McKinsey & Company

Risk Practice

The value for insurers in better management of nonfinancial risk

Is 6 percent or more of your net income flying out the window?

by Kevin Buehler, Marco Carpineti, Erwann Michel-Kerjan, Fritz Nauck, and Lorenzo Serino

November 2019

Insurers are in the business of taking risks. Financial risks are the most familiar kind. In the decade following the 2009 financial crisis, CEOs and boards of insurance companies largely focused their attention on better managing financial risks. However, nonfinancial risks—also known as operational risks—are a second critically important risk type that we believe has been largely overlooked.

Nonfinancial risk is more diffuse, affecting many aspects of the day-to-day operations of the insurer. Serious misconduct, execution risk, key personnel risk, fraud, failing IT systems, cyberattacks, data leakage, faulty model assumptions, reputational crises: insurance executives know the potential harm these risks can do to their organizations. What they may not know is that operational-risk incidents can cost firms 6 percent or more of their net income. In a sector with global revenue of $5 trillion, the values involved run into the tens of billions of dollars.

McKinsey research on global and regional insurers suggests that robust capabilities in operational-risk management can enable companies to prevent incidents (or reduce their downside) while also making them more competitive.[1] Since CEOs are increasingly making cost reduction a strategic priority, management teams can start considering operational risk as a source of value.

We found that a few leading organizations have a firm grip on nonfinancial risk—able to calculate, for example, how much they have lost directly and indirectly across all risk types over the past 12 months. These organizations take a strategic approach across the three lines of defense, to address operational risk events, measuring and actively monitoring them across the enterprise to rapidly mitigate. For the majority, however, the grasp is less certain. Tens of millions of dollars expended on operational losses annually, scattered across an organization, can go unreported and be little understood by top management and the board. It is as if net income and earnings per share are allowed to fly out the window.

The importance of nonfinancial risk has become more evident as the insurance industry goes through a multifaceted transformation. Powerful drivers are behind this shift, including rapidly escalating customer expectations, accelerating technological innovation, the emergence of new sales forces, the proliferation of complex models, and new imperatives for cost reduction. In consequence, the risks for insurers in executing business strategy are evolving more rapidly.

The industry has experienced more risk incidents in recent years, and operational-risk management has been elevated to a top-management priority. Our survey on managing nonfinancial risk in insurance found that more than half of participating companies are already increasing their budget for addressing these risks and hiring additional talent. Many companies reported spending a lot of time and resources on "firefighting"—addressing issues and incidents on an ad hoc basis as they occur. These companies are looking to take a strategic approach to nonfinancial risk to improve both efficiency and effectiveness.

Transforming nonfinancial risk management for value

Tangible financial impact can be achieved by reducing operational risk, in an approach that is clearly linked to the business strategy of the insurer and improves customer experience. Several foundational elements are needed to enable the approach: an accurate, business-driven risk taxonomy; governance based on

[1] McKinsey's Survey on Managing Nonfinancial Risk in Insurance was conducted in 2017 under the auspices of the Global Insurance Chief Compliance Officer Forum. Sixteen insurers (13 global and 3 regional firms) participated; the survey focused on the regulatory environment, the mandate and organizational dimensions of compliance and operational risk, and trends in the management of nonfinancial risk.

the three lines of defense; and relevant capabilities and skills. In this last category, both human talent and advanced analytics and artificial intelligence are vitally important. A further ingredient, which in some ways is the source of the others, is an elevated risk culture. These foundational elements enable the accurate measurement of nonfinancial risk and its appropriate management—opening the way for advanced-analytics approaches that help reduce losses and create value.

A business-driven risk taxonomy

Insurers must establish common definitions for operational-risk types across the organization. A comprehensive taxonomy typically articulates 10 to 15 risk types, including compliance requirements. Compiling this taxonomy therefore involves a coordinated effort by risk and compliance, working very closely with the business. The result should permit the different parts of the organization to use the same vocabulary while ensuring that the risk types considered in the organization's risk profile comprise the entire relevant risk landscape (usually with three levels of detail). To be effective, however, the taxonomy needs to be periodically updated based on emergent risks in the organization's changing business environment. The updates are the result of risk identification, a core risk process. They can form the basis of a dedicated enterprise-risk dashboard developed to link lagging and leading indicators (risk drivers) to help prioritize and reduce risk.

Governance: The three-lines-of-defense model

Insurers first developed the three-lines-of-defense model to address financial risk; they are now adapting it to create an effective governance structure to manage operational risk. This domain requires more complex governance, however, with oversight of almost all the organization's processes and business activities. According to the model, clear roles and duties are established for essential operational-risk management tasks, along with enhanced communications across the lines. This systematic approach to risk governance requires that the business and corporate functions (first line) clearly understand and own risks. These functions ensure the day-to-day management and ownership of operational risks and controls, keeping assumed risks aligned with the risk-appetite framework designed by the operational-risk function (second line). The second line comprises the chief risk office, legal, and compliance. It provides checks and balances as well as challenge and guidance to the first line on operational-risk aggregation and standardization. The second line should be able to come to the businesses with accurate calculations of losses and compelling business cases for discussion. This will help promote business accountability for operational-risk topics. Internal audit (third line) has an independent mandate for oversight of the first and second lines and reports to the board and the regulator. Those functions are complemented by risk committees (operational-risk committee, enterprise-risk committee, the board's audit committee), with clear mandates and composition, as well as decision-making power in their respective domains. A well-defined escalation path and remediation protocol should also be in place and exercised regularly.

Capabilities and skills

Most insurers responding to our survey highlighted the need to improve capabilities and skills, especially in digital and advanced analytics. Real-time analytics, for example, can have a transformative impact on the accuracy of risk detection. Yet many insurers still perform most of this work manually; furthermore, the efforts do not often address the totality of operational risks that can affect the organization. Another important dimension is talent development. Insurers need to acquire or develop talent to partner with

top management on nonfinancial-risk topics, and to manage and model specialized risk types. Leading insurers now have as many as half of their risk-function employees focusing on operational risks. On this point, many insurers say that they expect cybercrime, conduct risk, and privacy (including data protection) to be the three fastest-growing nonfinancial risks in the next several years. All three risk types are very complex and addressing them requires highly specialized knowledge.

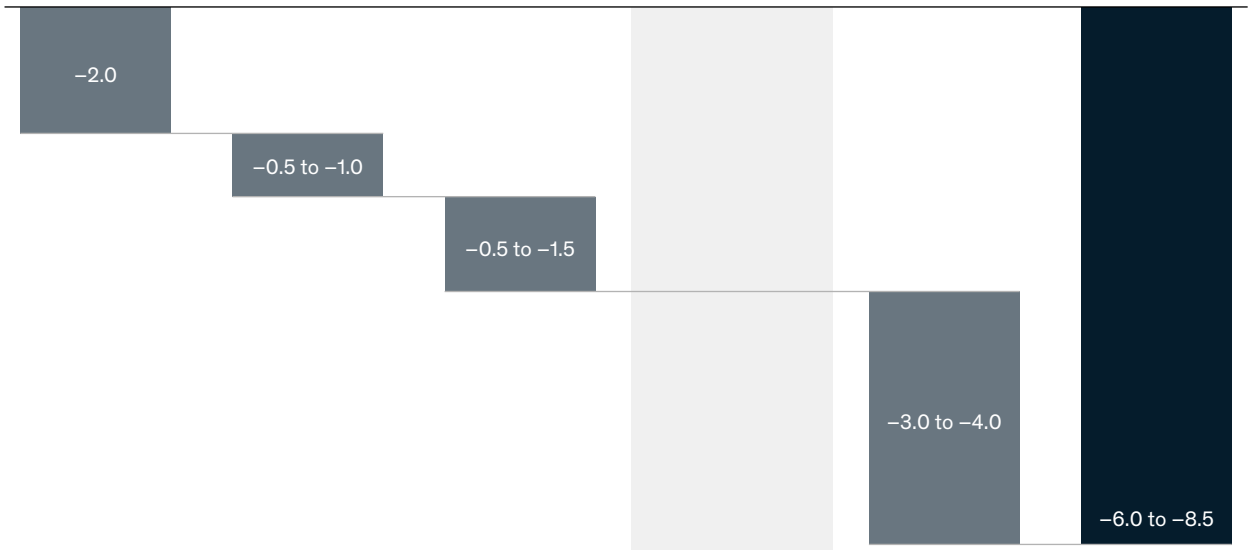
Risk culture

Risk culture involves the organization's basic orientation toward identifying and managing risk. Ideally, the orientation is promoted by top management and taken up by frontline and back-office personnel. Concretely, accurate measurement enables leaders to make informed decisions while highlighting the importance of operational risk as a means to create value. Many organizations have run dedicated diagnostics to measure their risk-taking culture. The outcome is an executive-level scorecard providing insurance decision makers with deep insights into business units and corporate functions. By moving the discussion from a fuzzy concept to a quantitative approach, sized across predefined dimensions, the scorecard helps leaders better evaluate their risk culture. They will be able to see weaknesses and root causes, and thus remediate much more effectively.

Exhibit

Direct losses and associated indirect costs stemming from operational-risk incidents can cut 6 to 8.5 percent from a company's net income.

Estimated losses by adjustment type, % of net income



Recorded incidents
Category is rarely comprehensive

Unrecorded incidents
Including detected and undetected incidents

Multiplier:
1.2–1.4×

Taxonomy risks with no data available
Not all elements in the risk taxonomy are measured

Multiplier:
1.2–1.7×

Potential costs of low-frequency, high-severity events
These possible events are measured through scenario analysis: impact excluded here

Indirect costs
Possibly twice the amount of direct costs

Multiplier:
1.5–2.0×

Total
Losses for unrecorded operational incidents can be three or four times the cost of recorded incidents, hence the overall total can climb above 6% of annual net income

Measuring the impact of operational-risk losses

Insurers seek to make comprehensive impact analyses of operational-risk incidents. Painful experience shows that such analyses can lead to more accurate assessments that are three or four times the size of the direct losses an organization suffers. Insurers have, by this measure, incurred losses of 6 to 8.5 percent of net income (exhibit).

The importance of accurately assessing the true impact of risk events cannot be overstated. Assessments obviously account for direct costs—financial loss resulting from risk events, including such costs as regulatory fines and customer remediation. However, indirect costs are often twice the direct losses.

Direct and indirect costs must furthermore be calculated for unrecorded incidents. Low-severity, high-frequency risk events must be thoroughly assessed, across the organization and including all risk types. In 2018, such events amounted to more than three-quarters of the total number of events and around half the monetary losses insurers incurred.[2]

Finally, the impact of low-frequency, high-severity events has been excluded from our calculation. These events are often addressed through scenarios that do not provide loss calculations. When they occur, the events can be very damaging, affecting the franchise of the insurer and its market capitalization. Recent events in this category have caused share-price declines of 10 to 15 percent, equivalent to billions of dollars in market-capitalization losses. The effects tend to be long-lasting, as investors lose confidence in the management team's ability to execute properly.

In light of these considerations, leading insurers have established a centralized operational risk–loss database, including in it the full range of risk events and their true impact. This allows near-complete visibility of the operational-risk profile, from which compelling business cases for operational-risk management can be developed. Such business cases will provide the basis for meaningful interactions on risk topics with the CEO and the board.

The next horizon: Advanced analytics

The revolution in data availability as well as the simultaneous development of advanced analytics have created transformative opportunities across all core risk processes—including in operational risk.

- *In conduct risk,* for example, leading financial-services firms have developed sales-monitoring programs using advanced analytics to identify high-risk advisers and flag risky incidents. One particularly effective approach draws on a wide array of internal data, including customer complaints; sales data by product, customer, and employee; service calls; and customer-feedback surveys. It also uses natural-language processing as well as classification-predictive algorithms to identify potential misconduct from the pool of customer complaints that have already been evaluated. In one instance, detection was significantly improved (to 70 percent effectiveness) using analytics and artificial intelligence.
- *In fraud,* a leading organization used a machine-learning algorithm to pilot improvement in fraud detection in claims reimbursement. The pilot addressed an inefficient claims-management process that was unable to prioritize claims waiting for auditor intervention. The company created an automated process relying on advanced analytics and machine learning that now identifies high-risk claims for prioritized review. The approach has led to significant reductions in the original invoiced amounts; the company believes that savings could surpass 50 percent.

[2] *Annual Insurance Loss Report*, O.R.X., June 2018, manageriskstogether.orx.org.

— *In complaints management,* one insurer developed an automated natural-language-processing tool to analyze complaints and extract key topics for monitoring emerging risks. Using the new approach on an unstructured complaints database with hundreds of thousands of items, the company was able to match most complaints to a dozen or so recognized risk topics. Also identified were a few emerging topics that could lead to reputation- and conduct-risk incidents.

In an environment where leading insurers can lose 6 to 8.5 percent of net income to nonfinancial risk, the operational-risk function has to transform itself into a value-creating business partner. With a proactive, analytics-driven profile, the optimized function can detect suspicious activity more accurately, prevent incidents more effectively, and focus on new risks as they appear on the horizon. From this position and with specialized talent, the risk function can now expertly partner with business executives to digitize infrastructure and automate controls. These powerful capabilities translate into lower costs and improved competitiveness for the company.

Given the rising level of operational risk, it is worth asking, how much should companies be willing to invest to remediate the situation?

Kevin Buehler is a senior partner in McKinsey's New York office, where **Marco Carpineti** is a consultant and **Lorenzo Serino** is a partner; **Erwann Michel-Kerjan** is a partner in the Philadelphia office; and **Fritz Nauck** is a senior partner in the Charlotte, North Carolina, office.