



Transforming safely – the emerging practice of risk-managing change

McKinsey & Company

report contacts:

Daniel Mikkelsen, Senior Partner

daniel_mikkelsen@mckinsey.com

Joseba Eceiza, Partner

joseba_eceiza@mckinsey.com

ORX report contacts:

Simon Wills, Executive Director

simon.wills@orx.org

Esther Renfrew, Senior Research Manager

esther.renfrew@orx.org

Follow McKinsey:

 @McKinsey & Company

 @McKinsey_NGI

Follow ORX:

 @ORX_Association

 @ORX_Association

[mckinsey.com](https://www.mckinsey.com) | [orx.org](https://www.orx.org)

Introduction

The financial services industry is undergoing a transformation that is rapidly introducing new business models, new technology, new competitors, and, as a result, new risks.

Not changing is not an option; indeed, it could be the biggest risk of all. But to what extent is the very change itself – both the process and the outcome – a risk that should be managed? And if it should be proactively managed, then how and by whom?

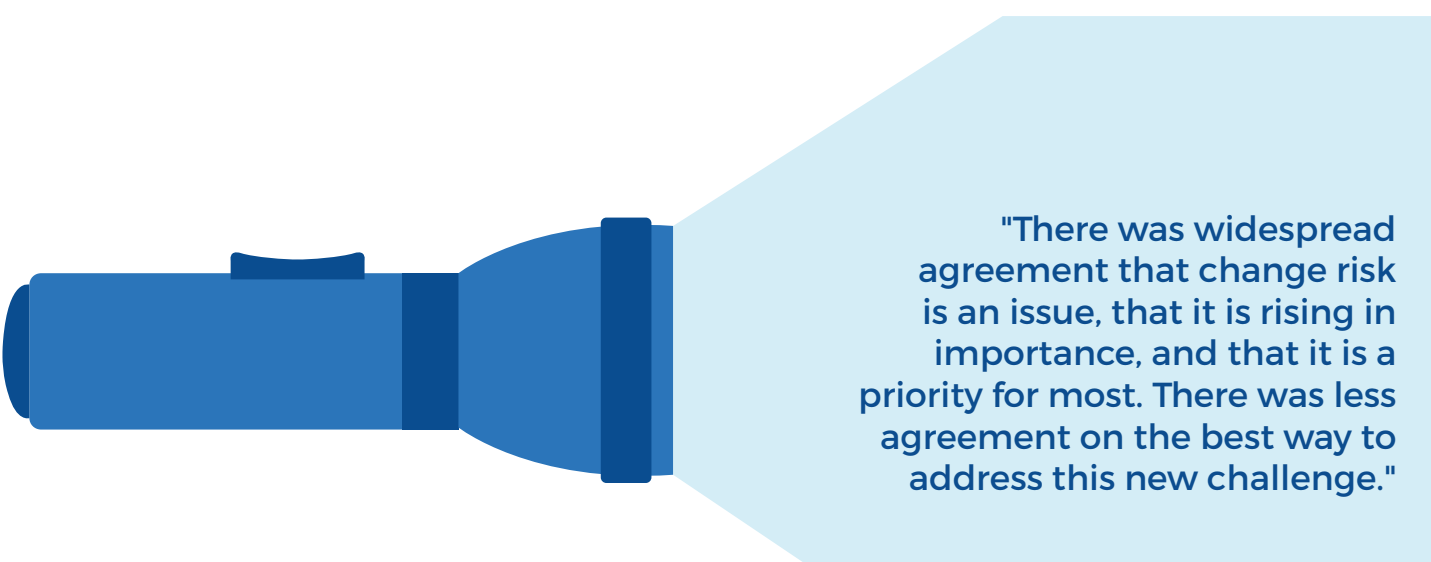
During the last quarter of 2018, ORX and McKinsey & Company conducted interviews on the risk management of change with the Chief Risk Officers (CROs) of 16 leading financial institutions, both banks and insurers, around the world. There was widespread agreement that change risk is an issue, that it is rising in importance, and that it is a priority for most. There was less agreement on the best way to address this new challenge.

Many CROs are focused on helping the business grow and “change safely” by delivering the change strategy rather than just prioritising avoiding loss. Most felt their institutions have a clear view of how major individual transformation projects are progressing, and there is no great need to increase oversight here. Instead, many CROs are focusing more on getting better at assessing and mitigating the risks that result from the effects and outcomes of these transformational projects – the “delivered risk” – rather than the risk of not

delivering the project on time, to specification, or on budget – the “delivery risk”.

No institution claimed to have a comprehensive worked-through approach to risk-managing change, but broadly, the CROs split into three groups. Roughly a quarter are content with their existing approach to change-risk management. About half are concerned about their institutions’ change-risk management but are seeking to address these concerns by using and enhancing existing processes and practices. The remaining quarter represent those institutions that are most actively improving their change-risk management processes. These CROs are typically most concerned about delivered risk and are actively developing new processes and practices to manage it.

No one expressed any appetite to create a formal new discipline or risk silo with a new framework. They frequently argued that their portfolio of operational risk (also known as non-financial risk), is already fragmented enough. Nevertheless, all the CROs were curious to learn more about what their colleagues in other institutions are doing, and we hope this report will offer some help in this regard.



"There was widespread agreement that change risk is an issue, that it is rising in importance, and that it is a priority for most. There was less agreement on the best way to address this new challenge."

What do CROs think?

The financial services industry is evolving at an ever-accelerating pace.

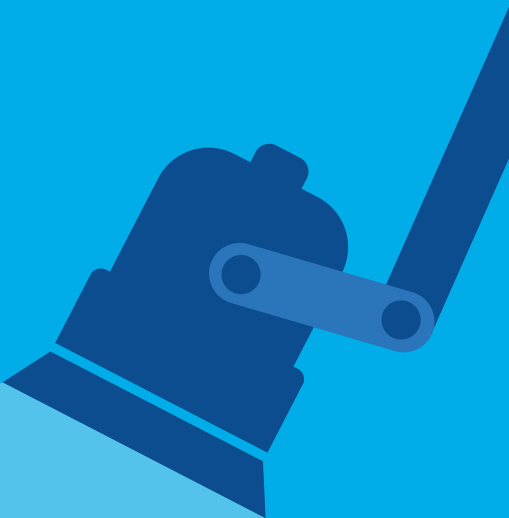
New business models are emerging that are upending how banks and insurance companies think about customers and value drivers. New technology is opening up impressive possibilities, but also introducing challenges. And new competitors are emerging, emboldened and enabled by such technology.

In response, financial services companies are launching dozens – hundreds in some cases – of change programmes. Such change creates its own risks – risks that are not always apparent and that can collectively affect an organisation's global risk profile. Yet reducing this risk by not changing may be the biggest risk of all.

If change is a strategic imperative – and every CRO we spoke to agreed it was – what does this mean for risk management? Change is not subsiding; all the respondents agreed that more change is coming and that the pace of change is accelerating. Half of them believed change-risk management is a high priority and 80 percent believed the risk itself is growing.

No surprise then that managing change safely is emerging as a key objective for many risk functions. Change-risk management is about being positive and proactive, meeting the demands of the business while having clear visibility on change risk, and aggregating those risks to understand the wider implications. Avoiding loss is important, but so is delivering the business strategy.

As one North American CRO said, “Overall, our strategy is to be more agile and to prepare for a higher speed of change. Risk has to tackle how to assess and manage the risk of all these change initiatives to enable the business to grow safely.”



“Overall, our strategy is to be more agile and to prepare for a higher speed of change. Risk has to tackle how to assess and manage the risk of all these change initiatives to enable the business to grow safely.”

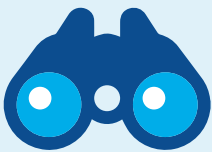
North American CRO

Why change-risk management is challenging

Every institution already has some way of managing change risk. Most participants said that their existing processes operate well in delivering projects on time, budget, and scope. Risk is also involved, often at a senior level, in providing oversight and control of these projects.

However, the environment of increasing change has highlighted several shortcomings of existing approaches, and many CROs recognised that improvements are necessary. Perhaps surprisingly, speed itself was not a core concern, although some CROs did mention the challenge of keeping up with the pace of change, and that they did not want to be (or be seen as) a block on progress. Overall, however, the more frequently cited challenges were visibility, prioritisation, aggregation, and assessment.

Visibility



Visibility came up most often as the major challenge and only one-fifth of CROs appeared satisfied with their current visibility of change risk. There are three specific issues: 1) the sheer number of initiatives, which makes it hard to get an overview of what is going on and what the risks are; 2) change initiatives not covered by existing processes can fall between gaps; 3) when the focus is on delivery risks (time, budget, and specifications), managing the delivered risks – such as risks to reputation or the impact on customers – relies on the awareness and engagement of individual managers or teams, which can be patchy.

Prioritisation

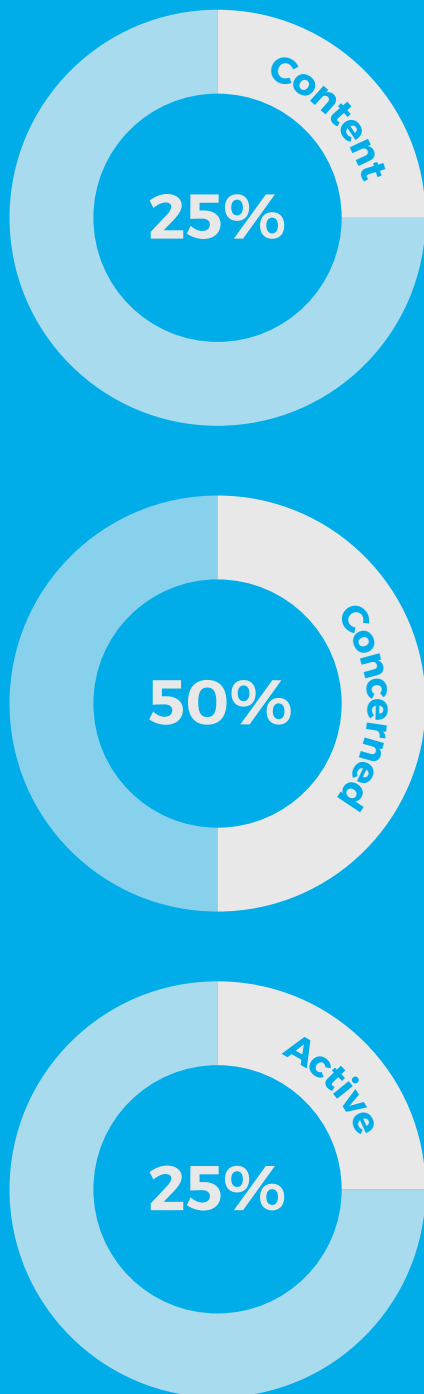


Some CROs told us that there can be a tendency to use size as the main arbiter of what is important, but most institutions recognise that this is not enough. For example, a small software change can have a disproportionate financial and reputational impact, as one bank found when it changed some code that broke links within its reporting system. This led to the bank inadvertently violating regulations regarding financial crime, which resulted in a very substantial fine.

Aggregation and assessment



Aggregating risk helps institutions understand their capacity to absorb change and handle the risks involved. Most CROs were concerned that perfectly sensible risk-management decisions might be made at a local, functional or entity level that – in aggregate – would present a problem at the global level. Such aggregation requires some standardisation of assessment, but most firms remain focused on qualitative assessment of change that is oriented toward highlighting potential risks rather than on understanding their appetite for change. Most firms default to some form of risk control self-assessment (RCSA) process.



About 25 percent are content with their current approach to risk-managing change. About 50 percent are concerned. The final 25 percent of CROs are active.

Three different CRO mindsets

Given the multitude of operational risks, most CROs were sceptical about addressing these challenges by developing new change-risk management silos that would require new definitions, teams, data and tools. Where they differed was in the degree to which they wanted to work within existing frameworks. Collectively, the CROs fell into three cohorts: content, concerned and active.

About 25 percent are **content** with their current approach to risk-managing change. They are typically focused on the delivery risk of large projects. They believe that their practices are generally good, but they know they can improve delivery. Interestingly, these CROs are often personally involved in change governance processes and senior committees.

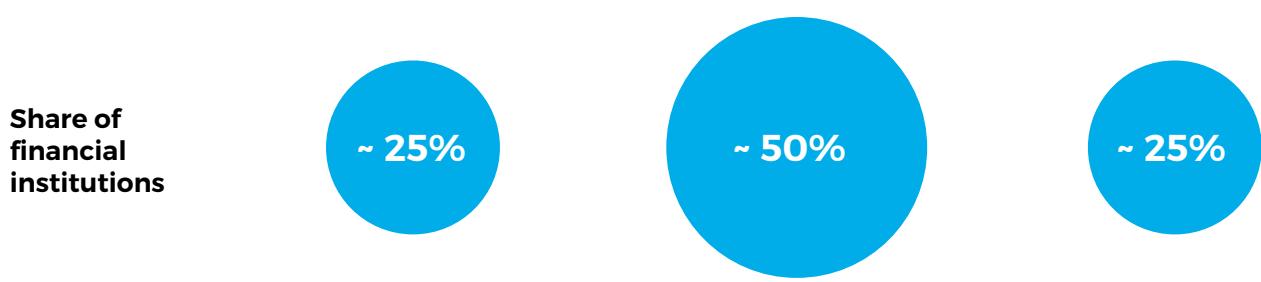
About 50 percent are **concerned**. They are also focused on delivery risk but worry about the delivered impact on their firms' risk profiles. Their approach is to incrementally adapt existing practices and processes, which means change risk is still defined by the scope of these existing processes, although CROs in this group are aware and concerned that this may leave gaps. CROs in this group typically try to ensure that Risk has a strong presence in the early stages of project governance, and they use existing processes such as RCSAs. Many are experimenting with new approaches to risk-managing change when the pace of transformation demands it. They are generally interested in creating a better aggregate view of the change-risk portfolio but struggle to do so.

The final 25 percent of CROs are **active**. They are purposefully developing and investing in new practices because they see risk-managing change as a strategic priority. Today they rely on existing change-management tools to manage delivery risk, but they want to expand the scope beyond existing change-management processes to become more granular. Some are developing new risk-assessment tools or introducing short-form versions of existing self- or risk assessment tools. Some are deploying or experimenting with sandbox and/or Risk Champion approaches, which we discuss below, and – like their “concerned” peers – they want an aggregate view of the change-risk portfolio but have yet to crack this.

Exhibit 1

CROs fall into three cohorts

	Content	Concerned	Active
Focus	<ul style="list-style-type: none"> • Delivery risk, traditional view of project-execution risk • Time, specifications, and budget 	<ul style="list-style-type: none"> • Mostly focused on delivery risk (similar to “Content”) • Some institutions starting to worry about delivered risk 	<ul style="list-style-type: none"> • Delivered-risk orientation, not just execution of projects or programs • Risk management as a strategic priority
Definition	<ul style="list-style-type: none"> • Traditional definition of change: <ul style="list-style-type: none"> - Project risk (typically large projects) - “Execution, delivery, and process management” (Basel taxonomy view) 	<ul style="list-style-type: none"> • Starting to think about what change means, both in terms of execution but also implications in the risk profile • Broader yet unclear definition: transformation, projects, new products, technological shift 	<ul style="list-style-type: none"> • Exposure that the portfolio of transformational initiatives create in the current risk profile and in the future risk profile • Expanding the scope beyond existing change management processes to get more granular
Key practices	<ul style="list-style-type: none"> • No aggregation of risk • Project management tools (focus on tracking milestones and budget) 	<ul style="list-style-type: none"> • Incrementally adapt existing practices (e.g., RCSA) • Ensuring Risk has a seat at the table • Aspiration to create the aggregate the risk view • Nonsystematic assessment of change risks 	<ul style="list-style-type: none"> • Emerging aggregation, and aspiration to create change risk appetite • Developing business change risk processes (similar to RCSA logic) • Risk Champions embedded into transformations



What are CROs doing?

While CROs recognise the obstacles they face, the challenge that they all must tackle – even those who are broadly content with their current approach – is how to identify, assess, prioritise and manage change risk without becoming an impediment to change or resented by the business and without inventing a whole new silo of risk management with all the associated costs and complexity.

As we spoke to CROs about their approach to change-risk management, we learned about a range of tactics they are adopting in terms of risk scope and definition, organisation, risk assessment, aggregation and appetite, and dealing with lessons learned.

Scope and definition

The scope of change risk is practically defined by the scope of existing change-management processes: major projects, new product approvals, etc. Risk typically engages in these processes, which create data that informs risk management. Where such processes exist, most CROs are confident that they work well, and that their institutions are good at overseeing the delivery of major projects. This particularly applies to projects that are well defined, linear and familiar to the institution.

However, even amid such confidence, there is a concern about gaps that can exist when existing change-risk management processes do not cover

initiatives that should be in scope – the visibility challenge mentioned above.

Even when CROs felt confident there were no major gaps, the processes are likely neither designed nor operated to identify and assess the delivered risk. Several firms are working hard to capture these risks by raising awareness of them and introducing risk assessment into change-risk management. As one European CRO said, “We have strong controls in getting from A to B. But we often don’t know the longer-term consequences of B.”

For this to work, institutions need to tightly define the focus of change-risk management in order that staff move away from looking at just the delivery risks. If CROs want staff to identify delivered risk as well, they need to communicate what exactly people should be looking out for and when to raise a flag. For example, one CRO was incredibly specific, asking staff to focus on the delivered impact on the priority areas of cyber risk and conduct risk.

“We have strong controls in getting from A to B. But we often don’t know the longer-term consequences of B.”

European CRO



Organisation

Rather than create a new change-risk function, CROs are focusing more on creating tools and a mindset that can be applied by the first and second lines of defence within existing change processes. Most CROs place change risk within the scope of operational risk and some mentioned that improving the general effectiveness of operational-risk management will help improve the effectiveness of change-risk management.

Several CROs observed that it is important to create opportunities for Risk to get involved early and have meaningful input in relevant change initiatives. There was positive feedback from CROs who are, for example, involved in investment committees. This level of engagement allows Risk to be proactive rather than reactive and works particularly well if Risk has real decision rights. One CRO from Asia-Pacific said, “How do you drive adoption of the methodology? Make it part of the existing change process and make it a mandatory stage gate.”

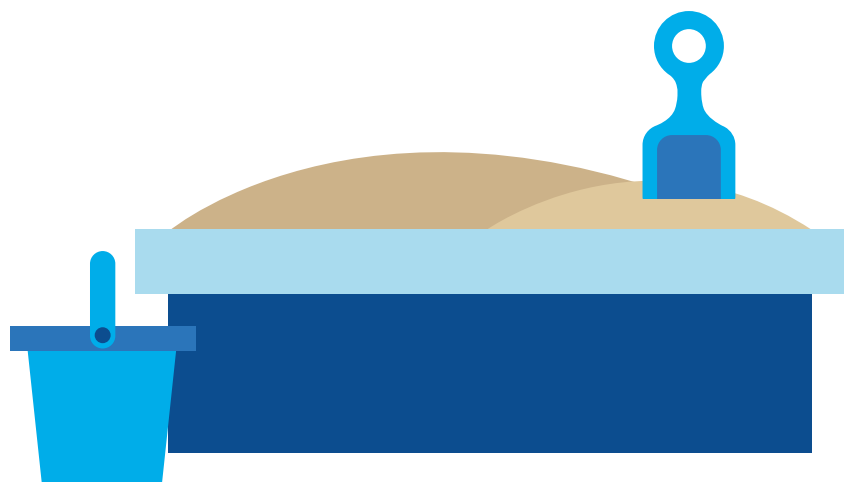
The exception to the concepts outlined above are those more radical ideas that are truly transformative rather than mere incremental improvements. These projects, often run by agile teams at a fast pace, are much harder for Risk to track and manage as they rarely conform to traditional governance structures. Agile delivery demands agile risk management. One solution mentioned by CROs is to use sandboxes during the development phase, which keep the project

isolated from the rest of the institution and actively encourage experimentation. Combining this with a Risk Champion can give Risk visibility on the potential delivered risk before the project reaches a scale where it is taken out of the sandbox and into normal governance processes. This is provided that they don't breach clearly defined parameters such as reputation or a financial loss of a certain amount.

Risk Champions are senior risk professionals who are comfortable with prioritising and decision making and who have subject-relevant skills, for example in IT. By embedding them in an agile project team, they act as a single voice to represent Risk and can bring in expert opinion when needed. The champion role helps Risk move at the speed of the business so it is no longer a blocker. For example, the Risk Champion can prioritise two or three key risks for initial assessment and mitigation rather than trying to be comprehensive.

Several CROs noted that the champion role is seen as increasingly attractive within the function because it is high-profile, fast-paced, and the person in the role is able to have real impact. On the flip side, several CROs noted that Risk staff tended to find the champion model “scary” because it means asking risk specialists operating in a generalist role to make significant decisions on topics such as which risks to prioritise for assessment and mitigation.

One solution mentioned by CROs is to use sandboxes during the development phase, which keep the project isolated from the rest of the institution and actively encourage experimentation.



Risk assessment

Approximately 60 percent of institutions have a defined process that specifically identifies and assesses risk in change, which in many cases is a variation of RCSA. Others use established tools such as their standardised RCSA or new-product approval processes in line with the general desire to use existing processes. Those processes often take the form of workshop-based assessments that bring together all the relevant stakeholders, including the first line of defence.

Some CROs deploy the same impact and probability scales used in RCSA, alongside dimensions such as financial, reputational, and regulatory risk. Only around one-quarter have metrics to quantify change risk on an ongoing basis.

Where a Risk Champion exists, they are often the person leading the assessment with the business and are tasked with looking at the material impact of the change programme on the overall operational risk profile and factoring in the environment into which the change will be delivered. A high-risk change project going into a high-risk environment will create considerably more concern than a high-risk project going into a low-risk environment. As one European CRO put it, “We look at it as a harbour. Is the harbour ready to receive the ship?”

CROs at the institutions that include this information noted that the environmental assessment is usually already available. Some mentioned that the business has given positive feedback on the added value of this step, which can be achieved at minimal additional cost.

In the agile setup we described above, a Risk Champion can dramatically speed up risk assessment and mitigation. At one firm, where Risk had acquired a reputation as an impediment to change, a move to be tougher on proposals up-front helped it reduce assessment time by 90 percent.

Another firm focused on broadening the scope of assessment because it was concerned that there was a lack of consistency around identifying change risk and the result was that only project size was being considered. The Risk team developed a tool that asks the business behind each change programme fewer than ten key questions. An expert team, including cyber risk specialists and financial-crime experts, reviews the answers and makes recommendations accordingly. This tool has now become part of the standard change process across the firm and has also helped drive engagement with the risk component of the projects.

As the majority of the CROs acknowledged, the volume of projects remains a significant challenge for most firms – assessing and identifying the risks when there could be thousands of changes per quarter, and tens of thousands a year is a herculean task. Consistency, simplicity and speed help meet this challenge, but the key is to see problems early and prioritise effectively. An engaged first line of defence is critical, assuming that everyone shares a common understanding of what is important.

“We look at it as a harbour.
Is the harbour ready to
receive the ship?”

European CRO



Aggregation and appetite

Aggregating change risk is a challenge shared by all participating CROs and a priority for most. Yet no one has found a powerful solution. Only one institution said it was satisfied with the way it aggregated the portfolio of change risks. Firms want to understand how the risks of different change initiatives are interrelated and identify concentrations of risk. Concentration, in this context, is not a matter of size but of impact in terms of locations, skills, people, functions, and business units.

Today, firms that attempt to aggregate change risk use qualitative measures such as RAG or scale assessments (high/medium/low). Measuring more quantitatively is aspirational, but in the short to medium term CROs just want to be confident that they can see where the problems might lie so that they can manage the risk, reallocate resources, and potentially adjust the timing of change initiatives.

Some firms have gone further and want to understand the aggregate view so that they can maximise the use of their firm's capacity to change. This approach treats the capacity for change as a scarce resource. The aspiration for most respondents is still to identify and assess the risk, aggregate the portfolio view, and eventually link it to risk appetite.

The biggest challenge for aggregation is the lack of consistency in assessment methodology. It is this goal, more than any other, that is driving a few firms to consider more standardisation of risk assessment. "A dashboard that says, 'Here is our appetite for change and measures against that.' That's nirvana," said one European CRO.

Lessons learned

As firms become more focused on assessing change risk, they are increasingly keen to take the opportunity to compare their assessments to the outcomes. At the moment, the very notion of change risk is not developed enough to make this more than an aspiration for many. But a number of CROs pointed out the value of tracking both positive and negative outcomes relative to the expected risk outcomes and expressed a desire to improve their firms' ability to do so.



“A dashboard that says, ‘Here is our appetite for change and measures against that.’ That’s nirvana,”

European CRO

Shining a light on the dark spots



While traditional ways of reviewing projects may measure time, budget and scope, it is the critical risks falling outside of the spotlight that are a cause for concern to CROs.

There may be good visibility of risks within individual projects, but having full visibility of the aggregated view is more challenging.

If the scope of change risk is defined by aggregating the output of existing change processes, then risk managers may not be clear on what might be falling through the gaps and whether new processes or a broadening of scope are needed to plug the gaps.

MIND THE GAP

Checklist for change

Based on all the input received, we have come up with a list of discussion topics for CROs to raise when addressing change-risk management.

This is very much a topic list, not a wish list of what an institution should or must do.

How do you define what change risk (and indeed change) means to your institution?

Definitions and naming conventions will vary by institution, as will the degree to which they focus primarily on delivery risk versus delivered risk. Whatever the definition, everyone needs a clear understanding of it, so they know what risks to look for and flag.

How much risk falls outside traditional risk management processes?

If the scope of change risk is defined by aggregating the output of existing change processes, then to what extent are risk managers clear on what might be falling through the gaps and whether new processes or a broadening of scope are needed to plug the gaps.

When does Risk get involved?

There are, of course, benefits to being proactive and acting on the change portfolio before initiatives get started, though some organisations still choose to wait to review potential risks once a change project is already well down the track.

Should you appoint Risk Champions?

The concept of a Risk Champion goes beyond a person; rather it's a model for how Risk partners with the business. Many institutions have successfully used the Risk Champion concept in order to have someone close to business decisions who can assess and triage the risk of change, including in agile change initiatives that may fall outside traditional project management processes. Would such a role be applicable in your organisation?

Is what you have enough?

There is likely no need to create a new risk silo; existing tools and approaches are probably perfectly acceptable, but to what extent do they need tailoring to this new change-led environment?

What is the environment in which change will happen?

There is value in assessing whether a high-risk project is going to take place in a high- or low-resilience environment (and the relevant data for this likely already exists), and this may inform a go/no-go decision.

How can you determine change risk appetite?

Understanding the organisation's capacity for change means aggregating change risk. Different levels of aggregation will be appropriate for different institutions. Any aggregation requires some degree of standardisation of change-risk assessments, but CROs we spoke to emphasised that it is more important to be effective than to be precise when it comes to such assessments. The outcomes help CROs answer questions such as "How much change is too much?", "Do we have enough of the right enablers of change?", or "Where do we have more change capacity in the organisation?"

Are you learning from history?

Examining what happened in previous change-risk situations helps many risk functions learn and refine their models and approaches. Similarly, those that have introduced a change-risk angle to incident reviews and post-mortem analyses of other non-business-as-usual situations have gained important additional information to improve change-risk management.

Closing thoughts

In light of what we heard from CROs, our own experiences working with clients on this topic, and broader discussions in the industry, we wanted to finish by sharing some of our thoughts on the topic.

Transformational change involving digitisation and advanced analytics will undoubtedly be a feature of financial services for years to come, and CROs increasingly recognise the importance of change risk. In the latest ORX survey of emerging risks, it entered the top 10 for the first time.¹ In fact, digital disruption was identified as the leading emerging risk, and, in our view, this is a major driver of the change risk that companies face.

Risk-managing change presents a welcome opportunity for operational risk management to proactively manage the risk profile, help the business grow safely and engage positively with senior management. Operational risk managers are already aware of this. When asked where they most usefully engage with the business, they often answer “new product or project approval.” These issues give operational risk managers the opportunity to engage in discussions and help make decisions on concrete proposals that create risk in return for expected business benefits – a bit like a credit officer approving loans. It provides an opportunity to help the business and make a difference – as well as to fix problems before they emerge.

Risk-managing change is that opportunity writ large. It provides a chance to manage not only the traditional project risks – i.e. failure to deliver on time, on budget and to specification – what we have called “delivery risk”. It also provides an opportunity to manage the impact of change initiatives on the broader future risk profile of the institution – what we have called “delivered risk” – not only for each individual initiative, but for the totality of all current and proposed change initiatives in the organisation.

This study has shown that the industry could enhance current practices, and that many see a good case for doing so. The volume of initiatives, the interconnectedness of efforts and the speed of change are very substantial, and hence the amount of both delivery risk and delivered risk is high – yet the latter in particular is often opaque to both risk management and senior executives.

Change-risk management is clearly still a discipline under development, though one of increasing focus. We believe this study provides some useful pointers for its evolution and the checklist for change above offers a starting point for CROs to think through how to tackle it. There are also already some sound practices and initiatives highlighted by the CROs we spoke to that are worth considering:

- Enhance the first line’s risk awareness and involvement. The front line is driving the change, so it is necessary that they are aware of the delivered risk in addition to the delivery risk.
- Make sure the second line is faster and a better partner for the first line. Operational risk must be early to the table where change decisions are being made. A key way to shape and steer the future risk profile is by acting on the change portfolio.
- Create a framework for ex ante analyses, challenges and decisions, using existing methodologies, tools and data. Start by clearly defining what change risk means for the institution, not only in terms of delivery risk but also in terms of delivered risk and then define a framework building on existing operational risk tools. Make sure you include all risk types, including AI/model risk, data risk, cyber risk and conduct risk in your analysis of delivered risk and aggregate up to create a portfolio view to steer change.

Change is here to stay, and it is undoubtedly a strategic imperative for most financial institutions. In this context, managing the risks created by change strikes us as a key strategic challenge and a necessary skill set for risk managers. We think this is an exciting emerging trend and CROs should act to ensure that their firms proactively shape their risk profiles.

¹ ORX Operational Risk Horizon Report 2019: <https://managingrisktogether.orx.org/research/operational-risk-horizon-2019>

The authors would like to thank Chief Risk Officers from the following institutions for participating in this study:

ABN Amro

AIB

AIG

Allianz

AXA

Barclays

CBA

Credit Suisse

DBS

Deutsche Bank

HSBC

Intesa SanPaolo

Morgan Stanley

OTP

RBC

US Bank

About McKinsey & Company:

We help organisations across the private, public, and social sectors create the change that matters. We have always helped our clients identify and set the direction toward their most important goals. Today, we go further: working together to turn these ambitious goals into reality.

From the C-suite to the front line, we partner with our clients to transform their Risk organisations in the ways that matter most to them. This means embedding digital, analytics, and design into core processes and mind-sets; building capabilities that help organizations and people to thrive in an ever-changing context; and developing excellence in execution to ensure that actions translate into outcomes, quickly and sustainably.

With exceptional people in 65 countries, we combine global risk expertise and local insight to help you create the change that truly matters.

About ORX:

ORX is the largest operational risk association in the financial sector and has been a leading support for the industry since 2002.

For nearly two decades, we have been an ever-expanding global community, bringing together thousands of operational risk professionals to share knowledge, expertise and experience.

Our services include a range of solutions focused on effective management and measurement of operational and non-financial risk. Alongside this, we run an extensive risk management and measurement research programme and hold events around the world.

We not only support individual organisations to assess their vulnerability to losses, but we also shape industry-wide development of best practice.

ORX is owned and managed by over 95 financial firms from all over the world. As a not-for-profit organisation, we invest all income back into providing high-quality benefits for operational and non-financial risk professionals. This ultimately helps develop the future direction of the discipline.



McKinsey
& Company

O.R.X