A practical guide to risk assessment*

How principles-based risk assessment enables organizations to take the right risks

*connectedthinking

PRICEWATERHOUSECOOPERS

Table of contents

December 2008

The heart of the matter

Effective risk assessment is increasingly important to the success of any business.

Today's business world is constantly changing—it's unpredictable, volatile, and seems to become more complex every day. By its very nature, it is fraught with risk.

Historically, businesses have viewed risk as a necessary evil that should be minimized or mitigated whenever possible. In recent years, increased regulatory requirements have forced businesses to expend significant resources to address risk, and shareholders in turn have begun to scrutinize whether businesses had the right controls in place. The increased demand for transparency around risk has not always been met or met in a timely manner, however—as evidenced by the financial market crisis, where the poor quality of underlying assets significantly impacted the value of investments. In the current global economic environment, identifying, managing, and exploiting risk across an organization has become increasingly important to the success and longevity of any business.

Risk assessment provides a mechanism for identifying which risks represent opportunities and which represent potential pitfalls. Done right, a risk assessment gives organizations a clear view of variables to which they may be exposed, whether internal or external, retrospective or forward-looking. A good assessment is anchored in the organization's defined risk appetite and tolerance, and provides a basis for determining risk responses. A robust risk assessment process, applied consistently throughout the organization, empowers management to better identify, evaluate, and exploit the right risks for their business, all while maintaining the appropriate controls to ensure effective and efficient operations and regulatory compliance.

For risk assessments to yield meaningful results, certain key principles must be considered. A risk assessment should begin and end with specific business objectives that are anchored in key value drivers. These objectives provide the basis for measuring the impact and probability of risk ratings. Governance over the assessment process should be clearly established to foster a holistic approach and a portfolio view—one that best facilitates responses based on risk ratings and the organization's overall risk appetite and tolerance. Finally, capturing leading indicators enhances the ability to anticipate possible risks and opportunities before they materialize. With these foundational principles in mind, the risk assessment process can be periodically refreshed to deliver the best possible insights.

Organizations that vigorously interpret the results of their risk assessment process set a foundation for establishing an effective enterprise risk management (ERM) program and are better positioned to capitalize on opportunities as they arise. In the long run, this capability will help steer a business toward measurable, lasting success in today's ever-changing business environment.

An in-depth discussion

Risk assessment forms the foundation of an effective enterprise risk management program.

Defining risk assessment

Risk assessment is a systematic process for identifying and evaluating events (i.e., possible risks and opportunities) that could affect the achievement of objectives, positively or negatively. Such events can be identified in the external environment (e.g., economic trends, regulatory landscape, and competition) and within an organization's internal environment (e.g., people, process, and infrastructure). When these events intersect with an organization's objectives—or can be predicted to do so—they become risks. Risk is therefore defined as "the possibility that an event will occur and adversely affect the achievement of objectives."[1]

While organizations have been conducting risk assessments for years, many still find it challenging to extract their real value. The linkage of risk assessment to drivers of shareholder value and key objectives has sometimes been lost. Risk assessments can be mandated by regulatory demands—for example, anti-money-laundering, Basel II, and Sarbanes-Oxley compliance all require formalized risk assessment, and focus on such processes as monitoring of client accounts, operational risk management, and internal control over financial reporting. Risk assessments can also be driven by an organization's own goals, such as business development, talent retention, and operational efficiency. Regardless of the scope or mandate, risk assessments must bring together the right parties to identify events that could affect the organization's ability to achieve its objectives, rate these risks, and determine adequate risk responses.

A robust risk assessment process forms the foundation for an effective enterprise risk management program. It constitutes a key component of the *Enterprise Risk Management—Integrated Framework* and related Application Guidance published by the Committee of Sponsoring Organizations in 2004 (COSO ERM).[2] It is important to recognize the interrelationships between risk assessment and the other components of enterprise risk management (such as control activities and monitoring) and understand the principles and steps that help ensure the relevance and effectiveness of a risk assessment.

A heightened interest by stakeholders and a growing number of requests to see the results of risk assessments have triggered questions about what a risk assessment should entail, who should be involved, how to sustain and refresh the process, and how to translate results into actions and risk-informed decision making. This paper provides practical guidance on risk assessment by examining these issues and detailing the benefits and opportunities available to organizations that systematically embed risk assessments into their existing business processes.

---

1 Committee of Sponsoring Organizations, *Enterprise Risk Management—Integrated Framework* (2004), p. 16.

2 COSO ERM was developed to help guide organizations in determining how much risk they are prepared to accept as they strive to create value. For more information, see www.coso.org.

A process for capturing and analyzing risks

Understanding both the nature of the organization's objectives and the types of possible risks under consideration is key to determining the scope of the risk assessment. Objectives may be broad (e.g., considering organization-wide strategic, operational, compliance, and reporting requirements) or more narrow (e.g., relating to a product, process, or function such as supply chain, new product sales, or regulatory compliance). Likewise, possible risks may span many categories (e.g., market, credit, product, liquidity, and accounting when considering credit crisis implications) or only a few if the discussion is more narrowly focused (e.g., supplier risk). Finally, the scope may be enterprise-wide or limited to a business unit or a particular geographical area.

Once the scope is defined, those possible risks deemed likely to occur are rated in terms of impact (or severity) and likelihood (or probability), both on an inherent basis and a residual basis. The results can be compiled to provide a "heat map" (or risk profile) that can be viewed in relation to an entity's willingness to take on such risks. This enables the entity to develop response strategies and allocate its resources appropriately. Risk management discipline then ensures that risk assessments become an ongoing process, in which objectives, risks, risk response measures, and controls are regularly re-evaluated. The risk assessment process therefore represents the cornerstone of an effective ERM program.

Risk assessment discipline evolves and matures over time. Organizations typically start with a broad, qualitative assessment and gradually refine their data and analysis as they collect and analyze sufficient relevant data points to support risk-informed decision making and allocation of resources.

The risk assessment process represents the cornerstone of an effective ERM program.

Qualitative assessments are the most basic form of risk assessment, categorizing potential risks based on either nominal or ordinal scales (e.g., classified by category versus ranked in comparison with one another). External validation should be obtained to guard against potential management biases.

More rigorous quantitative techniques—ranging from benchmarking to probabilistic and non-probabilistic modeling—can be used for assessing risk as more data becomes available through tracking of internal events (e.g., transaction errors, customer complaints, litigation) and external events (e.g., loss events recorded by peer organizations and made available through subscription to services such as the ORX or Fitch First databases). Such data enables greater analysis of potential risk exposures, development of relevant indicators that can be tracked regularly, and more rapid and efficient responses to risk situations. Risk categories, loss-event data, and key risk indicators are often refined through iterative efforts to support issue and trend analysis.

Building on qualitative or quantitative assessments, benchmarking can be done to compare risk information across like organizations, such as within an industry group or related to a certain issue (e.g., compliance with a new regulation). Meaningful analysis in this regard requires availability of relevant and timely data from peer organizations.

Analysis is often enriched by various modeling techniques using assumptions regarding distributions. Probabilistic models (e.g., “at-risk” models, assessment of loss events, backtesting) measure both the likelihood and impact of events, whereas non-probabilistic models (e.g., sensitivity analysis, scenario analysis, stress testing) measure only the impact and require separate measurement of likelihood using other techniques. Non-probabilistic models are relied upon when available data is limited. Both types of models are based on assumptions regarding how potential risks will play out.

The more mature risk assessment processes yield quantitative results that can be used to allocate capital based on risk, as required by regulation in certain industries (e.g., Basel II for the financial services industry). For organizations in industries not subject to such requirements, the best approach should be determined based on a cost/benefit analysis of the process for enabling timely and relevant discussion of risks, monitoring predictive indicators, escalating information on increased risk exposures, and making risk-informed decisions in an integrated manner.

Purpose and applicability

Risk assessment is intended to provide management with a view of events that could impact the achievement of objectives. It is best integrated into existing management processes and should be conducted using a top-down approach that is complemented by a bottom-up assessment process. Boards of directors—and particularly board audit committees—often request enterprise-wide risk assessments to ensure that key risks are identified and duly addressed. Such risk assessments should not be disconnected from other assessments performed within the organization. The internal audit function, for instance, may be assessing risks to plan its audits for the year. The finance function may look at similar information to perform its risk-based scoping for Sarbanes-Oxley compliance. Business units may also be assessing risks from a business planning or performance management perspective. These individual assessments should be aligned (e.g., using common terminology, risk categories, and congruent outcomes), cover key objectives, and be integrated to contribute to an enterprise-wide risk assessment.

Risk assessment can therefore be conducted at various levels of the organization. The objectives and events under consideration determine the scope of the risk assessment to be undertaken. Examples of frequently performed risk assessments include:

- Strategic risk assessment. Evaluation of risks relating to the organization's mission and strategic objectives, typically performed by senior management teams in strategic planning meetings, with varying degrees of formality.

- Operational risk assessment. Evaluation of the risk of loss (including risks to financial performance and condition) resulting from inadequate or failed internal processes, people, and systems, or from external events. In certain industries, regulators have imposed the requirement that companies regularly identify and quantify their exposure to such risks. While responsibility for managing the risk lies with the business, an independent function often acts in an advisory capacity to help assess these risks.

- Compliance risk assessment. Evaluation of risk factors relative to the organization's compliance obligations, considering laws and regulations, policies and procedures, ethics and business conduct standards, and contracts, as well as strategic voluntary standards and best practices to which the organization has committed. This type of assessment is typically performed by the compliance function with input from business areas.

- Internal audit risk assessment. Evaluation of risks related to the value drivers of the organization, covering strategic, financial, operational, and compliance objectives. The assessment considers the impact of risks to shareholder value as a basis to define the audit plan and monitor key risks. This top-down approach enables the coverage of internal audit activities to be driven by issues that directly impact shareholder and customer value, with clear and explicit linkage to strategic drivers for the organization.

- Financial statement risk assessment. Evaluation of risks related to a material misstatement of the organization's financial statements through input from various parties such as the controller, internal audit, and operations. This evaluation, typically performed by the finance function, considers the characteristics of the financial reporting elements (e.g., materiality and susceptibility of the underlying accounts, transactions, or related support to material misstatement) and the effectiveness of the key controls (e.g., likelihood that a control might fail to operate as intended, and the resultant impact).

- Fraud risk assessment. Evaluation of potential instances of fraud that could impact the organization's ethics and compliance standards, business practice requirements, financial reporting integrity, and other objectives. This is typically performed as part of Sarbanes-Oxley compliance or during a broader organization-wide risk assessment, and involves subject matter experts from key business functions where fraud could occur (e.g., procurement, accounting, and sales) as well as forensic specialists.

- Market risk assessment. Evaluation of market movements that could affect the organization's performance or risk exposure, considering interest rate risk, currency risk, option risk, and commodity risk. This is typically performed by market risk specialists.

- Credit risk assessment. Evaluation of the potential that a borrower or counterparty will fail to meet its obligations in accordance with agreed terms. This considers credit risk inherent to the entire portfolio as well as the risk in individual credits or transactions, and is typically performed by credit risk specialists.

- Customer risk assessment. Evaluation of the risk profile of customers that could potentially impact the organization's reputation and financial position. This assessment weighs the customer's intent, creditworthiness, affiliations, and other relevant factors. This is typically performed by account managers, using a common set of criteria and a central repository for the assessment data.

- Supply chain risk assessment. Evaluation of the risks associated with identifying the inputs and logistics needed to support the creation of products and services, including selection and management of suppliers (e.g., up-front due diligence to qualify the supplier, and ongoing quality assurance reviews to assess any changes that could impact the achievement of the organization's business objectives).[3]

3. To learn more about supply chain risk assessment, see the PricewaterhouseCoopers white paper *From Vulnerable to Valuable: How Integrity Can Transform a Supply Chain* (December 2008).

- Product risk assessment. Evaluation of the risk factors associated with an organization's product, from design and development through manufacturing, distribution, use, and disposal. This assessment aims to understand not only the revenue or cost impact, but also the impact on the brand, interrelationships with other products, dependency on third parties, and other relevant factors. This type of assessment is typically performed by product management groups.

- Security risk assessment. Evaluation of potential breaches in an organization's physical assets and information protection and security. This considers infrastructure, applications, operations, and people, and is typically performed by an organization's information security function.

- Information technology risk assessment. Evaluation of potential for technology system failures and the organization's return on information technology investments. This assessment would consider such factors as processing capacity, access control, data protection, and cyber crime. This is typically performed by an organization's information technology risk and governance specialists.

- Project risk assessment. Evaluation of the risk factors associated with the delivery or implementation of a project, considering stakeholders, dependencies, timelines, cost, and other key considerations. This is typically performed by project management teams.

The examples described above are illustrative only. Every organization should consider what types of risk assessments are relevant to its objectives. The scope of risk assessment that management chooses to perform depends upon priorities and objectives. It may be narrow and specific to a particular risk, as in some of the examples above. It may be broad but high level: e.g., an enterprise-level risk assessment or a top-down view that considers the broad strategic, operational, reporting, and compliance objectives; captures a high-level view of related risks; and can be used to drill down further into a specific area of concern, as necessary. Assessments may also be broad and deep, as with an enterprise-wide risk assessment or an integrated top-down and bottom-up view, considering the strategic, operational, compliance, and reporting objectives of the organization and its subsets (e.g., business units, geographies) and associated risks.

Risk assessment not only constitutes recommended practice but is also regarded as a requirement by stakeholders such as rating agencies. For example, Standard & Poor's[4] requires organizations to demonstrate awareness and attention to all of their risks. While credit rating agencies have already been evaluating how management at financial services organizations assesses and manages risk (considering industry risk factors, looking at historical risks, and performing forward-looking analysis), they will also begin to evaluate these processes in non-financial-services organizations starting in 2Q09. Organizations' effectiveness in analyzing risks will tend to impact the credit rating and outlook of rating agencies going forward.

Risk assessment is also a necessary component of an effective internal audit program. An emerging practice consists of aligning internal audit activities to business priorities through a comprehensive mapping process to determine where key risks lie within the organization.

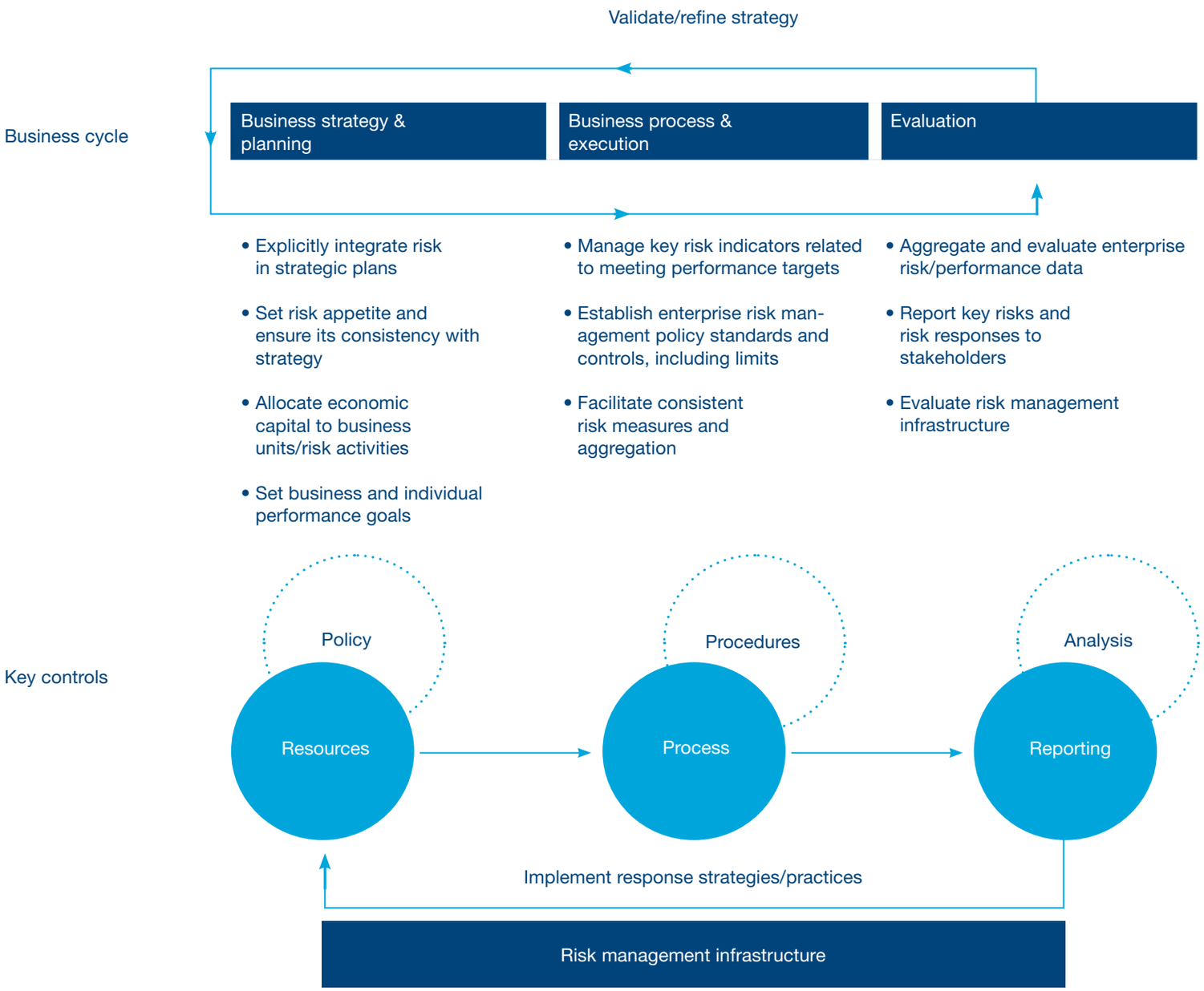
A foundation for enterprise risk management

To be effective, risk assessment cannot be merely a checklist or a process that is disconnected from business decision making. Rather, it should be integrated into the business process in a way that provides timely and relevant risk information to management. For risk assessment to be a continuous process, it must be owned by the business and be embedded within the business cycle, starting with strategic planning, carrying through to business process and execution, and ending in evaluation, as illustrated in Figure 1.

When the risk assessment process is incorporated into ongoing business practices, risk can be managed as part of day-to-day decision making, in a manner consistent with the organization's risk appetite and tolerance. Risk assessment should, for instance, be triggered within the business process when special circumstances arise outside of the ongoing business cycle—e.g., changes to the operating environment, evaluation of new projects, introduction of new products or investments, expansion into new markets, and corporate restructurings.

4 Standard & Poor's RatingsDirect of May 7, 2008, on enterprise risk management, outlines how the organization defines ERM, the effect on ratings, and next steps in its evaluation of ERM capabilities at rated companies.

Figure 1. Integrating risk assessment into business practices



The ability to identify, assess, and manage risk is often indicative of an organization's ability to respond and adapt to change. Risk assessment therefore helps organizations to quickly recognize potential adverse events, be more proactive and forward-looking, and establish appropriate risk responses, thereby reducing surprises and the costs or losses associated with business disruptions. This is where risk assessment's real value lies: in preventing or minimizing negative surprises and unearthing new opportunities. The more real-time and forward-looking the analysis of potential risks, the more controllable the achievement of objectives becomes.

The principles of enterprise risk management require not only that organizations perform a risk assessment but that they implement a process to address potential risks, putting in place the necessary internal environment, information, and communications; establishing objectives; adequately implementing risk responses through control activities; and monitoring how effectively objectives are achieved. COSO defines ERM[5] as a process that is (a) affected by an entity's board of directors, management, and other personnel; (b) applied in strategy setting and across the organization; (c) designed to identify potential events that may affect the entity, then manage risk and keep it within the organization's risk appetite; and (d) provide reasonable assurance regarding the achievement of the entity's objectives. When ERM is embedded in the organization, it prompts periodic review of objectives and relevant events (e.g., changes in market conditions) that could impact the achievement of its objectives, as well as the (re)assessment of risks and development of new risk responses, as necessary. The pace of change in today's business environment calls for a risk assessment process that is dynamic and involves continuous monitoring of risk exposures. Many organizations have leveraged internal audit risk assessments as a foundation for developing enterprise-wide risk assessments and pursuing a broader ERM program.

5 Committee of Sponsoring Organizations, *Enterprise Risk Management—Integrated Framework* (2004), p. 4.

Key principles for effective and efficient risk assessments

For risk assessments to yield meaningful results with minimal burden to the organization, the following key principles should be considered.

1. **Governance over the risk assessment process must be clearly established.** Oversight and accountability for the risk assessment process is critical to ensure that the necessary commitment and resources are secured, the risk assessment occurs at the right level in the organization, the full range of relevant risks is considered, these risks are evaluated through a rigorous and ongoing process, and requisite actions are taken, as appropriate.

   Consider, for example, the role of the board and audit committee in ensuring that risks facing the organization are identified and adequately addressed. While line management is responsible for managing risks, it is important to establish facilitator roles and a process to help analyze and prompt discussion of new or emerging risks. As sponsors of the risk assessment, the board and audit committee need to designate an appropriate process owner, such as a chief risk officer or a risk facilitator. This process owner must in turn engage the relevant parties (e.g., division general managers, business and line managers, and functional process owners) who are closest to the business activities and best understand business processes. It's then up to these parties to analyze internal and external information, identify risks that impact business objectives, and determine the appropriate responses for dealing with these new or evolving risks. By establishing and reinforcing the importance of this process and validating results, those results can be used not only to enable risk-informed decision making but also to guide strategy and objective setting.

2. **Risk assessment begins and ends with specific objectives.** Risks are identified and measured in relation to an organization's objectives or, more specifically, to the objectives in scope for the risk assessment (as further described on page 16). Defining objectives that are specific and measurable at various levels of the organization is crucial to a successful risk assessment. Evaluating the risks relative to such objectives facilitates the reallocation of resources as necessary to manage these risks and best achieve stated objectives.

As an organization defines its objectives, it should also define its risk appetite, or the amount of risk it is willing to accept in pursuit of its mission. Failure to define risk appetite could result in taking on too much risk to achieve objectives or, conversely, not taking on enough risk to seize crucial opportunities. An organization's definition of its risk appetite serves as a basis for determining risk tolerance, or the acceptable levels of variation that management is willing to allow for any particular risk as it pursues objectives. For example, consider the objective of pursuing employee satisfaction and retention, with an appetite of up to 6% employee turnover and an acceptable variation (or tolerance) of 2%. This would indicate that the organization deems employee motivation programs and compensation structures to be appropriately tuned as long as turnover remains at or below 6%. If turnover were to exceed 8% (6% plus 2% acceptable variation), the organization would need to take further measures to counter the potential loss of institutional knowledge and the likely decline in employee morale and customer service, all of which would impact its business too significantly. Risk tolerance levels differ based on the relative importance of the related objectives to the overall mission and the relative cost/benefit of achieving such results.

3. **Risk rating scales are defined in relation to organizations' objectives in scope.** Risks are typically measured in terms of impact and likelihood of occurrence. Impact scales of risk should mirror the units of measure used for organizational objectives, which may reflect different types of impact such as financial, people, and/or reputation. Similarly, the time horizon used to assess the likelihood of risks should be consistent with the time horizons related to objectives.

   Risk rating scales may be defined in quantitative and/or qualitative terms. Quantitative rating scales bring a greater degree of precision and measurability to the risk assessment process. However, qualitative terms need to be used when risks do not lend themselves to quantification, when credible data is not available, or when obtaining and analyzing data is not cost-effective. Organizations typically use ordinal, internal, and/or ratio scales. Ordinal scales define a rank order of importance (e.g., low, medium, or high), interval scales have numerically equal distance (e.g., 1 equals lowest and 3 equals highest, but the highest is not 3 times greater than the lowest), and ratio scales have a "true zero" allowing for greater measurability (e.g., a ranking of 10 is 5 times greater than a ranking of 2). Risk rating scales are not one-size-fits-all and should be defined as appropriate to enable a meaningful evaluation and prioritization of the risks identified and facilitate dialog to determine how to allocate resources within the organization.

Figure 2. Risks should be assessed considering the likelihood and impact of such risks in relation to specific objectives

Likelihood	Definition	Description	Example *Objective:* Hire staff with appropriate competencies *Event:* Burdensome recruitment procedures limit the organization's ability to attract talent
1	Unlikely	The risk is seen as unlikely to occur within the time horizon contemplated by the objective.	Although **recruitment procedures are burdensome**, talent with appropriate competencies can still largely be attracted and hired.
2	Likely	The risk is seen as likely to occur within the time horizon contemplated by the objective.	**Burdensome recruitment procedures** cause delays and lost opportunities in the hiring of talent with appropriate competencies.
3	Certain/ imminent	The risk is expected to occur within the time horizon contemplated by the objective.	**Burdensome recruitment procedures** cause talent with appropriate competencies to not be attracted or hired.

Impact	Definition	Description	Example
1	Negligible	The risk will not substantively impede the achievement of the objective, causing minimal damage to the organization's reputation.	The extent to which **recruitment procedures are burdensome** will not substantively impede our ability to attract and hire staff with appropriate competencies, causing minimal damage to the organization's reputation.
2	Moderate	The risk will cause some elements of the objective to be delayed or not be achieved, causing potential damage to the organization's reputation.	The extent to which **recruitment procedures are burdensome** will cause delays in our ability to attract and hire staff with appropriate competencies, causing potential damage to the organization's reputation.
3	Critical	The risk will cause the objective to not be achieved, causing damage to the organization's reputation.	The extent to which **recruitment procedures are burdensome** will cause us to be unable to attract and hire staff with appropriate competencies, causing damage to the organization's reputation.

Consider the example in Figure 2, which relates likelihood and impact of risks back to specific objectives to provide a meaningful indicator of performance. Risk rating scales should provide a common form of measurement to help prioritize risks and determine required actions based on defined risk tolerance.

4. **Management forms a portfolio view of risks to support decision making.** While risks are rated individually in relation to the objectives they impact, it is also important to bring risks together in a portfolio view that pinpoints interrelationships between risks across the organization. Correlations may exist, in which an increased exposure to one risk may cause a decrease or increase in another. Concentrations of risks may also be identified through this view. The portfolio view helps organizations understand the effect of a single event and determine where to deploy systematic responses to risks, such as the establishment of minimum standards.

   Consider a lending institution that has a number of business lines, each responsible for providing specific types of lending. Each of these business lines may be providing lending support to a large number of retail clients, each within its own risk tolerance level. A portfolio view of all business lines, however, might show that the organization as a whole may be facing risk exposure that may exceed what it deems acceptable. It is important for organizations to recognize such concentration and the associated level of exposure it presents. If an industry is suddenly affected by a downturn in a specific sector of the economy and the lending organization's clients suffer financial hardship, the consequences could be large enough to severely impact the organization's bottom line. A portfolio view of risks enables the organization to identify significant exposures across the enterprise, determine how to reduce these as necessary, and realize potential opportunities that may exist to diversify the client base across the organization and its lines of business.

   The portfolio view of risks can be presented in a variety of ways but requires a certain level of consistency to enable an organization to identify and monitor key issues, trends, and progress in relation to its strategic performance targets. A consistent portfolio view provides meaningful information that allows the owners and sponsors of risk assessments (senior management and the board) to make informed decisions regarding risk/reward trade-offs in operating the business. The portfolio view therefore enhances the ability to identify events and assess similar risks across the organization, to ensure that risks are managed consistent with risk tolerance levels reflecting growth and return objectives, and to develop adequate risk responses.

5. **Leading indicators are used to provide insight into potential risks.** Risk reports are most meaningful and relevant when they draw out not only past events but also forward-looking analysis. Historically, management has tracked key performance indicators (KPIs) to help detect issues affecting the achievement of objectives. In recent years, organizations have also been developing key risk indicators (KRIs) to help signal an increased risk of future losses or an uptick in risk events. KPIs and KRIs are tactical in nature, can be collected at any time, reported on a regular basis or as requested by management (e.g., as part of a balanced scorecard), and typically include statistics and/or metrics (often financial) that provide insight into an organization's risk position. Capturing KPIs and KRIs on management dashboards remains necessary, but it is also important for organization leaders to prompt broader consideration of market issues that could potentially create risk to the organization. Leading indicators—those data points that signal a change in the environment—are central to anticipating these types of potential risks, but they are often difficult to capture since they tend to arise from a broad set of circumstances, often in the macro-environment, that may seem remote and initially disconnected from day-to-day operations.

   To illustrate these three types of indicators, consider the credit crisis. Leading indicators included increasingly lax lending practices in which lending decisions were not adequately matched to risk (loan approval rates relative to credit ratings in the general population). KRIs included increases in refinancing activity, reduction in home values, and increases in late mortgage payments. KPIs included defaults and loan losses, including the corresponding decline in liquidity.

To identify meaningful leading indicators, management must identify and analyze changes in the business environment, such as rapid growth, changing technology, or the emergence of new competitors that could impact the organization's ability to reach its objectives. The discipline to look beyond past events and anticipate new risks requires a forum for discussion, along with strong leadership and facilitation as part of the risk assessment process.

What this means for your business

Effective risk assessment requires a consistent approach, tailored to the organization.

Essential steps for performing a risk assessment

Performing a risk assessment requires defining and consistently applying an approach that is tailored to the organization. Any risk assessment exercise should begin with the establishment of a scope and plan, considering objectives, responsibilities, timing, and input and output requirements. Responsibilities in the risk assessment process are assigned to those parties that can provide meaningful perspective on relevant risks (e.g., not only line management but also cross-functional representation). Sources of input are determined based on available information (e.g., prior assessments, loss data, KRIs, lessons learned). Output requirements are established based on the specific requirements of sponsors and other stakeholders (e.g., senior management, the board, regulators, stockholders, or business partners).

Once the scoping and planning are agreed, the execution of the risk assessment process should include the following essential steps:

1. Identify relevant business objectives.

It is important to begin by understanding the relevant business objectives in scope for the risk assessment. These will provide a basis for subsequently identifying potential risks that could affect the achievement of objectives, and ensure the resulting risk assessment and management plan is relevant to the critical objectives of the organization.

Objectives are defined at various levels of the organization (e.g., division, location, enterprise-wide), and it is important to understand how they are developed. Typically, an analysis of strengths, weaknesses, opportunities, and threats (SWOT) is performed, the organization's critical success factors are identified, or a strategy map is developed depicting the cause-and-effect relationships underpinning the organization's creation of shareholder value. Such underlying analysis helps illuminate not only the objectives but also key considerations from the perspective of stakeholders, such as customers and regulators. Objectives are typically laid out in annual reports, business unit strategic plans, presentations to analysts, functional unit charters, project/investment plans, and management documents.

The scope of the risk assessment may focus on objectives that are related to strategy, operations, compliance, and/or reporting, as previously discussed. Once the scope has been agreed and the relevant objectives identified, it is important to understand how these fit in with the strategy and how much risk the organization is willing to assume in pursuit of these objectives. Different strategies create exposure to different risks, and different levels of risk appetite guide different levels of resource allocation to respond to those risks. For example, an internal audit risk assessment that is most effective and maximizes value aligns internal audit activities to key organizational objectives. The focus on business objectives helps ensure relevance and facilitates the integration of risk assessments across the organization.

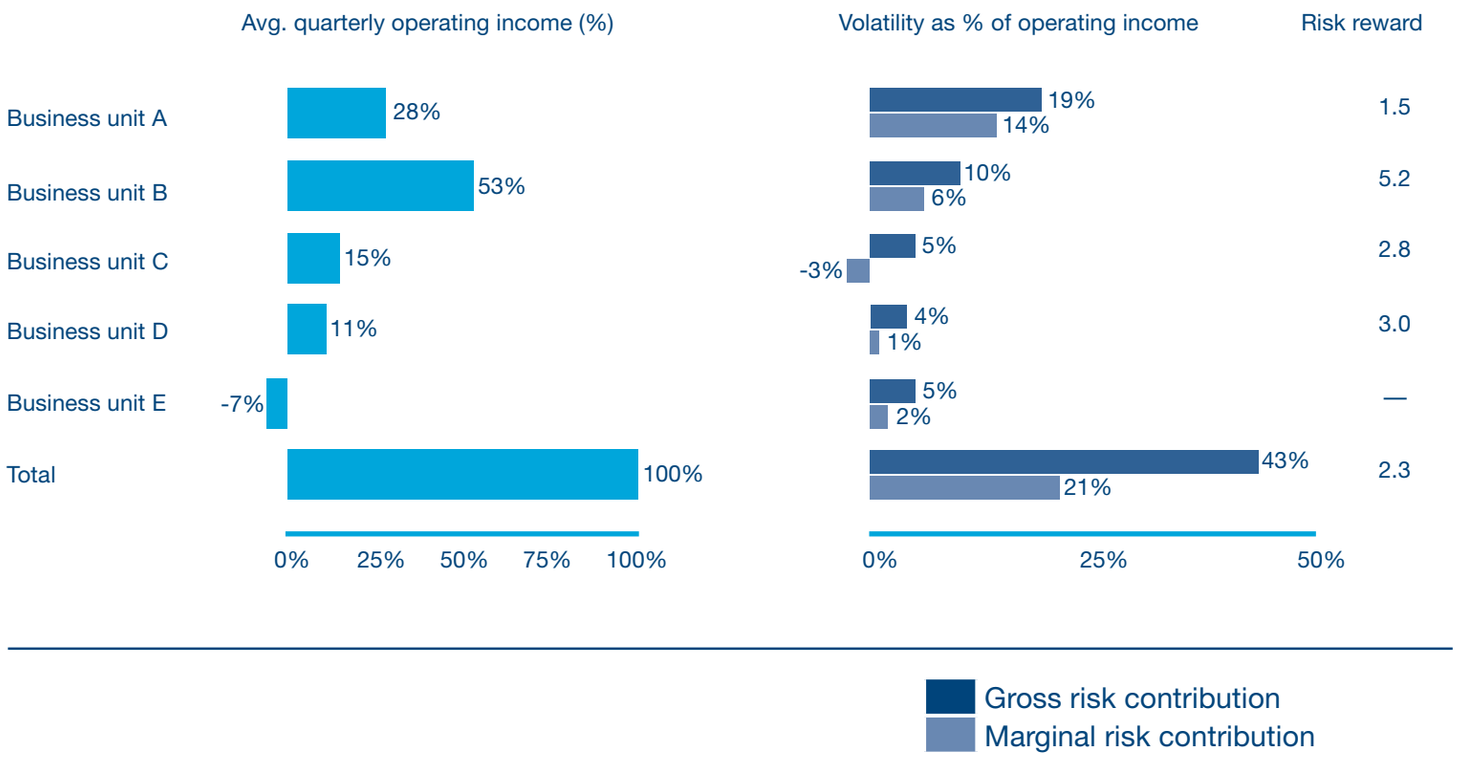
2. Identify events that could affect the achievement of objectives.

Based on the organization's objectives, the designated owners of the risk assessment should develop a preliminary inventory of events that could impact the achievement of the organization's objectives. "Events" refers to prior and potential incidents occurring within or outside the organization that can have an effect, either positive or negative, upon the achievement of the organization's stated objectives or the implementation of its strategy and objectives. Various taxonomies or libraries of common event types can help initiate the identification process.

A review of the external environment helps identify outside events that may have impacted the organization's shareholder value in the past or may impact it in the future. Drivers to consider include economic, social, political, technological, and natural environmental events, which can be identified through external sources such as media articles, analyst and rating agency reports, and insurance broker assessments.

To illustrate the value of such external research, consider the external disclosure snapshot in Figure 3, which illustrates the percentage of average quarterly operating income by business unit and region in relation to volatility of earnings as a percentage of operating income. From this information, a "risk/reward" measure can be derived to understand how levels of volatility affect operating income. This measure helps the organization pinpoint relative risk in earnings potential and target dependencies within lines of business.

Figure 3. External disclosure snapshot



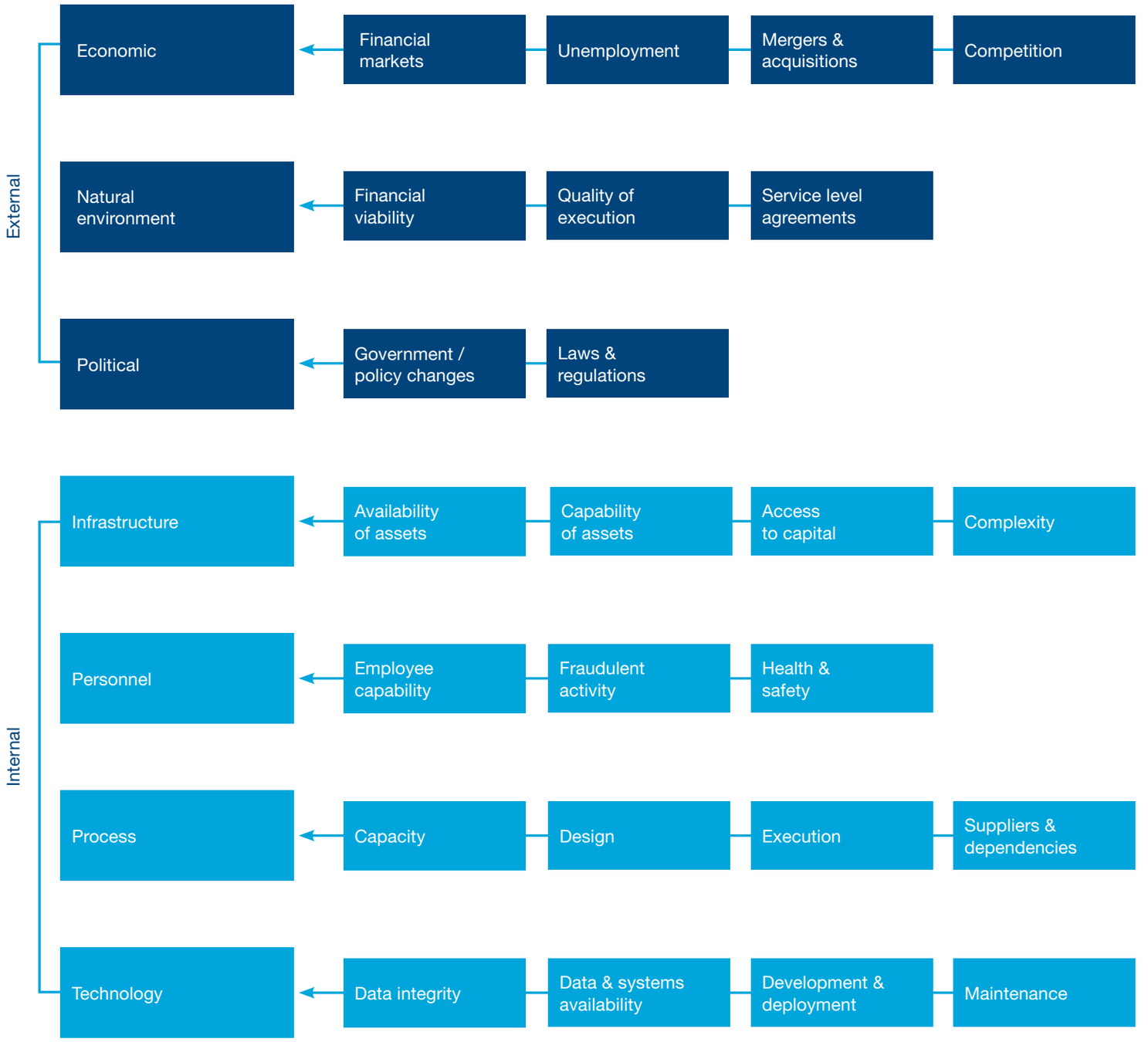
A review of the organization's internal processes, people, technology, and data helps identify further events. Relevant information is often derived from internal sources such as business plans and budgets, prior risk assessments, financial performance, litigation, board and annual reports, loss-event databases (e.g., ORX and Fitch First), and policies and procedures. Both external and internal data sources should be considered. For example, an information technology risk assessment should consider internal factors such as the number and length of systems failures, employee access controls, and protection of confidential data and information, as well as external factors such as the introduction of advanced software and hardware into the industry and incidents of cyber crime within the previous year. Such information can be obtained through interviews, workshops, surveys, process flow reviews, documentation reviews, or a combination of such data-gathering techniques. Through facilitated workshops, management can guide line management and cross-functional staff through the process of analyzing objectives, discussing past events that impacted those objectives, and identifying potential future events. A survey approach can also be used to collect relevant insights by sending a questionnaire to a cross-section of management and staff. Techniques should be selected based on fit with current management practices and the type of output required.

The events identified should be inventoried and translated into opportunities (positive events) or risks (negative events). Opportunities should flow into management's strategy- and objective-setting processes, whereas threats should be further categorized and assessed.

Events can be categorized in a variety of ways. For example, they may be brought together in a matrix, with horizontal columns capturing categories of root risk causes and vertical rows representing lines of business or functional areas. All applicable areas of risk are then marked accordingly. Another approach consists of capturing all relevant event types and linking these to broader categories, as illustrated in Figure 4.

The identification of event types should be periodically refreshed and is only as complete as the sources of input, which should involve all relevant business lines and functional areas. Such participants vary according to the type of risk assessment being performed. For example, for a fraud risk assessment, it may be critical to gain the perspective of members of the accounting, procurement, and corporate security divisions, whereas these may not be the right parties to provide input into a market risk assessment.

Figure 4. Event categories—considering external and internal factors



3. Determine risk tolerance.

Risk tolerance is the acceptable level of variation relative to the achievement of a specific objective, and should be weighed using the same unit of measure applied to the related objective. Risk tolerance considers the relative importance of objectives and aligns with risk appetite. Risk appetite must be clearly defined and reflected in risk tolerances and risk limits to help ensure that organizational objectives can be achieved. Risk tolerances should be defined for each key risk type.

For example, as an airline considers its objective of superior on-time service, it should include various marketing, customer service, and operational factors to determine its risk tolerance. The airline's pre-existing target of 85% on-time flight arrival may have generally been achieved over the years and be in line with messages in its marketing program, yet it may find that the industry average for on-time arrival has been around 80% and that there is minimal effect on customer flight bookings when on-time arrival statistics temporarily decrease to this level. The airline may also find that the cost to achieve more than 87% on-time arrival is prohibitive and cannot be passed through in ticket prices. With the added pressure to keep costs down, and based on this information, management may therefore maintain the objective of 85% average on-time arrival, with a tolerance of between 82% and 86%. Looking at the tolerances for multiple objectives such as customer retention and cost containment, management is better able to allocate resources to ensure reasonable likelihood of achieving outcomes across multiple objectives.

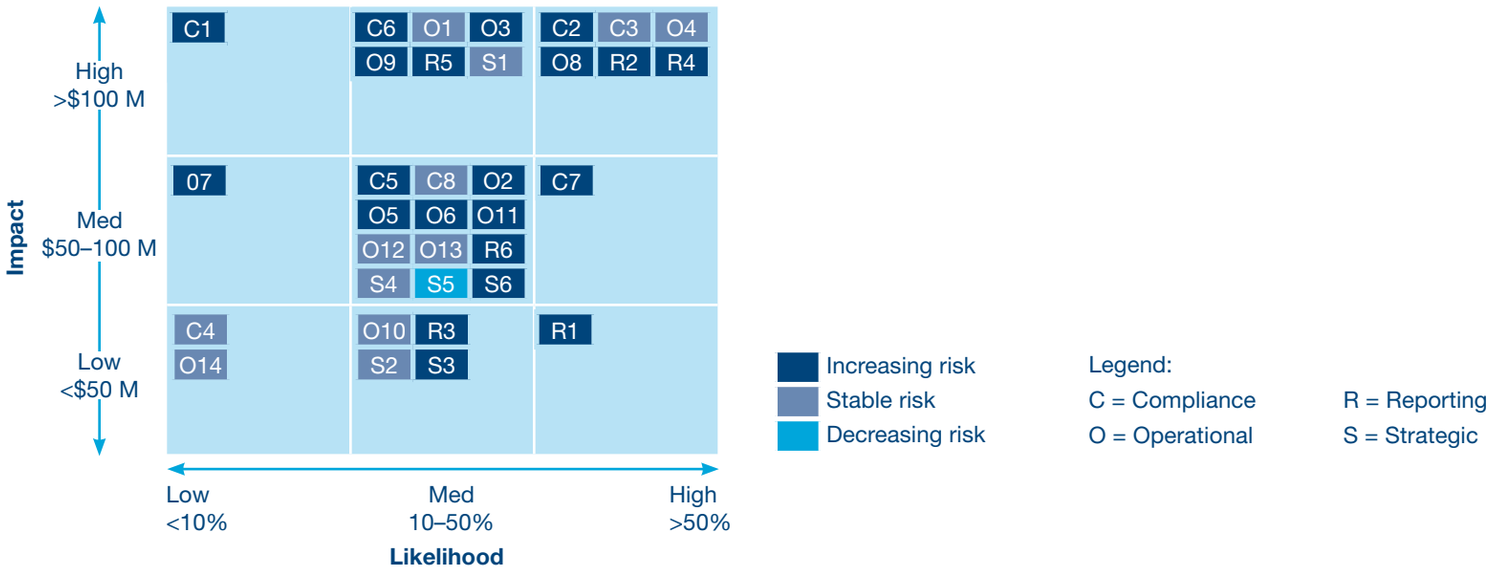
4. Assess inherent likelihood and impact of risks.

Events identified as potentially impeding the achievement of objectives are deemed to be risks and should be evaluated based on the likelihood of occurrence and the significance of their impact on the objectives. It is important to first evaluate such risks on an inherent basis—that is, without consideration of existing risk responses and control activities.

For example, an organization with headquarters on the banks of a river may seek to assess its exposure to the risk of flooding. On an inherent basis, it would consider the likelihood and impact of a flood by considering external data (such as the historical and projected frequency of floods) and internal data (such as the estimated damage to its physical assets if a flood were to occur). An impact and probability rating should then be assigned using defined risk rating scales, as discussed on page 16.

These individual risk ratings should then be brought together in the form of an inherent risk map (see Figure 5), which enables an analysis of risks not only on an individual level (e.g., high, medium, low) but also in relation to one another (e.g., a concentration of certain risks that potentially creates a greater overall risk exposure—for example, reputational damage—than the sum of the individual risk exposures). Additionally, as risk assessments are refreshed over time, a risk map can allow analysis over time (e.g., upward or downward trend of risks, and extent of positive or negative correlations between certain risks).

Figure 5. Risk map



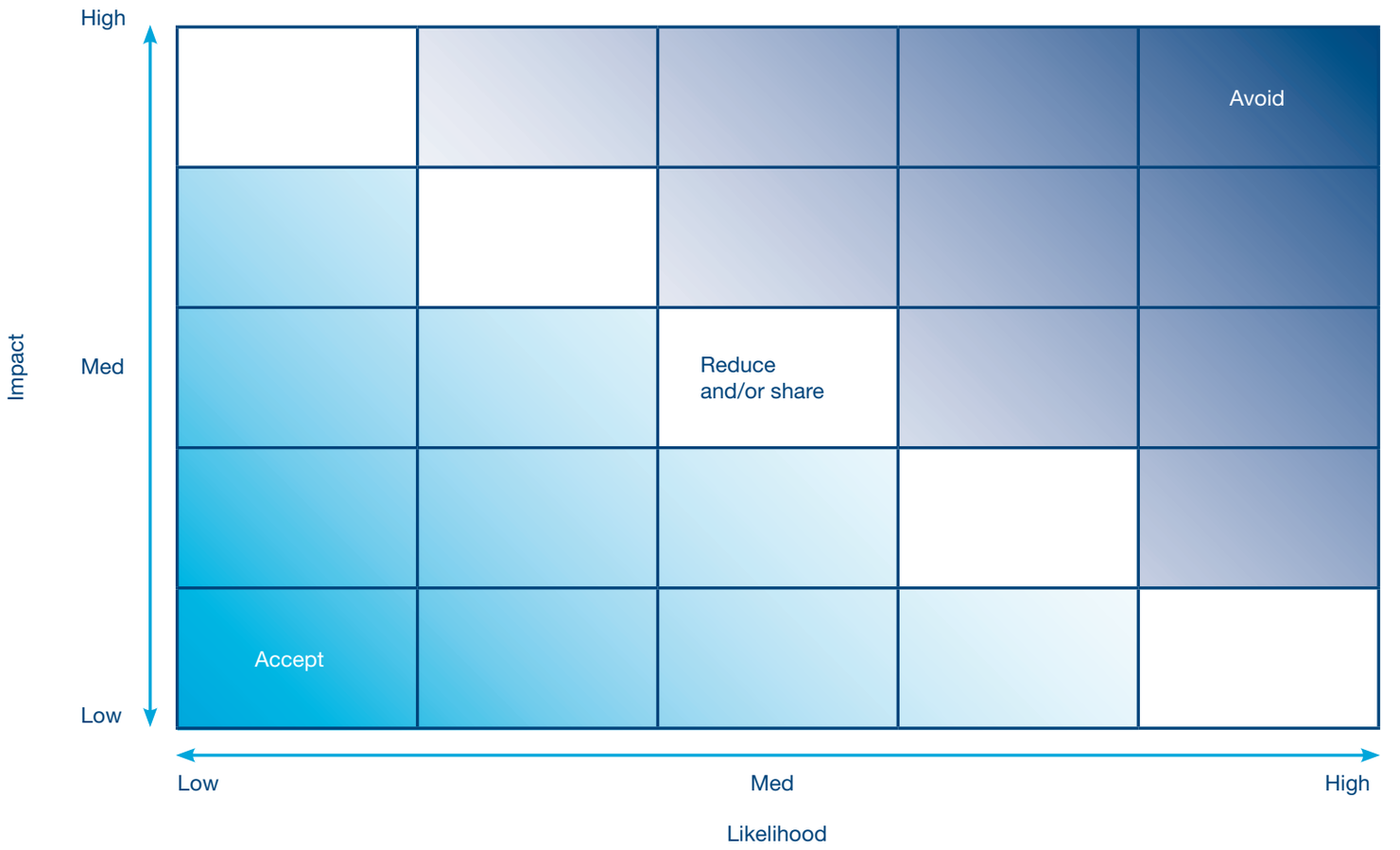
Categories	Description
[C1] Compliance	Non-compliance with laws, regulations, or policies
[C2] Ethics and integrity	Fraudulent, illegal, or unethical acts
[C3] Intellectual property	Inability to enforce patents and trademark; infringement
[C4] Legal and disputes	Changing laws, liabilities, and commercial disputes
[C5] Product quality	Producing off-spec products
[C6] Product safety	Unsafe products
[C7] Regulatory	Changing regulations threaten competitive position
[C8] Tax	Failure to adequately support tax positions
[O1] Catastrophic loss	Major natural or manmade disaster; terrorism
[O2] Customer	Failure to follow customer preferences/needs
[O3] Efficiency	Inefficient operations
[O4] Engineering	Inability to design and manage facilities projects
[O5] Environmental	Environmental incidents or exceedances
[O6] Equipment	Plant equipment failure
[O7] Health and safety	Health and safety incidents harm employees
[O8] IT	Failure of IT systems; cyber attack
[O9] People	Lack or loss of qualified employees

Categories	Description
[O10] Security	Security breaches at company sites
[O11] Sourcing	Lack of access to key raw materials; failure of supplier
[O12] Supply chain	Failure of transportation and logistics network
[O13] Technology	Development of new, potentially disruptive technologies
[O14] Weather	Prolonged, adverse weather conditions
[R1] Commodity	Variability and increasing trends in commodity prices
[R2] Credit	Failure of customers or counterparties to perform
[R3] FX	Volatility in foreign exchange rates
[R4] Interest rate	Variability in interest rates
[R5] Investment	Financial market volatility impacts investments
[R6] Process design and execution	Failure in the design and execution of key management processes
[S1] Alliance	Inefficient or ineffective alliance, joint venture, affiliation
[S2] Capital adequacy	Lack of access to capital or liquidity
[S3] Competitive	Actions of competitors or new market entrants
[S4] Industry	Industry changes threaten industry attractiveness
[S5] Macroeconomic	Changes in broad economic conditions
[S6] Political	Adverse actions by foreign governments

In Figure 5, a number of risk categories are identified and linked to several types of objectives through the alphanumerical coding of the risks (e.g., regulatory—coded C7—is the seventh risk category related to the organization's compliance objectives). The risks within each category may be individually rated and summarized to provide an aggregate rating for the risk category, or the risk category may be rated as a whole. The resulting score is then plotted on the risk map. Likelihood is labeled across the x-axis, from low to high in percentages. Impact is labeled over the y-axis, from low to high in dollar values. These ratings can be used to produce a risk map noting increasing, stable, or decreasing movement in risk exposure since the prior assessment. Item C7, relating to regulatory risk, shows increasing risk exposure; a likelihood of occurrence greater than 50%; and an impact, if this risk event occurred, of between $50 and $100 million.

An inherent risk map provides a portfolio view of risk that prompts analysis and action. It helps determine which risk areas are most significant and should be the focus of a more detailed assessment or implementation of a specific risk response. It also enables analysis of interdependencies and relative prioritization of risks, and determination of risk responses. In short, the risk map can provide focus for management's risk agenda.

Figure 6. Risk response strategies



5. Evaluate the portfolio of risks and determine risk responses.

Based on the defined risk tolerance and inherent risk assessment, management can determine how to address the identified risks. All organizations need to take on a certain level of risk when conducting business in order to generate returns for their stakeholders. Appetite for risk and tolerance for deviation from objectives must form the basis for determining how to address risks, considering their expected impact and likelihood of occurrence. Risk tolerance can vary from one risk type to another, depending on the importance to the organization's key mission, values, and objectives. Accordingly, responses to different "high" risks may vary, and a portfolio view of risk exposures should be considered to adequately determine risk responses, as further described below. Typical risk response strategies are to accept, share, reduce, or avoid, as depicted in Figure 6.

Figure 6 illustrates typical risk response strategies in relation to risk ratings. For each risk category, the organization should have defined risk tolerance levels to be used in relation to risk ratings to determine response strategies. While the thresholds vary by risk category, risks that present impact and likelihood are typically to be avoided and risk mitigation actions should be undertaken to halt and exit activities that create such risk. Risks that present low impact and low likelihood are typically accepted as part of the cost of doing business. No specific action is deemed necessary to further address these risks. Those risks that fall in between may require measures to reduce the impact and/or likelihood of these risks through strengthening or automation of controls. The organization may share the impact of these risks through the use of hedging instruments, outsourcing, or purchasing of insurance. Risk responses may be "quick wins" that yield immediate results and/or longer-term process improvement initiatives to help achieve organizational objectives. Responses are often incremental and build on each other.

Continuing with the individual risk example given in step 4, increasing an insurance policy may be a means to share the financial impact of damage in the case of a flood. Developing backup plans, acquiring new off-site facilities, and training the necessary resources may be a means to reduce identified risk. Risk responses therefore often need to be prioritized based on cost/benefit and relative importance to the organization's objectives and availability of resources. Risk responses are expected to bring the level of risk exposure down to defined risk tolerance levels. Control activities should be put in place and evaluated to ensure that these responses to risks are operating as intended.

6. Assess residual likelihood and impact of risks.

Residual risk assessment considers both the risks as previously identified and the related risk response mechanisms and control activities in place to determine the impact and probability of their occurrence. In other words, it evaluates the adequacy and effectiveness of the internal checks and balances in place, providing reasonable assurance that the likelihood and impact of an adverse event are brought down to an acceptable level.

Continuing with the example above, to rate the risk of flood damage on a residual basis, the likelihood and impact ratings should be assigned considering the risk response measures in place to protect critical systems and data against flooding (e.g., creation of an off-site IT and data storage center and an insurance policy to cover any residual damage). While these measures may not reduce the likelihood of a flood, they would help reduce the impact to the business if one were to occur. This residual risk assessment can help management determine whether risks are adequately controlled, overcontrolled, or undercontrolled in relation to the defined risk tolerance.

Bringing it all together. The organization can now bring its individual residual risk ratings together into a portfolio view to identify interdependencies and interconnections between risks, as well as the effect of risk responses on multiple risks. Management can then determine any actions necessary to revise its risk responses or address design or effectiveness of controls. Action plans should be assigned to parties with the capability and authority to effect change, with specified milestones and timelines that are documented and tracked for completion. Successful implementation should translate into reduced risk exposures on the organization's risk map.

Common challenges to effective risk assessment

While risk assessment provides the means to identify and address potential risk factors, failure to perform assessments effectively can lead to missed opportunities, both to avoid and capitalize on risk events. Common business challenges include the following.

Risk assessment is viewed as an episodic initiative providing limited value. The owner of a risk assessment must clearly communicate its purpose, process, and expected benefits. The right parties must be engaged to ensure relevant input, informed assessment, and meaningful and actionable results. Moreover, the assessment must be a repeatable process that integrates into regular business practices, adapts to change, and delivers more than one-time value.

The amount of information and data gathered is difficult to interpret and use. Failure to effectively organize and manage the volume and quality of assessment data makes interpreting that data a challenge. Tools, templates, and guidance are necessary to ensure consistency in data capture, assessment, and reporting.

Results of the risk assessment are not acted upon. Lack of clarity and accountability around objectives frequently leads to a failure to follow through on assessment findings. It is therefore important that the risk assessment process begins by clearly articulating objectives, designating their ownership, and linking them to the risks being assessed. Likewise, owners should be assigned to the action items related to risk responses as well as to milestones and timelines for completion, which serve as triggers for any necessary follow-up.

Overcontrolling risk can be costly and stifle innovation. An organization is responsible for ensuring that its controls are designed and operating effectively, focusing on key controls to the extent possible. It must also determine how much risk is acceptable and how much variability it can tolerate. It must prioritize risk responses based on a cost/benefit analysis and availability of resources. Lack of an effective risk assessment process and defined risk tolerance could result in an organization overcontrolling a risk, which could place an excessive cost burden on the organization and/or stifle its ability to seize opportunities.

Risk assessments become stale, providing the same results every time. Without refreshing their data capture, process, and reporting from time to time, risk assessments may lose relevance. Breakdowns may occur without triggering key risk indicators to management. Organizations must continuously challenge themselves to build upon the information and data collected. They must continually update their assessment techniques and mechanisms in order to refine their analyses of risks, have greater predictability over risk events, and create better response mechanisms for dealing with surprises.

Risk assessment is added onto day-to-day responsibilities without being integrated into business processes. While tools and templates are helpful to ensure consistency in data capture, assessment, and reporting, it is important that the risk assessment process be anchored and integrated into existing business processes. This may include building trigger levels into existing systems to raise potential issues to management as part of daily operations, or including an explicit risk assessment discussion as part of business planning, execution, and evaluation meetings. Risk assessment then becomes a discipline within a process rather than an additional process bolted on top of existing ones.

Too many different risk assessments are performed across the organization. A shared approach should be defined for performing risk assessments, using common tools or templates, common data sets (e.g., risk categories, libraries of risks and controls, rating scales), and flexible hierarchies to enable streamlined data capture, an integrated assessment process, and flexible reporting. This enables a reduction in the number of risk assessments requested of the business or functional units and an increased ability to rely on integrated processes while still meeting the risk requirements of the various stakeholders. In order to develop these integrated processes, an organization should inventory its current risk assessment processes and then share best practices and identify overlaps and gaps.

Risk assessment will not prevent the next big failure. As risk assessment provides a means for facilitating the discussion around key risks and potential control failures, it helps reduce the risk of breakdowns, unanticipated losses, and other significant failures. Effective governance over the process—in particular independent review by risk managers—is key to ensuring that risks are adequately assessed and that controls are not circumvented to cover up certain information. Risk assessments need to invoke the right subject matter experts and consider not only past experience but also forward-looking analysis.

Putting key principles to work. Customers, regulators, rating agencies, investors, and other stakeholders expect organizations to manage risk effectively, with a robust risk assessment process serving as a cornerstone to their risk management programs. The challenges listed above can impact organizations through business disruption, missed opportunities, financial penalties, or damage to reputation and brand value—but the key principles and essential steps laid out earlier in this section can help organizations avoid these challenges. With organizations facing a fluid and seemingly endless array of risks and obligations, leveraging these key principles can provide the consistent platform necessary to effectively manage these risks in a cost-effective and sensible way.

Risk assessment: benefits and opportunities

The risk assessment process forms the cornerstone of an effective ERM program. When assessments are performed systematically and consistently throughout the organization, management is empowered to focus its attention on the most significant risks and make more informed risk decisions. (See Figure 7.) For example, organizations gain the ability to prioritize the deployment of capital and measurement of relative performance across various objectives or entities, potentially reducing the occurrence and significance of negative events, and their associated losses. Through effective risk assessment, organizations can also better coordinate multiple risk responses, effectively addressing risks that threaten multiple business areas or functions.

Most importantly, an effective risk assessment yields forward-looking insight, not only allowing organizations to avoid risks, but providing greater and more meaningful clarity around the risks they do face. Armed with this insight and perspective, organizations are much better positioned to take the right risks, and can better manage them when they do. In the long run, organizations that continuously reposition themselves to capitalize on both quick wins and longer-term opportunities are more likely to meet—and surpass—their business objectives. It is this capability that will lead to measurable, lasting success in today's ever-changing business environment.

Figure 7. Key risk assessment principles, benefits, and opportunities

Key principles	Benefits	Opportunities
Governance over the risk assessment process must be clearly established	• Organizational commitment and cooperation • Ownership of the risk assessment process and output, resulting in greater quality of data • Engagement of requisite resources in the risk assessment process • Rigor and accountability for taking risks	• Collaborate on key risk discussion • Drive consistency in approaches to risk assessment
Risk assessment begins and ends with specific objectives	• Defined scope for the risk assessment • Accountability for the achievement of objectives • Risk discussion anchored in the context of specific objectives, risk appetite, and tolerance	• Evaluate risk-adjusted returns to the organization
Risk rating scales are defined in relation to organizations' objectives in scope	• Common basis for assessment of risks • Assessment of impact and probability of risks in relation to stated objectives	• Measure and monitor the ability to achieve objectives
Management forms a portfolio view of risks to support decision making	• Prioritization of the organization's most significant risks • Ability to view and manage risks that span multiple business or functional areas • Clarity on the interrelationships between risks and coordination of risk responses that may be required • Risks are not merely avoided but understood, and risk-informed decisions are made to seize opportunities	• Deliver integrated responses to multiple risks • Identify "quick wins" and longer-term improvement opportunities • Prioritize deployment of capital and measurement of relative performance across various objectives or entities
Leading indicators are used to provide insight into potential risks	• Forward-looking analysis in relation to the overall portfolio of risks • Analysis enables the detection of relevant changes in the environment that could impact the achievement of objectives and prompt action as necessary	• Reduce instances and/or significance of negative surprises and associated losses • Use relevant predictive risk information to guide decision making

pwc.com/us/grc

To have a deeper conversation about how this subject may affect your business, please contact:

Joe Atkinson
Principal
267.330.2494
joseph.atkinson@us.pwc.com

Catherine Jourdan
Director
646.471.7389
catherine.i.jourdan@us.pwc.com

This publication is printed on Finch Fine Recycled. It is a Sustainable Forestry Initiative® (SFI) certified stock using 10% post-consumer waste (PCW) fiber and manufactured in a way that supports the long-term health and sustainability of our forests.

10% total recycled fiber