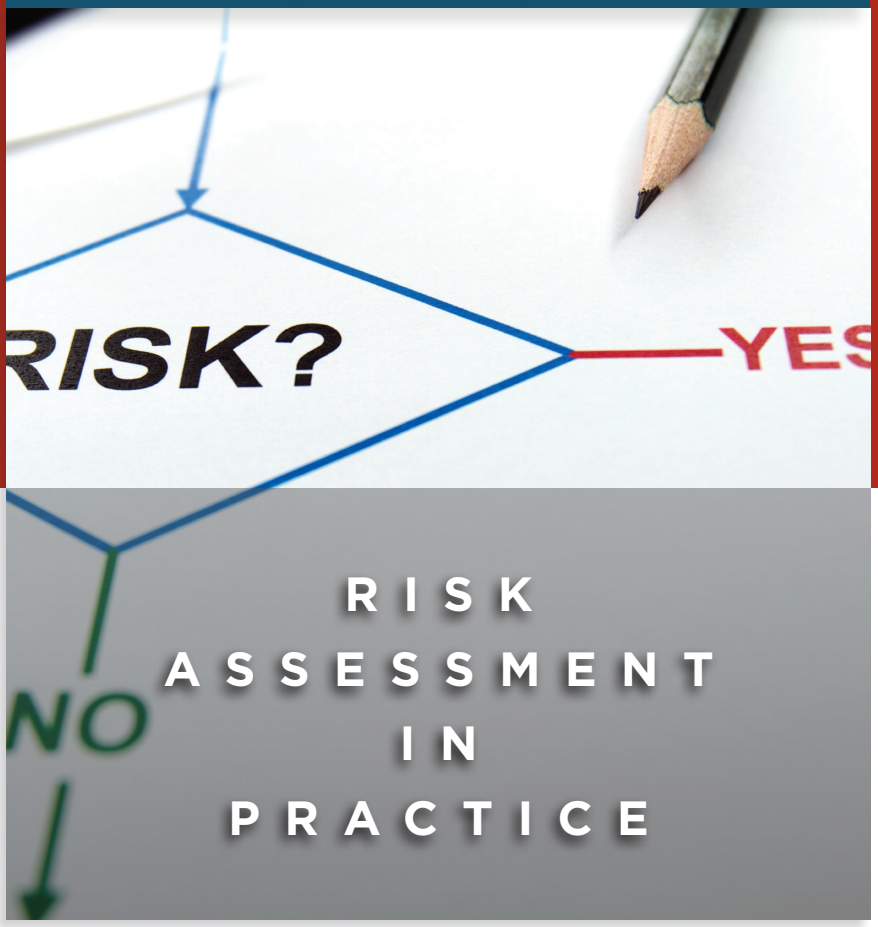
COSO

Committee of Sponsoring Organizations of the Treadway Commission

Thought Leadership in ERM



RISK ASSESSMENT IN PRACTICE

By

Deloitte & Touche LLP

Dr. Patchin Curtis | Mark Carey

Authors

Deloitte & Touche LLP

Principal Contributors

Dr. Patchin Curtis
Director,
Deloitte & Touche LLP

Mark Carey
Partner,
Deloitte & Touche LLP

COSO Board Members

Preface

This project was commissioned by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which is dedicated to providing thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control, and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations. COSO is a private-sector initiative jointly sponsored and funded by the following organizations:

American Accounting Association (AAA)

American Institute of CPAs (AICPA)

Financial Executives International (FEI)

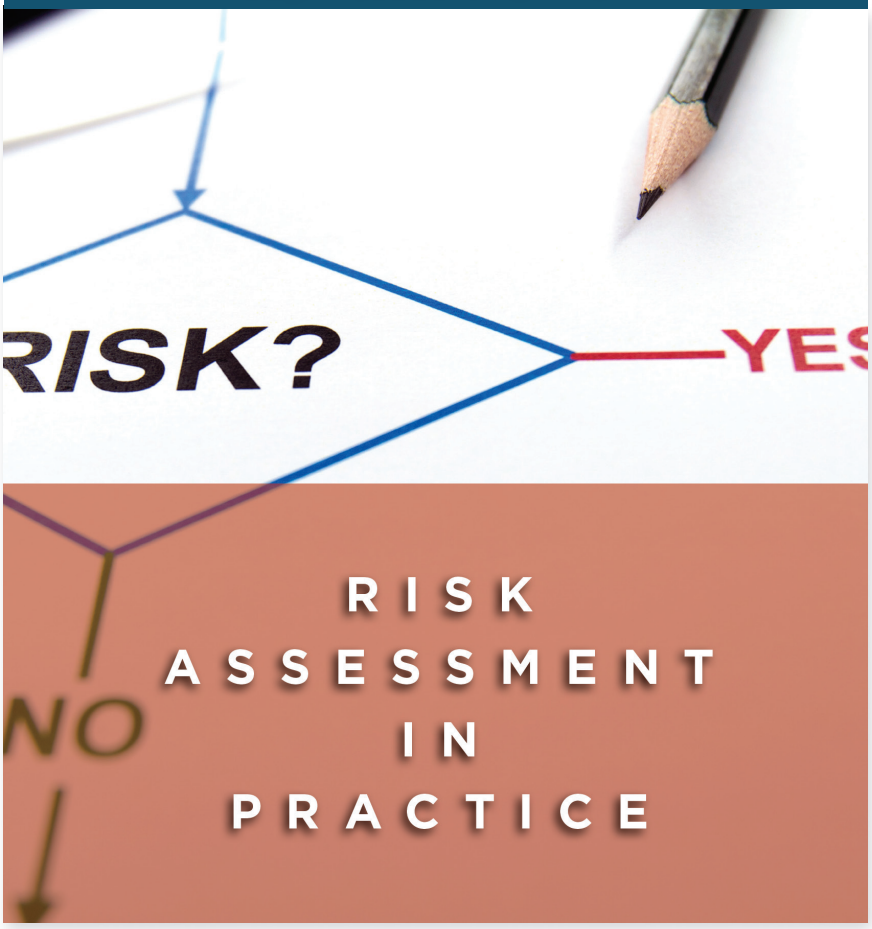
The Institute of Management Accountants (IMA)

The Institute of Internal Auditors (IIA)

COSO
Committee of Sponsoring Organizations
of the Treadway Commission

www.coso.org

Thought Leadership in ERM



RISK ASSESSMENT IN PRACTICE

Research Commissioned by

COSO

Committee of Sponsoring Organizations of the Treadway Commission

October 2012

Contents

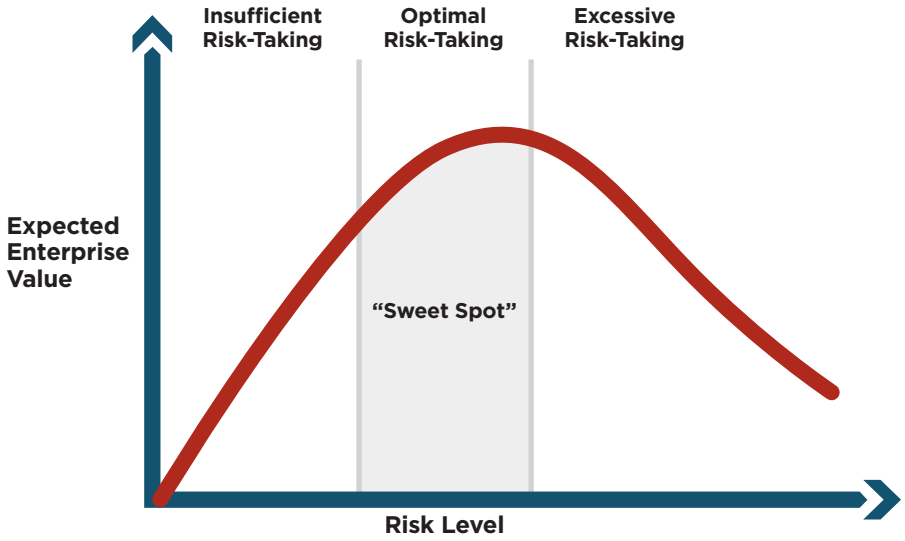
Introduction

Value is a function of risk and return. Every decision either increases, preserves, or erodes value. Given that risk is integral to the pursuit of value, strategic-minded enterprises do not strive to eliminate risk or even to minimize it, a perspective that represents a critical change from the traditional view of risk as something to avoid. Rather, these enterprises seek to manage risk exposures across all parts of their organizations so that, at any given time, they incur just enough of the right kinds of risk—no more, no less—to effectively pursue strategic goals. This is the "sweet spot," or optimal risk-taking zone, referred to in **exhibit 1**.

That's why risk assessment is important. It's the way in which enterprises get a handle on how significant each risk is to the achievement of their overall goals.

To accomplish this, enterprises require a risk assessment process that is practical, sustainable, and easy to understand. The process must proceed in a structured and disciplined fashion. It must be correctly sized to the enterprise's size, complexity, and geographic reach. While enterprise-wide risk management (ERM) is a relatively new discipline,[1] application techniques have been evolving over the last decade. The purpose of this paper is to provide leadership with an overview of risk assessment approaches and techniques that have emerged as the most useful and sustainable for decision-making. It represents another in a series of papers published by Committee of Sponsoring Organizations of the Treadway Commission (COSO) aimed at helping organizations move up the maturity curve in their ongoing development of a robust ERM process.

Exhibit 1: Optimal Risk-Taking



[1] Committee of Sponsoring Organizations of the Treadway Commission (COSO) *Enterprise Risk Management – Integrated Framework, 2004.*

The Risk Assessment Process

Within the COSO ERM framework,[2] risk assessment follows event identification and precedes risk response. Its purpose is to assess how big the risks are, both individually and collectively, in order to focus management's attention on the most important threats and opportunities, and to lay the groundwork for risk response. Risk assessment is all about measuring and prioritizing risks so that risk levels are managed within defined tolerance thresholds without being overcontrolled or forgoing desirable opportunities.

Events that may trigger risk assessment include the initial establishment of an ERM program, a periodic refresh, the start of a new project, a merger, acquisition, or divestiture, or a major restructuring. Some risks are dynamic and require continual ongoing monitoring and assessment, such as certain market and production risks. Other risks are more static and require reassessment on a periodic basis with ongoing monitoring triggering an alert to reassess sooner should circumstances change.

Exhibit 2: Assess Risks Process Flow Diagram

Identify risks. The risk (or event) identification process precedes risk assessment and produces a comprehensive list of risks (and often opportunities as well), organized by risk category (financial, operational, strategic, compliance) and sub-category (market, credit, liquidity, etc.) for business units, corporate functions, and capital projects. At this stage, a wide net is cast to understand the universe of risks making up the enterprise's risk profile. While each risk captured may be important to management at the function and business unit level, the list requires prioritization to focus senior management and board attention on key risks. This prioritization is accomplished by performing the risk assessment.

Develop assessment criteria. The first activity within the risk assessment process is to develop a common set of assessment criteria to be deployed across business units, corporate functions, and large capital projects. Risks and opportunities are typically assessed in terms of impact and likelihood. Many enterprises recognize the utility of evaluating risk along additional dimensions such as vulnerability and speed of onset.

Assess risks. Assessing risks consists of assigning values to each risk and opportunity using the defined criteria. This may be accomplished in two stages where an initial screening of the risks is performed using qualitative techniques followed by a more quantitative analysis of the most important risks.

Assess risk interactions. Risks do not exist in isolation. Enterprises have come to recognize the importance of managing risk interactions. Even seemingly insignificant risks on their own have the potential, as they interact with other events and conditions, to cause great damage or create significant opportunity. Therefore, enterprises are gravitating toward an integrated or holistic view of risks using techniques such as risk interaction matrices, bow-tie diagrams, and aggregated probability distributions.

Prioritize risks. Risk prioritization is the process of determining risk management priorities by comparing the level of risk against predetermined target risk levels and tolerance thresholds. Risk is viewed not just in terms of financial impact and probability, but also subjective criteria such as health and safety impact, reputational impact, vulnerability, and speed of onset.

Respond to risks. The results of the risk assessment process then serve as the primary input to risk responses whereby response options are examined (accept, reduce, share, or avoid), cost-benefit analyses performed, a response strategy formulated, and risk response plans developed.

Discussions of event identification and risk response are beyond the scope of this paper. For detailed treatment, refer to the COSO *Enterprise Risk Management – Integrated Framework* (2004).

[2] COSO, *Enterprise Risk Management – Integrated Framework (2004).*

Develop Assessment Criteria

Traditional risk analysis defines risk as a function of likelihood and impact. Indeed, these are important measures. However, unlikely events occur all too often, and many likely events don't come to pass. Worse, unlikely events often occur with astonishing speed. Likelihood and impact alone do not paint the whole picture.

To answer questions like how fast could the risk arise, how fast could you respond or recover, and how much downtime could you tolerate, you need to gauge vulnerability and speed of onset. By gauging how vulnerable you are to an event, you develop a picture of your needs. By gauging how quickly it could happen, you understand the need for agility and rapid adaptation.

Developing Assessment Scales

Some form of measurement of risk is necessary. Without a standard of comparison, it's simply not possible to compare and aggregate risks across the organization. Most organizations define scales for rating risks in terms of impact, likelihood, and other dimensions. These scales comprise rating levels and definitions that foster consistent interpretation and application by different constituencies. The more descriptive the scales, the more consistent their interpretation will be by users. The trick is to find the right balance between simplicity and comprehensiveness.

Scales should allow meaningful differentiation for ranking and prioritization purposes. Five point scales yield better dispersion than three point scales. Ten point scales imply precision typically unwarranted in qualitative analysis, and assessors may waste time trying to differentiate between a rating of six or seven when the difference is inconsequential and indefensible.

Illustrative scales are provided for impact, likelihood, vulnerability, and speed of onset. Every enterprise is different and the scales should be customized to fit the industry, size, complexity, and culture of the organization in question.

Impact

Impact (or consequence) refers to the extent to which a risk event might affect the enterprise. Impact assessment criteria may include financial, reputational, regulatory, health, safety, security, environmental, employee, customer, and operational impacts. Enterprises typically define impact using a combination of these types of impact considerations (as illustrated below), given that certain risks may impact the enterprise financially while other risks may have a greater impact to reputation or health and safety. When assigning an impact rating to a risk, assign the rating for the highest consequence anticipated. For example, if any one of the criteria for a rating of 5 is met, then the impact rating assigned is 5 even though other criteria may fall lower in the scale.

Some entities define impact scales for opportunities as well as risks.

Illustrative Impact Scale

Rating	Descriptor	Definition
5	Extreme	• Financial loss of $X million or more[3] • International long-term negative media coverage; game-changing loss of market share • Significant prosecution and fines, litigation including class actions, incarceration of leadership • Significant injuries or fatalities to employees or third parties, such as customers or vendors • Multiple senior leaders leave
4	Major	• Financial loss of $X million up to $X million • National long-term negative media coverage; significant loss of market share • Report to regulator requiring major project for corrective action • Limited in-patient care required for employees or third parties, such as customers or vendors • Some senior managers leave, high turnover of experienced staff, not perceived as employer of choice
3	Moderate	• Financial loss of $X million up to $X million • National short-term negative media coverage • Report of breach to regulator with immediate correction to be implemented • Out-patient medical treatment required for employees or third parties, such as customers or vendors • Widespread staff morale problems and high turnover
2	Minor	• Financial loss of $X million up to $X million • Local reputational damage • Reportable incident to regulator, no follow up • No or minor injuries to employees or third parties, such as customers or vendors • General staff morale problems and increase in turnover
1	Incidental	• Financial loss up to $X million • Local media attention quickly remedied • Not reportable to regulator • No injuries to employees or third parties, such as customers or vendors • Isolated staff dissatisfaction

[3] Financial impact is typically measured in terms of loss or gain, profitability or earnings, or capital.

Likelihood

Likelihood represents the possibility that a given event will occur. Likelihood can be expressed using qualitative terms (frequent, likely, possible, unlikely, rare), as a percent probability, or as a frequency. When using numerical values, whether a percentage or frequency, the relevant time period should be specified such as annual frequency or the more relative probability over the life of the project or asset. Sometimes enterprises describe likelihood in more personal and qualitative terms such as "event expected to occur several times over the course of a career" or "event not expected to occur over the course of a career."

Illustrative Likelihood Scale

Rating	Annual Frequency		Probability	
	Descriptor	Definition	Descriptor	Definition
5	Frequent	Up to once in 2 years or more	Almost certain	90% or greater chance of occurrence over life of asset or project
4	Likely	Once in 2 years up to once in 25 years	Likely	65% up to 90% chance of occurrence over life of asset or project
3	Possible	Once in 25 years up to once in 50 years	Possible	35% up to 65% chance of occurrence over life of asset or project
2	Unlikely	Once in 50 years up to once in 100 years	Unlikely	10% up to 35% chance of occurrence over life of asset or project
1	Rare	Once in 100 years or less	Rare	<10% chance of occurrence over life of asset or project

Vulnerability

Vulnerability refers to the susceptibility of the entity to a risk event in terms of criteria related to the entity's preparedness, agility, and adaptability. Vulnerability is related to impact and likelihood. The more vulnerable the entity is to the risk, the higher the impact will be should the event occur. If risk responses including controls are not in place and operating as designed, then the likelihood of an event increases. Assessing vulnerability allows entities to gauge how well they're managing risks.

Vulnerability assessment criteria may include capabilities to anticipate events such as scenario planning, real options,[4] capabilities to prevent events such as risk responses in place, capabilities to respond and adapt quickly as events unfold, and capabilities to withstand the event such as capital buffer and financial strength. Other factors can also be considered such as the rate of change in the industry or organization. There is no one-size-fits-all assessment scale. Every entity must define scales to meet its needs.

Illustrative Vulnerability Scale

Rating	Descriptor	Definition
5	Very High	• No scenario planning performed • Lack of enterprise level/process level capabilities to address risks • Responses not implemented • No contingency or crisis management plans in place
4	High	• Scenario planning for key strategic risks performed • Low enterprise level/process level capabilities to address risks • Responses partially implemented or not achieving control objectives • Some contingency or crisis management plans in place
3	Medium	• Stress testing and sensitivity analysis of scenarios performed • Medium enterprise level/process level capabilities to address risks • Responses implemented and achieving objectives most of the time • Most contingency and crisis management plans in place, limited rehearsals
2	Low	• Strategic options defined • Medium to high enterprise level/process level capabilities to address risks • Responses implemented and achieving objectives except under extreme conditions • Contingency and crisis management plans in place, some rehearsals
1	Very Low	• Real options deployed to maximize strategic flexibility • High enterprise level/process level capabilities to address risks • Redundant response mechanisms in place and regularly tested for critical risks • Contingency and crisis management plans in place and rehearsed regularly

[4] A real option is an option involving real, as opposed to financial, assets. Real assets include land, plant, and machinery. Real option analysis uses option pricing theory to value capital investment opportunities. An example of a real option would be the overbuilding of a facility to provide strategic flexibility in the event that demand were to increase faster than production capacity.

Speed of Onset (or Velocity)

Speed of onset refers to the time it takes for a risk event to manifest itself, or in other words, the time that elapses between the occurrence of an event and the point at which the company first feels its effects. Knowing the speed of onset is useful when developing risk response plans.

Illustrative Speed of Onset Scale

Rating	Descriptor	Definition
5	Very High	• Very rapid onset, little or no warning, instantaneous
4	High	• Onset occurs in a matter of days to a few weeks
3	Medium	• Onset occurs in a matter of a few months
2	Low	• Onset occurs in a matter of several months
1	Very Low	• Very slow onset, occurs over a year or more

Inherent and Residual Risk

When assessing risks, it's important to determine whether respondents will be asked to assess inherent risk, residual risk, or both. In *Enterprise Risk Management – Integrated Framework* (2004), COSO defines inherent risk as the risk to an entity in the absence of any actions management might take to alter either the risk's likelihood or impact. Residual risk is the risk remaining after management's response to the risk. Applying this concept is trickier than it might seem at first glance. Some entities interpret inherent risk to be level of risk assuming responses currently in place fail, and residual risk to be the level of risk assuming existing responses operate according to design. Other entities interpret inherent risk to be the current level of risk assuming existing responses operate according to design and residual to be the estimated risk after responses under consideration are put into place. The first approach is focused more on controls effectiveness of the current environment and the second approach on evaluating risk response options. There is no one right answer and either approach may be useful depending upon the purpose of the assessment and the nature of the risks being considered.

Assess Risks

Risk assessment is often performed as a two-stage process. An initial screening of the risks and opportunities is performed using qualitative techniques followed by a more quantitative treatment of the most important risks and opportunities lending themselves to quantification (not all risks are meaningfully quantifiable). Qualitative assessment consists of assessing each risk and opportunity according to descriptive scales as described in the previous section. Quantitative analysis requires numerical values for both impact and likelihood using data from a variety of sources.

The quality of the analysis depends on the accuracy and completeness of the numerical values and the validity of the models used. Model assumptions and uncertainty should be clearly communicated and evaluated using techniques such as sensitivity analysis.

Both qualitative and quantitative techniques have advantages and disadvantages. Most enterprises begin with qualitative assessments and develop quantitative capabilities over time as their decision-making needs dictate.

Measurement Techniques Comparison

Technique	Advantages	Disadvantages
Qualitative	• Is relatively quick and easy • Provides rich information beyond financial impact and likelihood such as vulnerability, speed of onset, and non-financial impacts such as health and safety and reputation • Is easily understood by a large number of employees who may not be trained in sophisticated quantification techniques	• Gives limited differentiation between levels of risk (i.e. very high, high, medium, and low) • Is imprecise – risk events that plot within the same risk level can represent substantially different amounts of risk • Cannot numerically aggregate or address risk interactions and correlations • Provides limited ability to perform cost-benefit analysis
Quantitative	• Allows numerical aggregation taking into account risk interactions when using an "at risk" measure such as Cash Flow at Risk • Permits cost-benefit analysis of risk response options • Enables risk-based capital allocation to business activities with optimal risk-return • Helps compute capital requirements to maintain solvency under extreme conditions	• Can be time-consuming and costly, especially at first during model development • Must choose units of measure such as dollars and annual frequency which may result in qualitative impacts being overlooked • Use of numbers may imply greater precision than the uncertainty of inputs warrants • Assumptions may not be apparent

For qualitative assessments, the most commonly used assessment techniques are interviews, cross-functional workshops, surveys, benchmarking, and scenario analysis. Quantitative techniques range from benchmarking and scenario analysis to generating forward looking point estimates (deterministic models) and then to generating forward looking distributions (probabilistic models). Some of the most powerful probabilistic models from an enterprise-wide standpoint include causal at-risk models used to estimate gross profit margins, cash flows, or earnings over a given time horizon at given confidence levels.

Analysis of Existing Data

Reviewing internal and external data can help individuals assess the likelihood and impact of a risk or opportunity. Sources of risk occurrence data include internal and external audit reports, public filings, insurance claims and internal loss event data including near misses, published reports by insurance companies, industry consortia, and research organizations. While relying on existing data provides objectivity, it's important to evaluate the relevance of the data under current and projected conditions. Adjustments may be warranted using expert judgment. In these cases, the rationale for adjustments must be clearly documented and communicated.

Interviews and Cross-Functional Workshops

Assessment can be conducted through one-on-one interviews or facilitated meetings. Cross-functional workshops are preferable to interviews or surveys for assessment purposes as they facilitate consideration of risk interactions and break down siloed thinking. Workshops improve understanding of a risk by bringing together diverse perspectives. For example, when considering a risk such as information security breach, workshop participants from information technology, legal and compliance, public relations, customer service, strategic planning, and operations management may each bring different information regarding causes, consequences, likelihoods, and risk interactions. Interviews may be more appropriate for senior management, board members, and senior line managers due to their time constraints. Workshops may not work well in cultures that suppress free sharing of information or divergent opinions.

Surveys

Surveys are useful for large, complex, and geographically distributed enterprises or where the culture suppresses open communication. Survey results can be downloaded into analytical tools allowing risks and opportunities to be viewed by level (board members, executives, managers), by business unit, by geography, or by risk category.

Surveys have drawbacks too. Response rates can be low. If the survey is anonymous, it may be difficult to identify information gaps. Quality of responses may be low if respondents give survey questions superficial attention in a rush to completion, or if they misunderstand something and don't have the opportunity to ask clarifying questions. But perhaps most of all, respondents don't benefit from cross-functional discussions which enhance people's risk awareness and understanding, provide context and information to support the risk ratings, and analyze risk interactions across silos. For these reasons, surveys should *not* be considered a substitute for workshops and other techniques for in-depth analysis of key risks.

Benchmarking

Benchmarking is a collaborative process among a group of entities. Benchmarking focuses on specific events or processes, compares measures and results using common metrics, and identifies improvement opportunities. Data on events, processes, and measures are developed to compare performance. Some companies use benchmarking to assess the likelihood and impact of potential events across an industry. Benchmarking data are available from research organizations, industry consortia, insurance companies and rating agencies, government agencies, and regulatory and supervisory bodies. For example, an oil field services company might benchmark its safety risk using measures such as lost time injuries using data for similar companies available from the Bureau of Labor Statistics, the Occupational Health and Safety Administration (OSHA), the American Petroleum Institute (API), or others.

Scenario Analysis

Scenario analysis has long been recognized for its usefulness in strategic planning. It is also useful for assessing risks and tying them back to strategic objectives. It entails defining one or more risk scenarios, detailing the key assumptions (conditions or drivers) that determine the severity of impact, and estimating the impact on a key objective. In the example below, management wanted to understand how earnings could be negatively impacted.

Six scenarios impacting earnings were identified, causal factors (such as price or volume changes or state of the economy) determined, detailed assumptions calibrated, and the earnings impact estimated. Scenarios can be developed jointly by risk owners and ERM personnel and built out and validated with specialists from various functions and management.

Scenario Analysis

Scenario Description	Detailed Assumptions	EBIT* Impact ($MM)
1) Currency changes impact competitive landscape	• 15% volume decrease • 20% price decrease • Sustained for 9 months • Recovery takes additional 9 months	- $500
2) Natural gas prices increase	• $5/MM Btu increase • Sustained for 12 months • No ability to pass through increase	- $150
3) Crude oil prices increase	• 100% increase • Sustained for 3 months • Pass through 25% of cost increase	- $15
4) Technology shift	• 15% volume decrease/year • 15% price decrease/year • $2MM less in R&D expenditures	- $275
5) Competitive pressure	• 10% price decrease • Sustained for 24 months	- $200
6) Supply chain disruption	• 10% volume decrease • Sustained for 6 months	- $175

* Earnings before interest and taxes.

Source: Frederick Funston and Stephen Wagner, *Surviving and Thriving in Uncertainty* (Hoboken, NJ: John Wiley & Sons, Inc., 2010), 69.

Causal At-Risk Models

Gross Margin at Risk (GMaR), Cash Flow at Risk (CFaR), and Earnings at Risk (EaR) are metrics built on causal models where specific risk factors drive future uncertainty of key cash flow or earnings components. Each risk factor can be modeled in detail and incorporated into the overall model. Using a causal at-risk model can provide insight into how historical relationships might become uncoupled and deviate meaningfully from expectations. Armed with the knowledge of how each risk factor could vary in the future and impact cash flow or earnings, risk can be better measured and managed. It is the added insight of the risk factors driving uncertainty that makes causal models a step up from simply extrapolating past relationships in a *pro forma* approach.

In reality, both *pro forma* models built around historical ratios and causal at-risk models can be helpful and should be seen as complementary views of an uncertain future. Regardless of the type of model, the confidence placed on estimates of levels of risk and assumptions made in the analysis should be clearly stated.

Model inputs may be derived from past records, relevant experience, relevant published literature, market research, public consultation, experiments and prototypes, and economic, engineering or other models. Where historical data are not available, not relevant, or incomplete, expert elicitation may be used. Expert elicitation is most commonly used to estimate reasonable probabilities especially for low likelihood, high impact events. Experts are valuable sources of information and knowledge. But experts also bring biases. Fortunately, a large body of knowledge exists with regard to heuristics and biases and ways to address them. For example, see COSO's recently issued thought paper, *Enhancing Board Oversight: Avoiding Judgment Traps and Biases* (March 2012).

Assess Risk Interactions

ERM enables an integrated and holistic view of risks. The key here is that the whole does not equal the sum of the parts. To understand portfolio risk, one must understand the risks of the individual elements plus their interactions due to the presence of natural hedges and mutually amplifying risks. Understanding risk interactions and then managing them requires breaking down silos.

A simple way to consider risk interactions is to group related risks into a broad risk area (such as grouping risks related to sourcing, distribution channels, vendor concentrations, etc. into supply chain risk) and then assigning ownership and oversight for the risk area. Three explicit ways to capture risk interactions increasing in level of complexity and richness of information are risk interaction maps, correlation matrices, and bow-tie diagrams.

Risk Interaction Map

A risk interaction map is the simplest form of graphical representation in which the same list of risks form the x and y axes. Risk interactions are then indicated by an X or other qualitative indicator.

Exhibit 3: Illustrative Risk Interaction Map

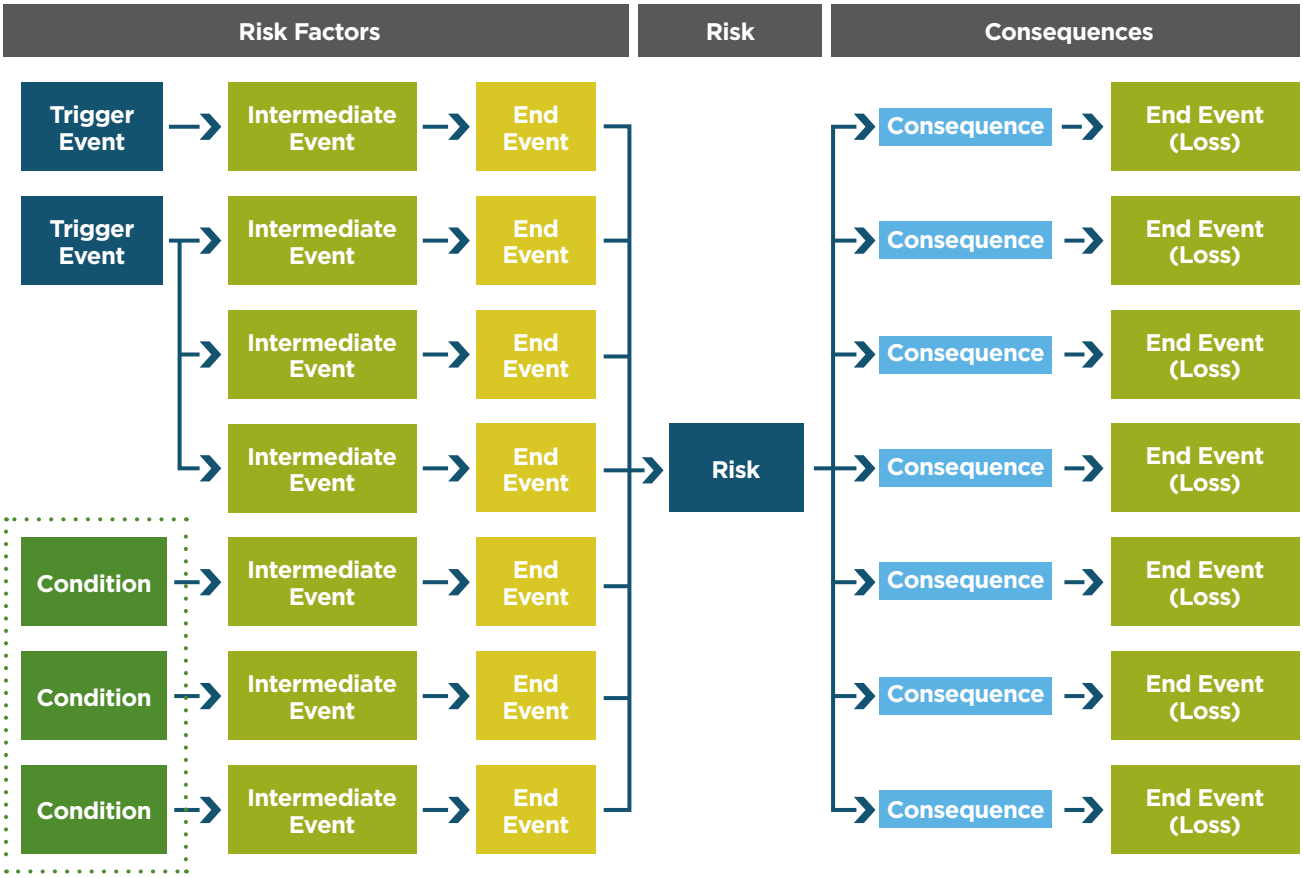
Risk	Supply Chain Disruption	Customer Preference Shift	Copper Price Increase >25%	Work Stoppage >1 Week	Economic Downturn	Supplier Consolidation	Local Competitor Enters Market	New Substitutes Available	Cost of Capital Increase >5%	Tighter Emission Standards	FCPA Violation	Exchange Rate Fluctuations
Supply Chain Disruption			X	X	X	X	X					
Customer Preference Shift					X		X	X		X		X
Copper Price Increase >25%	X				X	X						X
Work Stoppage >1 Week	X				X	X					X	
Economic Downturn	X	X	X	X		X	X	X	X		X	X
Supplier Consolidation	X		X	X	X				X			
Local Competitor Enters Market	X	X			X							X
New Substitutes Available		X			X					X		
Cost of Capital Increase >5%					X	X						X
Tighter Emission Standards		X						X				
FCPA Violation				X	X							
Exchange Rate Fluctuations		X	X		X		X		X			

Where historical data are available, risk interactions can be expressed quantitatively using a correlation matrix. This is an especially useful technique to apply within a risk category such as market risk. Difficulties in determining correlations for risks include the possibility that past causal relationships will not be indicative of future relationships, lack of historical data, differences in time frames (short-, medium-, and long-term), and the large numbers of risks required for an enterprise-wide assessment.

Developing the Full Picture—Fault Trees, Event Trees, and Bow-Tie Diagrams

Diagrams that break a complex risk occurrence into its component parts showing the chains of events that could lead to or result from the occurrence can be indispensable for identification and assessment of risk responses and key risk indicators. The diagrams can be qualitative or serve as the basis for quantitative models. Three commonly used diagrams are fault trees, event trees, and bow-ties. Fault trees are used for analyzing events or combinations of events that might lead to a hazard or an event. Event trees are used for modeling sequences of events arising from a single risk occurrence. A bow-tie diagram combines a fault tree and an event tree and takes its name from its shape. Probabilistic models built on bow-tie diagrams are versatile for quantifying inherent and residual risk levels and performing what-if, scenario, and sensitivity analyses.

Exhibit 4: Bow-Tie Diagram



Note: The terms fault tree, event tree, and bow-tie diagram are sometimes used interchangeably.

Prioritize Risks

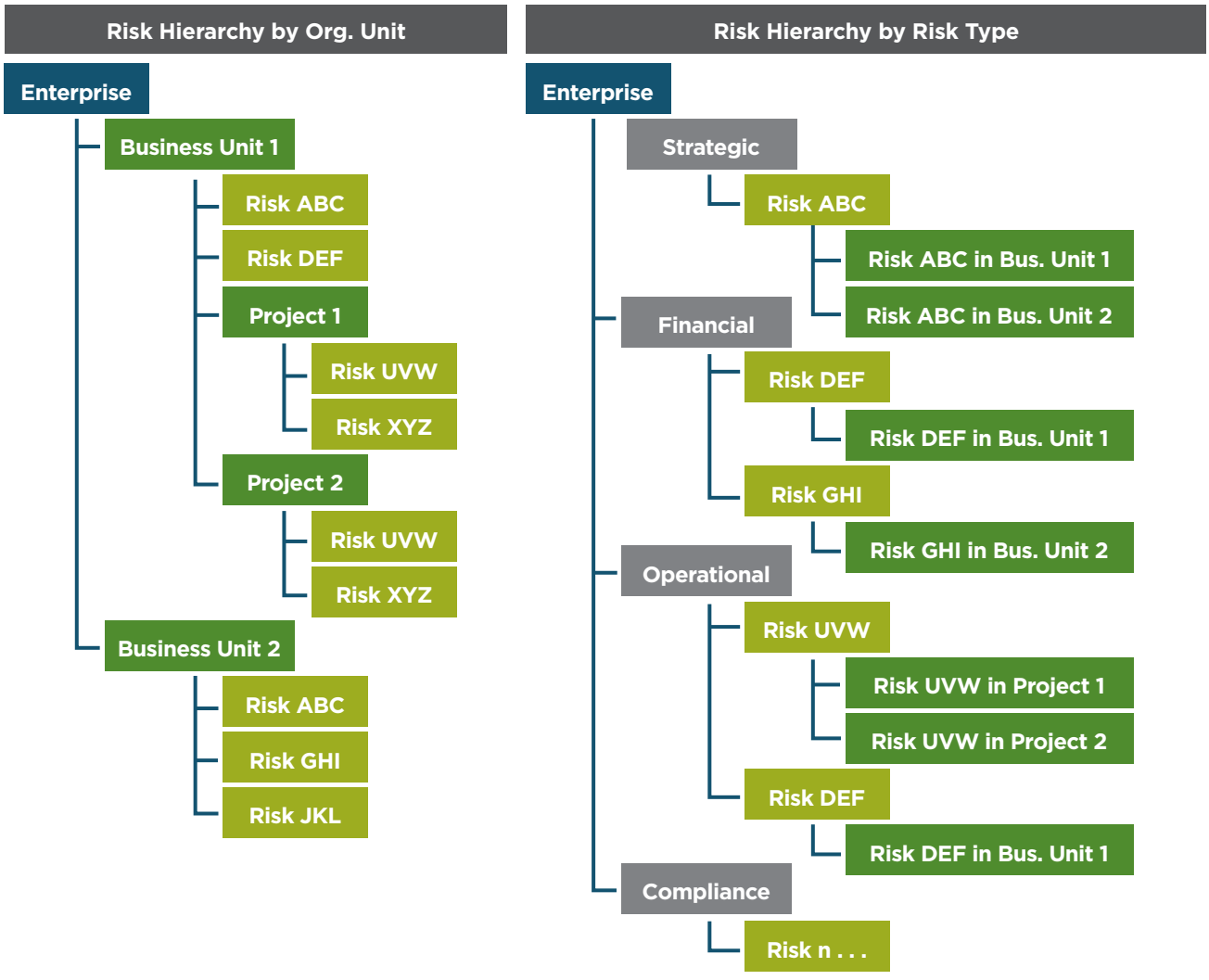
Once the risks have been assessed and their interactions documented, it's time to view the risks as a comprehensive portfolio to enable the next step – prioritizing for risk response and reporting to different stakeholders. The term risk profile represents the entire portfolio of risks facing the enterprise. Some entities represent this portfolio as a hierarchy, some as a collection of risks plotted on a heat map. Entities with more mature ERM programs and quantitative capabilities may aggregate individual risk distributions into a cumulative loss probability distribution and refer to that as the risk profile.

Similar to assessing risks, ranking and prioritizing is often done in a two-step process. First, the risks are ranked according to one, two, or more criteria such as impact rating multiplied by likelihood rating or impact multiplied by vulnerability. Second, the ranked risk order is reviewed in light of additional considerations such as impact alone, speed of onset, or the size of the gap between current and desired risk level (risk tolerance threshold). If the initial ranking is done by multiplying financial loss by likelihood, then the final prioritization should take qualitative factors into consideration.

Hierarchies and Rolling Up and Drilling Down

The simplest way to aggregate risks is to organize them according to a hierarchy. This is often done in risk management systems where risks can be organized by organizational unit, risk type, geography, or strategic objective. The better systems allow users to roll up and drill down for analysis and reporting. This provides a complete listing of the assessed risks but does not help with prioritizing.

Exhibit 5: Risk Hierarchies



Risk Maps

Another simple way to view the portfolio is to create a risk map, often called a heat map. These are usually two-dimensional representations of impact plotted against likelihood. They can also depict other relationships such as impact versus vulnerability. For even richer information, the size of the data points can reflect a third variable such as speed of onset or the degree of uncertainty in the estimates.

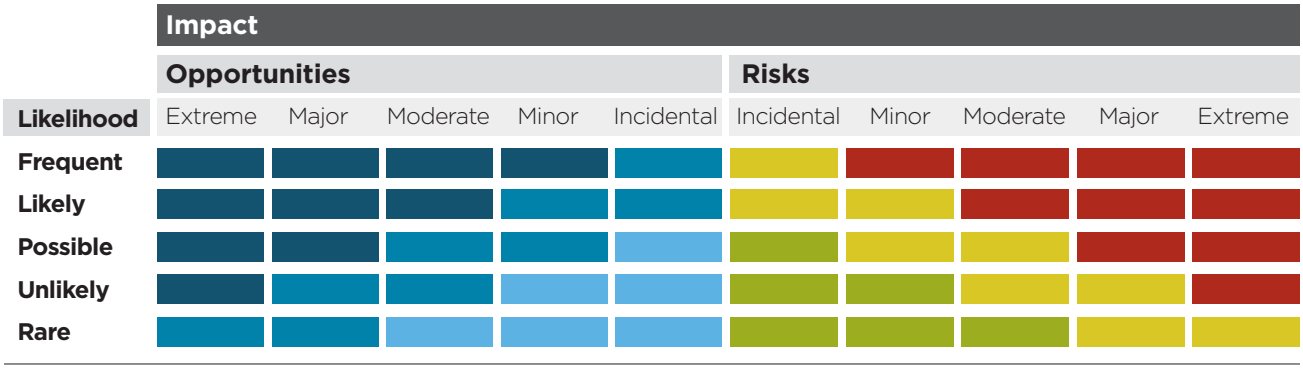
The most common way to prioritize risks is by designating a risk level for each area of the graph such as very high, high, medium, or low, where the higher the combined impact and likelihood ratings, the higher the overall risk level. The boundaries between levels vary from entity to entity depending on risk appetite. For example, an entity with a greater risk appetite will have boundaries between risk levels shifted toward the upper right, and an entity with greater risk aversion will have boundaries between risk levels shifted toward the bottom left. Also, some entities adopt asymmetric boundaries placing a somewhat greater emphasis on impact than on likelihood. For example, a risk having an impact rating of moderate and likelihood rating of frequent has an assigned risk level of high, whereas a risk having an impact rating of extreme and a likelihood rating of possible has an assigned risk level of very high.

After plotting on the heat map, risks are then ranked from highest to lowest in terms of risk level. These rankings may then be adjusted based on other considerations such as vulnerability, speed of onset, or detailed knowledge of the nature of the impact. For example, within a group of risks having a designation of very high, those risks having extreme health and safety or reputational impacts may be prioritized over risks having extreme financial impacts but lesser health and safety or reputational impacts.

When using numerical ratings in a qualitative environment, it's important to remember that the numbers are labels and not suitable for mathematical manipulation although some entities do multiply the ratings, such as for impact and likelihood, to develop a preliminary ranking.

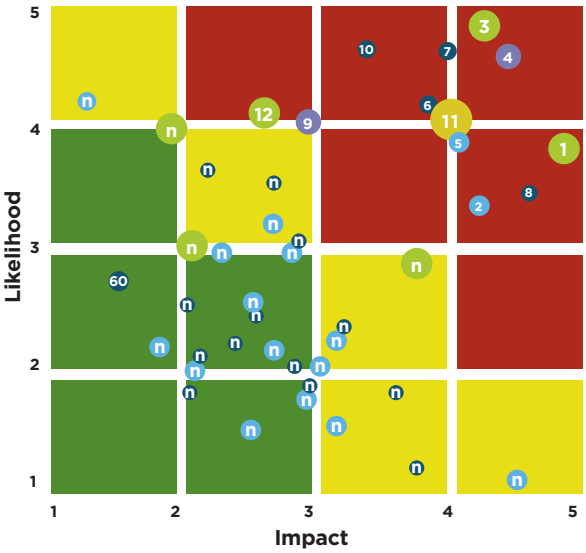
Where entities have defined impact scales for both opportunities and risks, they may plot risks on a map such as that illustrated in **exhibit 6.** This allows a direct comparison of the highest rated opportunities and risks for consideration and prioritization.

Exhibit 6: Illustrative Combined Risk and Opportunity Map



Consider the following example: A company identified 60 risks to include in its risk universe. It then determined appropriate assessors. It used a combination of interviews, workshops, and a survey to perform an initial qualitative assessment of impact, likelihood, vulnerability, and speed of onset criteria. Risk interactions were evaluated for the highest risks and the assessments were refined. Risks were plotted on a heat map to perform an initial prioritization. Twelve risks plotted in the 'Very High' risk level designated as red in the below heat map. These risks were designated 'key' risks meaning that they will be reported to and monitored by executive leadership and the board of directors.

Exhibit 7: Illustrative Heat Map



Dots represent risk #1 - #n
Dot size reflects speed of onset:
Very Low Low Medium High Very High

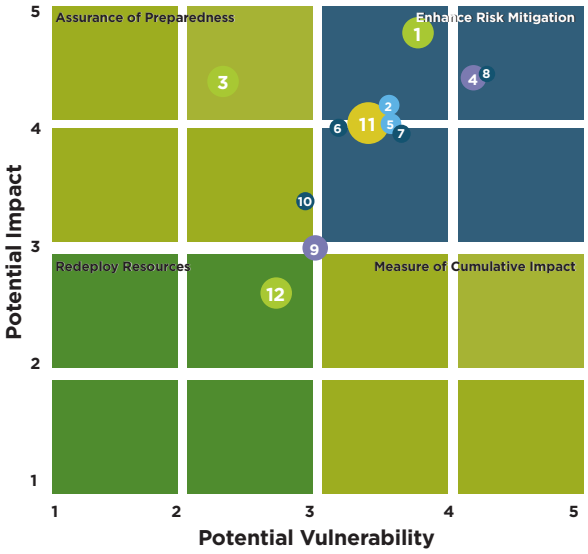
ID	Risk	I	L	V	S
1	Supply chain disruption	4.8	3.7	3.8	4
2	Customer preference shift	4.1	3.3	3.5	2
3	Copper price rise >10%	4.3	4.7	2.3	4
4	Work stoppage > 1 week	4.4	4.5	4.1	3
5	Economic downturn	4.0	3.7	3.5	2
6	Supplier consolidation	3.8	4.2	3.2	1
7	Local competitors enter	3.9	4.5	3.6	1
8	New substitutes available	4.5	3.6	4.2	1
9	Cost of capital rise >5%	2.9	4.0	2.9	3
10	Tighter emission standards	3.4	4.6	2.9	1
11	FCPA violation	4.0	4.0	3.3	5
12	Exchange rate fluctuations	2.7	4.1	2.7	4
n	. . .	...	...	...	...
60	Impairment of assets	1.6	2.7	1.6	1

I = Impact L = Likelihood V = Vulnerability S = Speed of onset

Another useful plot for prioritizing is the MARCI chart (for Mitigate, Assure, Redeploy, and Cumulative Impact), depicted in **exhibit 8.** 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. This is particularly useful when the primary purpose of the prioritization exercise is for risk response: risks plotting the farthest in the upper right quadrant represent the highest impact and vulnerability and would benefit the most from additional management effectiveness in managing the risks.

Continuing our example, the 12 risks rated 'Very High' were plotted on a MARCI chart to further refine the prioritization and to perform a preliminary evaluation of the type of appropriate risk response. In this view, the company can see how its hedging program reduces its vulnerability to copper price increases (risk 3), and evaluate its previous decision to not hedge against currency fluctuations (risk 12). Leadership can also see that supply chain disruption (risk 1) can occur with little warning and severe impact. This and the other risks in its quadrant require action to reduce vulnerability. The executive leadership team and board members will pay particular attention to management's actions to respond to these risks. The top 12 risks were tagged for further quantification and probabilistic modeling.

Exhibit 8: Illustrative MARCI Chart



ID	Risk	I	L	V	S
1	Supply chain disruption	4.8	3.7	3.8	4
2	Customer preference shift	4.1	3.3	3.5	2
3	Copper price rise >10%	4.3	4.7	2.3	4
4	Work stoppage > 1 week	4.4	4.5	4.1	3
5	Economic downturn	4.0	3.7	3.5	2
6	Supplier consolidation	3.8	4.2	3.2	1
7	Local competitors enter	3.9	4.5	3.6	1
8	New substitutes available	4.5	3.6	4.2	1
9	Cost of capital rise >5%	2.9	4.0	2.9	3
10	Tighter emission standards	3.4	4.6	2.9	1
11	FCPA violation	4.0	4.0	3.3	5
12	Exchange rate fluctuations	2.7	4.1	2.7	4

I = Impact L = Likelihood V = Vulnerability S = Speed of onset

Dots represent risk #1 - #n
Dot size reflects speed of onset:
Very Low Low Medium High Very High

Aggregating in a Quantitative Environment

In situations where key risks have been quantified using a common measure such as financial loss or an at-risk measure, it is possible to aggregate the individual probability distributions into a single distribution reflecting correlations and portfolio effects. Measures that are gaining traction for this purpose are gross margin at risk, cash flow at risk, and earnings at risk.

The primary applications for a single at-risk measure presenting an aggregate view of risk (over a given time horizon at a specified confidence level) are capital allocation, solvency assessments, and measures of risk utilization and capacity relative to risk appetite. Risk aggregation models are extremely variable from one enterprise to another, even within the financial services industry.

Putting It into Practice

To be effective and sustainable, the risk assessment process needs to be simple, practical, and easy to understand. Success depends upon executive commitment and resources. The process must be performed by people with the right skills supported by technology that is correctly sized for the task at hand.

A corporate-level ERM function is indispensable for defining common standards, coordinating assessments across business units, and facilitating analysis of risk interactions. The central ERM function must be staffed by people with the necessary facilitation, project management, and analytical skills along with knowledge of risk management leading practices. The ERM function must be augmented by people in line positions closest to the risks. The risk owners ultimately bear responsibility for the assessed levels of risk and defining and implementing risk response plans to bring risks within tolerance. This hybrid top-down and bottom-up approach brings the best of both worlds achieving consistency and comprehensive coverage while embedding accountability and leveraging expertise of the people in the organization closest to the risks.

People aren't enough. To be efficient, they must be supported by the right technology. Many entities begin their ERM journey in a simple spreadsheet environment. This can be practical in the early stages of development as both risk owners and senior leadership ascertain their analytical and reporting requirements. Later years can be quite challenging without automation, especially if the entity is large, complex, and geographically distributed.

Fortunately, a large number of software vendors have entered the ERM space, and each year brings new innovations and improved offerings. Systems exist at an array of price points with analytical capabilities increasing with price. Most systems will quickly pay for themselves in saved labor costs.

Finally, risk assessment cannot exist in a vacuum or it becomes a fruitless exercise. COSO's *Enterprise Risk Management – Integrated Framework* emphasizes the need to assess and oversee risks from a holistic perspective. The process must sit within a larger framework that uses the information gleaned to make decisions about risk responses and monitoring, and feeds information back into the strategic planning process. The ERM function must be empowered to monitor and oversee implementation of risk responses. If participants don't see that their contributions and hard work during risk assessment lead to concrete actions that make a real difference, they will become cynical and withdraw from the process in future years.

You'll know you're doing risk assessment right when leaders at every level use the information to make decisions regarding value.

About COSO

Originally formed in 1985, COSO is a joint initiative of five private sector organizations and is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management (ERM), internal control, and fraud deterrence. COSO's supporting organizations are the Institute of Internal Auditors (IIA), the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), and the Institute of Management Accountants (IMA).

About the Authors

"Deloitte" is the brand under which tens of thousands of dedicated professionals in independent firms throughout the world collaborate to provide audit, consulting, financial advisory, risk management and tax services to selected clients. These firms are members of Deloitte Touche Tohmatsu Limited (DTTL), a UK private company limited by guarantee. In the United States, Deloitte LLP is the member firm of DTTL. Deloitte & Touche LLP, a subsidiary of Deloitte LLP, provides internal control and enterprise risk services in the United States. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

The contributing authors from Deloitte & Touche LLP are Dr. Patchin Curtis, Director, and Mark Carey, Partner.

Thought Leadership in ERM

COSO

Committee of Sponsoring Organizations
of the Treadway Commission

www.coso.org

RISK ASSESSMENT IN PRACTICE

COSO

Committee of Sponsoring Organizations of the Treadway Commission

www.coso.org