

# Risk Sensing

The (*evolving*) state of the art





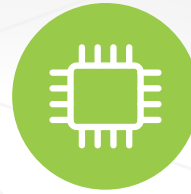
**Economic upheaval**



**Market evolution**



**Regulatory demands**



**Technological change**

...will continue to disrupt ways of doing business, as well as entire industries. In response, organizations have been developing risk sensing capabilities of various types in various ways. How organizations define, design, and deploy those capabilities will largely determine the success and sustainability of their risk sensing programs.

To gauge the current state of risk sensing, Deloitte, in a survey conducted with Forbes Insights, asked C-level executives in large organizations about their companies' risk sensing capabilities. This document, directed to senior executives, presents a definition of risk sensing, key results of the survey, and an approach to developing and enhancing risk sensing capabilities.

### **Why present an approach to risk sensing?**

This survey revealed that most executives state that their organizations have risk sensing capabilities. However, the survey also indicates—in keeping with Deloitte's experience—that these capabilities often miss key elements, lack technical depth and analytical sophistication, reside in narrow technical units, fail to focus broadly enough, or otherwise leave the organization open to the very risks that risk sensing should be detecting and monitoring.

Moreover, sensing emerging strategic risks can position an organization not only to avoid and mitigate risks but also to generate risk-powered performance. The latter creates value from risk by moving early to address nascent market movements and customer needs, harness benefits from emerging technologies, and block competitors' efforts to gain first-mover advantage.

# Contents

Define and design	3
Risk sensing now	5
What to do?	10
An evolving capability	13



# Define and design

Risk sensing employs human insights and advanced analytics capabilities to identify, analyze, and monitor emerging risks to the organization's business model, long-term viability, and ability to create value. This is done by identifying and then monitoring strategic risk indicators of events, trends, and anomalies in structured and unstructured data from internal and external sources and comparing them with the organization's risk tolerance levels and thresholds. Advanced analytics, combined with business-driven risk indicators, provides the ability to analyze this data in various scenarios to identify the risks most relevant to the organization's business leaders and decision makers.

Risk sensing aims to detect emerging risks so that management can mitigate those risks before they generate potentially significant damage or costs or require higher investments. Companies can also identify emerging trends and thus enhance their understanding of the risk/reward tradeoffs inherent in value creation and improve their funding decisions and allocation of resources.

**A robust risk sensing capability encompasses the following characteristics:**

## Strategic focus

Most major organizations monitor financial, operational, regulatory, reputational, and other risks specific to the business. Risk sensing should incorporate these risks to the extent that they help inform strategic decision making. Significant additional opportunities to expand value come from identifying and monitoring strategic risks—those that could undermine strategic objectives, negate management's assumptions, or exceed the organizations' risk appetite.

## Listening posts

Listening posts and observable indicators enable tracking of trends and emerging disruptors. An example would be monitoring emerging technology trends that could disrupt the industry or changes in customer sentiment expressed in statements about the company and its products and services. Listening posts can also be established to monitor employee sentiment to assist the organization in shaping its culture and its ability to retain talent.

## C-suite engagement

Senior executives possess the influence, resources, and organization-wide view to ensure that risk sensing does not become siloed, narrowly focused, or overly tactical. Equally important, senior management should integrate risk sensing into the risk governance and risk management program. That integration generates actionable insights related to plans, key metrics, and thresholds to support decisions of senior-level executives. It also ensures that those insights are communicated to the right senior stakeholders and result in coordinated actions.

## Metrics and tracking

Objective baseline measures of risk—strategic risk indicators and parameters—should be developed so risks can be tracked against those measures going forward. Ideally, the risk sensing program includes triggers (relative to risk tolerances) for evaluating, communicating, and mitigating risks.

## Outside-in points of view

Views of external analysts who understand the organization, its goals, and the risks it faces provide “another set of eyes” as well as a necessary corrective to the inevitable cognitive biases that can distort the views of management and other internal parties.

## Combined technological and human resources

Analyzing and predicting rare and emerging events has become increasingly possible with advances in data analytics and technology. Yet human analysis completes the job, enriching these views and providing valuable, otherwise unavailable information and insights.



# Define and design

Not all events result in significant impact. Understanding which events pose the greatest risk and opportunity enables leaders to focus resources on what matters most. This implies that the risk sensing program should not be sequestered in a lab, or relegated to technical specialists untethered to the goals of the organization. Rather, it should be informed by the decision-making requirements of senior executives, aligned with risk management requirements, and guided by an enterprise-wide view of risks. Since risks are often interrelated and can amplify one another, they should be monitored and addressed in a coordinated manner.

Risk sensing should focus on key risks—those that could affect competitive advantage, market position, and performance. It should incorporate mechanisms for developing an integrated view of risks and opportunities, and support economical, practical, productive responses. It should be developed with ongoing input from C-suite executives to ensure that it remains relevant, timely, and responsive to their planning and decision-making needs and to those of the business units, risk managers, and compliance function.

Risk sensing should also be integrated into the risk management and governance program. This calls for clear communication and response plans combined with actionable reports useful to executives, risk managers, and business unit heads, which means that summary reports and visualization tools such as dashboards are also an essential element. A direct line from the sensing team and CRO to the CEO and board would be useful, particularly in the case of emerging strategic risks.

# Risk sensing now

To assess the state of risk sensing in large organizations, Forbes Insights, on behalf of Deloitte Touche Tohmatsu Limited, conducted a survey of 155 executives from companies representing every major industry and geographic region. The survey, conducted in May/June, 2015, targeted companies with revenue of at least US\$1 billion.

The results clearly indicate that these organizations have been developing their risk sensing capabilities, at least as the respondents and their companies define them. The responses reveal that although most companies in our sample have deployed risk sensing in some capacity, the capabilities vary. Companies also vary in the risks they monitor, the people to whom risk sensing efforts report, and the risks they view as most important.

Among the most interesting findings are the following:



Companies apply risk sensing, but less often to strategic risks



Two-thirds believe they have the right people



The risks of most concern are shifting



The value of external points of view merits further discussion



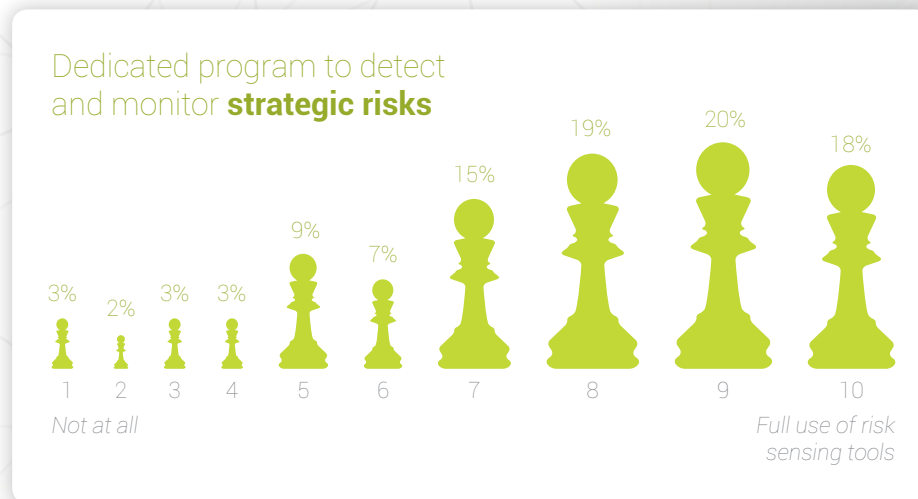
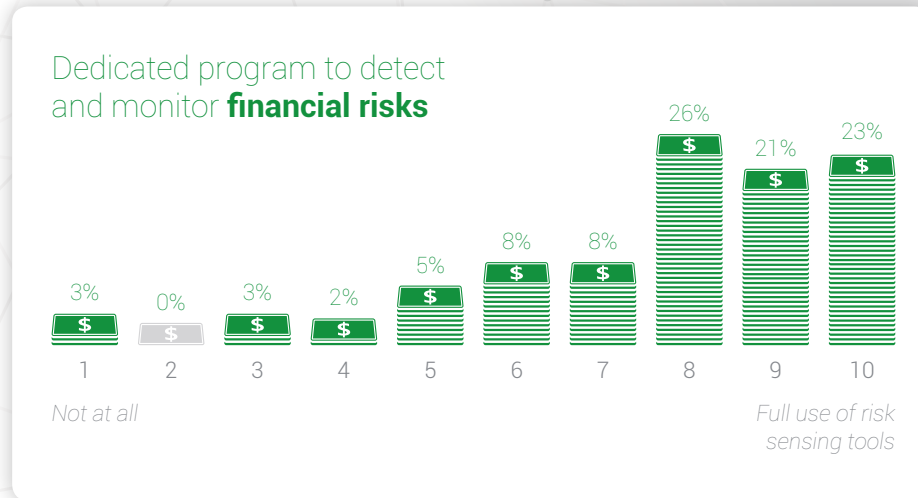
# Risk sensing now

## Companies apply risk sensing, but less often to strategic risks

Overall, about 80 percent of respondents agree that they use risk sensing tools. However, based upon the top three "Agree" answers on a scale of 1 to 10 (Figure 1), they apply them most often to financial risk (70 percent), compliance risk (66 percent), and operational risk (65 percent), and less often to strategic risk (57 percent). Yet strategic risks tend to be most important to senior executives.



Figure 1: A look at four specific risks\*



\* Percentages throughout may not add up to 100% due to rounding



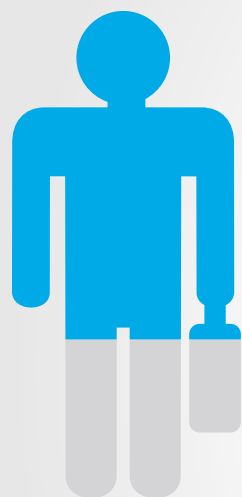
# Risk sensing now

## Two-thirds believe they have the right people

While approximately two-thirds of respondents agree (based on the top three “Agree” responses) that they employ people with the knowledge needed to monitor, analyze, and act on risk sensing data (Figure 2), about one-third are less certain that they have the right people.



**Figure 2: Do you have the right people in risk sensing?**



65%

agree/strongly agree that they employ people with adequate knowledge to both monitor and analyze risk sensing data and make it actionable for the business.

Not surprisingly, the largest companies—those with at least US\$5 billion in annual revenue (as opposed to those in the US\$1 billion to US\$5 billion range)—most often agree, given their deeper talent pool.

Depending on the size of the team in a respondent’s company, this may also be an indication that they rely solely on people, while additional, broader, and more in-depth analysis could be done using tools. Such tools reduce the mundane, initial data-

gathering and analysis time and effort and free resources for more complex analysis and higher value added activities.

In practice, some companies that have the right people may not always equip them with the right tools. Those tools include not only data scanning and sensing, but measurement, analytical, and visualization tools—the latter being essential to applications of risk sensing and analysis of big data and strategic risks. Many companies focus on visualizations, dashboards, and analyses of historic trends in internal data, but few use pattern analysis, scenario analysis, or other complex analytics, such as rare event analysis, and thresholds to monitor risk over time and trigger early warning signals.

By definition, rare events occur infrequently and thus provide few, if any, observations from which to extrapolate. Analytical and modeling techniques that account for low-probability outliers can provide more insight into these rare events (see sidebar).

### Looking for Anomalies

True risk sensing—strategic risk identification and monitoring—encompasses detection of rare events and observations, that is, the anomalies outside the expected patterns or existing trends.

Here are a few first steps to consider in outlier detection and analysis:

- Embrace data scarcity: Rare events by their nature provide few observations to detect and analyze. Sophisticated analysis and modeling can work with low-probability outliers to provide more insight into developments and events, despite scarce data. Today’s technologies can compensate for data scarcity and help in monitoring changes over time.
- Build context: Rather than dismissing outliers as insignificant, consider each new event or piece of information as providing an opportunity to refine the organizational vision and recalibrate the context. If an occurrence is strategically relevant, its rarity does not in itself diminish its potential significance and impact on the organization.
- Maintain situational awareness: Keeping the 5 W’s (who, what, when, where, and why) in sight ensures that rare event analyses align with evolving business goals and realities. Linking anomaly detection to the organization’s strategy and business context keeps it rooted in risk management rather than reducing it to forecasting for its own sake.

Consider this: After virtually every major risk event, analysts discover a few signs, warnings, or data points that presaged the event or something very similar. Anomaly detection and analysis aims to locate and interpret these signals before the event occurs.

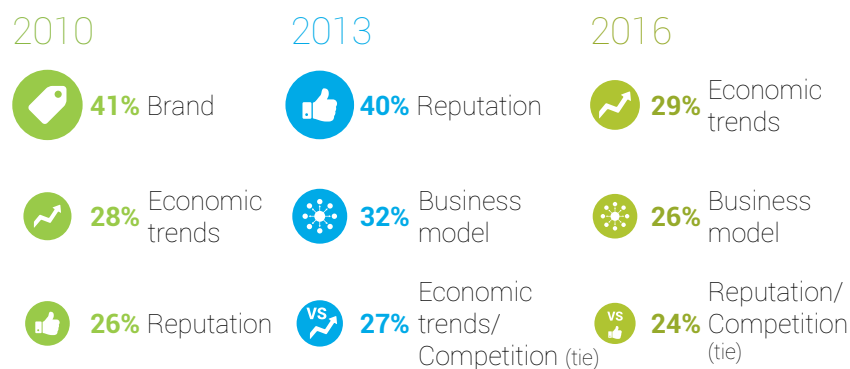




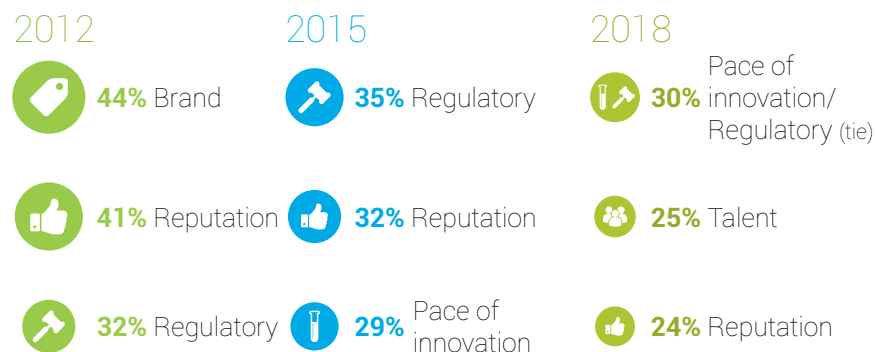
## The risks of most concern are shifting

**Figure 3-A: Risks of most concern in 2013\***

Which of the following risk areas have the most impact on your business strategy (three years ago, today, and three years from now)?\*\*



**Figure 3-B: Risks of most concern in 2015\***



Reputation risk remains among the top three in all three timeframes in both the 2013 and 2015 surveys, while economic trends are no longer as great a concern in 2015 (as one would assume well into a U.S. economic recovery).

In 2015, regulatory risks join reputation as risks of concern in all three timeframes. Interestingly, the pace of innovation stands among the top three risks in 2015 and (in a tie with regulatory risk) tops the list in 2018 and reflects, for example, the technology disruption that has impacted many sectors.

These findings underscore the fact that management's views of risks are always shifting, although not radically. That in turn underscores the value of casting a wide net when defining risks, because definitions of risk tend to direct risk sensing efforts. Also bear in mind that many risks are interrelated. For example, risks related to regulation, reputation, brand, and talent (the ability to attract and retain

it) have the power to amplify one another. Moreover, yesterday's risks are rarely the same as those of today or tomorrow, which argues strongly for forward-looking risk sensing capabilities.

Thus, risk sensing should support risk and impact assessment across the entire relevant time horizon to address risks that are of immediate, near-term, and long-term concern, as the organization defines those timeframes.

Finally, the above trends may also indicate an increasing level of maturity or sophistication of analysis. Early on, sensing tools tended to be marketing and brand driven. Over a longer term, companies tend to focus more on strategic issues such as funding, investments, and value creation. For example, use of economic models is a sign that a company is looking outward for data, such as growth rates, commodity prices, and the like, but still at a fairly rudimentary level.

\* Respondents could choose more than one answer, the top three to five are shown above.

\*\* A similar Deloitte/Forbes Insights survey conducted in 2013 asked respondents to choose the major strategic risks they faced three years prior, at the time of the survey, and three years ahead, as did our 2015 survey. The more-recent survey shows that perceptions of risks have shifted somewhat. *Exploring Strategic Risk: 300 executives around the world say their view of strategic risk is changing, Deloitte, 2013*







## The value of external points of view merits further discussion

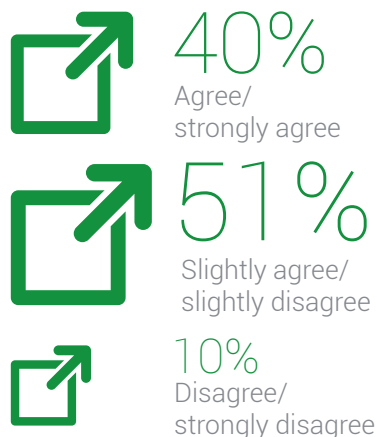
A high percentage of respondents agree that outside parties have more objectivity about risks than insiders, but an even higher percentage do not. A total of 40 percent “Agree” (as measured by the top three levels of agreement), yet those in the middle range (answers 4 through 7) total 51 percent (Figure 4), indicating uncertainty about the value of external viewpoints. This finding may be skewed by respondents who consider external views as including—or mainly consisting of—social media or reviews and ratings on websites. It may also reflect the focus of current risk sensing efforts, as external data is less relevant for near-term and tactical decision making than for adjusting the longer-term strategic focus and direction.

Meanwhile, 10 percent disagree or disagree completely that an outside perspective can analyze risks with greater objectivity, perhaps indicating the presence of truly strong, and potentially dangerous, internal cognitive biases.

Due to rounding, percentages do not add up to 100%

### Figure 4: The value of an outside perspective

Outsiders, detached from management’s agendas and biases, can analyze risks with greater objectivity and expertise than insiders.



Thus, a significant element of risk sensing—external analysts who can correct for the cognitive biases of internal analysts and executives—may be missing in many companies. Those biases include confidence bias (overestimating the truth of what we believe), availability bias (overweighting the importance of what we most recently saw, read, or

experienced), confirmation bias (focusing mainly on information that fits our existing beliefs), and optimism bias (thinking that nothing bad will happen to us)—among others.

An outside-in point of view corrects for these biases. External observers can provide agenda-free views on risks to the organization. An outside-in view integrates, and adds insight to, risk sensing results. News reports, blogs, public filings, social media, and the like provide fragmented views. An external, integrated view can provide greater context to internal data and analysis and thereby help in evaluating assumptions and potentially erroneous data and conclusions. Additionally, external data points can be presented to management, facilitate internal discussions, and used to test scenarios designed to gauge likelihood of outcomes and their potential impacts.

External points of view can be particularly useful for weighing risks related to reputation and the pace of innovation. Companies can

underestimate risks to reputation by overweighing positive customer survey results and dismissing negative views. As to innovation, a number of major companies have erroneously considered new technologies or products to be immature or irrelevant only to find themselves battling new competitors with disruptive business models sooner than they ever thought possible.

Although the board does not engage in risk sensing, directors do have a role in ascertaining that risk management practices are sufficiently robust and forward looking. In addition, as risk sensing capabilities mature, they extend beyond an operational and tactical focus to a more strategic focus that provides more data and insight of relevance to the board. External viewpoints would be a component of a robust risk management program, and of a robust risk sensing program. (Indeed, providing external viewpoints and correcting for management’s biases is the responsibility of certain directors.)

# What to do?

A starting point for monitoring strategic risks would be to identify the primary building blocks and strategic objectives of the organization that, if negatively impacted, would alter the key forces that drive your sector. Those forces can be organized into domains, such as economic, regulatory, customer, technological, operational, funding, and research and development, and include scientific, engineering, or other advances that could affect basic drivers of value.

Within specific domains there will be ongoing trends and possible events related to the sector or organization. Consider, for example, the following sample issues and themes within each of these six common domains:



## **Economic domain**

Regional and national growth, interest rate and currency, environments, sector developments, input costs (including labor), supply and demand dynamics



## **Regulatory domain**

Legislative developments, regulatory agency priorities, compliance methods and costs, case law and litigation trends



## **Customer domain**

Product and service preferences, factors influencing purchase, evolving customer journey, competitive product and pricing strategies, technology adoption curve



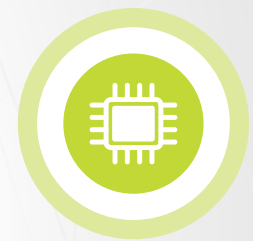
## **Operational domain**

Supply chain, alternate suppliers, capacity issues, production and delivery challenges, outsourcing, use of alliances and channel partners



## **Funding domain**

Access to and availability of public and private sources of funding to support growth plans and strategic objectives, and ability to generate adequate returns on capital



## **Technology domain**

Basic science and R&D trends, knowledge transfer, technology commercialization, academic activity, patent filings and citations, technology acquisitions

These are only general sample factors within each of these domains. The actual issues and themes (and domains) would be far more specific to the sector and organization. Also, identifying the forces affecting each domain represents only one step. Domains overlap in ways that must be identified so interactions among them can be mapped to identified risks and potential opportunities. Additionally, each organization needs to determine the severity and impact that a potential trend or disruption could have on its business viability and prepare an appropriate response plan.



# What to do?

## Getting with the program

Developing, launching, and maintaining a risk sensing program requires dedicated resources. Having internal resources that understand the company's business and unique risks is key. External resources may also be required, given the need for a technology platform, sophisticated analytics, and outside-in perspectives. Risk sensing also requires the expertise of data scientists, data engineers, and sector analysts to identify required data and data sources, define optimal workflows, and develop alerts and formats for dashboards and reports as well as insights and other deliverables.

Here are four steps to consider when framing and implementing a true risk sensing program:

### 1 Identify the strategic risks to be monitored, and the scope of the effort

- Conduct working sessions with senior leaders and key stakeholders to identify, validate, and prioritize strategic risks
- Agree on the risks and on the sector factors and potential industry disruptors to be monitored
- Identify and define the strategic risk indicators to be monitored, the metrics to be tracked, and the thresholds that will trigger communication, escalation, and countermeasures

### 2 Define the elements required to enable strategic risk monitoring

- Identify the applications and other resources, such as human analysts, best suited to analyzing the key strategic risks
- Establish the relevant data extracts and structured and unstructured data sources
- Outline the workflows required to analyze the focal risks
- Identify the outputs constituting the data, analyses, flags, and insights, and the visualization methods best suited to representing them in a comprehensible form and format
- Designate which stakeholders receive or have access to which outputs, and what actions they are expected to take in terms of communicating, applying, or otherwise using the output

### 3 Configure the platform to enable scanning, analyzing, and tracking of strategic risks

- Conduct analysis in keeping with the established scope to gather relevant information
- Review information to draft initial insights on the key strategic risks
- Enrich the data and findings by connecting them with sector trends, trends in related industries, and economic, marketplace, technology, regulatory, and other trends
- Launch the initial platform, combining automated and human scanning and analytical capabilities
- Review reports with sector specialists and other relevant parties

### 4 Continue monitoring the data sources and generating ongoing insights

- Develop insights in practical ways and connect them with the strategic issues facing the organization and its business units and functions, taking into account the severity of the impact of the risks on the organization
- Incorporate the insights into strategic and business plans, and into key decisions such as product development and discontinuation, IT purchases, funding plans, and outsourcing and merger and acquisition decisions
- Work to continually sharpen scanning and analysis, expand or narrow scope and frequency, improve dashboards and reports, and deepen information and insights
- Review and validate the models periodically and revise them accordingly. While in use, models should be tightly governed and controlled to allow for consistent application across the organization



# What to do?

In addition, the following experts would be necessary in developing and refining a risk sensing program:



## Specialists

Individuals with expertise in a wide range of advanced analytic methods, such as developers of process modules



## Platform sector analysts

Analysts working with specialists to develop the sector analysis based on an understanding of the sector and data, and to define workflows



## Dedicated data analysts

Analysts who use the platform, with guidance from sector analysts and specialists, to refine specific reports and reporting mechanisms

It is the combination of technological capability and human insight that, when properly focused, gives risk sensing its detection and analytical powers. The tools and the people who use them are both critical to success.



# An evolving capability

However it is defined, developed, and deployed, risk sensing has become a necessary capability for large organizations in most industries. Part-time, half-hearted, underfunded efforts that lack coordination will not provide a coherent picture of the risk landscape, let alone methods of detecting, measuring, and tracking emerging strategic risks.

## A strategic approach to risk sensing will do three things:

1

First, it will focus primarily on strategic risks—those that can undermine management's fundamental assumptions or the organization's ability to achieve its strategic goals.

2

Second, it will elevate risk sensing from data mining or media monitoring to the level of a true program, covering relevant risks to the organization and integrating risk sensing with risk management and risk governance.

3

Third, the results will benefit and be used by senior executives—and the businesses and functions—in planning and decision making. If practical application does not occur, then the risk sensing program has not been properly designed, developed, and managed.

Risk sensing must evolve as the organization and its strategies and risk environment evolve. Continuous improvement via periodic recalibration should be designed into the capability, as should a feedback loop from executives, risk managers, and business units back to the analysts to ensure that results are of practical use.


Deloitte's recent risk sensing survey and our field experience indicates that most large organizations have risk sensing efforts underway, but that many may have a way to go if those efforts are to become true risk sensing programs. More to the point, the value of these programs will reflect the extent to which they are tied to strategic risks and priorities, supported by senior executives, integrated with risk governance and risk management, and comprised of the right technological and human resources.

## Talk to us



We look forward to hearing from you and learning what you think about the ideas presented in this study. Please contact us at [risk@deloitte.com](mailto:risk@deloitte.com).





This report is from a survey of more than 150 executives from major companies around the world to understand how businesses are leveraging risk sensing tools.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) for a more detailed description of DTTL and its member firms.

Deloitte provides audit, consulting, financial advisory, risk management, tax and related services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries and territories, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte's more than 220,000 professionals are committed to making an impact that matters.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte network") is, by means of this communication, rendering professional advice or services. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2015. For information, contact Deloitte Touche Tohmatsu Limited.

**Forbes Insights** is the strategic research and thought leadership practice of Forbes Media, publisher of Forbes magazine and Forbes.com, whose combined media properties reach nearly 75 million business decision makers worldwide on a monthly basis. Taking advantage of a proprietary database of senior-level executives in the Forbes community, Forbes Insights conducts research on a host of topics of interest to C-level executives, senior marketing professionals, small business owners and those who aspire to positions of leadership, as well as providing deep insights into issues and trends surrounding wealth creation and wealth management.

