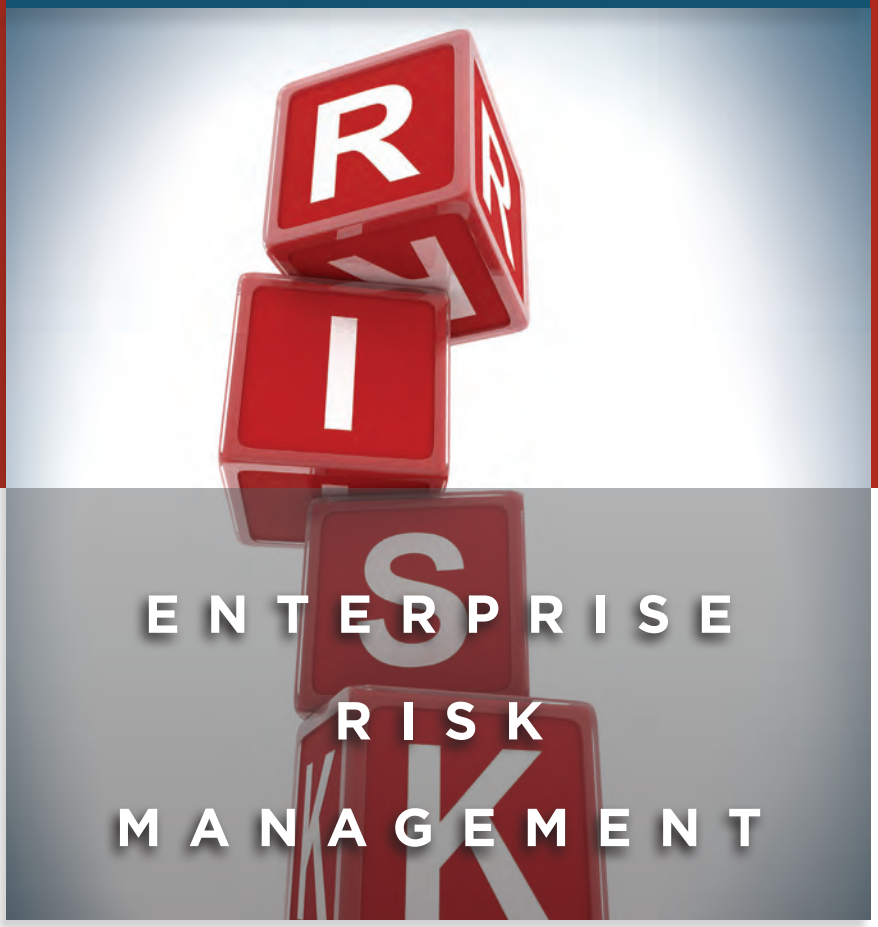
COSO

Committee of Sponsoring Organizations of the Treadway Commission

Thought Leadership in ERM



Understanding and Communicating Risk Appetite

By

Dr. Larry Rittenberg and **Frank Martens**

Authors

Dr. Larry Rittenberg
Ernst & Young Professor of Accounting
University of Wisconsin-Madison School of Business

Frank Martens
Director, PricewaterhouseCoopers (PwC)

COSO Board Members

Preface

This project was commissioned by 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)

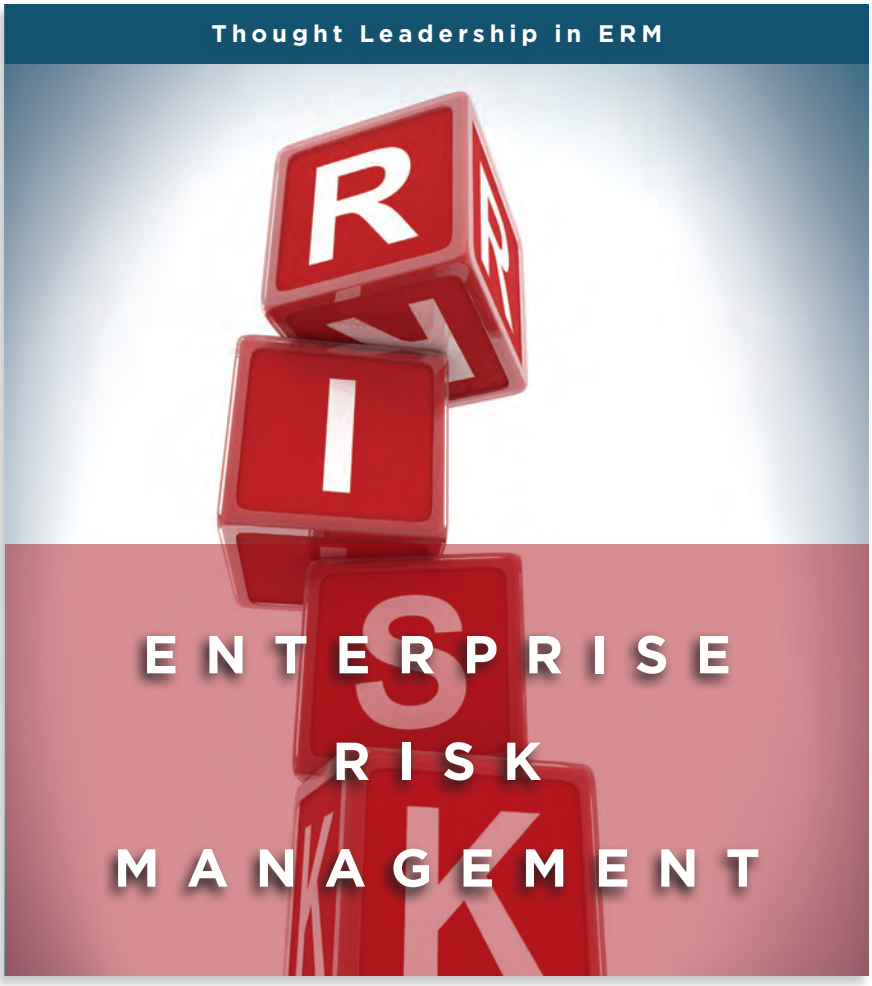
The Institute of Management Accountants (IMA)

The Institute of Internal Auditors (IIA)

Committee of Sponsoring Organizations
of the Treadway Commission

www.coso.org

Thought Leadership in ERM



ENTERPRISE RISK MANAGEMENT

Understanding and Communicating Risk Appetite

Research Commissioned by

COSO

Committee of Sponsoring Organizations of the Treadway Commission

January 2012

1 2 3 4 5 6 7 8 9 0 PIP 198765432

www.coso.org

Content Outline

Executive Summary

Organizations encounter risk every day as they pursue their objectives. In conducting appropriate oversight, management and the board must deal with a fundamental question: How much risk is acceptable in pursuing these objectives? Added to this, regulators and other oversight bodies are calling for better descriptions of organizations' risk management processes, including oversight by the board.

This thought leadership document is one of a series of papers, sponsored by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), to help organizations implement enterprise risk management (ERM). The COSO document *Enterprise Risk Management — Integrated Framework* explicitly states that organizations must embrace risk in pursuing their goals. The key is to understand how much risk they are willing to accept. Further, how should an organization decide how much risk it is willing to accept? To what extent should the risks accepted mirror stakeholders' objectives and attitudes towards risk? How does an organization ensure that its units are operating within bounds that represent the organization's appetite for specific kinds of risk?

> Risk appetite is the amount of risk, on a broad level, an organization is willing to accept in pursuit of value. Each organization pursues various objectives to add value and should broadly understand the risk it is willing to undertake in doing so.

These questions are embodied in the notion of an entity's "risk appetite." The objective of this paper is to help an organization — its senior management, board, and key operating personnel — to develop and communicate a clear understanding of its risk appetite, both to determine which objectives to pursue and to manage those objectives within the organization's appetite for risk.

Many organizations view risk appetite as the subject of interesting theoretical discussions about risk and risk management, but do not effectively integrate the concept into their strategic planning or day-to-day decision making. We believe that discussions about applying risk appetite go well beyond theory, and that when properly communicated, risk appetite provides a boundary around the amount of risk an organization might pursue. An organization with an aggressive appetite for risk might set aggressive goals, while an organization that is risk-averse, with a low appetite for risk, might set conservative goals.

Similarly, when a board considers a strategy, it should determine whether that strategy aligns with the organization's risk appetite. When properly communicated, risk appetite guides management in setting goals and making decisions so that the organization is more likely to achieve its goals and sustain its operations.

Enterprise Risk Management and Decision Making

ERM is not isolated from strategy, planning, or day-to-day decision making. Nor is it about compliance. ERM is part of an organization's culture, just as making decisions to attain objectives is part of an organization's culture.

To fully embed ERM in an organization, decision makers must know how much risk is acceptable as they consider ways of accomplishing objectives, both for their organization and for their individual operations (division, department, etc.). For example, one CEO recently reported that his organization needed to increase its risk appetite amid expectations that key measures of its profitability would fall or stagnate. A financial organization with a lower risk appetite might choose to avoid opportunities that are more risky, but offer greater returns. Finally, another organization with a high risk appetite might decide to procure natural resources from a volatile country where the total investment could be wiped out at the whim of the political leader. The rewards may be high, but so too may the risks. Organizations make decisions like these all the time. Only if they clearly think about their risk appetite can they balance risks and opportunities.

An organization must consider its risk appetite at the same time it decides which goals or operational tactics to pursue. To determine risk appetite, management, with board review and concurrence, should take three steps:

1. Develop risk appetite
2. Communicate risk appetite
3. Monitor and update risk appetite

These three steps are discussed briefly below, and in detail in the body of this paper.

Develop Risk Appetite

Developing risk appetite does not mean the organization shuns risk as part of its strategic initiatives. Quite the opposite. Just as organizations set different objectives, they will develop different risk appetites. There is no standard or universal risk appetite statement that applies to all organizations, nor is there a "right" risk appetite. Rather, management and the board must make choices in setting risk appetite, understanding the trade-offs involved in having higher or lower risk appetites.

Communicate Risk Appetite

Several common approaches are used to communicate risk appetite. The first is to create an overall risk appetite statement that is broad enough yet descriptive enough for organizational units to manage their risks consistently within it. The second is to communicate risk appetite for each major class of organizational objectives. The third is to communicate risk appetite for different categories of risk.

Monitor and Update Risk Appetite

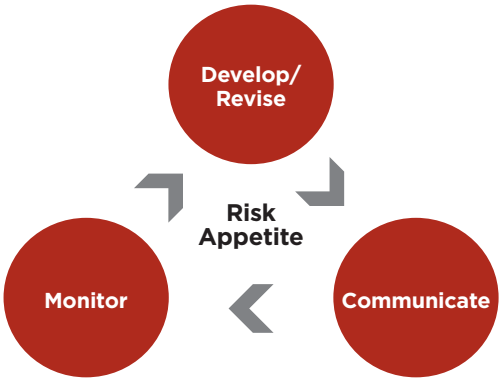
Once risk appetite is communicated, management, with board support, needs to revisit and reinforce it. Risk appetite cannot be set once and then left alone. Rather, it should be reviewed in relation to how the organization operates, especially if the entity's business model changes. Management should monitor activities for consistency with risk appetite through a combination of ongoing monitoring and separate evaluations. Internal auditing can support management in this monitoring. In addition, organizations, when monitoring risk appetite, should focus on creating a culture that is risk-aware and that has organizational goals consistent with the board's.

Can It Be Done?

This is a common question. Its tone implies two things: (1) articulating risk appetite is too difficult, and (2) risk is considered when management sets strategies, and to further communicate risk appetite is an exercise that simply adds overhead and does not contribute to organizational growth.

Recent world events — involving governments, businesses, not-for-profit organizations, and the recent financial crisis — clearly show that having a communicated risk appetite built into organizational activities could have preserved a considerable amount of capital. We all know the costs of failing to manage risk. Examples include the cost to companies and travellers when air travel closed down after a volcanic eruption in 2010 in Iceland; the cost of the financial crisis to U.S. taxpayers, stockholders, and debtholders; and the social cost of government budgets in Greece, Spain, Ireland, and Portugal.

Perhaps organizations are still tied to the old-school thinking that "it will not happen here." The easy rebuttal is that it has happened somewhere, so all organizations should work to manage their risks within their risk appetite. Rather than asking "Can it be done?" let's say "Let's get it done." Determining risk appetite is an element of good governance that managements and boards owe to stakeholders.



Overview

Risk Appetite Is an Integral Part of Enterprise Risk Management

COSO's Enterprise Risk Management — Integrated Framework defines risk appetite as follows:

> *The amount of risk, on a broad level, an entity is willing to accept in pursuit of value. It reflects the entity's risk management philosophy, and in turn influences the entity's culture and operating style. … Risk appetite guides resource allocation. … Risk appetite [assists the organization] in aligning the organization, people, and processes in [designing the] infrastructure necessary to effectively respond to and monitor risks.*[1]

This definition raises some important points. Risk appetite

- is strategic and is related to the pursuit of organizational objectives;
- forms an integral part of corporate governance;
- guides the allocation of resources;
- guides an organization's infrastructure, supporting its activities related to recognizing, assessing, responding to, and monitoring risks in pursuit of organizational objectives;
- influences the organization's attitudes towards risk;
- is multi-dimensional, including when applied to the pursuit of value in the short term and the longer term of the strategic planning cycle; and
- requires effective monitoring of the risk itself and of the organization's continuing risk appetite.

As an organization decides on its objectives and its approach to achieving strategic goals, it should consider the risks involved, and its appetite for such risks, as a basis for making those important decisions. Those in governance roles should explicitly understand risk appetite when defining and pursuing objectives, formulating strategy, and allocating resources. The board should also consider risk appetite when it approves management actions, especially budgets, strategic plans, and new products, services, or markets (in other words, a business case).

In working towards their objectives, organizations choose strategies and develop metrics to show them how close they are to meeting those objectives. Managers are motivated to achieve the objectives through reward and compensation programs. The strategy is then operationalized by decisions made throughout the organization. Decisions are made to achieve the objectives (increase market share, profitability, etc.). But achieving objectives also depends on identifying risk and determining whether the risks are within the organization's risk appetite.

[1] COSO, *Enterprise Risk Management — Integrated Framework*, p. 19.

Considerations Affecting Risk Appetite

Risk appetite is not developed in isolation from other factors. An organization should consider its capacity to take on extra risk in seeking its objectives. It should also consider its existing risk profile, not as a determinant of risk appetite but as an indication of the risks it currently addresses. An overview of the considerations affecting risk appetite is shown in Exhibit 1.

Exhibit 1

Overview of Considerations Affecting Risk Appetite

There may be other factors to consider as well. Some organizations may gauge how quickly their competitive environment is changing. A telecommunications company, for example, must anticipate how technology and user preferences will affect product development, making a relevant time frame important.

As an example of high risk appetite, a defense contractor dealing in trucks decided that the risk of being behind in technology was so large that it essentially "bet the company" on developing a vehicle appropriate for the types of wars occurring around the world. If the contractor had been unsuccessful in procuring a new government order, it would have been out of business. The risk appetite was high, but it was understood by all involved in the process. However, the board was well aware of the risks, having debated the issue extensively in board meetings, and it concurred with management's decision (an acknowledgement of risk appetite and the linkage of risk appetite and strategy). The investing public was also aware because the nature of the risks had been communicated (and the stock dropped to historic lows). What is notable is that the risk was carefully debated and the company was going to succeed or die — as opposed to almost certainly dying (slowly) if it did not take on risk through an aggressive strategy.

The point is that risk and strategy are intertwined. One does not exist without the other, and they must be considered together. That consideration takes place throughout the execution of the strategy, and it is most important when strategy is being formulated with due regard for risk appetite.

An organization has a number of goals and objectives it can pursue. Ultimately, it will decide on those that best meet stakeholder preferences for growth, return, safety, sustainability and its willingness to accept risk. The objectives, in turn, may be pursued using a number of alternative strategies. As shown in Exhibit 2, the articulation of a risk appetite provides bounds on the choice of strategies and the operational decisions that are made to pursue those objectives.

One major problem that led to the current financial crisis was that although objectives had been created, there was no articulation of risk appetite or identification of those responsible when risks were incurred.

Exhibit 2

Interrelationship of Strategy, Management Decisions, and Risk Appetite

Steps in Adopting Risk Appetite

Each organization must determine its own risk appetite; there is no single universal risk appetite. But how does an organization get to the point of having a risk appetite statement that can be communicated through the organization? And how does risk appetite stay relevant over time?

To effectively adopt risk appetite, an organization must take three key steps:

1. Management develops, with board review and concurrence, a view of the organization's overall risk appetite.
2. This view of risk appetite is translated into a written or oral form that can be shared across the organization.
3. Management monitors the risk appetite over time, adjusting how it is expressed as business and operational conditions warrant.

These three steps will be discussed in detail in later sections of this paper.

In a recent survey, less than half of the respondents said they had a formal process for developing and communicating risk appetite.[2]

[2] Towers Watson, *2011 Risk and Finance Manager Survey*

Risk Appetite Statements

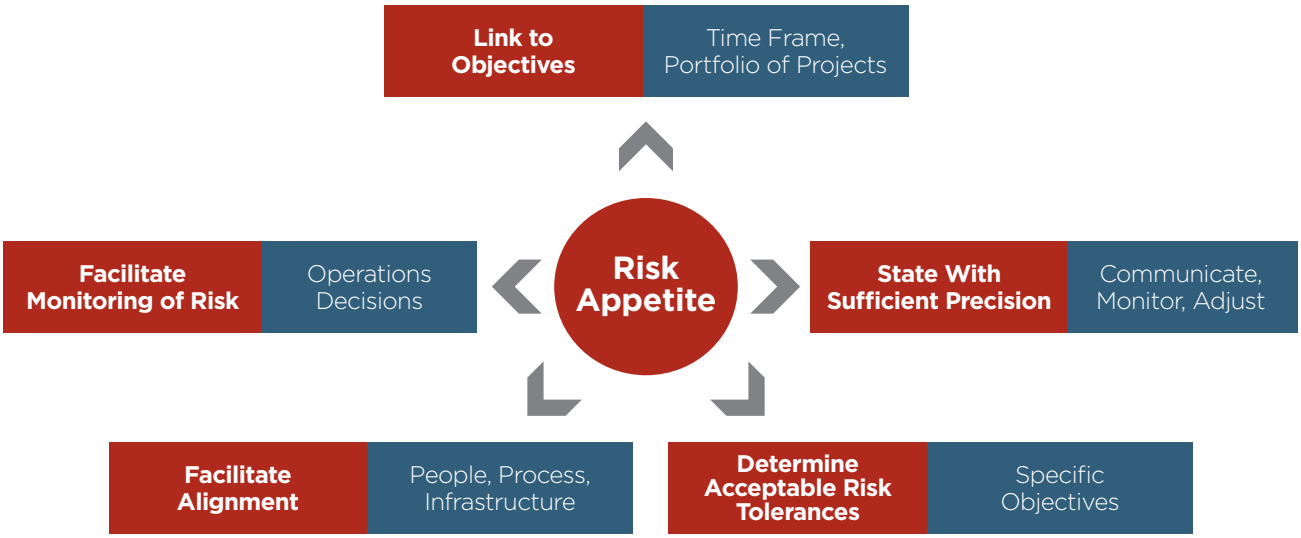
An organization's risk appetite should be articulated and communicated so that personnel understand that they need to pursue objectives within acceptable limits. Without some articulation and communication, it is difficult for management to introduce operational policies that assure the board and themselves that they are pursuing objectives within reasonable risk limits. A risk appetite statement effectively sets the tone for risk management. The organization is also more likely to meet its strategic goals when its appetite for risk is linked to operational, compliance, and reporting objectives.

The length of a risk appetite statement will vary by organization. Some statements require several sentences to express how much risk is acceptable, while others may be more succinct and still clearly communicate management's appetite for risk. The aim is to balance brevity with the need for clarity.

Characteristics of Effective Risk Appetite Statements

A risk appetite statement is useful only if it is clear and can be implemented across the organization. As we noted earlier, risk appetite must relate to the pursuit of organizational objectives and must start at the top. In developing and evaluating a statement, the organization should ensure that risk appetite (Exhibit 3)

Exhibit 3



- directly links to the organization's objectives;
- is stated precisely enough that it can be communicated throughout the organization, effectively monitored, and adjusted over time;
- helps with setting acceptable tolerances for risk, thereby identifying the parameters of acceptable risks (discussed in the next section);
- facilitates alignment of people, processes, and infrastructure in pursuing organizational objectives within acceptable ranges of risk;
- facilitates monitoring of the competitive environment and considers shareholders' views in identifying the need to reassess or more fully communicate the risk appetite;
- recognizes that risk is temporal and relates to the time frame of the objectives being pursued; and
- recognizes that the organization has a portfolio of projects and objectives, as well as a portfolio of risks to manage, implying that risk appetite has meaning at the individual objective level and at the portfolio level.

Risk appetite should be descriptive enough to guide actions across the organization. Management and the board should determine whether compensation incentives are aligned with risk appetite, not only for top management but throughout the organization.

Reluctance to Embrace Risk Appetite

Some organizations are reluctant to develop and communicate risk appetite. Others might argue that risk management did not prevent the recent financial crisis and thus question the usefulness of ERM in general. Others believe that they have expressed their organization's risk appetite in the normal course of business, and that developing further risk appetite statements will not result in any new approach to managing risk.

Such arguments can be misleading to management and the board. To forgo discussion of an organization's risk appetite is to assume that everyone will understand vague comments. History shows that when risk appetite is not considered (especially in compensation schemes), the organization often suffers from greater risks than anticipated. For example, had financial institutions clearly communicated a risk appetite for unsecured mortgage-backed financial instruments, their management and boards would have likely asked questions that would lead to better risk identification, such as the following:

- What if housing failures differ from the historical model?
- What if mortgages fail systematically and are highly correlated to an area we are investing in?
- Could decisions made by some of our operational personnel be creating risks that go beyond our risk appetite?

Risk Appetites Are Not All the Same

Regulators and investors are calling for greater disclosure of risk management processes so that shareholders can better understand not only the risks an organization faces, but the organization's appetite for risk and how it manages (or accepts) that risk. For example, a mining company we are aware of clearly identified its risk appetite and risk mitigation procedures for operational risks. At the same time, it decided it could not manage commodity price risk, leaving stakeholders to decide how to consider that risk in developing their portfolios.

> To earn an "adequate" score for overall ERM from some rating agencies, management must be able to articulate risk appetite and assess and reconcile the appropriateness of individual risk limits given to operational management.

Some companies embrace a high appetite for regulatory risk believing that it will lead to greater profitability because regulator fines were significantly lower than the cost of mitigating the compliance risks. One company ignored many health and safety regulations and fines when incurred, but it did not fully understand the magnitude of risks, such as the government shutting down its operations. While the company had a high risk appetite for fines, its lack of appreciation for the risk of shutdown led to a poorly articulated and implemented risk appetite. Organizations can choose to have high or low risk appetites, but those appetites need to consider shareholder interests and the type and magnitude of risks that the organization needs to manage. We have no preference for a particular level of appetite. Whatever the risk appetite is, it should be stated clearly enough that it can be managed throughout the organization, and reviewed by the board of directors.

Examples of Risk Appetite Statements

Risk appetite statements often start out broad and become more precise as they cascade into departments and operations across the organization. Some organizations find that broad statements crafted around terms such as "low," "medium," or "high" appetite meet the characteristics of risk appetite statements listed above. Others are more precise, making statements like "We are not comfortable accepting more than a 10% probability that we will incur losses of more than a set dollar amount in pursuit of a specific objective."

Which type of statement is best for a particular entity is a management decision. Some organizations may find terms like "low appetite" clear enough to be communicated and monitored effectively within the organization. However, such statements are vague and can be difficult to communicate and implement. Often, as organizations become more experienced in risk management, their risk appetite statements will become more precise.

The following examples of risk appetite statements illustrate the characteristics we identified above.

Health Care Organization: The following represents one part of the health care organization's risk appetite statement. The organization has specific objectives related to (1) quality of customer care, (2) attracting and retaining high-quality physicians and health researchers, and (3) building sustainable levels of profit to provide access to needed capital and to fund existing activities. The statement starts as follows:

> *The Organization operates within a low overall risk range. The Organization's lowest risk appetite relates to safety and compliance objectives, including employee health and safety, with a marginally higher risk appetite towards its strategic, reporting, and operations objectives. This means that reducing to reasonably practicable levels the risks originating from various medical systems, products, equipment, and our work environment, and meeting our legal obligations will take priority over other business objectives.*

In our view, this risk appetite statement does three things effectively:

- Communicates, with sufficient precision, that the organization wants to sustain its business over a long period of time
- Expresses a low risk appetite in pursuing all the organization's objectives
- Expresses a very low appetite for risks associated with employee safety and compliance

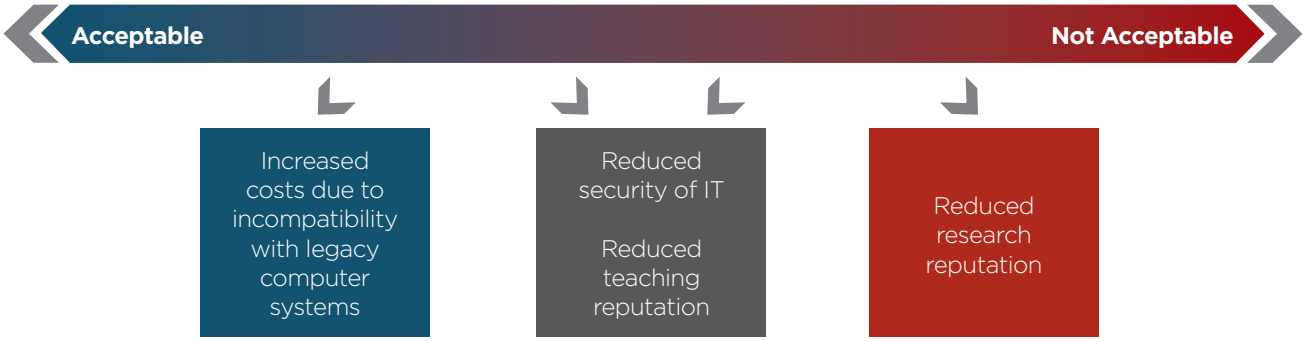
"Business performance can be increased if capital and resources are allocated more effectively, reflecting the balance of risks and rewards in a more integrated and dynamic fashion. In that respect, risk appetite can be considered the cornerstone of modern approaches to bank management, such as value-based management (VBM) and its various implementations." [3]

[3] IBM, *Risk Appetite: A Multi-faceted Approach to Risk Management*, April 2008.

University: The university's main objective is to continue as a preeminent teaching and research university that attracts outstanding students and is a desired place of work for top faculty.

The university's risk appetite statement acknowledges that risk is present in almost every activity. The critical question in establishing the risk appetite was "How willing is the university to accept risk related to each area?" In thinking through the process, members of management used a continuum (Exhibit 4) to express risk appetite for the university's major objectives (teaching, research, service, and operational efficiency). They placed various risks along the continuum as a basis for discussion at the highest levels.

Exhibit 4



From an operational viewpoint, for example, management assigned a high risk appetite to the cost of computer incompatibility, a more moderate risk appetite to issues of teaching excellence, a low risk appetite to information system security, and a very low risk appetite to its reputation as a leading research organization.

The university found that ordering its risk appetites across the continuum helped it shape a risk statement. Putting this into practice, the university

- exhibited a higher risk appetite when approving a new computer system that offered greater processing capacity but also had potential compatibility issues with legacy systems;
- exhibited a low risk appetite for significant breaches of security or unauthorized access to classified records (the new system was viewed as better controlled than the legacy system, thus supporting the decision to approve the new system);
- expressed a moderate risk appetite for teaching quality; and
- expressed a very low risk appetite for risks that would significantly reduce its research reputation.

This example illustrates how risk appetite and strategy interact at the highest levels of an organization. The discussion of risk appetite guided the university's strategies for dealing with issues such as budget cuts and their effect on teaching, research, service, and operations.

Financial Services Organization: This company considers quantitative measures to be part of setting risk appetite, and it focuses on economic capital as a primary measure. The company manages its financial operations to attain a reasoned risk/return relationship, which serves as a guideline for acceptable credit risks, market risks, and liquidity risks. The company's business operations also involve risks related to strategic, reporting, compliance, and operations objectives.

This organization's view of risk appetite specifies not only risk appetite but also acceptable tolerances around that risk appetite that require action to be taken. For example, the company communicates its risk appetite for loan impairment losses by stating that such losses should not exceed 0.25% of the loan portfolio. The company has a low tolerance for exceeding this level, and significant remediation is expected should losses go beyond 0.28%. The same company has a low risk appetite related to its insurance business, stating that claims incurred should be no more than 70% of insurance premium revenue.

This organization reviews its risk appetite annually, adjusting it by type of risk and setting target values for risk-specific indicators in light of the economic cycle and market prospects. The board reviews the risk appetite and associated policies whenever the economic outlook changes significantly.

Risk Appetite and Risk Tolerance

Risk tolerance relates to risk appetite but differs in one fundamental way: risk tolerance represents the application of risk appetite to specific objectives. Risk tolerance is defined as:

> *The acceptable level of variation relative to achievement of a specific objective, and often is best measured in the same units as those used to measure the related objective. In setting risk tolerance, management considers the relative importance of the related objective and aligns risk tolerances with risk appetite. Operating within risk tolerances helps ensure that the entity remains within its risk appetite and, in turn, that the entity will achieve its objectives.*[4]

While risk appetite is broad, risk tolerance is tactical and operational. Risk tolerance must be expressed in such a way that it can be

- mapped into the same metrics the organization uses to measure success;
- applied to all four categories of objectives (strategic, operations, reporting, and compliance); and
- implemented by operational personnel throughout the organization.

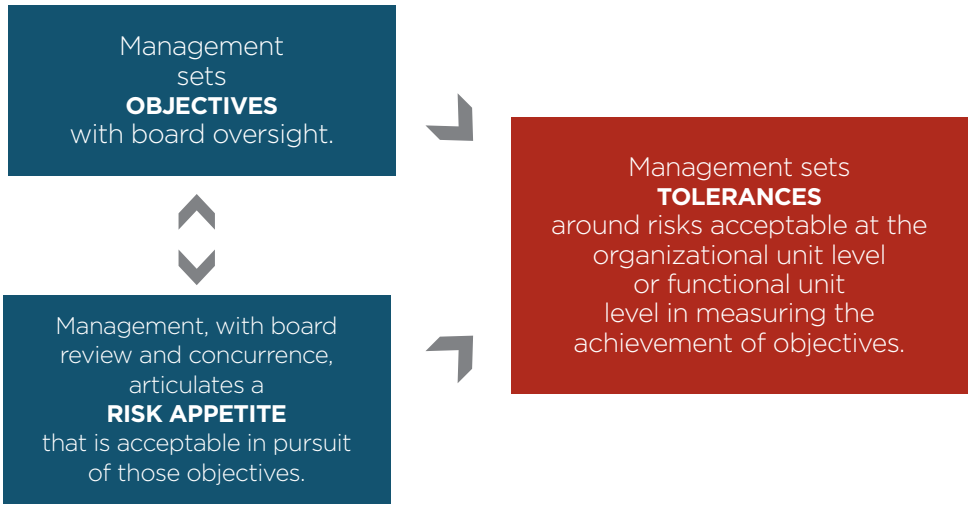
Because risk tolerance is defined within the context of objectives and risk appetite, it should be communicated using the metrics in place to measure performance. In that way, risk tolerance sets the boundaries of acceptable performance variability. A simple example in the financial industry would be to state an appetite for risks associated with collateralized debt obligations (CDO) where the CDOs are divided into tranches reflecting the estimated credit worthiness of the underlying debt. An entity buying these CDOs may set minimum risk rating levels for these tranches and then set a tolerance reflecting the maximum downside risk that is acceptable.

Risk tolerances guide operating units as they implement risk appetite within their sphere of operation. Risk tolerances communicate a degree of flexibility, while risk appetite sets a limit beyond which additional risk should not be taken.

Some tolerances are easy to express in qualitative terms. For example, an organization may have a low risk appetite for non-compliance with laws and regulations and may communicate a similarly low tolerance for violations — for example, a zero tolerance for some types of violations and slightly higher tolerances for other types of violations. Or tolerance may be stated in quantitative terms. A company could say that it requires backup on its computer systems so that the likelihood of computer failure is less than 0.01%.

Risk tolerances are always related to risk appetite and objectives (Exhibit 5). Tolerances can apply to detailed areas such as compliance, computer security, product quality, or interest rate variability. Risk appetite and risk tolerances, together with objectives, guide the organization's actions.

Exhibit 5



[4] COSO, *Enterprise Risk Management — Integrated Framework*, p. 20.

Most organizations have multiple operational objectives related to profitability, some of which might create additional or complementary risks. For example, the managers of an aerospace company might want to improve a product's profitability but know the company has a low risk appetite for not meeting client expectations. They know they cannot reduce product costs if such changes would decrease performance. For example, the company might use new technology, but it cannot use inferior components.

To further illustrate, assume management and the board have set specific profit objectives by product line — for example, maintain a specific gross margin or return on capital for the product line. But they have communicated a low risk appetite for product failure, for loss of customers because of product quality or delivery, and for potential lawsuits related to product design or performance. The articulation of risk tolerances helps guide the company's operational development.

Linking Risk Appetite and Risk Tolerance

The following examples illustrate the relationship between risk appetite and related risk tolerances.

Aerospace Supplier: This company translates its risk appetite statement into tolerances for operational implementation. A high-level objective is to grow by 8% a year (revenue and operating earnings) by working with customers to improve products and market share. Because of the long-term nature of its supply arrangements and product development, the company has communicated the broad parameters of its risk appetite, which then cascade into risk tolerances relating to operations, reporting, and compliance, as shown below. While the company seeks to grow at this rate, acquisitions should not put the company's capital structure at risk. There is a low risk appetite for allowing the capital structure to be so leveraged that it hinders the company's future flexibility or ability to make strategic acquisitions.

Operations Tolerances

- Near zero risk tolerance for product defects
- Low risk tolerance for sourcing products that fail to meet the company's quality standards
- Low, but not zero, risk tolerance for meeting customer orders on time, and a very low tolerance for failing to meet demands within x number of days
- High risk tolerance for potential failure in pursuing research that will enable the company's product to better control, and increase the efficiency of, energy use

Reporting Tolerances

- Low risk tolerance concerning the quality, timing, and accessibility of data needed to run the business
- Very low risk tolerance concerning the possibility of significant or material deficiencies in internal control
- A low risk tolerance related to financial reporting quality (timeliness, transparency, GAAP, etc.)

Compliance Tolerances

- Near zero risk tolerance for violations of regulatory requirements or the company's code of ethics

Company management has been comfortable communicating risk appetite through its actions and performance reviews. However, as the company has grown, it has found that the risk appetite is not fully understood, especially among new operational units. Nor is it understood that policies relate to objectives and are often designed to minimize the risks involved in pursuing those objectives. One division, for instance, failed to follow a company policy because it did not fully understand that the policy was in place to mitigate a significant risk, thus leading to losses. Linking the policy to the risk and risk appetite would have led to better mitigation of the underlying risks.

University: The university in our earlier example has a very low appetite for risk associated with its research reputation. However, given budget shortages, the university also knows it cannot make the same commitment to research and teaching as in the past. The organization has expressed a higher risk appetite for actions resulting in lower-quality teaching. In other words, research that leads to better understanding and innovation is extremely important, but the quality of teaching, though important, is an area where the university can accept more risk for potential decreases.

The university communicated its risk appetite in broad terms, both through the university and, as a public institution, within the state. However, to operationalize the risk appetite within each of its schools, the university had to express risk tolerances for the two key objectives of excellence in research and teaching — while dealing with a 10% budget decrease. The risk tolerances were expressed as follows.

Research: Tolerance Statements Consistent With Low Risk Appetite

- The university does not expect any decrease in the nature, quality, or number of publications related to its research mission.
- The university does not expect any decrease in the number or dollar value of outside research grants generated by faculty.

Teaching: Tolerance Statements Consistent With Moderate Risk Appetite

- Student teaching evaluations should not decline by more than 5%.
- Where individual schools within the university are ranked by outside evaluators on student preparedness and quality of students, there should be no more than a 5% decline.
- The caliber of students wanting to attend the university should not decline by more than 2%, as measured by standard university admissions data such as SAT or ACT scores, percentile ranking in high school graduating class, or extent of community service before attending university.

The idea behind the risk tolerances is that if the university falls below any of the measures, corrective action will take place. Corrections will come not from adjusting the risk appetite but from reassessing the risk appetite and the strategies the university has implemented in the context of the risk appetite.

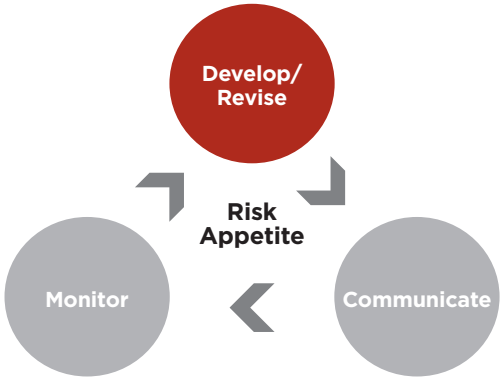
Examples of Risk Tolerance Statements

The following examples from organizations show how risk tolerance might be stated and aligned with broader risk appetite.

Risk Appetite	Risk Tolerance
The organization has a higher risk appetite related to strategic objectives and is willing to accept higher losses in the pursuit of higher returns.	While we expect a return of 18% on this investment, we are not willing to take more than a 25% chance that the investment leads to a loss of more than 50% of our existing capital.
The organization has a low risk appetite related to risky ventures and, therefore, is willing to invest in new business but with a low appetite for potential losses.	We will not accept more than a 5% risk that a new line of business will reduce our operating earnings by more than 5% over the next ten years.
A health services organization places patient safety amongst its highest priorities. The organization also understands the need to balance the level of immediate response to all patient needs with the cost of providing such service. The organization has a low risk appetite related to patient safety but a higher appetite related to response to all patient needs.	We strive to treat all emergency room patients within two hours and critically ill patients within 15 minutes. However, management accepts that in rare situations (5% of the time) patients in need of non-life-threatening attention may not receive that attention for up to four hours.
A retail company has a low risk appetite related to the social and economic costs for sourced products from foreign locations that could be accused of being child sweatshops or having unhealthy working conditions.	For purchasing agents, the risk tolerance is set at near zero for procuring products that do not meet the organization's quality and sourcing requirements.
A manufacturer of engineered wood products operates in a highly competitive market. To compete, the company has adopted a higher risk appetite relating to product defects in accepting the cost savings from lower-quality raw materials.	The company has set a target for production defects of one flaw per 1,000 board feet. Production staff may accept defect rates up to 50% above this target (i.e., 1.5 flaws per 1,000 board feet) if cost savings from using lower-cost materials is at least 10%.

Developing Risk Appetite

We have identified the characteristics of an effective risk appetite statement and noted how those characteristics are useful in managing risk. We have also examined the relationship between risk appetite and risk tolerances. Now we will discuss how an organization can bring out the many "implicit feelings" that management and the board may have about what they believe is the organization's risk appetite and how discussion of those feelings leads to development of risk appetite.



Developing a risk appetite is not an end in itself and should not require an inordinate amount of time. Remember the purposes of risk appetite are

- to provide effective communication throughout the organization in order to drive the implementation of enterprise risk management;
- to change discussions about risk so that they involve questioning of whether risks are properly identified and managed within the risk appetite; and
- to provide a basis for further discussion of risk appetite as strategies and objectives change.

Developing risk appetite is about managing the organization. It is not about developing a statement to be filed in a report. There are many ways to create a clear statement of risk appetite. Organizations should identify the parameters of their risk appetite along key strategic, operational, reporting, and compliance objectives.

Also, keep in mind that any expression of risk appetite must be preceded by a discussion of strategies and objectives. The risk appetite must be linked to those objectives.

Management and boards often use one of three approaches to discuss and develop their risk appetite: (1) facilitated discussions, (2) discussions related to objectives and strategies, or (3) development of performance models.

Facilitated Discussions

Facilitated discussions can be very effective for a variety of organizations. After several iterations, management and the board can develop a risk appetite statement that reflects the combined views of the organization's leadership and governance bodies.

The major advantage of this approach is that the facilitators encourage management and the board to clearly prioritize their objectives and their risk appetite. In addition, various scenarios can be discussed to see how the risk appetite would influence decision making throughout the organization. When discussing risk appetite, those involved should keep the organization's strategic plan, including goals and mission, at the forefront.

A questionnaire can help capture views on risk appetite and business scenarios. Exhibit 6 shows an example. Note that the questions are broad and should be tailored to the unique factors that drive an organization's success.

Discussions Related to Objectives and Strategies

Often the risk appetite an organization is willing to accept becomes more evident when management considers major issues facing the organization, such as new product lines, acquisitions, or joint ventures. Management of organizations with a lower risk appetite will usually react differently to acquisition, expansion, competition, and market volatility than will peers with a higher risk appetite. Reviewing and assessing these reactions can provide insight into the organization's current risk appetite.

This approach allows management to go the extra step in discussing major strategies because it asks what the perceived risks are in pursuing objectives. The board then reviews and supports management's identification and communication of risk appetite as it relates to specific objectives.

Exhibit 6

Questions to Facilitate Discussion of Risk Appetite at Management and Board Level

1. On a scale of 1 to 10, with 1 being the lowest, describe what you believe the organization's overall risk appetite has been and what you think it should be. Explain any differences between what you perceive it has been and what you believe it should be. Relate this to your number one strategic goal.
2. Various operations help an organization achieve its objectives. Using the categories below, or other categories consistent with the organization's operations, rate the desired risk appetite related to the following (rating can be broad, such as high, medium, or low, or precise, such as specific metrics that should not be exceeded):
   - **a.** Meeting customer requirements
   - **b.** Employee health and safety
   - **c.** Environmental responsibility
   - **d.** Financial reporting
   - **e.** Operational performance
   - **f.** Regulatory compliance
   - **g.** Shareholder expectations
   - **h.** Strategic initiatives / growth targets

   As you rate each category, indicate areas where you believe the organization is taking either too much or too little risk in pursuing its objectives.
3. How would you rate the effectiveness of the organization's process for identifying, assessing, managing, and reporting risks in relation to the overall risk appetite? What are the major areas for improvement?
4. Are management's strategies communicated sufficiently for there to be meaningful discussion of risk appetite in pursuit of those strategies, both at the broad organizational level and at the operational level, and for consistency to be analyzed?
5. How satisfied are you that the board is providing effective oversight of the risk appetite through its governance process? This includes board committees and/or the board itself to help set the appetite and to monitor over time that management is adhering to the overall risk appetite in pursuit of value.
6. Whom do you see as more accepting of risk, or more willing to take risks to meet the goals of the organization?
   - **a.** Management
   - **b.** Board
   - **c.** Management and board have similar levels of acceptable risk
7. Does the organization motivate management (senior management and operational management) to take higher than desired risks because of the compensation plans in place? If yes, how do you believe the compensation plans should be modified to bring approaches for generating high performance within the risk appetite?
8. What do you believe the organization should do?
   - **a.** Reduce its risk appetite
   - **b.** Increase its risk appetite
   - **c.** Make no change
9. Do you believe there are risks considered to be above the organization's existing risk appetite that need to be reduced? In other words, are there areas where the risk appetite, as currently used, is too low?
10. What risks over the past five years were, in your view, above the organization's risk appetite? Were the risks understood when a strategy was developed? How could management have communicated its risk appetite so that the board could both (a) evaluate the risk appetite and (b) provide proper oversight? How could management have communicated its risk appetite so as to hold operational units to actions consistent with the risk appetite?

One advantage to this approach is that the board can be seen as supporting or challenging management's risk appetite. Another is that management gains a sense of the board's risk appetite for specific strategies and can incorporate that knowledge into a risk management process. The major disadvantage of this approach is that it can be less comprehensive. It often does not generate the specificity needed for the organization's day-to-day activities.

Development of Performance Models

Some organizations, particularly financial institutions, use quantitative measures to express their overall risk appetite. They often arrive at these measures through performance modelling.

A company could, for instance, use economic capital to express risk appetite. Economic capital is the amount of capital a financial institution needs to remain solvent. This determination is based both on regulatory requirements and on management's assessment of how much economic capital the institution needs to retain.

As an example, management might set its economic capital at 6% of total assets. As the organization models different scenarios of economic activity, economic situations, and its asset portfolio, it needs to set some probability around the ability to maintain economic capital. A management and board with a low risk appetite might want to be 99.9% confident (999 out of 1,000 model results) that economic activities will not place the institution below its desired level of economic capital. A company with a higher risk appetite might start with the same dollar amount but require a confidence level of only 95% (950 out of 1,000 model results). Thus, risk appetite can be composed of both dollar elements and probability elements.

As part of developing (and monitoring) risk appetite, a company may model its overall risk profile. This involves taking "bottom-up" risk information and developing models that consider company-specific risks, including industry factors and broad economic factors, to create a calculated risk profile. The profile can then be compared to the overall risk appetite, helping management and the board to discuss how much risk the organization is prepared to accept. Some organizations also review key ratios from peer companies and industries to gain more input into the risk level suitable for their organization.

Modelling is typically only one part of the process of setting risk appetite. For one thing, an organization needs considerable data to prepare these calculations. For another, there are usually certain risks that are difficult to quantify and model with precision. Management and the board still need to debate and discuss the levels above which capital at risk is seen to be too high and in excess of appetite.

Communicating Risk Appetite

Once an overall risk appetite is developed, management must then choose the right mechanism for communicating it. As we noted earlier, risk appetite statements will vary, and organizations may communicate risk appetite at various levels of detail or precision. The point is that each organization should determine the best way to communicate risk appetite to operational leaders in a specific enough manner that the organization can monitor whether risks are being managed within that appetite.

To be effective, risk appetite must be

- operationalized through appropriate risk tolerances;
- stated in a way that assists management in decision making; and
- specific enough to be monitored by management and others responsible for risk management.

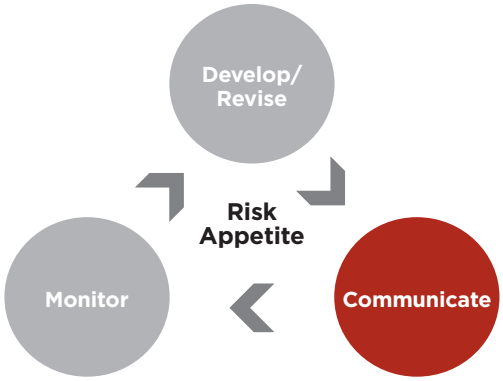
We have encountered three main approaches for communicating risk appetite: (1) expressing overall risk appetite using broad statements, (2) expressing risk appetite for each major class of organizational objectives, and (3) expressing risk appetite for different categories of risk.

Broad Risk Appetite Statement

Organizations that communicate overall risk appetite in broad terms may develop high-level statements that reflect acceptable risk levels in pursuing their objectives.

Some organizations use graphics, like those at right, in discussing risk appetite. A common approach is to apply some form of color banding within a heat map that indicates acceptable versus unacceptable risk levels. With this approach, risks are grouped by objective, summarized, and then plotted on the risk map. The organization sets either the assessment criteria or the location of the color banding to express higher versus lower risk appetites. For instance, the heat maps on the right show that risks related to objectives 1 and 2 would exceed the appetite of a company with a low risk appetite, but not necessarily that of a company with a high risk appetite. Risks related to objective 3 would exceed the appetite of both companies.

The advantage of this approach is that it is simple to convey the level above which risks are seen as unacceptable. We also find that discussions with management and the board on the relative positioning of the bands can draw out important differences between management's and the board's views on desired risk appetite.

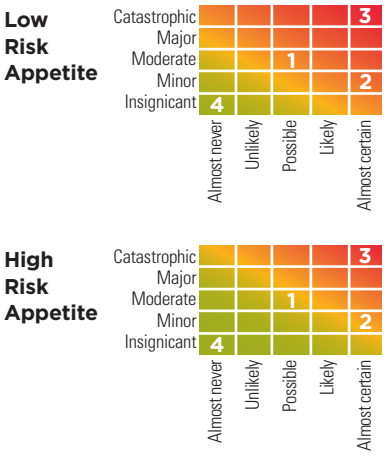


The broad descriptions are effective when they are partitioned to show that not all objectives have the same risk appetite.

Risks Related to Organizational Objectives

Organizations that communicate risk appetite for each major class of organizational objectives are likely to communicate risk appetite in some form of statement. Consider the risk appetite statement from the health care organization we referred to earlier:

> *The Organization operates within a low overall risk range. The Organization's lowest risk appetite relates to safety and compliance objectives, including employee health and safety, with a marginally higher risk appetite towards its strategic, reporting, and operations objectives. This means that reducing to reasonably practicable levels the risks originating from various medical systems, products, equipment, and our work environment, and meeting our legal obligations will take priority over other business objectives.*



The advantage of this approach is that it allows for more delineation between the levels of acceptable risk for each class of objectives. It does not, for instance, treat risks related to legal compliance the same way as risks related to operations. This approach may also help with decision making, especially if resources are limited and need to be allocated across a company's organizational units. Another advantage is that viewing risks in relation to classes of objectives requires less effort than, say, the third approach below. The challenge is to develop a statement that accommodates specific risk types that should be viewed differently in terms of acceptable level of risk.

Categories of Risk

The third option is to communicate appetite for categories of risk. Some organizations use broad, generic risk categories, such as economic, environmental, political, personnel, or technology, in their risk appetite statements. Others use more tailored risk categories that apply to their field. For example, a company in information processing may group risks related to system availability, data security and privacy, system scalability, system design, and release management.

A mining company we are aware of has specific objectives for cash flow and capital structure that include maintaining low volatility of cash flow. There are many causes of cash flow volatility, ranging from operations to uncertain commodity prices. Management believes that investors understand commodity price risk, and it has pursued objectives that enable the company to benefit from price increases while being exposed to losses from price decreases. Management believes that this price risk — even though it can result in volatile earnings — is within the appetite of the organization (and its stakeholders). Therefore, the company has not attempted to mitigate this exposure through a commodity price hedge program. Conversely, the same company is unwilling to accept a similar level of cash flow volatility caused by production delays, and it has adopted rigorous processes to maintain steady production.

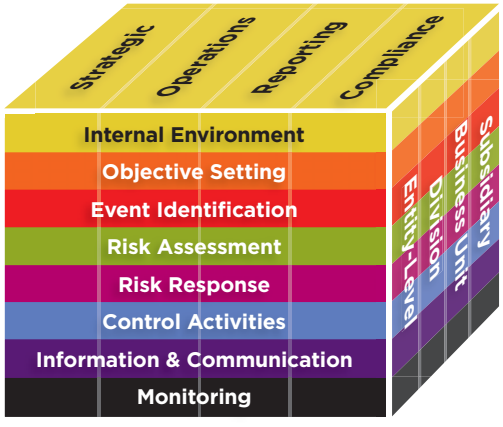
The advantage of communicating risk appetite according to categories of risk is that management can exercise judgment about acceptable levels given the unique considerations of each group of risks. By allowing for greater judgment, this approach reduces the perception that risk management is overly prescriptive.

Risk Appetite Cascades Through the Organization

The method of communicating a risk appetite statement is important, but so is the ability to communicate that statement across the organization in a way that ensures operations are consistent with the risk appetite. It is especially important for those who pursue the operational tactics related to organizational objectives (e.g., local sales forces, country managers, strategic business units) to clearly understand and be aligned with risk appetite. All too often, the risk appetite and tolerances set by the organization are not adhered to or understood in context by those managing the day-to-day business, facing customers and potential risks every day.

Risk appetite needs to be communicated by management, embraced by the board, and then integrated across the organization. The ERM framework is often depicted as a cube (see below). It is important not to overlook the side of the cube, which shows that all units must understand the organization's risk appetite and related risk tolerances.

Risk appetite and risk tolerances are set across the organization. Risk appetite is set at the highest level of the organization in conjunction with goals and objectives. As risk appetite and objectives are communicated throughout the organization (subsidiary, division, or business unit level) the strategic goals and risk appetite are expressed in more specific performance terms. Strategies are reflected in performance objectives, and risk appetite is expressed in terms of risk tolerance. The more precise articulation of performance objectives and risk tolerances helps management to identify situations where corrective actions are needed. Performance metrics and risk tolerances that are more specific lend themselves to better monitoring.



Monitoring and Updating Risk Appetite

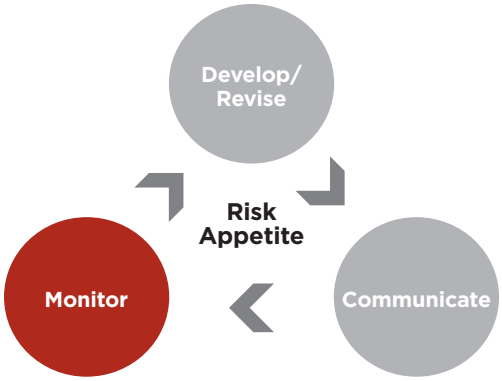
Once an organization's risk appetite is developed and communicated, management, with board support, must revisit and reinforce it. Risk appetite cannot be set once and then left alone for extended periods. Rather, it should be reviewed and incorporated into decisions about how the organization operates. This is especially important if the organization's business model begins to change.

Management cannot just assume that responsible individuals will implement risk management within the appropriate risk appetite. Therefore, some organizations will review the application of risk appetite through a series of monitoring activities. Management should monitor the organization's activities for consistency with risk appetite through the specifics identified with risk tolerances. Most organizations have key performance risk metrics that they use to measure performance. It is easy to integrate risk tolerances into the monitoring process used to evaluate performance. Internal auditing can provide independent insight on the effectiveness of such processes.

Creating a Culture

For many organizations, monitoring risk tolerances requires a culture that is aware of risk and risk appetite. Management, by revisiting and reinforcing risk appetite, is in a position to create a culture whose organizational goals are consistent with the board's, and to hold those responsible for implementing risk management within the risk appetite parameters.

Many organizations are effective at creating a risk-aware culture: a culture that emanates from senior management, cascades through the organization, and is supported by the board. In an effective culture, each member of the organization has a clear idea of what is acceptable, whether in relation to behaving ethically, pursuing the wrong objectives, or encountering too much risk in pursuing the right objectives.



Creating a culture is one way of reinforcing overall risk appetite. The approach is best used when the organization has a well-communicated risk appetite and associated risk tolerances, to the point at which the following outcomes exist:

- Consistent implementation across units
- Effective monitoring and communication of risk and changes in risk appetite
- Consistent understanding of risk appetite and related tolerances for each organizational unit
- Consistency between risk appetite, objectives, and relevant reward systems

This approach draws on ongoing and separate evaluations conducted as part of the organization's monitoring. The individuals doing the monitoring consider whether the objectives being set and the risk response decisions being made are consistent with the organization's stated risk appetite. Any variation from the stated (or desired) risk appetite is then reported to management and the board as part of the normal internal reporting process.

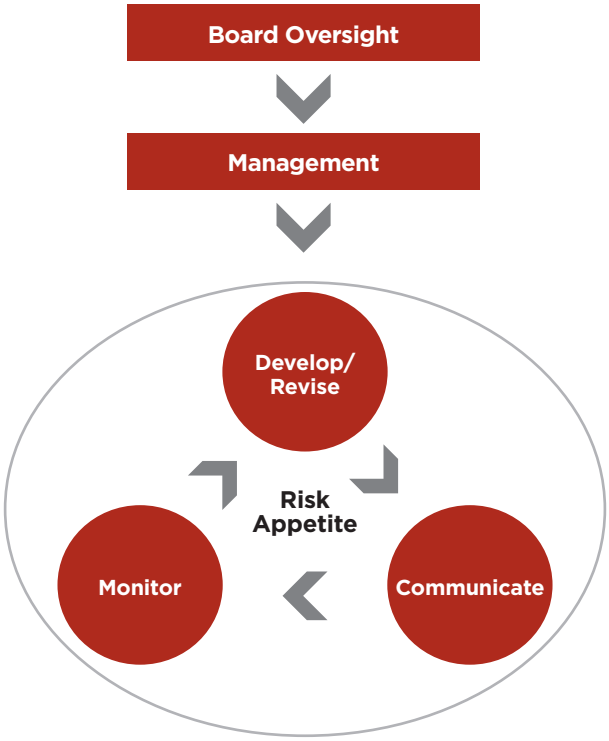
Roles

It is management's role to develop the risk appetite and to obtain the board's agreement that the risk appetite is suitable for the organization. We believe that the board is in place to oversee management and to monitor the broader risk management process, including whether the organization is adhering to its stated risk appetite. Any board, serving any organization of any size or structure (for-profit, not-for-profit, private), has a fiduciary responsibility to question management's development and implementation of a risk appetite and to require changes if it believes the risk appetite is either badly communicated or inconsistent with shareholder values.

Effective board oversight of an organization's risk appetite should include

- clear discussion of the organization's objectives and risk appetite;
- oversight of the organization's compensation plan for consistency with risk appetite;
- oversight of management's risk identification when pursuing strategies to determine whether the risks exceed the risk appetite;
- oversight of strategies and objectives to determine whether the pursuit of some objectives may create unintended consequences or organizational risks in other areas; and
- a governance structure that requires regular conversations on risk appetite, through the board and board committees, concerning matters such as strategy formulation and execution, M&A activity, and business cases to pursue major new initiatives.

Governance does not stop with board oversight. It includes management's development of the infrastructure for risk management and the allocation of resources across the organization. Exhibit 7 is a summary of matters for the board and management to consider in evaluating how effective their processes are for developing, communicating, and monitoring risk appetite.



Boards are very good at questioning strategies. They are only a step away from addressing meaningful questions that can help with setting the organization's risk appetite. For example, when the board asks how much an organization should pay for an acquisition, it is an expression of risk appetite.

Exhibit 7

Board and Management Responsibilities

1. **Management establishes risk appetite:** An organization cannot know how well it is managing risk unless it establishes ranges of acceptable risk it can take in pursuit of its objectives. In doing so, management must effectively and clearly communicate:
   - **a.** Goals and objectives
   - **b.** Strategies
   - **c.** Metrics (to know whether objectives are being achieved)
   - **d.** Relevant time periods for pursuing the objectives
   - **e.** Ranges of risk the organization is willing to take in pursuing the objectives
2. **Board oversees risk appetite:** Oversight of the risk appetite (or acceptable ranges of acceptable risk) should be considered at the board level in conjunction with the senior management team.
3. **Applies throughout organization:** Risk appetite needs to be applied regularly throughout all functional units of the organization. Culture is important: the organization must work to build the board's view of risk appetite into the organizational culture.
4. **Aligns with stakeholders and managers:** Because individuals are accountable for their results, every organization needs a robust governance process to ensure that compensation and incentive systems are aligned with the organization's objectives and are managed to fall within the organization's risk appetite.
5. **Manages risks and risk appetite over time:** Organizations need to understand that risk appetites may change over time. Boards must be proactive on two levels:
   - **a.** Communicating their articulation of risk appetite
   - **b.** Monitoring organizational actions, processes, etc., to determine whether organizational activity has strayed outside the organization's risk appetite
6. **Monitors to ensure adherence to risk appetite:** Adherence to an organization's risk appetite, as well as to its risk management processes, should be monitored regularly. The results of the monitoring should be reported to the audit committee and/or board and to the relevant members of executive management.
7. **Supports culture:** The tone at the top influences the culture of the organization. The tone can be either positive or negative in ensuring that risks are managed within acceptable limits. Ideally, prudent risk taking is built into the organization's culture in its public statement of core values.
8. **Considers resources:** It takes effort to operate within the organization's risk appetite. Resources must be available and dedicated to operating within this appetite.
9. **Communicates through strategies and objectives:** Risk appetite is communicated effectively only if the organization can clearly communicate its major strategies and objectives at both the global level and the functional/operational level.
10. **Clearly communicates how much risk the organization is willing to accept at all levels:** Risk appetite and risk tolerance are complementary concepts. They can be combined to determine acceptable ranges of risk for the organization.

Risk appetite is developed by management and reviewed by the board. COSO's *Enterprise Risk Management — Integrated Framework* emphasizes the board's important role in overseeing risk management. Oversight should begin with a studied discussion and review of management's articulation of risk appetite relative to the organization's strategies.

Summary of Considerations

The COSO *Enterprise Risk Management — Integrated Framework* sets out five principles related to risk appetite:

1. It is a guidepost in strategy setting.
2. It guides resource allocation.
3. It aligns organization, people, processes, and infrastructure.
4. It reflects the entity's risk management philosophy and influences the culture and operating style.
5. It is considered in strategy setting so that strategy aligns with risk appetite.

Risk appetite does not exist in a vacuum; rather, it is an integral part of an organization's strategies for achieving objectives. The concept of risk appetite permeates all organizations, from charities and governments to small businesses and publicly traded corporations.

A statement of risk appetite is an effective way to communicate across an organization a sense of acceptable risks. In addition, it provides a basis for evaluating and monitoring the amount of risk an organization faces to determine whether the risk has risen above an acceptable range.

Organizations can, and should, come to terms with what they believe to be their appetite for risk. Once stated, risk appetite can be communicated and refined over time as the organization becomes more experienced with the concept.

Most importantly, developing risk appetite is the start of an organization's commitment to effective enterprise risk management. As with pursuing corporate objectives, the end objective is adding value through effective enterprise risk management in pursuit of organizational goals. Developing and communicating a risk appetite moves organizations in that direction.

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

Dr. Larry Rittenberg is the Ernst & Young Professor of Accounting at the University of Wisconsin-Madison School of Business. He is one of only eight academics on the list of the United States' 100 most influential people in finance. Dr. Rittenberg was on the COSO steering committee that oversaw the development of *Enterprise Risk Management — Integrated Framework* and later served as chair of COSO. As chair, he led the effort to provide guidance for small and midsize companies on developing effective internal controls, and later led COSO in developing guidance on monitoring of internal controls.

On the University of Wisconsin faculty since 1976, Dr. Rittenberg teaches in the area of audit and assurance, including risk management and corporate governance. His current research deals with the effectiveness of audit committees, corporate governance, and assurance services. He has received The Institute of Internal Auditors' highest award, the Bradford Cadmus Memorial Award, for his contributions to the internal auditing profession.

Frank Martens is a Director in the Advisory Practice of PricewaterhouseCoopers (PwC). He provides services related to enterprise risk management, internal audit, and internal control to a wide range of companies. Mr. Martens is a Chartered Accountant with over 20 years of external audit experience.

Mr. Martens was one of the principal contributors from PwC in developing COSO's *Enterprise Risk Management — Integrated Framework*. He was also a principal contributor to COSO's *Internal Control over Financial Reporting — Guidance for Smaller Public Companies*, a guidance document for using COSO's *Internal Control — Integrated Framework*.

Note to Readers

The information contained herein is of a general nature and based on authorities that are subject to change. Applicability of the information to specific situations should be determined through consultation with your professional adviser. This thought paper represents the views of the authors only, and does not necessarily represent the views or professional advice of the University of Wisconsin, PwC, or COSO.

COSO

Committee of Sponsoring Organizations
of the Treadway Commission

www.coso.org

ENTERPRISE RISK MANAGEMENT

Understanding and Communicating Risk Appetite

COSO

Committee of Sponsoring Organizations of the Treadway Commission

www.coso.org