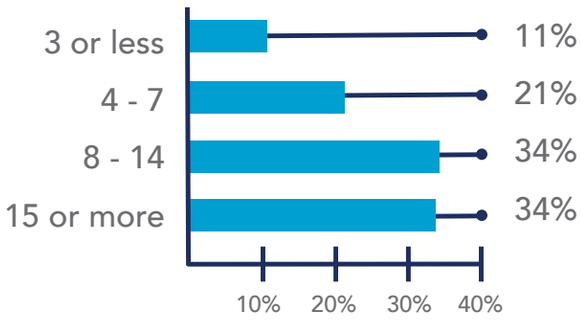

Figure 2

THE WORKPLACE ENVIRONMENT IN WHICH OPERATIONAL RISK OPERATES

In this section, we highlight the characteristics of the workplace and operational risk environment in which respondents operate. In Figure 3, we demonstrate the size of the operational risk function in the respondents' organization by the number of FTE dedicated to operational risk. Further research is required to understand what is meant by respondents' perceptions of 'dedicated' to operational risk, as functions often comprise systems support and analytics/reporting. Analysis should also be undertaken to understand whether numbers quoted are only 'central' functions, or comprise all resources performing aspects of operational risk, whether in the business or elsewhere. The findings, given the numbers reported at the higher end, may suggest the wide spread use of the internationally recognized 3 Lines of Defense Model; however, we would not wish to assume this to be the case (see Figure 9 also).

How many employees are dedicated to working on the operational risk function in your organization?

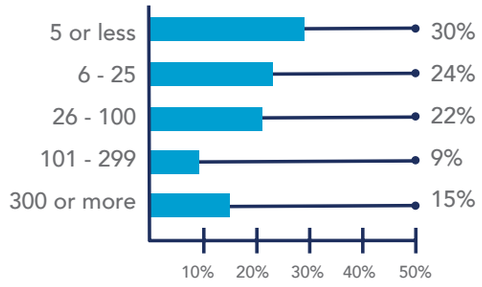

Figure 3

Select any of the following risk categories if they are included within your organizations' operational risk framework (multiple choice).

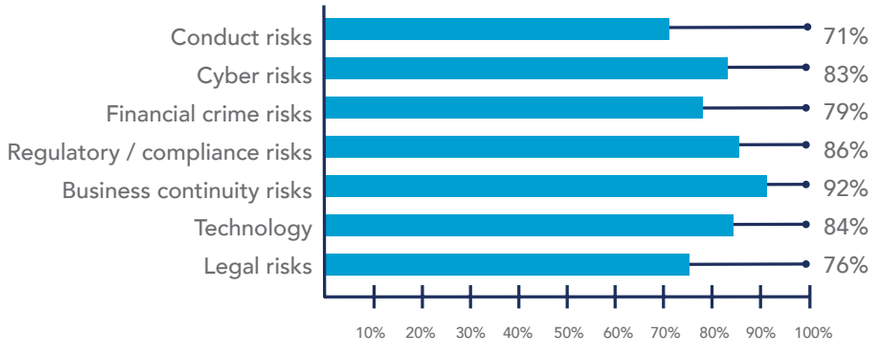

Figure 4

It is also relevant to gauge the scope and breadth of operational risk practice in respondents' operational risk frameworks. In this question we allowed respondents more than one response and we see that a wide range of risk categories are represented, see (Figure 4). It is both interesting and encouraging that all categories are included in the operational risk frameworks for over 70% of respondents' firms. Unlike more traditional risk types, organizational definitions and the scope of operational risk remain fluid. The results of this survey highlight a more defined insight into the broad remit and criticality of the function.

In Figure 5, we highlight the development status of operational risk management as a practice within their organization. Noting that the survey largely reflects the position in financial services, we see that the majority of respondents (72%) report that operational risk systems, practices and risk management were "in use" or "mature", with 22% in implementation. This is consistent with the focus on implementation activity driven by regulators since the early 2000s. However, there is a suspicion that frameworks, once established, tend not to be challenged, despite a constantly changing environment.

Which of these statements best describes the status of operational risk in your organization?

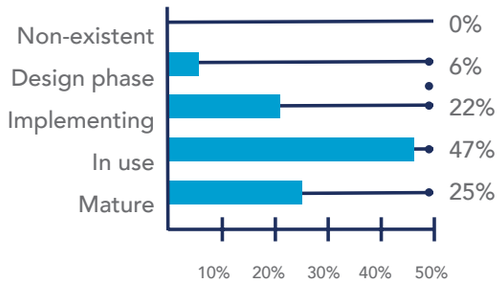

Figure 5

Another interpretation may be that the 'designing' and 'implementing' responses could, in fact reflect activity aimed at upgrading or further maturing existing "in use" frameworks. Furthermore, with the forecast change of regulations to an SMA methodology, previous non-AMA banks may require similar AMA systems to model complexity and data, thus driving this response. Again, perhaps further research would be helpful on this as no commentary is provided on the "quality" of the frameworks implementation, either from self-assessment or independent review via regulators and others.

FRAMEWORK APPROACH AND BOARD PERCEPTION

Which of the following statements best describes your organization's approach towards operational risk frameworks and toolkits?

Figure 6

The survey also sought to understand the respondent firms' approaches to operational risk innovation, as opposed to basic regulatory compliance. In Figure 6, we see that the majority of respondents report that the primary objective of their firm is to align with standard practice within their industry which, given the wide breadth of industries represented, could indicate a diversity of practice. However, the second highest response (26%) showed that respondents were aiming to innovate and be leaders in industry best practice. This and the next largest response, which relates to "develop bespoke solutions", shows a generally outward and innovative approach by practitioners.

It is worth highlighting that just under 10% take a de minimis regulatory driven approach.

The operational risk profession has grown and developed over the last few years. With new challenges in the industry, the increasing demands within organizations and the increasing oversight by regulators, there is an acceptance that growth and innovation is required. Nearly half of the respondents (46%) stated that their role was not only to comply with regulatory requirements, but to drive revenue while also minimizing business disruption (see figure 7).

Which of the following best describes how operational risk management is perceived within the organization by Board and senior executives?

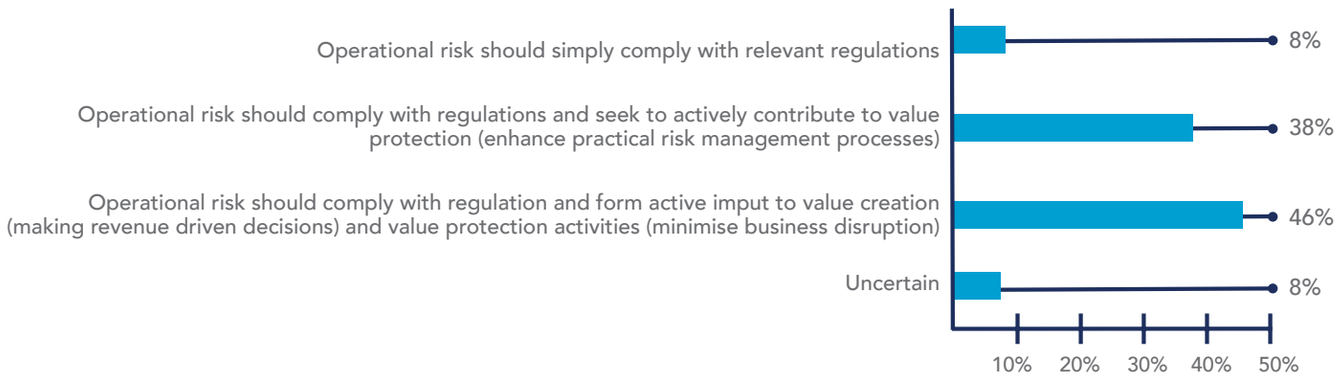

Figure 7

It is also important, given an accepted need for an appropriate "tone from the top", to gauge the significance given to operational risk management and practice at the senior executive level of respondents' firms. In Figure 7, we show responses to this topic, indicating that the majority of respondents considered that their senior executive management had the perception that operational risk should not only comply with regulation, but form an active input to value creation. It begs the question as to whether Boards and senior management are aware of the innovative tendencies of their operational risk managers, as indicated in Figure 6. Certainly, the responses shown in Figure 7 indicate that operational risk has moved beyond the phase of simple regulatory compliance to a valued component of decision-making.

Operational risk in my organization is…

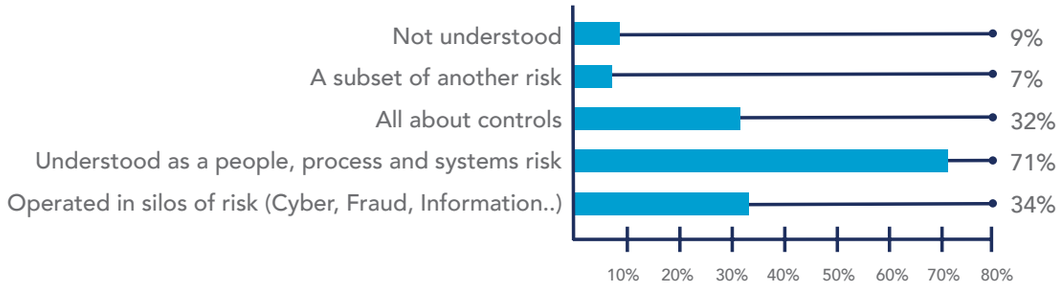

Figure 8

In a related strand of questioning, we also tried to discern additional perspectives on the role of operational risk in respondents' institutions, where they may respond to more than one category selection relating to the perception of operational risk. The specific selections offered, and their responses, are provided in Figure 8. The clear and unsurprising majority of respondents (71%) identified their organization's perception of operational risk as focusing primarily on people, processes and system risk a more traditional perception of operational risk, even with the broadened remit highlighted in Figure 4. The second two dominant categories selected were: operational risk is a control-driven discipline or that it is often operated or implemented in practice in silo-based structures, rather than uniformly integrated across an institution. This is an interesting point to raise regarding change management and governance structures, as well as understanding the relationship of these responses within the context of responses related to Figure 5 (operational risk development) and Figure 6 (relating to innovation).

Select the option most relevant to the governance structure for operational risk management in your organization

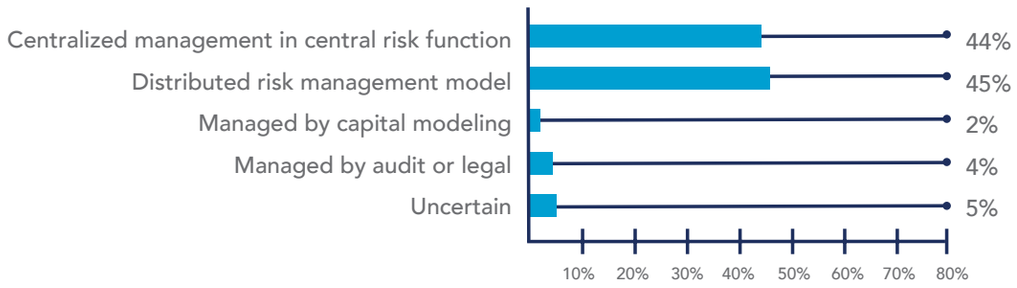

Figure 9

The survey then sought to learn about the governance structure of the respondents' organizations and how they are structured with regard to operational risk. Figure 9 shows that the majority of respondents identified their governance structure, perhaps inevitably, as one of two structures: the leading one being a central risk function, with the second being one where operational risk was distributed throughout the organization. Further research may help understand if this reflects the widely used 3 Lines of Defense Model, with a central function providing frameworks and tools and embedded ownership of risk management in the 1st Line business areas. What is clear though, is that the majority of respondents, (88%) have the dual task of centralized management in a risk function center, while also balancing a distributed risk management model.

What is the objective of your approach to operational risk? Select all that apply (multiple choice):

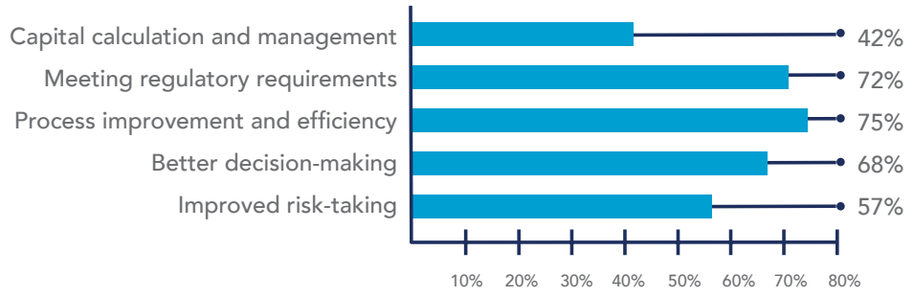

Figure 10

In Figure 10, respondents were given the option to select one or more categories for their response as to what was relevant to their firm's operational risk management, seeking responses regarding the core objective of their approach to operational risk. The leading category was process improvement and efficiency, closely followed by meeting regulatory requirements and improved decision-making. These findings are consistent with Figure 7 where operational risk is described as regulatory compliance, alongside both value protection and creation. Interestingly, when given the option to choose more than one, the results appear to conflict with Figure 6. The role of the operational risk professional appears to require regulatory compliance and process improvement, but increasingly to ensure a better decision-making process and active input to value creation. Of note, therefore, is that improved risk-taking falls near the bottom of the list, albeit with a 57% response.

Rank these in order of preference when recruiting operational risk resources. 1 being of high preference, through to 5 being of low preference:

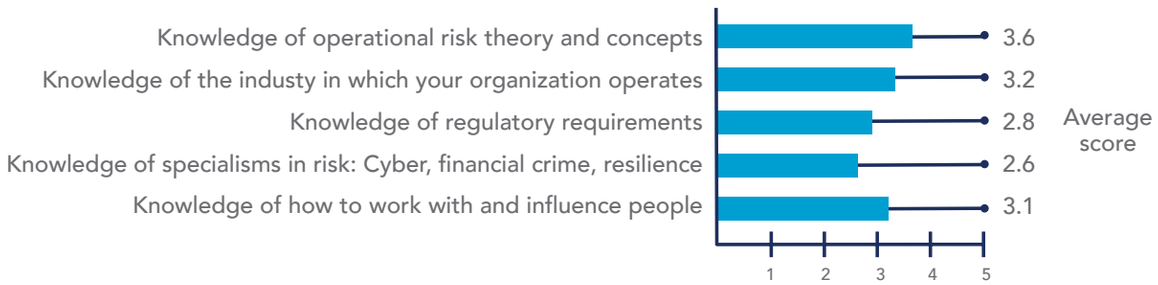

Figure 11

The next question related to the skill sets that respondents identified as leading attributes of individuals they would seek to hire in an operational risk role in their organization. Figure 11 demonstrates that most respondents believe the required leading skill to be knowledge of operational risk theory and concepts, followed by a knowledge of the industry in which they would be working. Interestingly, despite identifying cyber as the major development in the future (see Figure 15) and highlighting it as a major risk (Figure 4), recruitment of specialists, such as for cyber, came last in respondents' criteria. They were more consistent in looking for resources who could influence people, having acknowledged in Figure 8 that operational risk is a people risk.

An interesting conclusion is that although many of the headlines, and potentially future operational risks, focus on areas such as cyber risk or financial crime, respondents were clear that knowledge of the industry they worked in, and operational risk theory and concepts more specifically, currently ranked more important than future risks. In fact, the ability to influence and work with others ranked higher than the knowledge of regulatory requirements or specialism, such as cyber risk or financial crime.

OPERATIONAL RISK DATA AND INPUTS

In this section, we explore the aspects of data collection, data use and modeling in respondents' organizations. In Figure 12, we show respondents' views on the role played by scenario analysis in their operational risk management. Most respondents (43%) clearly identified that, at this stage, scenario analysis is only utilized indirectly in their decision-making process. With scenario analysis typically used across the industry in almost all risk disciplines, and with 69% of respondents using scenario analysis either directly or indirectly in decision making, it may be of concern to some stakeholders to see 21% not utilizing their value at all. This, together with the significant percentage who use scenarios indirectly for decision making, suggests the real benefits are not being understood or realized.

In your experience, how important is the role played by scenario analysis in operational risk management?

Figure 12

In your experience, how important is the role played by Key Performance Indicators, Key Risk Indicators or Key Control Indicators (BEICFs) in operational risk management?

Figure 13

With regard to the role of indicators (Figure 13), 43% of respondents identified that they were used directly in decision-making double the amount for scenario analysis. This reflects the previous results indicated in Figure 7 and questions the level at which decisions are being taken, whether at process or Board level. Responding later in the survey to question 23, approximately 30% of respondents indicated that operational risk 'model outputs' were highly significant to their decision-making processes and business practices; only 3% of respondents indicated that operational risk was unimportant for such decision-making processes. This chimes with previous results seen in Figures 7 and 8.

In addition, approximately 15% of respondents claimed that models used to quantify operational risk were directly used in operational risk management practice and decision processes. However, approximately 14% of respondents indicated that, in their opinion, the output from operational risk modeling had no bearing on the management practice of the decision process, indicating clear differences between measurement versus management approaches to operational risk in these organizations. Further research after the proposed regulatory changes on the focus on models, and how that change will transpire, would be interesting given these statistics.

CLASSIFICATION, STANDARDIZATION AND COLLECTION FRAMEWORKS

A number of respondents identified the increased need for organizations to focus on improving the classification and collection frameworks for such operational risk data, with many responses relating to taxonomy and centralization of data collection.

HERE ARE A REPRESENTATIVE SAMPLE OF RESPONSES:

"Centralized data sources used within our company. Databases developed to pull data from disparate systems drives enhanced reporting relied on for decision-making."

"Better source systems, taxonomy to ensure consistency in interpretation."

"Better analytics and data management."

"Consistent taxonomies, better quality data and use of external benchmark data."

"Internal data - Clearly defining operational risk losses for ground level as a part of mandatory training just like InfoSec."

"System improvement to collect relevant and good quality data. Provide training to staff and ensure participation of the 1st and 2nd Lines of Defense in the risk and control assessment."

"Regular reviews of metrics, measurements and thresholds, in order to assess gaps and automation."

"Increased clarity on senior level ownership of operational risk data will help drive further enhancements to quality and level of accountability."

When respondents were asked to comment, based on their experience, on how the collection of operational risk data (internal and external losses, scenario analysis and BEICFs) could be enhanced, an interesting array of responses was received.

The three main themes were:

- Classification and collection frameworks;
- automation and standardization of indicators; and
- regulatory guidance and requirements.

Further research would be worthwhile to expand on these themes and the role of other framework elements, such as an RCSA, in supporting operational risk management.

REGULATORY GUIDANCE AND REQUIREMENTS

A separate but related theme was identified as respondents offered their perception of a need for regulators to be more specific on guidance, especially regarding BEICFs and their standardization, collection and use in models.
See below excerpts from the responses received:

"Clear guidance in how the data should be captured, including what data should be captured."

"Clear rules and guidelines on how to capture risk data, and training for those recording risk events. More use of indicators."

"Improvement of data standards, data definitions, data aggregation."

"Consistent terminology and agreed upon KRIs, monitoring, and reporting."

When respondents were asked, based on their industry and sector experience, to list the three most significant sources of loss in the Basel II operational risk event types for their institution, the following emerged:

- Fraud (external and internal) - 23%;
- execution, delivery and process management - 19%; and
- clients, products and business practices - 11%.

THE FUTURE OF OPERATIONAL RISK

In this section, we sought respondents' views in regard to their future expectations of the development and impact of operational risk in the future, with a particular focus on resources. While many would recognize the importance of operational risk, there is a belief amongst some industry practitioners that it still lags behind credit, market and compliance in both profile and support. Therefore, we thought it important to gain the opinions of practitioners on their views of operational risk over the coming five years.

In Figure 14, we summarize the views of operational risk resources in their organizations. It is clear that, overall, most respondents anticipate the number of operational risk resources increasing in future. This is consistent with the importance of operational risk as a core risk class and the growing focus on conduct and behavior issues that may lead operational risk to surpass market and credit risk in its significance. The future risk challenges, such as cyber risk and financial crime, are shown as growing concerns within the survey, along with growing operational best practice. This could indicate why 38% of respondents believed that operational risk resources will increase over the coming years. As noted earlier within Figure 8, it is predominantly considered a people risk. This was followed by the perception that specialist risk resources will increase, again highlighting the significance of the growing concern of specialist areas under the operational risk umbrella, including cyber and information security amongst others.

Choose the option which best describes how operational risk resources in your organization might evolve over the next 5 years.

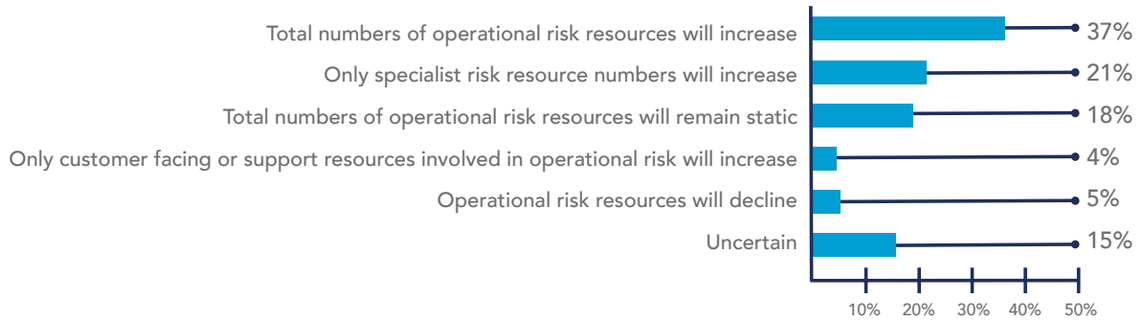

Figure 14

Rank in order of significance the following categories that you foresee an operational risk manager having mastery of in 5 years' time. 1 most significant, 7 least significant

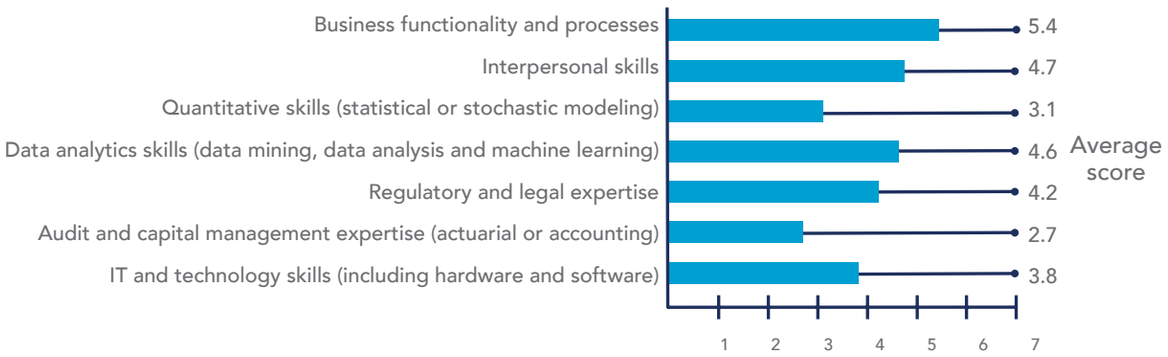

Figure 15

In Figure 15, we show what participants believed were critical skill sets for operational risk managers over the coming five years. The leading attribute identified by respondents, who were asked to rank their selections, was an understanding of business functionality and processes followed by interpersonal skills and data analytics skills (which included aspects of machine learning and statistical data analysis). Aspects of regulatory and legal expertise were typically ranked third, followed by IT and technology skill sets. For now, it seems the day-to-day business functionality and processes were of key importance, though the increasing IT, technology, machine learning and data requirements are areas for future concern and discussion.

Rank the following categories from most significant to least significant for your organization over the next 12 months, (1 most significant, 6 least significant).

Figure 16

In Figure 16, we present views of operational risk development in the near future, looking at a twelve month horizon. Respondents were asked to rank their view on key priorities for operational risk development within their organization. The leading focus in the next year seems to be primarily the continued development of operational skills and knowledge of employees, followed closely by the improvement of operational risk frameworks and processes. Meeting regulatory requirements was systematically ranked down by respondents when assessing the most significant categories over the next year, suggesting that regulation related to frameworks has been stable for a time, or change such as the SMA has either to work through, or may have limited impact. Emerging areas such as cyber and financial crime have been highlighted, technology solutions rated lowest on the scale. Despite in the future 21% in Figure 14 who thought specialist resources would increase. Technology solutions to counteract some of these emerging threats ranks lowest on the priorities over the next 12 months.

DATA, ANALYTICS AND AUTOMATION

The vast majority of expressed views about the next five years in the sectors surveyed included a clear indication of the dominance that people perceive of big data, data analytics and machine learning in transforming the automation and interpretation of operational risk data. In addition, many conceptualized a risk universe in which automation by such methods would also feed more directly into risk processes and management, as well as setting risk appetites from the top executive level through to day-to-day business risk managers' decisions and actions. A sample of responses below provides an insight:

"A discipline leveraging technology to enable risk resources to be more focused on proactive risk management (vs current fire-fighting reactive mode)."

"With the rise of machine learning and AI… the focus will shift more to the human factors that affect risk."

"Data-driven - support strategic decisions through the use of data and technology. AI (Artificial Intelligence) may start to change things."

"It will be manager level positions with the data and reporting functions belonging to the lines of business or being done by systems. Risk identification will be partially automated with AI and individuals employed within area will have to understand how to make strategic tactical decisions."

"The key challenges will be:
- The business still doesn't see the benefits of complying with all the OR framework requirements and there will be a push back based on appropriate allocation of resources; - Much greater demand for specialized operational risk resources (cyber, data security, third party management, etc.) and therefore business oversight will become reduced in coverage and quality;
- Need to apply AI/machine learning to reduce the cost of compliance with operational risk frameworks;
- Getting quality risk information out of systems designed for risk data input will still be difficult regardless of the promises of data lakes and oceans and the next generation of business intelligence tools."

FUTURE DEVELOPMENTS IN OPERATIONAL RISK

Apart from data analytics and AI, some main themes emerged:
One was that operational risk would consolidate a number of risk areas, including third party risk, as well as cyber, conduct and reputational risks. One respondent suggested, "ORM framework will evolve into a GRC framework covering all non-financial risks". Another, similarly, stated that operational risk will "take a leading role in the context of Enterprise Wide Risk Management / Non-financial risks".

As a result, there was a general view that operational risk would play a more important role at senior management and Board level agenda, and as one respondent put it, "A more integrated and engaged conversation of operational risk driving strategic decision-making." In addition, following that, working alongside business strategy to determine risk reward when creating or establishing new business activities.

Another theme highlighted by a number of respondents was the continually changing environment and the need for operational risk to be nimble and be constantly horizon-scanning.

Finally, also highlighted was the importance of 'Experienced risk managers with well-developed interpersonal skills.' It is not only a people risk in itself, but operational risk professionals also need people skills to be able to communicate effectively.

THE PROFESSIONALIZATION OF OPERATIONAL RISK

When questioned on professional development and attainment of professional certification in risk management, we see that the majority of respondents reported that their respective organizations actively supported the attainment of professional qualifications in risk management.

THE PREFERRED OPTIONS THAT AROSE MOST PROMINENTLY INCLUDED:

- IOR CORM
- GARP/FRM
- CISI
- IRM
- CRISC, CISM, CISA, CISSP
- CERTIFIED RISK ANALYST (CRA) CERTIFIED RISK MANAGER (CRM)

However, given the current and future challenges, over a third of respondents (39%) stated that their organization did not encourage the attainment of professional certifications in risk management. Given the ever-increasing importance of the operational risk professional, and the ever-increasing demands, where do professional industry standards get set?

In order to foster knowledge exchange, guidance on best practice and awareness of emerging issues, we asked respondents to identify if their organization supports or encourages participation in industry initiatives such as operational risk workshops and conferences. The majority of respondents (47% occasionally and 33%) regularly work in organizations which encourage participation in conferences and workshops. This, together with their support for 'certification', suggests an increasingly outward and long-term view. They would like professional and industry bodies to contribute to the development of the operational risk discipline from the perspective of practitioners.

It was clear from these responses that the vast majority of respondents saw the role of such networks and professional institutes, such as the IOR and CeFPro, as critical components to further the development of best practice, regulatory and standardizations of practice.

CONCLUSIONS

As regards the current status and approach to operational risk, it is evident that it has gone well beyond regulatory compliance. Operational risk is seen by senior management, including Boards, as a value-added discipline, helping to improve and make more efficient processes and informed decision-making.

What is also encouraging to see is the impetus for innovation and seeking best practice beyond practitioners' own industries. Operational risk professionals are outward-looking and are keen to develop the discipline through industry fora and professional bodies.

When it comes to data and inputs, there is a clear sense of a need for consistency of taxonomies. There needs to be more conversations within the discipline and, to an extent, with regulators on this. Collection of data is another current priority; the comments about the future on AI, machine learning, data analytics and automation point to the solution, but also raise a number of interesting points and questions, in addition to the need for more sharing of information.

Looking to the future, there seemed to be a general consensus that operational risk would consolidate a number of risk areas and, as a result, would play a more important role at senior management and Board level and drive strategic decision-making.

A number of respondents highlighted the fact that the environment is continually changing and operational risk professionals need to be nimble and be constantly horizon-scanning. As has been said a number of times in this report, operational risk is a people risk. Operational risk professionals also need people skills to be able to communicate effectively, influence others and make the opportunities outlined above happen.

The report also recognizes the need for operational risk practitioners to be skilled, knowledgeable and credible, with the growing complexity demanded of practitioners driving a desire for the attainment of formal qualifications.

In summary, we believe this research shows that...

> "Operational risk tools and frameworks are well-established. There is a recognition that data sets and what influences them need to be improved as a core enabler for the future, and those involved in the future of operational risk will be expected to be even more capable and qualified."

This article is designed as an industry facing report version of an associated research report available on SSRN at the following address:
Peters, Gareth, Global Perspectives on Operational Risk Management and Practice. A Survey by Institute of Operational Risk (Ior) and the Center for Financial Professionals (Cefpro) (March 5, 2018).
Available at SSRN: https://ssrn.com/abstract=3134925