




# European Insurance CRO Survey 2018

Minds made for shaping  
financial services





**When the financial services industry works well, it creates growth, prosperity and peace of mind for hundreds of millions of people. No other industry touches so many lives or shapes so many futures.**

At EY Financial Services, we share a single focus – to build a better financial services industry, not just for now, but for the future.

We train and nurture our inclusive teams to develop minds that can transform, shape and innovate financial services. Our professionals come together from different backgrounds and walks of life to apply their skills and insights to ask better questions. It's these better questions that lead to better answers, benefiting our clients, their clients and the wider community. Our minds are made to transform a better financial services industry. It's how we play our part in building a better working world.

[ey.com / fsminds](https://ey.com/fsminds)

---

## In this report

1

Introduction and methodology

2

Organization and the role of risk

8

Operational resilience

12

Digital risk

18

Conduct risk

---

# Introduction and methodology

**70 firms**

surveyed across  
Europe



## About this report

This European Insurance CRO Survey 2018 highlights the key views expressed by chief risk officers (CROs) of larger insurance companies across the region. It aims to provide a succinct and targeted perspective of the current and future risk trends and issues impacting the insurance industry in these countries.

Survey samples include a diverse mix (both in size and products) of life and non-life insurance companies that benefit from an established presence in both traditional and non-traditional lines of business.

This EMEIA survey complements past findings from other EY research, developed through engagement with the largest life and non-life insurance groups operating across Europe.

## Approach and methodology


From June to September 2018, EY commissioned a CRO survey targeting 70 CROs at life and non-life insurance entities operating in 11 European countries. The aim was to obtain a snapshot of the status of these firms in four key risk areas:

1. Organization and the role of risk
2. Operational resilience
3. Digital risk
4. Conduct risk

For five of the larger companies, interviews were held with CROs operating in two different countries.

EY professionals are grateful to the CROs and organizations that contributed to this survey and appreciate their insights into these complex topics.





# Organization and the role of risk

The role of the CRO today remains as critical as it was when we last undertook the European survey in 2016. All the CROs we spoke to sit at the center of their organization's decision making, as they implement strategic changes in an increasingly uncertain economic and political environment.

*“In reporting lines, we have also seen a shift; more CROs report directly to the chief executive officer rather than the chief financial officer.”*

When we undertook the survey in 2016 we noted that most CROs had some form of change fatigue. At that time CROs split into those who saw change as a valuable way of keeping function evolving and those who wanted a period of stability to reflect on where to go next. The impact of regulatory and accounting changes, such as the Insurance Distribution Directive (IDD) and International Financial Reporting Standards (IFRS 17), has meant that the activities of the CRO and their function have not decreased in any way and the opportunity for reflection has disappeared.

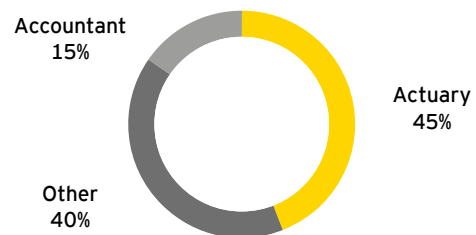
Since 2016, a number of CROs have sought to embrace technology and increase their use of analytics and visualization, but the investment here is insignificant compared to staff costs. The impact of digitization will be explored later in this publication as organizations change their process activities and the risk function responds.

## Skills and competencies

The risk function continues to help the business succeed and provides challenge and insight. This can be evidenced by the changing composition of the function and the CROs' areas of focus.

In this survey, we sought to understand the background of the CRO. Overall 45% of CROs interviewed were actuaries, with accountants making up a further 15%. The remainder of CROs came from multiple backgrounds including banking, underwriting and scientific roles.

### What is the background of the CRO?



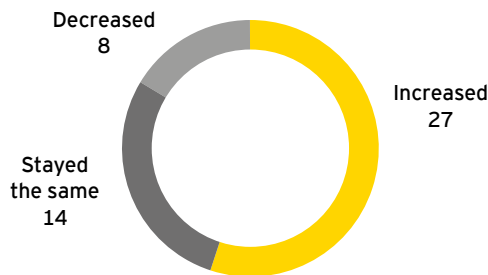
Based on responses from 52 of our participants

In reporting lines, we have continued to see more CROs reporting directly to the chief executive officer (CEO) rather than the chief financial officer (CFO). This shift began six years ago as the importance of the CRO role increased. It should be noted that all the CROs have close relationships with the chairs of their board risk committees who they meet more frequently now than they did in 2016.

The shift in CROs reporting lines to the CEO, along with access to the board and associated committees, means that their voice is heard strongly as one of the key decision influencers within the organization. The CROs role in training and empowering non-executive directors has continued to rise since 2016 as expectations around accountability expand.

While the role of the CRO covers both strategic and tactical matters, it now permeates through to decisions around remuneration for senior executives as CROs provide feedback on the behavior they observe.

### Have risk functions changed in size in the last 12 months?



Based on responses from 49 of our participants

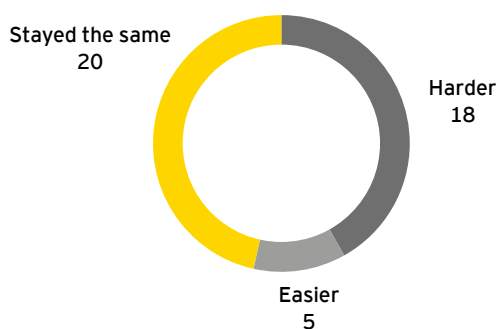
Many CROs now provide input to their remuneration committee on the risk behaviors evidenced by the senior management, including executives in their organizations. CROs in several countries also highlighted that the reports they were preparing had received more regulatory attention than previously.

### Resourcing the risk function

Despite cost constraints across many insurers, the increase in activities performed by the risk function has resulted in the headcount for more than 50% of firms has increased. Also, several CROs have seen additional resources moved under them because of compliance, internal control and regulatory teams being brought within their remit.

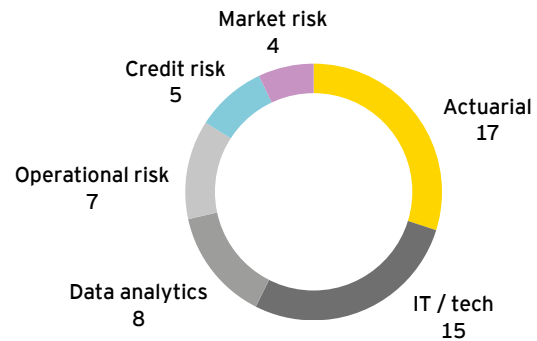
CROs who have been able to reduce headcount have typically done so by moving resources into business lines supporting their approaches to embed risk.

### Is it easier or harder to recruit than 12 months ago?



Based on responses from 43 of our participants

### What skills are challenging to obtain?



Based on responses from 40 of our participants

The overall costs of risk functions continue to increase for most firms.

Organizations continue to face challenges in hiring and retaining good talent which is noticeably harder outside major cities. When looking to recruit, a number of CROs flagged the increasing importance of having individuals who had both technical and real business understanding, not just theoretical knowledge. Consequently, many CROs now are actively recruiting resources internally within their organizations rather than relying on the external market.

Which are the hardest skills to recruit for?

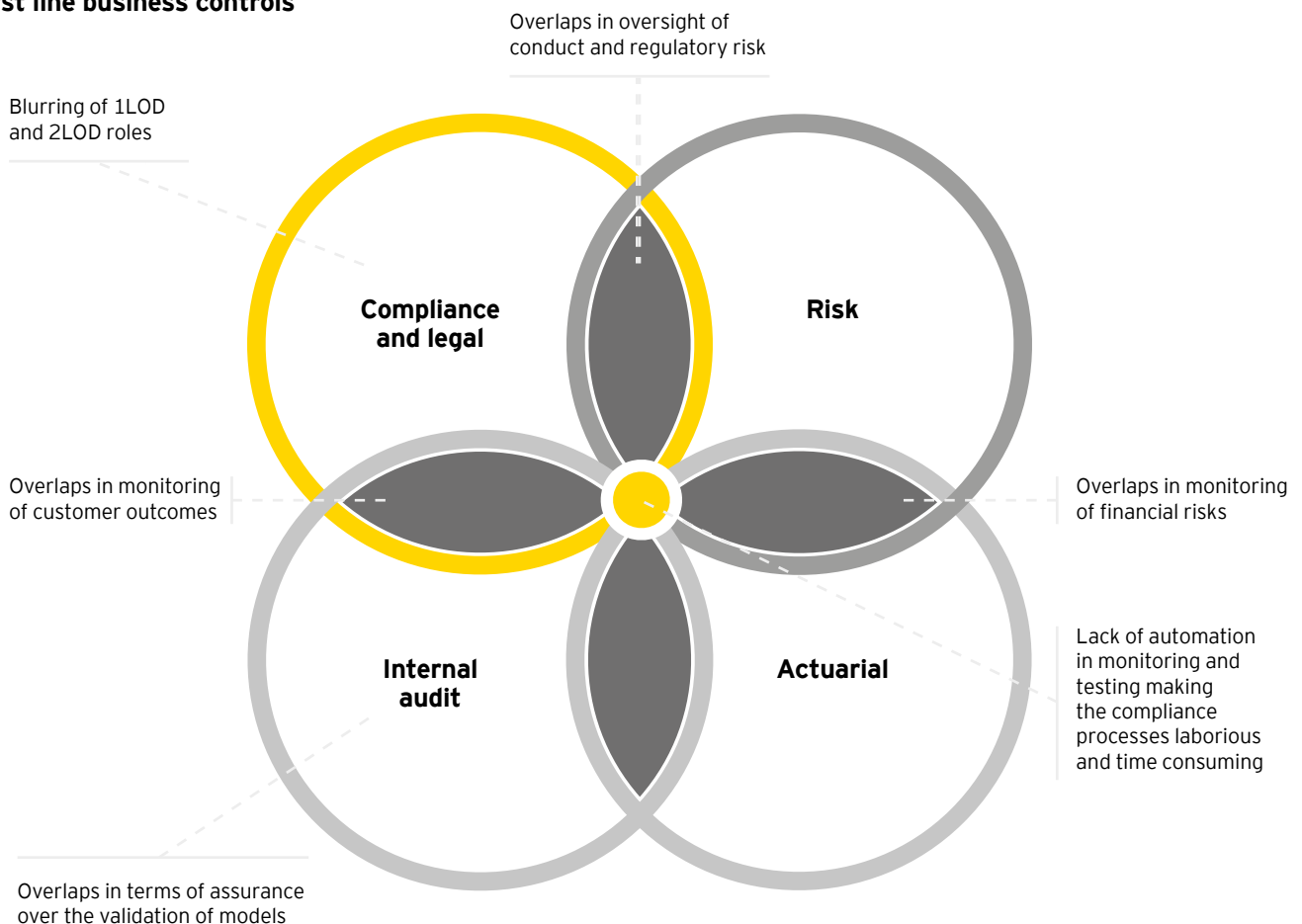
1. Actuarial validation
2. IT and technology
3. Data analytics
4. Operational risk (third-party management and change management)
5. Credit risk
6. Market risk

### Three lines of defense model

In our 2016 survey we observed that a lot of work has been done to evidence compliance with the three lines of defense (3LOD) principles, but more work was needed. Since then, risk functions have sought to clearly articulate their roles and align their activities with the first line. They have also worked with internal audit and compliance to integrate assurance related activities. However, when asking how well activities were aligned, only 11 out of 59 CROs felt it was very high, with 14



## First line business controls



respondents feeling that more could be done around sharing information regarding risks and responsibilities – which is currently remaining informal and ad-hoc. Various challenges continue for several insurers between their lines of defense as set out below.

For many organizations there remains a healthy tension between risk as a business partner participating in major transformation projects and adding value to the business, while remaining a second line of defense function with an independent stance. This is becoming particularly significant with respect to digital, where some CROs lack digital competencies in their teams and choose to rely on first line expertise, which makes independence harder to demonstrate.

## How would you rate the level of alignment between the three lines of defense?

Medium: Collaborations between 3LOD takes place to share information, but rather on an informal and ad-hoc basis

14

High: Formal coordination between 3LOD takes place on a regular basis. But there is no or only part alignment in terms of terminology, methodology, reporting etc

34

Very high: Formal coordination between 3LOD functions takes place on a regular basis. Fully aligned risk identification and assessment

11

## CROs focused on 12 key areas in 2018

When we asked CROs about the main challenges impacting the industry today, 12 topics came through consistently. Unsurprisingly, political and economic movements across Europe were a significant focus for organizations. The other areas of focus can be clustered under four headings:

**1. Economic-related concerns** are focused around continued low interest rates and the impact this has on investments as organizations seek higher returns. While such rates have driven global stock markets to rise over a number of years, it is feared that the “bull market” will end and significantly impact investments. In addition, a number of organizations have invested in more complex products which may not be as liquid as desired, or where the underlining collateral strength would be damaged with a sudden market movement.

**2. Operational-related issues** are becoming more apparent to organizations as they seek to operate in a digital world while managing legacy IT systems. In the last 12 months, risk functions have centered more on

IT stability issues, cyber-attacks and the strength of third-and fourth-line relationships. Many CROs have adopted a more direct approach in these areas, meeting their counterparties in other organizations as they seek a higher comfort level and resilience with the systems and controls they have in place. This paper explores operational resiliency challenges further in the second section. It comes as no surprise that organizations operating globally need to put in formal requirements for inter-firm servicing arrangements as regulatory focus increases in their area.

**3. Strategic challenges** face both life and non-life insurance providers across Europe. For the latter, the soft market combined with past catastrophe exposures is leading to profitability strains and risk functions for a number of organizations have played a prominent part in re-positioning books of business. Across EMEIA, conduct risk issues are becoming more apparent in relation to life and savings products, as investment yields remain low and charges need to be positioned fairly for the customer. Most CROs surveyed were facing challenges in aspects of their conduct risk frameworks in 2018, as discussed further in this report.





As organizations embrace digital ways of working that require the risk function to team with the business to ensure that the systems and controls in place are robust, the costs for building in these aspects can be surprisingly high. One organization noted the need to become true business partners when it comes to digitalization.

Best-in-class CROs are in the right place, at the right time, supporting the business with insight and knowledge about risk and a framework on how to manage and monitor risk.

To do this, they need to enhance their internal capabilities to respond and work with the business.

The impact of climate change is also coming to the fore of CROs' attention in both the life and non-life sector as the changing environment is recognized more,

investors' expectations increase, and insurers focus on corporate responsibility.

**4. Regulatory relationships** continue to be important for CROs, particularly as the reporting lines for regulatory risk and compliance directors switch to reporting to the CRO rather than elsewhere in the organization.

## A broader set of issues in 2019

While attention has focused on the 12 key areas previously mentioned, CROs face 2019 with a much broader set of issues, meaning that the time for reflection will remain limited.



### Political, legal and regulatory

- Impact of political movements (such as Brexit)
- IFRS 17
- G7 to G20
- Uncertain political tax environment
  - US tax reform
  - Base erosion and profit shifting (BEPS)
- Risk of high tax governments



### Economic

- US interest rates
- Bull market stops
- Low interest rates providing cheap capital
- Organic growth is challenging in some economies
- Better informed clients with changing risk management requirements
  - Intangible asset protection
  - Larger more complex tangible risks
- Fourth Industrial Revolution
- Trade (barriers)
- Competitive environment and excess capacity in GI/non-life



### Environmental

- Changing global climate
- Environmental footprint of insurance industry
- Active shareholder activism
- Solar storms



### Social

- Diversity – insurance behind the curve
- Behavioral expectation that to trade digitally is healthy
- The world is moving and changing faster and will only accelerate
- Talent – millennials have very high expectations of their work experience
- Flexibility – workforce has a greater propensity to work-life balance and flexible working is a hygiene factor
- Mortality improvements



### Technological

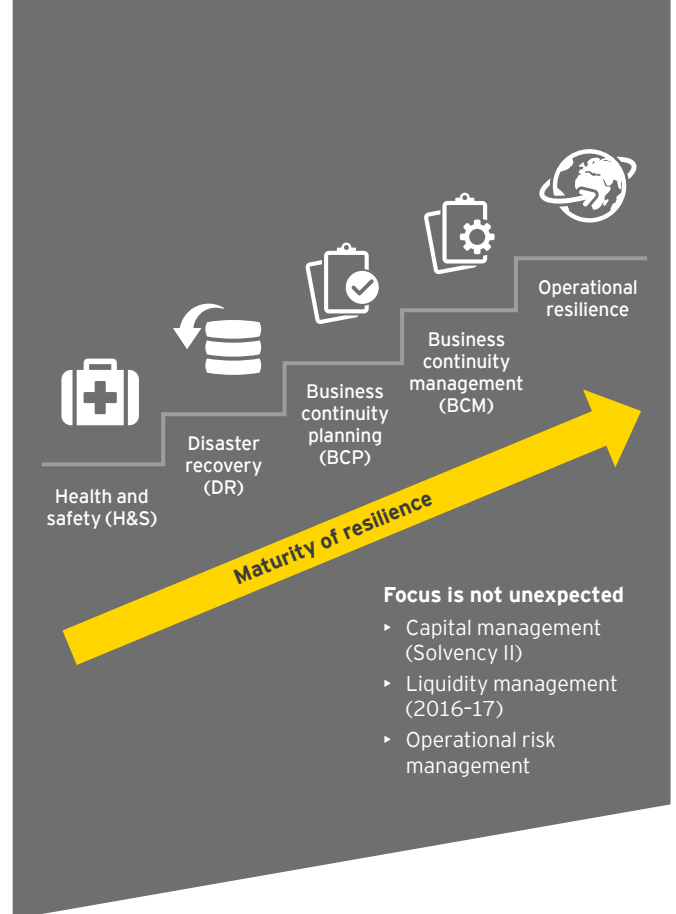
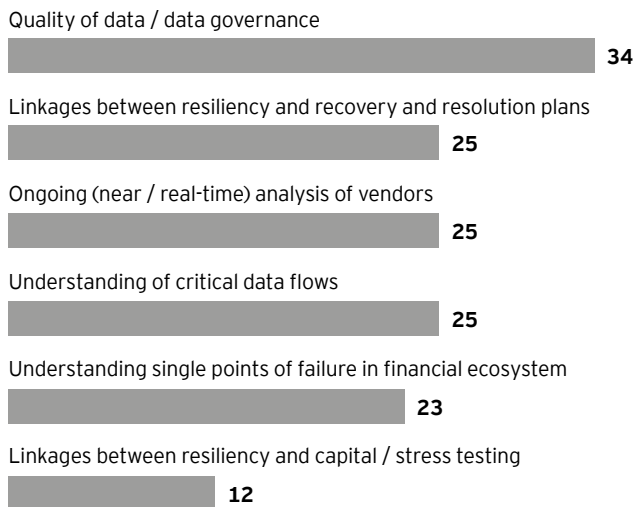
- A more connected world
- Enabled by new technologies
  - Sensors
  - Distributed, secure ledgers
  - Robotics
  - Connected devices
- Changing the role of the broker and carrier from loss managers to digital risk managers in the GI/non-life space

A man with glasses and a light-colored shirt is seen from the side, looking at a server rack. He is holding a blue marker and writing on a glass partition. The background is a server room with many server units and glowing lights. The text 'Operational resilience' is overlaid on the left side of the image.

# Operational resilience

The CRO survey asked what needs to be done to have a more robust firm-wide resiliency program. From the responses, it was clear that CROs are increasingly focused on IT and considering issues such as detailed scenario testing, enabled by IT capabilities and greater interest from the Board. The most significant issue is the ability to understand underlying data, its consistency and what it is showing, along with the need to link recovery and resolution planning to resilience thinking. Moreover, we should not forget the importance of understanding single points of failure in the financial ecosystem or the inevitable linkages between resiliency and capital or stress testing.

### What IT areas do you feel need to be enhanced to have a more robust firm-wide resiliency program? (Select the top three)



### What is operational resilience?

Operational resilience is frequently discussed, but what does it really mean? It can be described in various ways and may be impacted by many factors. For example, it can be information security and cyber terrorism, and the impact these have on an entity's operations. It can be system stability and the preponderance of legacy systems in the IT estate – something that is widely known and well documented in the insurance industry. Overall, operational resilience is one of the biggest challenges CROs are facing in the rapidly developing digital environment.

In the past the focus was on business continuity, making sure that an organization did all it could to make sure that its service was not interrupted. With the digital economy that has changed and is continuing to change, technology has brought in so many interdependencies and multiple points of failure. The upshot now is that disruption will happen, and organizations need to have a response to that disruption when it does. Operational resilience is an outcome. It is the ability of an organization to adapt and recover when things go wrong. The focus on this area is not unexpected and the need for increasing maturity follows high profile developments in the insurance industry, such as capital management and liquidity management. In recent months, the Financial Stability Board has set up a new working group to study "issues related to cyber risk and broader operational resilience."

### The importance of managing resiliency

For the CRO to know how to react, it is important to understand what has changed. Resilience has shifted the focus of business continuity from "prevention" to "response." Management, under the careful watch of the CRO, needs to set its impact tolerance or its appetite on what is the maximum impact it is able to accept and explain to customers and other stakeholders. This has to be done formally by devising a set of impact tolerance statements, with clearly defined metrics such as time and volume. In addition, senior management has responsibility for the resilience of the organization with the inevitable penalties if it fails.

Why is operational resilience important and where should an organization place the greatest emphasis? Business services are at the heart of an entity, and the various systems that operate across an entity need to be mapped to these business services. Management is responsible for carrying out a full risk assessment.

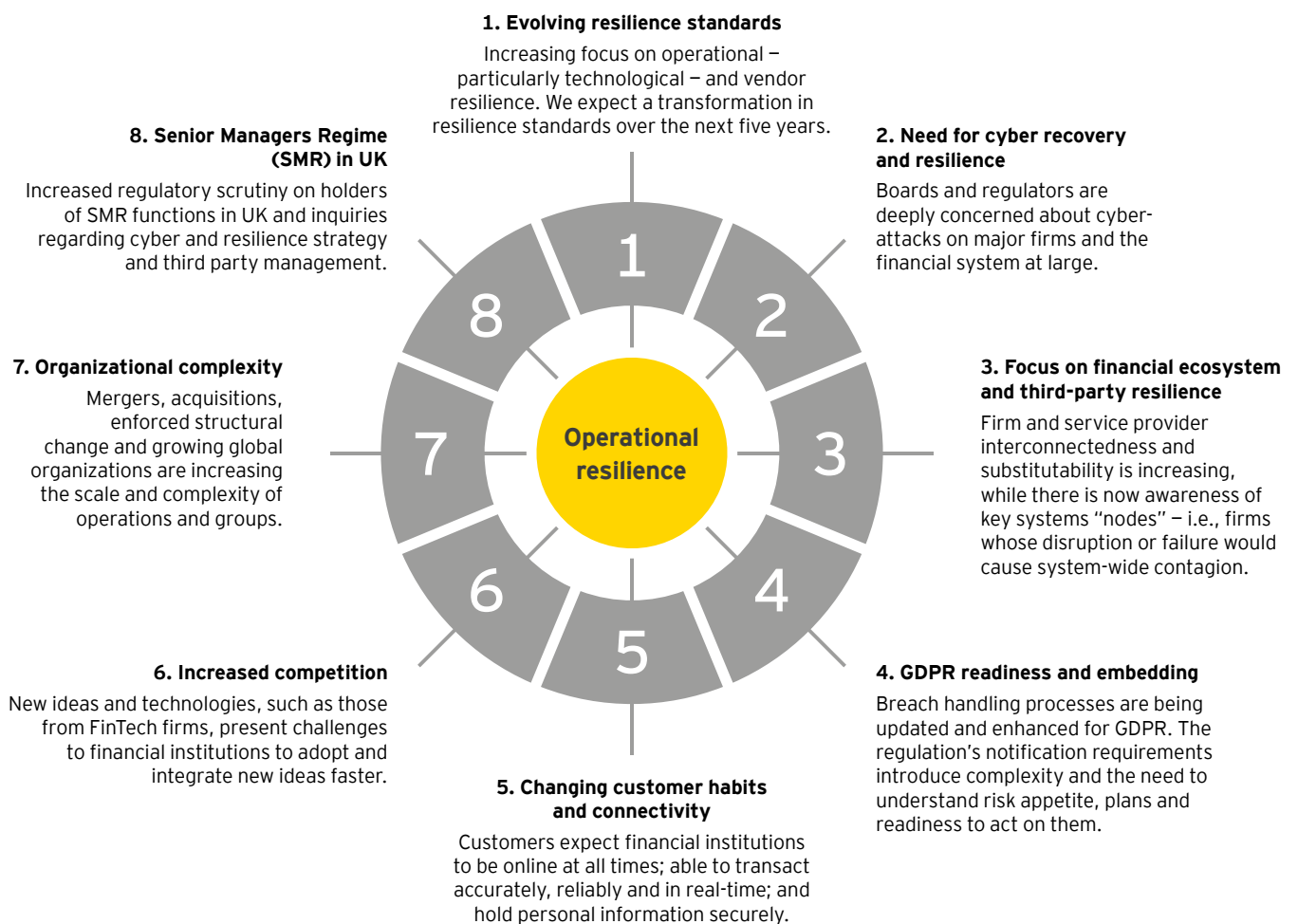
Organizations are more and more reliant on third, and even fourth, parties such as vendors and other service providers. In the age of specialization, services are often outsourced and, in turn, those outsourcers can have a reliance on their own third parties. This does not lessen an organization's responsibility for systems, whether they are outsourced or not. Every organization needs to develop its own resilience framework which sets the boundaries and defines its activities.



## What are the greatest resilience challenges for the CRO in 2019?

1. Establishing responsibility and accountability for operational resilience
2. Providing a customer-driven focus
3. Managing third (and even fourth) parties, vendors and intra-company service arrangements
4. Defining and implementing suitable metrics
5. Building resilience by design
6. Recognizing that the topic is much broader than just IT and cyber

CROs are all too familiar with the key risks relating to the digitalization of insurance, and this is clear in the responses to the survey. Topping the list are cyber security concerns, the shortage of IT resources and talent, and current infrastructure not supporting new technologies. CROs have technology constraints in the risk function which, combined with poor data, results in challenges in providing reasonable management information. More than one-third of EMEA CROs cited quality of data and data governance as the most important area to be enhanced for a more robust firm-wide resiliency program.



When asked in the survey, two-thirds of CROs cited at least one of the following as technology constraints preventing them from receiving their desired level of monitoring and reporting of risks:

- ▶ Production of management information is time consuming
- ▶ Data required for management information production is not available
- ▶ Model run times take too long

Going forward, a way of identifying internal and external risks to the organization is required, including the threat of cyber-related issues. Companies need to manage these risks and focus on the ability to maintain levels of service. Robust testing has to be in place over protective, response and recovery capabilities. An organization has to have the ability to react to both gradual change and sudden disruption. There needs to be a continuous learning curve from recent industry events and a fast-changing risk profile in which modern business operates.

What is essential is a holistic and integrated approach to the people, processes and technology used across the organization, including the third parties that are relied upon. All this demonstrates that operational resilience should be firmly on the insurance CRO's agenda.

*“What is required going forward is a way of identifying internal and external risks to the organization, including the threat of cyber-related issues.”*



# Digital risk

In recent years, CROs have been engaged with solvency calculations, building internal models and obtaining an aggregated view of the company's risk profile. The Own Risk and Solvency Assessment (ORSA) process has contributed to a better understanding of how risk and capital are interlinked. More recently, executives and boards have shifted their focus from solvency to growth and digitalization. The CROs must shift their focus too. So how is digital changing the risk profile of insurers, and how are CROs supporting their organizations by managing digital risks?

How does digitalization change the risk profile of insurers?



## Fact box:

### What is the purpose of digitalization?

Digitalization impacts all aspects of insurance. The aim is to achieve one, or several of the following:

- ▶ Revenue growth: new products, services, revenue streams and/or ways of interacting with clients to sell more.
- ▶ Margin improvement: improved pricing and risk selection through big data, artificial intelligence (AI) and machine learning (ML) models.
- ▶ Operational excellence: digitalization of operations to improve efficiency and /or reduce risk through change of core systems, automation of tasks and use of AI or ML to perform core processes, such as underwriting and claims. The use of technology is also an imperative to manage conduct risk, financial crime and to ensure compliance with regulations like GDPR, AML and International Direct Deposit (IDD).

**Digitalization is more than technology; it is a transformation.** Digitalization of insurance is not only about implementing new technology. It is about becoming more innovative and agile, as well as digital, and using data effectively while working within the General Data Protection Regulation (GDPR).

Leading insurers are approaching digitalization as a transformation. They are adapting every part of the organization, including; strategy, KPIs, operating models, IT-architecture, roles, responsibilities, talent, incentives and culture.

#### **Digital changes the nature of operational risk.**

One of the most common aims of digitalization is to improve operational excellence through automation and digitalization of core processes from pricing to underwriting, billing, and policy administration to claims handling and payments. This significantly reduces the traditional human errors that have been an important source of operational risk. However, new vulnerabilities arise. These include risks relating to system upgrades and changes, and the need to have 24/7 access to systems. Automated underwriting processes by definition will be consistent with the underwriting conditions programed into the system. However, a flaw in an ML algorithm in the pricing process may mean that entire products and/or segments may be over or under-priced. Similarly, flaws in automated claims processing could lead to consistent over or under payment, or payment of illegitimate claims.

**Changes are implemented faster.** Insurers seek growth through innovation. Decisions about new products, services and ways of delivering are being launched quicker than before. Agile ways of working imply that more ideas should be tested, and it is important to “fail fast.” This impacts the risk profile of insurers, meaning that CROs and their risk teams need to be technologically aware to help push the business forward.

One example is the launch of new concepts to reach new market segments. A team consisting of digital, marketing and sales, launched an innovative concept that was quickly picked up by clients. The pricing actuaries and risk professionals were informed after the launch. The result was an underperforming insurance portfolio that needs significant re-pricing or which is put in run-off a year later. Significant time and effort was spent on building a less profitable insurance risk profile.

On the other hand, several insurers have succeeded in significantly improving their insurance risk profile by the use of predictive modeling of churn rates, allowing them to proactively target customers that are about to leave the company. Success is achieved through agile, multidisciplinary teams that both understand the fundamentals of insurance risk and have skills in data, analytics and digital distribution channels.

## How does the risk function support the organization in managing risks relating to digitalization?

Aspirations for growth, innovation and digitalization force the risk function to shift its focus too. Risk needs to become a true business partner when it comes to digitalization. Best in class CROs are in the right place, at the right time, supporting the business with insight and knowledge about risk and a framework on how to manage and monitor it.

**Right time and place.** As insurers seek to spur innovation and speed up change, decisions about new products, services and ways of delivering are being launched quicker than before. Best in class risk functions are involved from the start, and when decisions are being made. They are permanent members of the product approval board, the committee that approves major investments and initiates new change programs, and the innovation board. Being present where the priorities are discussed and decisions are being made gives the risk manager the opportunity to ensure that adequate questions regarding risk and the management of risk are being addressed at an early stage. The function provides value by contributing to strong risk management by design, and is seen as a constructive business partner for the business leaders.

**Insight and knowledge.** Digital risk managers provide insight and analysis which helps the decision makers understand the impact of strategic decisions, such as entering a new market or developing new products (e.g., parametric insurance). They also help the business design their new processes in a way that minimizes risks; for example, by ensuring that the ML models in pricing are transparent so that they are in compliance with regulatory requirements to treat customers fairly. The digital risk managers are insightful when it comes to new technologies, provide an alternative and complementary perspective, and not the least, have a collaborative and supporting attitude.

**Risk management framework.** Best in class risk managers not only ask “what are the risks of implementing this new system, product or process, and how will it be managed,” they provide the business with a framework to analyze and manage the risk. This

helps the business leader achieve his or her objective, by building trust into design of the framework. More importantly, it also ensures that the risk is consistently managed throughout the organization.

The table illustrates how the risk profile is impacted through digitalization, and how the risks can be managed. In recent years, risk management functions have been involved in implementing frameworks for third-party risk management, cyber security risk management, program risk management, conduct risk management and model risk management. Some also are involved in talent, teaming, culture and incentives, which are particularly important fundamentals to manage risks in an agile and fast-paced organization.

Even though much has happened within this area in recent years, few insurers have consistent frameworks for all types of risks relating to digital developments and operations. The survey reveals that few CROs have a holistic perspective of how the digital risk profile evolves, whether the risks are adequately managed, and whether the organization is sufficiently resilient if and when a risk event occurs. We expect that digital risk management will become more professional and holistic in the years to come.

**Improved risk management through technology (RegTech).** One aspect of risk management that is expected to improve over the next years, is automation of controls and the use of RegTech. We see this in areas like financial crime, where ML is contributing to reducing false positives that need to be manually checked.

Monitoring of limits can be continuous and supported with denial of execution as soon as processes are fully digital. Many organizations are introducing tools to manage sensitive data to comply with GDPR. These are examples of how technology is used to reduce operational and compliance risk.

Monitoring controls is an integrated part of any business leader's responsibility. Therefore the controls should be executed, and automated, in the business – which is the case in most organizations. Still, the risk function has an important role to play. Best in class risk managers give advice on how and when to use RegTech, and how to build an integrated, digital internal controls framework. Once processes are digital, the risk function can also

## Fact box:

How does digital impact the operational risk profile of insurers, and how can it be managed?

Impact on risk profile	How to manage it
<p>Implementation of new technology:</p> <ul style="list-style-type: none"> <li>▸ Core systems changes -&gt; program risk</li> <li>▸ Customer experience platforms -&gt; conduct risk</li> <li>▸ Cloud solutions -&gt; data protection risks</li> </ul>	<ul style="list-style-type: none"> <li>▸ Program risk management</li> <li>▸ Testing procedures</li> <li>▸ Data governance</li> <li>▸ Conduct risk management</li> </ul>
<p>Digital processes:</p> <ul style="list-style-type: none"> <li>▸ 24/7 access and 100% systems dependence</li> <li>▸ Potential for fraud and cybercrime through unauthorized access and changes</li> <li>▸ Data loss</li> </ul>	<ul style="list-style-type: none"> <li>▸ Information security management systems</li> <li>▸ Access and identity management</li> <li>▸ Cyber risk management programs</li> <li>▸ Back-up and recovery procedures</li> </ul>
<p>Automated decision-making through the use of ML impacts:</p> <ul style="list-style-type: none"> <li>▸ Insurance risk profile through underwriting and pricing decisions</li> <li>▸ Costs and insurance risk profile if used in claims</li> <li>▸ Conduct risk if used in customer interaction</li> </ul>	<ul style="list-style-type: none"> <li>▸ Model validation procedures</li> <li>▸ Algorithm documentation</li> <li>▸ Performance monitoring</li> <li>▸ Stop-loss mechanisms</li> </ul>
<ul style="list-style-type: none"> <li>▸ Ecosystem of vendors and partners</li> <li>▸ Greater flexibility and increased complexity</li> </ul>	<ul style="list-style-type: none"> <li>▸ Third-party risk management</li> </ul>
<ul style="list-style-type: none"> <li>▸ Speed of change: "fail fast" with limited consequence</li> </ul>	<ul style="list-style-type: none"> <li>▸ Culture</li> <li>▸ Incentives</li> <li>▸ Talent and team composition</li> </ul>

use the information, analyze it and translate it into an aggregate perspective on the control effectiveness of the digital operation.

### What are the greatest digital opportunities for the CRO?

Digital presents an opportunity for the CRO. The risk functions finally can move from risk monitoring to risk intelligence. Greater computing power, easy-to-use visualization tools and opportunities to combine data sources make it possible to provide broader and deeper

insight into the risks facing the business. Automation of monitoring and reporting will free up time to be a trusted advisor for the business and support the board and the CEO.

**From risk monitoring to risk intelligence.** New ways of using data and tools for data visualization and analytics provide great opportunities for CROs. More data provides a broader and deeper perspective of risk. Data visualization and analytics make it easier to present insights and share facts and knowledge necessary for executives to take action.



## Fact box:

### Examples of risk dashboard topics

- ▶ Adherence to limits in the sales of insurance products: the risk function can get a full picture of breaches and approved deviances to understand if growth is being achieved to the detriment of profitability.
- ▶ Adherence to testing procedures in the launch of systems changes can indicate to what extent innovation is agile and working or out of control.
- ▶ Tracking product changes by monitoring terms and conditions produced in the system can give an indication of whether the speed of change is appropriate.
- ▶ Conduct risk can be monitored through voice recognition with alerts at the use of certain terminology.
- ▶ Social media analytics can be used to monitor the firm's reputation.
- ▶ Risk culture can be monitored through employee turnover and the number of people who have completed ethical training.
- ▶ Cyber-risk analytics can address threats, and attacks, as well as patches to be completed.

A key role of any CRO is to support top management with an aggregate view of the risk profile. This task has been a challenge for many CROs as data is stored in numerous systems, often unstructured and hard to get hold of. Traditional risk reporting has been fragmented, with backward-looking reports produced several weeks before a board meeting and aggregated to such a high level that they are not actionable. New methods of data collection, increased computer power and new ways of analyzing data means that it is more realistic for all risk functions to present an up-to-date and fact-based view of the risk profile.

Best in class risk functions are establishing a risk dashboard that presents data from numerous sources and several perspectives. The dashboard is presented on live data, and are a reference tool for decision-making. The risk dashboard gives executives deeper insight into their business, helps them understand trends, strengths and weaknesses, and enables them to manage risks more proactively than before. It ensures that the risk function is consulted continuously before decisions are made – not after the fact.

Many risk functions are exploring the opportunities of providing risk intelligence services. This is a work in progress, and few have arrived at their destination. Some start by acquiring skills in tools; others collect new types of data. No matter where you start, the risk function will benefit from taking similar approaches to digitalization and the rest of the business. Use an agile approach. Start small, establish integrated teams,

build minimum viable products to gain understanding and experience, get feedback from the users of the dashboard and continue developing.

**Operational excellence in risk.** Digitalization offers opportunities for operational excellence for the risk function. Most CROs in the survey plan to spend additional resources to automate reporting and controls.

Risk functions often spend considerable time collecting data, verifying and reporting information, reconciling management reporting, legal entity reports, financial and business reporting, and ORSA information. Many CROs report that there is little time to analyze and digest the information. Use of robotics process automation, programing and technology have the potential to reduce the time spent on these tasks, including data collection, validation and report production. At the same time, the quality may improve as manual errors and inconsistencies can be removed. Many CROs have started this journey. Some invest in better technology, others in talent and capacity. Those who spend the resources will reap the benefits of increased efficiency.

Lessons learned from digitalization of operations show that only those that manage to allocate the surplus capacity and talent on something more valuable will be rewarded. This is why the best in class CROs maintain their seat at the table. They are already spending time assessing the digital governance model, talent, leadership, incentives and culture.

## Looking forward to 2019

As CROs in digital insurers look to 2019, they not only need to keep abreast of new technologies. They also must understand how the risk profile changes, and how strategies, operating models, cultures and incentives are realigned to a digital and innovative business model. Digitalization is rapidly changing the risk profile of insurers. This is a challenge for the business. Best in class CROs provide a framework for how to manage and monitor risk, and are updated on how risks can be managed better through the use of technology.

As CROs look forward, they are taking the opportunity to automate their own tasks, particularly for monitoring

and reporting. Many CROs are starting to use analytics and data visualisation tools to provide risk intelligence rather than mere after-the-fact monitoring. The ability to provide continuous and more detailed information than before will improve their value in the eyes of business leaders as well as the CEO and the board.

Ambitious CROs not only support the business in managing digital risk. They also take steps to enhance the contribution from the risk function, taking a greater role in insurers' innovation and growth agendas. They provide more insight into the upside risks, helping to answer questions regarding which risks to embrace and how to best manage those risks by understanding the technology being used.

## Fact box:

### Additional insights from the survey

#### Who is responsible for digital risk?

The survey indicates that there are significant differences between CROs' perspectives on their responsibility when it comes to digital risk. In certain countries, CROs do not see this as their responsibility. They are in charge of quantitative risk management and solvency modeling, but will not spend time on operational risks. In some cases, it is explained through their mandate, as internal controls and operational risks are allocated to compliance or a separate internal controls entity. In other cases, it may be due to lack of skills and/or resources. Independent of the explanation, CROs in this position are at risk of making themselves less important and less valuable for the firm since the firm's strategies and resources are moving in the direction of digital, growth and innovation.

#### Who takes responsibility for cyber risk?

We see both an opportunity and a need for risk managers to step-up when it comes to cyber. Few CROs have skills or resources to follow-up on cyber risks. Instead, they rely on the Chief Information Security Officer (CISO). This is an effective interim solution given the scarcity of resources and the need to quickly build stronger cyber risk management capabilities across the organization. Still, it makes it harder for the CRO to present a holistic perspective on digital risks.

Many CISOs are technical experts with an operational focus and spend their time handling cyber security issues. They seldom have capabilities, skills or resources to build a consistent framework and governance model to manage risk. This is an area where the risk function could be a strong partner to the CISO, supporting with methods and advice on how to build a strong risk management framework.



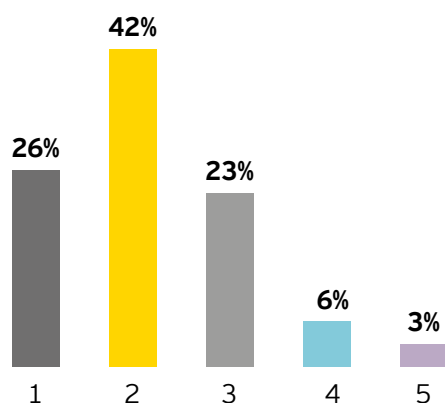
# Conduct risk

Conduct risk has been a regulatory focus across Europe for almost a decade, yet remains a significant concern for CROs across the industry. In a number of countries, the approach to conduct risk focuses on aggregating several areas considered separately in order to fulfil specific regulatory requests.

In this section, we consider the areas of greatest concern for CROs and the underlying drivers of the key challenges facing the risk function in the insurance industry today.

## How many elements of their conduct risk framework did CROs believe were mature?

Number of mature elements



To assess the high-level maturity of frameworks, we asked CROs across the industry to rank the maturity of five key elements of their conduct risk frameworks:

- Strategy and product development
- Conduct risk reporting and MI
- Risk breach assessments
- Risk appetite metrics and tolerances
- Governance, including the role and responsibilities of the Board

## How mature are conduct risk frameworks across the industry?

The 2018 CRO survey focused on assessing the current state maturity of conduct risk frameworks within the insurance sector, and priorities for CROs to further enhance their effectiveness in 2019.

### Key themes

- The maturity of conduct risk frameworks varies across Europe, with 27% of respondents saying these frameworks were not mature in any area discussed, and a small minority saying their frameworks were mature in all areas tested (3%). Those that were most confident in their conduct risk frameworks were insurers forming part of a wider group including retail or investment banks. In a number of countries, the approach is around aggregating areas such as customer protection and complaints management to fulfill specific regulatory requests.
- Areas of maturity varied among respondents, with six businesses prioritizing different areas to enhance over the next 12 months. These priorities were driven by individual challenges and areas of perceived weakness.

### Fact box:

#### Which areas were mature within respondents' conduct risk frameworks?



% of respondents comfortable their conduct risk framework was mature in each area





3. Only one respondent considered all of the five areas discussed to be mature. The highest number of respondents cited risk appetite metrics and business governance.

## **What do CROs see as the biggest challenges facing their businesses?**

Respondents told us they are facing a range of challenges. These depend on how mature their existing framework is, the range of products they offer and the culture of business leadership. Firms with established conduct risk frameworks have struggled to maintain and update them effectively to reflect changes in regulatory expectations. This has been driven primarily by the need to prioritize resources to address other industry challenges – such as increasing market uncertainties and volume of regulations.

While insurance companies are responding to their own individual challenges, three key trends emerged from the survey which highlighted ongoing areas of concern for CROs in the insurance sector:

1. Respondents face challenges identifying emerging conduct risks in product design and distribution following implementation of the IDD.
2. Respondents are experiencing difficulties developing meaningful, insightful management information which provides insights into conduct risks within their business.
3. Respondents have not managed to effectively transition ownership of conduct risk frameworks to the first line of defense (1LOD).

### **Identifying emerging risks in product design and distribution**

A number of respondents stated that understanding the risks posed by legacy and new products was a key concern facing their business in 2019. CROs cited these issues:

- ▶ Regulatory pressure from a combination of IDD requirements and a number of regulators focusing on the treatment of customers with legacy products. This has led to respondents seeking to enhance their product governance procedures, and make them more efficient, but facing challenges to effectively embed changes.
- ▶ To drive more effective product governance, CROs are focusing on the measures used to enhance product approval and review criteria. However, they have faced capacity challenges in the 1LOD to ensure products are effectively reviewed.
- ▶ Greater pricing focus between new and legacy customers in non-life insurance, requiring greater analysis and assessment of unfair pricing risks.
- ▶ Revisions of product governance procedures have coincided with needs to assess the clarity of customer communications, often extending the time required for each product review.
- ▶ Product governance challenges are having the greatest impact on respondents that have a wide range of products, as they have to assess the risks associated with different products, developed and sold at different times.
- ▶ Respondents that have quantitative MI that is not effective in providing business insights and requires revisions.
- ▶ Respondents that have quantitative metrics, but need to improve qualitative commentary and context to ensure stakeholders understand risks posed to the business.
- ▶ Respondents that do not have quantitative reporting at this time and rely primarily on qualitative analysis and commentary.
- ▶ Respondents operating multiple legacy systems face significant challenges in gathering and collating MI effectively. They are considering how best to interrogate data sources, including the need to initiate large data integration programs, such as utilizing “data lake” technology to create consistent records across product sets to improve analysis.
- ▶ Respondents do not receive first-hand information on complaints, and depend on the information provided by third parties, who may aggregate and provide data in a different way.
- ▶ Regular changes to frameworks introduce ongoing challenges to keep MI up to date and relevant, while also allowing trend data to be developed and understood.

### **Development of insightful conduct risk MI**

Developing effective MI which provides meaningful insights into business operations and emerging risks has proved challenging for the industry. A number of respondents stated that they have struggled to develop insightful quantitative conduct risk metrics. Others have had challenges effectively implementing them due to limited ability to access and interrogate business information, often due to the fact that policy administration is outsourced or sits within banking agencies (in the case of bancassurance).

- ▶ A majority of respondents stated they planned to make enhancements to MI and reporting, but within that group, the businesses they represented were in a range of different positions. These ranged from:

### **Transitioning ownership of the conduct risk framework to the 1LOD**

Throughout the survey, CROs noted that a key priority for 2019 was ensuring conduct risk frameworks were effectively owned and embedded within the 1LOD. This has been a priority over the past 12 months, but respondents have faced a range of challenges:

- ▶ 1LOD acknowledging and accepting it is a business responsibility to manage conduct risk, preferring to consider it a “compliance led” issue.
- ▶ Respondents struggling to determine which areas of the 1LOD should be responsible for the conduct risk framework.

- ▶ Data availability and consistency when third-party agents are involved including banking agencies for bancassurance arrangements.
- ▶ Shortages of capacity, and appropriate skills and experience in the 1LOD, creating reluctance in the second line of defense (2LOD) to hand-over responsibility.
- ▶ Lack of a centralized conduct risk function in the 1LOD providing a holistic view of conduct risk across departments, business lines and legal entities within firms.
- ▶ Aggregation of different business line reporting being undertaken by the 2LOD, resulting in reporting being redrafted by the 2LOD rather than challenged.

## Where do CROs plan to invest in 2019?

While insurance companies have different priorities in 2019, and will be focusing on enhancing different areas of their conduct risk frameworks, two key areas were identified by CROs as areas for investment across businesses surveyed: people and digital.

To relieve pressure on compliance and risk functions, CROs are looking to invest in digital solutions which reduce the level of manual assessments that need to be performed on a regular basis. How digital will be utilized varied among respondents and countries. Key areas referenced by respondents included:

- ▶ Utilization of digital tools to standardize and streamline reviews.
- ▶ Use of data analytics tools to achieve better insights over large data sets, and improve the functions' ability to identify emerging risks.
- ▶ More sophisticated, automated, reporting tools which will simplify the development of MI and allow individuals more time to focus on understanding existing and emerging risks faced by the business.

More prevalently, CROs are seeking to invest in having the appropriate people, with the right skills to effectively oversee business risks. More than two-thirds (65%) of respondents intend to invest in enhancing the capabilities of either the 1LOD, the 2LOD or both. Investment in this area is anticipated to be split between:

- ▶ Training to increase understanding of conduct risk in the 1LOD.
- ▶ Onboarding individuals with experience in emerging risk areas (such as digital and cyber) into the 2LOD to enhance capabilities.
- ▶ Creating new roles in the 1LOD, with a primary focus on conduct risk.

# CROs need to embrace strategic change

Findings from our survey reveal that CROs across Europe face economic, operating, strategic and regulatory challenges. Perspectives and levels of maturity differ by country. However, many still have some form of change fatigue – as we reported in our last survey in 2016. Most see their roles changing – with 50% saying that their headcount has increased along with the need for additional resources to manage an onslaught of market, environmental, cyber and technological risks.

As the digital environment evolves, one of the biggest issues will be operational resilience. How companies adapt, respond and recover when disruption occurs. We believe every organization needs its own resilience framework to define its activities. Also high on the CROs list is digital risk and the imperative for organizations to realign strategies, operating models and cultures to ensure trust is built into digital business models. More than two-thirds of CROs are seeking to invest in the right people, with the right skills to effectively oversee business risks.

Against this backdrop, CROs must monitor and manage regulatory compliance, while spurring their organizations toward change and a greater focus on the customer. Ambitious CROs not only support the business, but enhance their contribution to the risk function by taking a greater role in the insurance innovation and growth agenda.



# Notes

# Contacts

---

## Global

### Martin Bradley

mbradley@uk.ey.com  
+44 (0) 20 7951 8815

---

---

## EMEIA

### Phil Vermeulen

phil.vermeulen@ch.ey.com  
+41 58 286 3297

---

---

## Belgium

### Roy Alexander Boukens

roy.alexander.boukens@be.ey.com  
+32 27 491760

---

---

## Portugal

### Carla C Pereira

carla.pereira@pt.ey.com  
+35 1211 542948

---

---

## France

### Jean-Philippe Roy

jean-philippe.roy@fr.ey.com  
+33 146 937976

---

---

## Spain

### Manuel Martínez Pedraza

manuel.martinezpedraza@es.ey.com  
+34915727223

---

---

## Germany

### Peter Ott

peter.ott@de.ey.com  
+49 891433 116298

---

---

## Switzerland

### André Dylan Kohler

andre-dylan.kohler@ch.ey.com  
+41 582 863378

---

---

## Italy

### Lorenzo Fattibene

lorenzo.fattibene@it.ey.com  
+39 0667 535258

---

---

## UK

### Niranjan Nathan

nnathan2@uk.ey.com  
+44 (0) 20 7980 9132

---

---

## Ireland

### James A Maher

james.maher@ie.ey.com  
+353 12 212117

---

---

## Lead author

### Neal Writer

nwriter@uk.ey.com  
+44 (0) 20 7951 7028

---

---

## Netherlands

### Jennifer van Eekelen

jennifer.van.eekelen@nl.ey.com  
+31 884 071794

---

---

## Contributors

Kristin Bekkeseth  
Michael Elysee  
Mantas Semeta  
Steve Southall  
Michael Vaughan  
Gareth Wong

---

---

## Nordics

### Kristin Bekkeseth

kristin.bekkeseth@no.ey.com  
+47 94 247130

---

## How EY can help

Our dedicated team of finance, risk and actuarial professionals possesses both deep technical know-how and understanding of the insurance industry. Working with you, we provide the insights, tools and platforms you need to transform legacy systems, deploy new technology to streamline operations, and connect finance, risk and actuarial functions. We have successfully developed solutions that manage the change driven by:

- ▶ Intensifying prudential regulatory regimes
- ▶ Accounting change and the need for finance transformation
- ▶ The need to strengthen and embed risk-management capabilities
- ▶ Rising standards of business conduct or customer interaction, and the compliance agenda
- ▶ Commercial pressures arising from a difficult macroeconomic environment, combined with enhanced regulatory requirements

**EY** | Assurance | Tax | Transactions | Advisory

### About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit [ey.com](http://ey.com).

### EY is a leader in shaping the financial services industry

Over 30,000 of our people are dedicated to financial services, serving the banking and capital markets, insurance, and wealth and asset management sectors. At EY Financial Services, we share a single focus – to build a better financial services industry now and for the future.

© 2019 EYGM Limited. All Rights Reserved.

Artwork by JDJ Creative Ltd.

ED None

EYG no. 000942-19Gbl



In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

Information in this publication is intended to provide only a general outline of the subjects covered. It should neither be regarded as comprehensive nor sufficient for making decisions, nor should it be used in place of professional advice. Ernst & Young LLP accepts no responsibility for any loss arising from any action taken or not taken by anyone using this material.

[ey.com / fsminds](http://ey.com/fsminds)