Deloitte.

Risk Intelligent enterprise management

Running the Risk Intelligent Enterprise™

Contents

Preface

This publication represents the second installment in Deloitte's series on the fundamental principles of Risk Intelligence. The papers in the series are intended to offer plain-English descriptions of the foundational elements of a Risk Intelligence program, as well as insights and practical steps you may consider for incorporating the concepts within your own organization. In the following pages, you will find a discussion of concepts necessary for making Risk Intelligence an integral part of managing the enterprise's strategy and operations. We believe application of these concepts will help create what we consider the epitome of enlightened risk management: The Risk Intelligent Enterprise™.

Keep in mind that the application of these concepts will differ based on your industry practices, regulatory environment, and organizational maturity. For example, in the financial services and energy industries, many of these concepts have been discussed for over a decade and thus may seem elementary; but for many other industries, we see these concepts just starting to be embraced. Regardless of what industry you are in, the concepts in this paper still apply.

Open communication is a key characteristic of a Risk Intelligent Enterprise. Consider sharing this whitepaper with other executives, board members, and key managers in your organization. The issues and concepts outlined herein should provide an excellent starting point for a crucial dialogue on enhancing your organization's Risk Intelligence. To download other whitepapers on the subject of Risk Intelligence, visit www.deloitte.com/RiskIntelligence.

Risk Intelligent enterprise management

Embedding risk into decision making

Risk has never been a hotter topic than it is today. In an age of extraordinary uncertainty and turbulence, when scandals and disasters are daily front-page news, no one – and no enterprise – is immune to the potential impact of unexpected events. Executives and boards are expressing extremely high interest in ways to manage risk more effectively, and many are searching for ways to address key questions about risk that have lately come into the forefront of their consciousness. "How prepared is our enterprise for the opportunities and risks that lie ahead? How can we find the unexpected before it finds us? How do we effectively link strategy and risk management?"

We believe that executives and boards can find answers to such questions by practicing Risk Intelligent enterprise management – an approach that considers risk as a key input into leadership decisions versus as an outcome to be managed after the fact. Perhaps the best way to describe the concept is to contrast it with the way many companies are approaching enterprise risk management (ERM) today.

Many companies have implemented ERM programs in response to investor and regulator demands for more effective risk management. These ERM programs are intended to evaluate, monitor, and document an organization's risks, bringing some degree of structure to what might formerly have been a disparate set of information-gathering and risk mitigation processes. But while an ERM program can help an enterprise better organize its risk-related activities, it is not, in itself, enough to embed a thoughtful, sustainable consideration of risk into the organization's key decision-making processes.

Risk Intelligent enterprise management, unlike many companies' approach to ERM, treats risk management as an integral part of managing the enterprise's strategy and operations, not as a separate, siloed process. In Risk Intelligent enterprise management, executives understand that every action that could create value also carries the potential for risk. They recognize that the discussion of risk and value cannot be separated, and, they therefore view risk as a decision driver rather than as a consequence of decisions that have already been made. Knowing this, they endeavor to make Risk Intelligent choices that expose the enterprise to just the "right" amount of risk needed to pursue value creation. They consider risk on the front end of every decision they make, both to identify potential threats and to strategically select the risks they choose to take in order to pursue value.

We can think of at least two reasons that Risk Intelligent enterprise management can help take traditional approaches to ERM to the next level. The first is that traditional ERM programs are often implemented as stand-alone initiatives, which can be perceived as bureaucratic, burdensome, and temporary rather than serious, systematic, and sustainable. In our view, it is critical for Risk Intelligence to be "built in" to the way an organization does business, not "bolted on" – which means that senior management must be meaningfully involved in the risk management program.

The second, more important reason is that integrating risk management into the enterprise's core decision-making processes puts an organization on a proactive, not reactive, footing with respect to the unexpected – both the undesirable and the desirable. Executives who factor risk into their decisions as a matter of course are less likely to be blindsided by threats and opportunities, and an enterprise whose leaders have thought through their options in advance will be better prepared to respond effectively to both.

By "building it in" rather than "bolting it on," Risk Intelligent enterprise management allows an organization to be both more resilient in dealing with adversity, and more agile in pursuing opportunity.

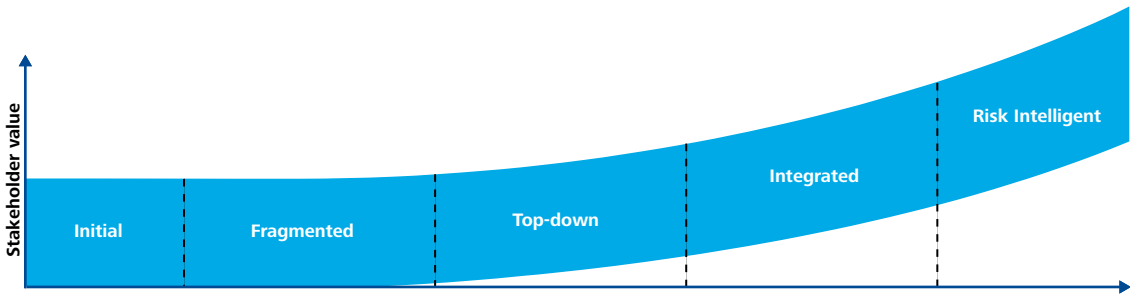
Build on what you already have

The good news for most organizations is that they're likely to already have many of the elements of Risk Intelligent enterprise management in place. The path forward should be much more a matter of building on what currently exists than of starting from scratch. For this reason, we think it's important for organizations to take stock of their current risk management capabilities before making major changes or investments in risk management.

When performing such an assessment, it's vital to understand not just where your enterprise currently stands, but where you want and need it to be from a risk management perspective – which, importantly, may not always be at the very top of the heap. Various areas of risk differ in importance from industry to industry, and even from company to company within the same industry. Hence, it's not always necessary to maintain top-notch risk management capabilities with respect to every possible aspect of risk. The challenge is to understand exactly in which areas "good enough" really is good enough – and in which areas the enterprise truly needs top-notch capabilities to meet stakeholders' risk management expectations.

One way to better understand both where you are and where you "should" be is to evaluate your organization's risk management capabilities against a maturity model such as Deloitte's Risk Intelligence maturity model (Figure 1). For leaders, an assessment against such a maturity model can be a be a useful way to frame the discussion of what types of initiatives to pursue in various risk areas, as well as how much of the organization's limited resources to invest in each initiative.

Figure1. Risk Intelligence maturity model



Representative attributes

Initial	Fragmented	Top-down	Integrated	Risk Intelligent
• Ad hoc/chaotic • Depends primarily on individual heroics, capabilities, and verbal wisdom	• Risk is defined differently at different levels and in different parts of the organization • Risk is managed in silos • Limited focus on linkages between risks • Limited alignment of risk to strategies • Disparate monitoring and reporting functions	• Identified risk universe • Common risk assessment/response approach developed and adopted • Organization-wide risk assessment performed • Action plans implemented in response to high-priority risks • Communication of top strategic risks to the senior management team	• Risk management activities coordinated across business areas • Risk analysis tools developed and communicated • Enterprise risk monitoring, measuring, and reporting • Scenario planning • Opportunity risks identified and exploited • Ongoing risk assessment processes	• Risk discussion embedded in strategic planning, capital allocation, product development, etc. • Early warning system to notify board and management to risks above established thresholds • Linkage to performance measures and incentives • Risk modeling

The players

Who should be responsible for what?

Key questions to ask:

- How can the board effectively oversee the senior executive team's risk management efforts?
- Which senior executives should serve in the enterprise risk group? Who should chair it?
- Have we clearly defined risk management roles and responsibilities at all organizational levels?

We conceive of the Risk Intelligent Enterprise as having three levels of responsibility with respect to risk management, as depicted in Figure 2. At the apex lies the responsibility for risk *governance*, including strategic guidance and risk oversight, which rests with the board of directors. In the middle lies the responsibility for risk *infrastructure and management*, including designing, implementing, and maintaining an effective risk program, led by executive management. And at the base lies the responsibility for risk *ownership*, including identifying, measuring, monitoring, and reporting on specific risks, led by the business units and functions. In Risk Intelligent enterprise management, activities across all these levels are integrated into a systematic, enterprise-wide program that embeds a strategic view of risk into all aspects of business management, and that gives leaders a clear view into the challenges and opportunities that risk can create.

Figure 3 gives a closer look at the groups at each level of the enterprise that may be involved in executing various risk management responsibilities. While the figure is largely self-explanatory, we want to make special note of two of the groups in the risk infrastructure and management layer: the "enterprise risk" group and the "risk management" group.

The "enterprise risk group" is a subset of the executive management team. Its role is to come together to review enterprise risks and actions taken to mitigate them, as well as to review and aggregate risk information from different groups in the business and escalate risk issues to the full C-suite and/or the board if necessary. These responsibilities may be given to an existing executive committee, if the organization already has one with an appropriate mix of members. Or a company may create an entirely new committee to serve as the enterprise risk group.

The "risk management" group represents an organization's risk management specialists, if any: that is, dedicated professionals who focus on risk and risk alone. Whether or not an organization has such resources will depend on factors such as industry and the organization's size. In the financial services industry, for instance, most large organizations will have a group that focuses on specific industry risks, such as liquidity, credit, and currency risk. Or as another example, airline companies typically have a staff of specialists who work on fuel hedging strategies, since changes in fuel cost is such a large risk in the aviation industry. Such specialist groups play an important role in the risk management infrastructure by addressing specific classes of risks that most directly threaten an organization's ability to operate.

We think that it's essential for a member of the C-suite to take a leadership role with respect to risk management – regardless of whether he or she is formally known as the Chief Risk Officer. This executive should chair the enterprise risk group and serve as liaison with the organization's risk management specialist groups. He or she should receive risk updates from the business units and functions, and escalate significant risks to the enterprise risk group and/or the board of directors as necessary. He or she should take

the lead in discussing risks with other C-suite executives to identify potential risk interactions and their impact on the organization. However, we recommend that he or she should *not* be directly responsible for managing risk or supervising the organization's risk management functions, which could create a conflict of interest that leads him or her to defend the organization's risk management actions rather than constructively challenging them. The chief risk executive role is much more that of a coordinator than a controller, serving as a central switchboard and clearinghouse for enterprise risk information, providing decision support for executive management and other business leaders, and facilitating cross-enterprise dialogue.

We believe that the groups depicted here, working together, can give an organization the right resources to perform the six core processes of Risk Intelligent enterprise management discussed in the following section.

Figure 2. The Risk Intelligent Enterprise

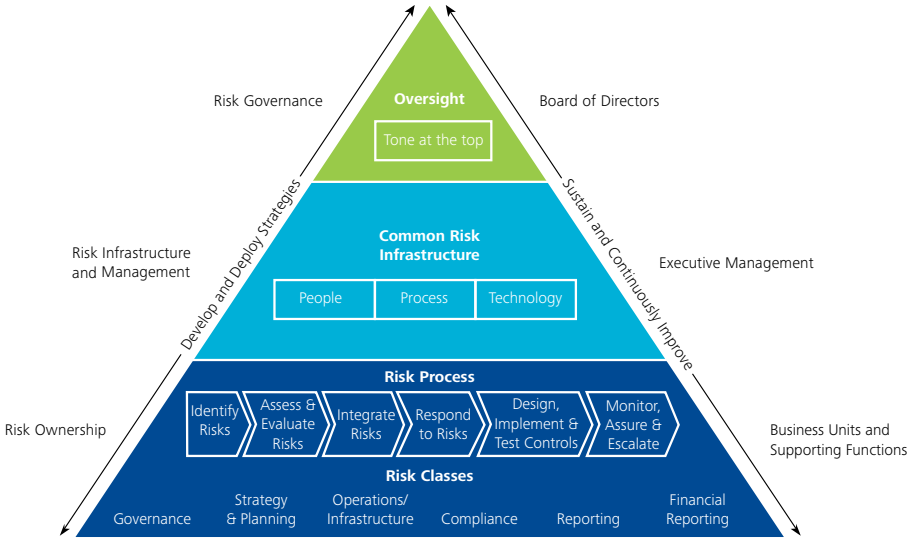


Figure 3. Typical groups involved in Risk Intelligent enterprise management

Risk governance	**Board of directors** • Foster a Risk Intelligent culture • Ratify key components of the Enterprise Risk Management (ERM) program • Discuss enterprise risks with executive management • Meet with internal audit				**Technology (all pervasive):** • Provide periodic/ real-time dashboards to oversee risks • Make monitoring and reporting easier • Support timely maintenance and pre-empt problems • Facilitate risk escalations
Risk infrastructure and management	**Executive management:** • Define the risk appetite • Evaluate proposed strategies against risk appetite • Provide timely risk-related information	**Enterprise risk group:** • Aggregate risk information • Identify and assess enterprise risks • Monitor risks and risk response plans	**Internal audit:** • Provide assurance on effectiveness of the ERM program • Evaluate controls and risk response plans for significant risks	**Risk management:** • Create a common risk framework • Provide direction on applying framework • Implement and manage technology systems • Provide guidance and training	
Risk ownership	**Business units:** • Take intelligent risks • Identify and assess risks • Respond to risks • Monitor risks and report to the enterprise risk group		**Support functions:** • Provide guidance/support to the enterprise risk group and business units		

The processes

Six building blocks of Risk Intelligent enterprise management

The processes we describe here form the building blocks of a risk-informed approach to running an enterprise. Boards and executive management use a top-down approach to understand risk at a strategic level, while risk owners in the business units and functions use a bottom-up approach to identify and monitor specific risks, escalate concerns to management, and generate the risk-related data to inform leadership's strategic view. As a whole, the six processes come together in a dynamic system that facilitates the flow of information up, down, and across the enterprise, and that allows an organization to effectively manage specific risks while keeping leaders focused on risk management at a more strategic level.

Set high-level guidelines

Risk philosophy and appetite

Who: Executive management and the board of directors
When: As soon as possible; to be reviewed at least annually

Key questions to ask:

- How much risk are we prepared to take to pursue our strategic objectives?
- What kinds of risks are most relevant to our enterprise? How have we defined them?
- How should we define our risk appetite and tolerances?

The first step toward Risk Intelligent enterprise management is to set high-level guidelines for how people throughout the organization should identify, evaluate, and communicate about risk. Developing a common set of standards for risk identification and measurement allows leaders to make the necessary apples-to-apples comparisons to gain a coherent view of risk across the enterprise. It also makes it easier for different groups in the enterprise to discuss risk with each other and with leadership, so that "high," "medium," and "low" risk mean the same level of risk whether it relates to information technology, talent, supply chain, tax, or any other area of the business.

Setting consistent guidelines for discussing and measuring risk is a multi-part effort. In our view, leaders can take the following steps to set overarching guidelines for the enterprise's treatment of risk:

Establish the enterprise's risk philosophy.
Management and the board should develop a risk philosophy statement that describes, in broad terms, the degree to which the enterprise will seek out, tolerate, and/or avoid risk in the pursuit of the organization's goals. One example of a risk philosophy statement might be, "Our company will value risk-taking in relation to its major strategic initiatives and will not tolerate risk-taking in areas of non-compliance and violations of business ethics."

Establish a risk management framework.
A risk management framework is the enterprise's basic conceptual structure for how people should think about risk. It should be customized for every company, and it should include formal definitions of areas of risk that are meaningful to the enterprise.

Define the enterprise's risk appetite.
This is a current "term of art." The risk appetite translates the risk philosophy into specific guidelines for the level of risk that leaders consider acceptable for the enterprise. A statement of risk appetite may include quantitative elements as well as qualitative but clearly described elements that leadership considers important (see sidebar, "Sample risk appetite elements"). Developed by management and ratified by the board, the risk appetite serves as the fundamental standard by which all enterprise risks are judged acceptable or unacceptable.

Sample risk appetite elements

- **Selling, general, and administrative (SG&A):** Willing to invest no more than $100 million in SG&A to achieve revenue growth goals.
- **Return on capital employed (ROCE):** Willing to accept no more than a 20 percent reduction in target ROCE to achieve goals.
- **Reputation:** Only willing to endure minimal, short-term adverse local media attention that can be quickly contained.

Risk criteria defined

Impact: "Impact," or "inherent risk," refers to the extent to which a risk event would affect the enterprise (e.g., financial, reputational, customer, or other effects) in the absence of any actions a company might take to address its effect on the business.

Vulnerability: "Vulnerability," or "residual risk," refers to the extent to which a risk event would affect the enterprise, taking into consideration all of a company's current efforts to address the risk.

Speed of onset: "Speed of onset" refers to the time it takes for a risk event to manifest itself (e.g., the time that elapses between the occurrence of an event and the point at which the company first feels its effects).

Define risk tolerances.

Once the risk appetite is defined, management then should define specific risk tolerances, also known as risk targets or limits, that express the specific threshold level of risk by incident in terms that decision-makers can use as a guide as to which risks they may and may not take. For instance, in completin an acquisition, the risk tolerance may be defined as a stop-loss threshold of a specified value. For compliance with laws and regulations there may be zero tolerance for risk-taking.

Define risk assessment criteria.

Using the risk appetite as a guide, leaders should establish common standards for evaluating risk along three dimensions: the *impact* of a risk event (also known as "inherent risk"), the organization's *vulnerability* to the event (also known as "residual risk"), and the event's *speed of onset* (see sidebar, "Risk criteria defined"). Enterprise-standard parameters for what would be considered "high," "low," and "medium" should be established for all three dimensions. These parameters can then be used by various groups in the organization to assess risks in their area, as well as on an enterprise level.

Develop a Risk Intelligent strategy

Strategy development and deployment

Who: Executive management and the board of directors
When: During each strategic planning cycle; to be revisited regularly as major factors in the business environment change (e.g., factors relating to the economy, the competition, legal matters, or the industry landscape)

Key questions to ask:

- How valid are the core assumptions that underlie our strategy?
- Which strategic options fall within our risk appetite?
- What risks must we take or risk being left behind?

One of the core elements of Risk Intelligent enterprise management is to set a Risk Intelligent strategy: a strategy that is appropriately informed by the risks associated with both the strategy's selection (the risks *of* the strategy) and its execution (the risks *to* the strategy). To do this, we think leaders should consider embedding least two activities into the strategy-setting process.

The first activity is for leaders to make explicit the assumptions on which the strategy is based, and then to constructively challenge those assumptions to test their validity. This is important because a strategy will only "work" to the extent that the assumptions that underlie it hold true. By examining the validity of their own most strongly held assumptions and beliefs, leaders can help themselves identify previously unseen risks of a strategy and take appropriate steps to mitigate those risks, up to and including the development of alternative strategies that rest on different assumptions.

One way that executives and boards can help themselves challenge their own basic assumptions is through a method known as the Thesis-Antithesis-Synthesis (TAS) framework.[1] Briefly, the TAS framework encourages leaders to explicitly state the assumptions underlying the proposed strategy – the "white swans," or the events and circumstances that leaders expect to occur.[2] For each assumption, leaders then state its antithesis – its exact opposite, or the "black swan."[3] The "black swan" represents the unconventional view, the unexpected event, or the improbable circumstance; it forces leaders to ask the question, "What if we are wrong?" Finally, leaders describe the implications of the thesis and antithesis for the enterprise, and develop a unified approach that synthesizes both the thesis and the antithesis into a "best of both worlds" scenario. Ideally, this exercise can help leaders identify strategic options and risk responses that the organization can pursue under a range of different circumstances – whether or not those circumstances play out as expected.

Once a company's strategic options are on the table, the second activity we recommend is for leaders to consider the potential interactions among risks that those options might entail, both with respect to individual strategic choices and with respect to different combinations of strategic choices. (For instance, the executive team may consider that sourcing products from a particular region of the world may pose only moderate risk to an enterprise from a quality and safety perspective. When that risk is combined with the likely reputational impact of any lapse in quality and safety, however, executives may decide that the total risk is too great to pursue such a sourcing strategy.) Leaders are then in a position to evaluate the risks associated with each strategic option against the organization's risk appetite, short-listing the alternatives that fall within the risk appetite and discarding those that fall outside it.

Strategic decisions happen outside strategy-setting, too

Decisions that touch strategy are made in many more places and at many more times than just in the annual strategy-setting cycle. Decisions as to whether to pursue a merger or acquisition, which products or services to develop, which markets to enter, what customer segments to pursue – all of these decisions and more can profoundly affect, if not the core strategy itself, then certainly the organization's effectiveness in pursuing it.

In our view, leaders should insist that risk be considered in all decision-making processes in areas that have business implications, such as M&A, new product development, and customer and market strategy. All personnel involved in making such decisions should have a thorough understanding of the organization's risk appetite, and leaders should equip them with risk tolerances that specify the extent of the risk that is permissible to incur in each of these areas. This way, decision-makers receive clear guidance on how risk factors should shape their choices, and boards and executives can have greater confidence that risk is being appropriately factored into choices that managers are making on the enterprise's behalf.

[1] Frederick Funston and Stephen Wagner, *Surviving and Thriving in Uncertainty: Creating the Risk Intelligent Enterprise* (Hoboken, New Jersey: John Wiley & Sons, Inc., 2010).
[2] Terminology borrowed from Nassim Nicholas Taleb, *The Black Swan: The Impact of the Highly Improbable* (New York: Random House, 2007).
[3] Ibid.

Get tactical with risks

Risk identification and assessment

Who: Business units and functions
When: At least quarterly as part of an enterprise risk committee or management committee agendas; as needed as new risks are identified

Key questions to ask:

- What risks are we taking?
- How prepared are we to address the risks we are taking?
- How would each risk, if it becomes actual, affect enterprise value?

No Risk Intelligence program can get very far without an in-depth understanding of the specific risks that face an enterprise. That's why risk identification and assessment is important – as a way for the enterprise to get a handle on the universe of significant risks it faces, and to determine how important each risk is to the achievement of its overall goals.

The risk identification and assessment process should take place in a structured, disciplined fashion that considers input from line managers and functional representatives as well as business-unit and executive leaders. Gathering perspectives from the people "on the ground" goes a long way toward helping leaders understand what risks could have the most significant impact on the organization.[4]

Depending on its size and complexity, an organization can take several approaches to breaking down its risk assessment activities into meaningful, manageable chunks. One frequent approach is to have each business unit, division, or location perform its own risk assessment, with the results to be aggregated later and reported to management.

The assessment process begins with identifying people across the enterprise who have specific knowledge or competencies relating to the risk areas described in the organization's risk taxonomy. These people may participate in workshops or surveys to generate a preliminary list of risks in their area. One tool that can help people zero in on specific risks is Deloitte's Risk Intelligence Map, which divides risks into five classes (governance, strategy and planning, operations/infrastructure, compliance, and reporting) and lists a number of common risks in each category.

Once key risks have been identified, selected individuals, such as business-unit leaders, process owners, and others who may have more in-depth knowledge about particular risks, may assess each risk for its impact, the organization's vulnerability to the risk, and the risk's expected speed of onset. When rating each risk, it is important to seek input from individuals across organizational silos in order to understand the many different ways a risk might affect the enterprise. For instance, a company's supply-chain risks include not only risks directly related to the production and movement of goods, but also associated tax considerations (both pitfalls and opportunities) that can have a significant financial impact on supply-chain decisions.

The information gathered in this process can be consolidated into a report that describes the specific risks facing each part of the organization and indicates the significance of each. This report can then be reviewed by the enterprise risk group and other leaders, who can then aggregate risks across the enterprise and add any enterprise-level risks that may not be apparent at a lower level.

[4] The Risk Intelligence Map is available online at http://www.deloitte.com/us/rimap.

Develop action plans

Risk response

Who: Business units and functions; reviewed by executive management

When: Every time a new risk is identified; plans should be reviewed periodically

Key questions to ask:

- How will we know if a risk is imminent?
- How will we respond to specific risk events?
- How can we appropriately allocate our risk management investments?

Typically developed by risk owners in the business units and functions, risk response plans are the organization's action plans for responding to risks and opportunities that have been determined to be significant. In developing action plans, it is important to understand the contributing factors to each risk and what, if anything, can be done about them. Risk owners should examine each risk carefully to understand how it might affect the business as well as to determine how to respond and who should be involved in that response. Important, too, is to clearly define the desired outcome of the risk response – whether the intent is to lessen the impact of a risk event, or conversely, to incur the risk so as to pursue an opportunity.

An important step in creating action plans is to identify *key risk indicators* (KRIs) that can serve as signals that the enterprise's exposure to a particular risk may be changing. In many cases, a company may be able to track the status of a risk using existing key performance indicators (KPIs); for example, an organization's voluntary attrition rate, often monitored by HR as part of its talent management responsibilities, may do double duty as a KRI for talent risk. Other risks may demand the development of new KRIs, particularly for risks affected by the external environment; for example, a company might want to examine analyst and media reports for signs that its reputation might be coming under fire.

Thresholds should be established for each KRI that risk owners can use as guidelines to monitor the status of each risk. In addition, risk responses should be developed that dictate the course of action to be taken when a KRI crosses successive thresholds. These responses can range from simply communicating the changed status of the risk to the appropriate organizational level, all the way up to mobilizing resources to deal with an actual risk event. A risk response plan may also include a description of contributing factors and avoidance approaches for each risk, as well as general guidance on how to react swiftly to risk events to help control damage.

One way to help clarify what type of response may be appropriate for specific risks is to use a tool known as a MARCI chart (for *M*itigate, *A*ssure, *R*edeploy, and *C*umulative *I*mpact), depicted in Figure 4. The MARCI chart plots risks along the two axes of impact and vulnerability, and indicates each risk's speed of onset by the size of the data points.

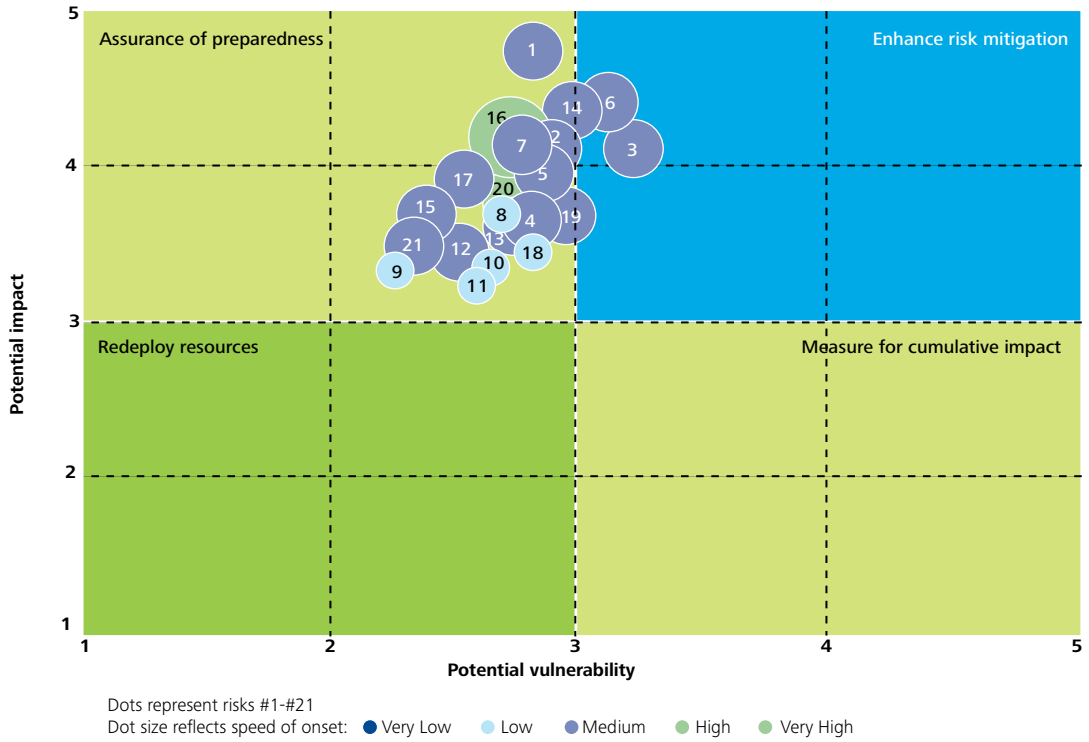
Risks in the top right (Mitigate) quadrant represent high-impact risks to which the organization has high vulnerability – that is, risks for which the organization's efforts have been relatively *in*effective in holding the risk to a level consistent with leadership's risk appetite. For these risks, risk owners should consider investing resources in developing and designing controls to reduce exposure, as well as in tracking progress on remediation plans.

Risks in the top left (Assurance) quadrant are high-impact risks to which the organization has low vulnerability – that is, the risk owners consider the organization's mitigation efforts adequate to bring the level of each risk within leadership's appetite for that kind of risk. For risks in this quadrant, risk owners should be able to provide reasonable assurance to management that the controls to prevent, detect, correct, or escalate a risk continue to be both effective and efficient in keeping the vulnerability to that risk within the company's appetite. Internal audit or other processes can be used to validate the assurances.

Risks in the bottom left (Redeploy) quadrant are low-impact risks that are currently being adequately controlled by the organization's risk management efforts. Given their relatively low impact, an organization may want to consider whether it is spending more to manage these risks than necessary, and whether it can or should redeploy resources from risks in this quadrant to risks in the Mitigate quadrant. It is important, however, to consider whether the risks in this quadrant interrelate with other risks in a more significant fashion before making a decision to redeploy resources.

Finally, risks in the lower right (Cumulative Impact) quadrant are low-impact risks to which the organization has relatively high vulnerability. It may be worth considering whether the risks in this quadrant could, in aggregate, have a more significant impact on the organization – and, if so, where the new, aggregated risk would fall on the MARCI chart. (For example, a series of quality risks may each have a relatively low impact when considered individually, but may have greater impact and significance when considered as a group.)

Figure 4. A sample MARCI chart



Take an enterprise-wide view

Risk aggregation and prioritization

Who: Business units/functions and risk management specialists, the enterprise risk group, and executive management; reviewed by the board
When: Regularly (at least quarterly or bi-annually) as part of the management process, and in management reports to the board of directors

Key questions to ask:

- What are the enterprise's top risks?
- What interactions among risks can we identify?
- How significant are these interactions to the organization's overall risk profile?

Risk identification and assessment at the business-unit and functional level can generate mountains of data that, while useful to risk owners within the business units and functions, do not necessarily give senior executives the insights they need to make risk-informed decisions on an enterprise level. For that, the risk information generated in risk identification and assessment efforts need to be reviewed and aggregated, and enterprise-level risks added that may have been missed in the business-unit and functional assessments.

The enterprise risk group may meet with business-unit and functional leaders to review their business-unit and function-specific risk assessments, identifying any groups of related risks that may become apparent through cross-functional and cross-business dialogue. The enterprise risk group should also identify higher-level risks that may arise outside any of the business units and functions – risks such as succession planning or organizational reputation – and add them to the aggregated list of risks.

Once such a "master list" of risks is developed, the enterprise risk group, or even the executive management team as a whole, can examine the list to identify the top several risks – say, the top 10 – that have the greatest potential consequences for the enterprise, referring to the chosen risk management framework as a guide. Boards should provide oversight over the development of the top risk list by management.

The executive risk group should periodically review the status of the top risks, based on reports from the business units and functions as well as from any specialized risk management groups. One way to consolidate this information into an easily digestible format is to create a dashboard reporting system that presents leaders with a snapshot of key information on each top risk, such as the KRIs associated with each risk, any changes in the KRIs since the last report (e.g., increase, decrease, or no change), and the status of any efforts that might be underway or planned.

We think that the entire executive team should make risk a standing agenda item for their regular meetings. In these discussions, drawing on the perspectives of the enterprise risk group, executives can discuss the top risks and their status; potential risk interactions and their impact; and the readiness of the enterprise to respond if any of the risks or their interactions were to occur. These discussions are essential to keeping executive management engaged, involved, and informed about the organization's risks and mitigation efforts.

Maintain constant vigilance

Risk monitoring and reporting

Who: Business units/functions; enterprise risk group; executive management
When: Ongoing

Key questions to ask:

- How can we most effectively monitor the internal and external environment for signals that a risk is increasing, decreasing, or remaining constant?
- What are the thresholds for escalation with respect to enterprise risks?

Risk monitoring and reporting activities supply the entire risk management system with the information leaders need to practice Risk Intelligent enterprise management. It's essential for an organization to develop effective signal detection and interpretation capabilities that can alert leaders that the status of a risk has changed. Such "early warning" processes should track circumstances external to the organization as well as internal performance indicators. Organizations should consider how the external environment can affect the risks to which they are exposed, and monitor selected external risk indicators (such as analyst reports, major media outlets, and/or capital market activity) for triggers in the same way as they track internal indicators. Many organizations may be able to take advantage of their existing marketplace intelligence capabilities to perform this monitoring.

Another key component of risk monitoring is to keep abreast of the KRIs that have been established for specific risks. In our view, the responsibility for monitoring KRIs should rest with risk owners within the business units and functions. Thresholds should be set and escalation procedures established that guide risk owners in reporting changes to KRIs to the appropriate levels of the organization. For example, if the organization has identified voluntary attrition rate as a KRI for talent risk, leaders might require the risk owner – say, a middle manager in the talent management group – to report voluntary attrition rates to various parties as follows:

- Below 5 percent: No report
- Between 5 and 8 percent: Head of the talent management group
- Between 8 and 10 percent: CHRO or Chief Talent Officer
- Between 10 and 12 percent: CEO
- 12 percent and above: Enterprise risk group and board of directors

In addition to receiving reports on individual KRIs, the enterprise risk group should monitor key enterprise risks – the "top ten" list described earlier – to determine their current and probable future status and decide whether changes to any of the top ten risks warrant a consultation with the board of directors.

Risk Intelligent infrastructure: Getting Risk Intelligence done

To execute the processes described in this paper, organizations need to maintain what we call a Risk Intelligent infrastructure: the right people, processes, and technology elements to enable Risk Intelligence throughout the organization.[5]

- **People:** The goal of the people component of the Risk Intelligent infrastructure is to identify, engage, and develop the necessary talent to manage risk effectively, and to make it possible to employ that talent to accomplish the organization's risk management objectives. An effective people infrastructure is best enabled by role-based training, risk-aligned compensation and rewards, and a risk-aware culture. These sustain Risk Intelligence for the long term. The objective is to help people everywhere in the organization understand why they need to make decisions about risk and what risk-related decisions they need to make; to give them the tools and training to make Risk Intelligent decisions; and to help them understand how they themselves will be rewarded for Risk Intelligent behavior.
- **Process:** Where applicable and appropriate, the Risk Intelligent organization will take advantage of common process elements in order to improve effectiveness, remove redundancies, and improve efficiency. It will also establish processes for pushing down a unified view of risk – standardized risk definitions, a common risk language, and so on – from the risk governance bodies to all parts of the organization. And it will also set up processes for consolidating risk information from different groups, effectively sharing it across the enterprise, and presenting an integrated view of organizational risks to leadership.
- **Technology:** The main role of technology in risk management is to deliver the right type and amount of information to the right people in a timely manner, distilled in a way that can help them understand the risk associated with particular decisions. To this end, technology can provide support by delivering a high-quality, reliable continuum of information from dispersed operations; integrating operational, transactional and financial information to help in proactively identifying and resolving risk-related issues; and predicting, preventing, detecting, managing and reporting both internal and external risks that may otherwise threaten an organization's ability to fulfill its business objectives. However, technology is not, by itself, a magic bullet; the three elements: people, process, and technology, must work together to sustain Risk Intelligence.

[5] For more on risk management infrastructure, see Deloitte's paper "Creating a Risk Intelligent infrastructure," available online at Creating a Risk Intelligent infrastructure.

Afterword

Risk Intelligent enterprise management is all about making strategic and day-to-day decisions across the entire enterprise with full awareness of the attendant risks and opportunities. A systematic approach to identifying, assessing, and planning for risks is essential, as is a well-defined process for making key risk information available to decision-makers at every organizational level.

Risk management today is a far broader concept than it was years ago, when many businesspeople viewed it mainly as insuring assets against loss or damage. Leaders must recognize that the pursuit of value inevitably means exposure to risk – and that they must therefore take responsibility for addressing risk with every decision they make. We believe that the processes outlined here provide the broad brushstrokes for putting Risk Intelligent enterprise management into practice. We hope that you find these concepts useful as you continue to pursue Risk Intelligence at your own organization.

Nine fundamental principles of a Risk Intelligence program

1. In a Risk Intelligent Enterprise, a common definition of risk, which addresses both value preservation and value creation, is used consistently throughout the organization.
2. In a Risk Intelligent Enterprise, a common risk framework supported by appropriate standards is used throughout the organization to manage risks.
3. In a Risk Intelligent Enterprise, key roles, responsibilities, and authority relating to risk management are clearly defined and delineated within the organization.
4. In a Risk Intelligent Enterprise, a common risk management infrastructure is used to support the business units and functions in the performance of their risk responsibilities.
5. In a Risk Intelligent Enterprise, governing bodies (e.g., Boards, Audit Committees, etc.) have appropriate transparency and visibility into the organization's risk management practices to discharge their responsibilities.
6. In a Risk Intelligent Enterprise, executive management is charged with primary responsibility for designing, implementing, and maintaining an effective risk program.
7. In a Risk Intelligent Enterprise, business units (departments, agencies, etc.) are responsible for the performance of their business and the management of risks they take within the risk framework established by executive management.
8. In a Risk Intelligent Enterprise, certain functions (e.g., HR, finance, IT, tax, legal etc.) have a pervasive impact on the business and provide support to the business units as it relates to the organization's risk program.
9. In a Risk Intelligent Enterprise, certain functions (e.g., internal audit, risk management, compliance, etc.) provide objective assurance as well as monitor and report on the effectiveness of an organization's risk program to governing bodies and executive management.

Contacts

Advisory & Consulting

Roland Bastin
Partner
Information & Technology Risk
+352 451 452 213
rbastin@deloitte.lu

Mathieu Brizard
Senior Manager
Governance,
Risk & Compliance
+352 451 453 096
mbrizard@deloitte.lu

Xavier Zaegel
Partner
Capital Markets/Financial Risk
+352 451 452 748
xzaegel@deloitte.lu

Jean-Philippe Peters
Directeur
Business Risk
+352 451 452 276
jppeters@deloitte.lu

Marco Lichtfous
Partner
Capital Markets/Financial Risk
+352 451 454 876
mlichtfous@deloitte.lu

Laurent Berliner
Partner
Business Risk
+352 451 452 328
lberliner@deloitte.lu

Jérôme Sosnowski
Directeur
Business Risk
+352 451 454 353
jsosnowski@deloitte.lu

Bert Glorieux
Directeur
Business Risk
+352 451 452 947
bglorieux@deloitte.lu

Laurent de la Vaissière
Directeur
Information & Technology Risk
+352 451 452 010
ldelavaissiere@deloitte.lu

Audit

Martin Flaunet
Partner
Audit
+352 451 452 334
mflaunet@deloitte.lu

Vafa Moayed
Partner
Audit
+352 451 452 424
vmoayed@deloitte.lu

Deloitte Luxembourg
560, rue de Neudorf
L-2220 Luxembourg
Grand Duchy of Luxembourg

Tel.: +352 451 451
Fax: +352 451 452 401
www.deloitte.lu

Designed and produced by MarCom at Deloitte Luxembourg