4

CHAPTER FOUR

# Understanding Risk Management through COSO ERM

INFORMATION TECHNOLOGY (IT) AND other internal auditors need to identify all of the business risks they face in their review activities—IT, financial, and operational as well as social, ethical, and environmental risks—and to assess that these risks are managed at an acceptable level. Understanding risks is a major component of achieving Sarbanes-Oxley (SOx) compliance, as discussed in Chapter 1, and is part of the international audit standards of the Institute of Internal Auditors (IIA) and the Information Systems Audit and Control Association (ISACA) discussed in Chapter 3. *Risk* has too often been one of those terms where IT auditors and internal control specialists often say ''Yes, we must consider risks!'' even though their understandings and assessments of risk are not well understood or defined. One professional's concept and understanding of risk may be very different from another's, even though they are both working for the same enterprise and in similar areas.

IT auditors need to have an understanding of risk management and how it impacts their approaches for assessing or developing effective internal controls. This chapter begins by discussing some of the fundamental concepts behind risk management for IT auditors, considers the various types of risk facing an enterprise, and then looks at quantitative approaches for assessing risks.

We then introduce internal audit risk management standards, tools, and approaches as defined in ISACA and IIA guidance materials and standards. An ongoing problem in an IT auditor's use and understanding of the concept of risk had been the lack of a consistent definition of what is really meant by *risk.* The word has some origins in the insurance industry, but the concept of risk has not been consistently used even in insurance areas, let alone by IT auditors or other business professionals. Many have talked about how they had ''considered risk'' when implementing a control or process, but they often had no consistent definitions here. The question of what steps were followed in such a risk consideration might produce a wide range of answers.

This all changed when the Committee of Sponsoring Organizations (COSO) released its enterprise risk methodology, COSO Enterprise Risk Management Integrated Format standards (COSO ERM).[1] This is a framework to allow an enterprise to consider and assess its risks at all levels, whether it is in an individual area, such as for an IT development project, or for global risks regarding an international expansion. Because it was released by the same COSO guidance-setting function that is responsible for the COSO internal controls framework, COSO ERM sometimes looks like its internal controls ''brother.'' However, COSO ERM has a much different feel and approach.

This chapter introduces the COSO ERM framework and its elements, with an emphasis on why COSO ERM can be an important tool to better understand and evaluate the risks surrounding internal controls at all levels, but with an emphasis on IT resources. We describe major elements of the COSO ERM framework and also look at how IT auditors can better build COSO ERM concepts into their internal controls audits and reviews of IT resources. Although the basic framework models look similar to the COSO internal controls framework, COSO ERM, with its emphasis on enterprise-wide risks, is different.

## RISK MANAGEMENT FUNDAMENTALS

Every enterprise makes business decisions and invests in resources to provide value for its stakeholders, but these investments and other activities have uncertain outcomes and are always subject to uncertainties or risks—whether the failure of a key IT business process, the challenge caused by a new and aggressive competitor, or the damage and even loss of life caused by a major weather disturbance. Risk management is a concept where an enterprise should use insurance mechanisms to provide a shield or protection from those risks. We make these decisions based on assessments of relative risks and the costs to cover them through the purchase of insurance. These risks and insurance costs also change over time. Fire insurance to cover an individual's home is an example of this evolving change. Back in the days of oil lanterns as a source for light and straw stored in a nearby stable, there was always a high risk of fires. We need only to think of the great Chicago fire of 1871 where, as legend suggests, a cow kicked over a lantern and caused a fire that devastated the city. The risk of fires in the typical building is not that great today, and fire insurance is not too expensive, in a relative sense. However, there is always the possibility of a lightning strike or electrical malfunction causing a fire in a structure, and mortgage finance companies require fire insurance coverage. Even if there is no mortgage, all prudent persons today purchase such fire insurance even if not required. A destructive fire to one's home presents a low-level but consistent risk. An individual homeowner might assess other potential risks, such as for earthquakes, and not purchase insurance for that type of risk. In a given geographic area, the possibility of an earthquake may appear so low that an owner would not consider purchasing any insurance, despite its low cost. In another situation, an individual may live by a body of water where there are damaging floods every several years. Even if one can purchase flood insurance in such an environment—and most insurance companies will not even offer it—the cost of flood insurance here will be very expensive. Some people may decide to accept the risk of a flood in future years and go without insurance coverage. In all of these cases, there has been an insurance purchaser risk management decision.

Starting with these insurance-buying foundations, enterprise risk management, as it is practiced today, is essentially a post-1960s phenomenon. Moving beyond concerns about natural weather-related events, risk management began to emphasize protecting enterprises against a major catastrophe, such as the risks surrounding a computer system back in the mainframe days, when most information systems assets were stored in centralized facilities. The concern about managing risks surrounding that one centralized computer system moved to a general concern about managing a wide range of other business risks. (IT disaster recovery planning is discussed in Chapter 23.)

Risk assessment, in combination with other audit techniques, should be considered in making such planning decisions, with consideration given to the nature, extent, and timing of any planned audit procedures; the areas or business functions to be audited; and the amount of time and resources to be allocated to an audit. A key risk assessment and audit planning concept, IT auditors should understand and make their assessments in terms of the levels of what are known as inherent, control, and detection risks.

- **Inherent risk.** As defined by the U.S. government's Office of Management and Budget (OMB), *inherent risk* is the "potential for waste, loss, unauthorized use, or misappropriation due to the nature of an activity itself." Inherent risk is the susceptibility of an audit error to occur in a way that could be material, individually or in combination with other errors, assuming that there were no related internal controls. Major factors that affect enterprise inherent risk are the size of its budget, the strength and sophistication of management, and the very nature of its activities. Inherent risk is outside the control of management and usually stems from external factors. For example, the major retailer Wal-Mart is so large and dominant in its markets that it faces various inherent risks due to its sheer size. Inherent risk for most IT audit areas is usually high, since the potential effects of errors ordinarily span several business systems and many users.
- **Control or residual risk.** This is the risk that remains after management responses to risk threats and countermeasures have been applied. There is virtually always some level of residual risk. These are also the risks of an error occurring in an audit that could be materially significant, individually or in combination with other errors, but that will not be prevented or detected and corrected on a timely basis by the internal control system. For example, the control risk associated with manual reviews of computer system activity logs can be high because activities requiring investigation can be easily missed, owing to the volume of logged information. The control risk associated with IT data validation procedures is ordinarily low because the processes are consistently applied.
- **Detection risk.** This is the risk that the IT auditor's substantive procedures will not detect an error that could be material, individually or in combination with other errors. For example, the detection risk associated with identifying breaches of

security in an application system is ordinarily high because logs for the whole period of the audit may not be available at the time of the audit. The detection risk associated with identifying a lack of disaster recovery plans is ordinarily low, since existence is verified easily.

Inherent, control, and detection risk are fundamental risk assessment concepts. IT auditors should have a general understanding of these concepts and how they will help an IT auditor to review and assess controls.

Enterprises today face a wide variety of IT-related risks. Management needs to assess these risks in order to make rational decisions related to cost and risk avoidance. This is the process of risk management. Although an enterprise today can just make seat-of-the-pants decisions to assess a potential threat as high, medium, or low risk and then make quick insurance or risk protection decisions based on those options, more sophisticated qualitative or quantitative tools are available to help them understand and evaluate these risks. IT auditors should have a general understanding of these processes as well. The next sections briefly survey some fundamental modern risk management approaches with the aim of helping to establish more effective IT risk management procedures in an enterprise.

An effective risk management process typically requires four steps:

1. Identify the relevant potential risks facing an activity.
2. Quantitatively or qualitatively assess those identified risks.
3. Prioritize risk and response planning.
4. Perform ongoing risk status monitoring.

There is always a need to identify and understand the various risks facing an enterprise, to assess those risks in terms of their cost or impact and probability, to develop responses in the event of a risk occurrence, and to develop documentation procedures to describe what happened as well as corrective actions going forward. This is true for specific IT-related risks as well as for other enterprise-wide non-IT risks.

The four-step risk management process should be implemented at all levels of an enterprise and is particularly useful for IT systems and related resources. Whether the company is a smaller one operating in a limited geographic area or a larger, worldwide enterprise, these risk management approaches should be developed for the entire enterprise. Doing so is particularly important for the worldwide enterprise with multiple operating units engaged in different business operations and with facilities in different countries. Some risks in one unit may directly impact or be related to risks in another, while other risk considerations may be independent from the whole. Although the overall focus of this book is on the activities of IT auditors, risk management should be an enterprise-wide responsibility, managed by risk management specialists in the enterprise. Many have established a chief risk officer (CRO) to take responsibility for these activities.

## Risk Identification

As the first step in the previously outlined four-part risk management process, the enterprise's CRO or a supporting team should try to identify all possible risks that may impact the success of their enterprise, ranging from the larger significant risks to the overall business down to lesser risks associated with individual projects or smaller business units. This type of risk identification process requires a studied, deliberate approach to looking at potential risks in each area of operations and then identifying the more significant risk areas that may impact each operation in a reasonable time period. The idea here is not to list every possible risk but for an enterprise to identify those that might have a major impact on operations within a reasonable time period. This exercise can be difficult; it requires estimating the probabilities of various identified risks occurring or the nature of the consequences if the enterprise has to face the risk. This risk identification process should occur at multiple levels, with an understanding that a risk that impacts an individual business unit or project may not have that great of an impact on the entire enterprise or beyond. Conversely, a major risk that impacts the entire economy will flow down to the individual enterprise and its separate business units. Some major risks are so infrequent but can be so cataclysmic that it is difficult to identify them as possible future events.

For a larger enterprise, a good way to start a risk identification process is to begin with a high-level organization chart that lists corporate-level as well as operating units. Each of those units may have facilities in multiple locations and may also consist of multiple and different types of operations. Each separate facility will then have its own departments or functions. Some of these separate business units may be closely connected to one another while others represent little more than corporate investments. An enterprise-wide initiative, which is a difficult and sometimes complicated task, should be launched to identify all significant risks in these individual areas. This type of exercise can have interesting and sometimes troubling results. For example, a corporate-level senior manager may be aware of some product liability risks, but a front-line supervisor in an operating unit may look at the same risks from an entirely different perspective.

A marketing manager, for example, may be concerned about a competitor's pricing strategies or the risk of pricing activities that would put the enterprise in violation of restraint of trade laws. An IT manager may be concerned about the risk of a computer virus attack on application systems but will have little knowledge of pricing issue risks. More senior management typically will be aware of a different level and set of risks than would be on the minds of the operations-oriented staff. Still, all of these risks should be identified and considered on an operating unit–by–operating unit basis and over the entire enterprise.

To be effective, this risk identification process requires much more than just sending out an e-mail to all operating units with a request for recipients to list the key risks in their units. Such a request typically will result in a wide range of inconsistent answers with no common approach. A better method is to ask people at all levels of the enterprise to serve as risk assessors. Within each significant operating unit, key people should be identified from operations, finance/accounting, IT, and unit management. Their goal should be to identify and then help assess risks in their units built around a risk identification model framework. This type of initiative can be led by the CRO or a designated risk assessment team. IT auditors often play a key role here because of their ongoing understandings of IT disaster recovery risks.

**Enterprise-Wide Strategic Risks**

**External Factors Risks**

- Industry Risk
- Economy Risk
- Competitor Risk
- Legal and Regulatory Change Risk
- Customer Needs and Wants Risk

**Internal Factors Risks**

- Reputation Risk
- Strategic Focus Risk
- Parent Company Support Risk
- Patent/Trademark Protection Risk

**Operations Risks**

**Process Risks**

- Supply Chain Risk
- Customer Satisfaction Risk
- Cycle Time Risk
- Process Execution Risk

**Compliance Risks**

- Environmental Risk
- Government Rules and Regulatory Risk
- Policy and Procedures Risk
- Litigation Risk

**People Risks**

- Human Resources Risk
- Employee Turnover Risk
- Performance Incentive Risk
- Training Risk

**Finance Risks**

**Treasury Risks**

- Interest Rate Risk
- Foreign Exchange Risk
- Capital Availability Risk

**Credit Risks**

- Capacity Risk
- Collateral Risk
- Concentration Risk
- Default Risk
- Settlement Risk

**Trading Risks**

- Commodity Price Risk
- Duration Risk
- Measurement Risk

**Information Risks**

**Financial Risks**

- Accounting Standards Risk
- Budgeting Risk
- Financial Reporting Risk
- Taxation Risk
- Regulatory Reporting Risk

**Operational Risks**

- Terrorist Attack
- Pricing Risk
- Performance Measurement Risk
- Employee Safety Risk

**Technological and IT Risks**

- Information Access Risk
- Business Continuity Risk
- Availability Risk
- Infrastructure Risk

**EXHIBIT 4.1** Types of Enterprise Risks

An effective idea here is to outline some high-level "straw man"[2] risks that may impact various operating units. Knowledgeable people can then look at these lists and modify them as appropriate. Exhibit 4.1 shows some types of major risks that may impact an enterprise, including various strategic, operations, and finance risks. A chief executive officer (CEO) might use such a high-level list to respond to a shareholder annual meeting question "What worries you at the end of the day?" This is the type of first-pass list that an enterprise can use to get started on a detailed risk identification. Other senior managers in the enterprise—often the CEO and supporting staff—can meet with senior management and ask some of these types of questions to identify such high-level risks.

This very general, high-level risk model can serve as a basis to better define the broad range of specific risks facing various units of an enterprise. An IT auditor should be able to expand an entry, such as Business Continuity Risk listed under Technological Risks, into a long list of detailed technology-related risks associated with business continuity. An operations manager who is the user of IT resources might look at business continuity risks from a different perspective and may introduce other risks associated with what happens if IT services are not available. In order to have a better understanding of the risks facing an enterprise, it is often best to expand these lists to establish a more complete set of risks.

An enterprise management team should then use this more complete list of potential enterprise risks and ask themselves such questions as:

- Is the risk common across the overall enterprise or unique to one business group?
- Will the enterprise face this risk because of internal or external events?
- Are the risks related, such that one risk may cause another to occur?

The idea is to gain a strong understanding of the nature of enterprise-level risks and then to highlight major risks, including, for example, the risks of: a significant fall in customer satisfaction ratings, a new and very large competitor entering the market, and an identified significant internal control weakness as part of the financial statement close. Any of these major risks could present significant challenges to an enterprise.

Enterprise management should review their risks and highlight those that appear to be most critical in order to prepare a final set of risks by the overall enterprise and by specific operating units. Because viewpoints and perspectives will vary across the enterprise, these identified risks should be shared with responsible operating, IT, and financial management, giving them opportunities to provide feedback. The idea here is to identify the population of risks that threaten an enterprise, both at an individual unit level and on a total enterprise basis. These risks will not necessarily be the enterprise's core risks but they often are a starting point for enterprise risk assessments.

## Key Risk Assessment Principles

After the significant enterprise risks are identified, a second important step is to assess their likelihood and relative significance. A variety of approaches can be used here, ranging from best-guess qualitative conjectures to detailed mathematical quantitative analyses. The idea is to help decide which of a series of potentially risky events management should worry the most about.

A simple but often effective approach is to take the list of identified risks and circulate them to key managers with a questionnaire asking for each risk:

- What is the likelihood of this risk occurring over the next one-year period? Using a range of 1 to 9, assign a best-guess score as follows:
  - Score 1 if you see *almost no chance* of that risk happening during the period.
  - Score 9 if you feel the event will *almost certainly happen* during the period.
  - Score 2 through 8 depending on how you feel the likelihood the event will fall between these two ranges.
- What is the significance of the risk in terms of cost to the enterprise? Again using the same 1 to 9 scale, scoring ranges should be set depending on the financial significance of the risk. A risk whose costs could lower earnings per share by perhaps 1 cent might qualify for the maximum score of 9.

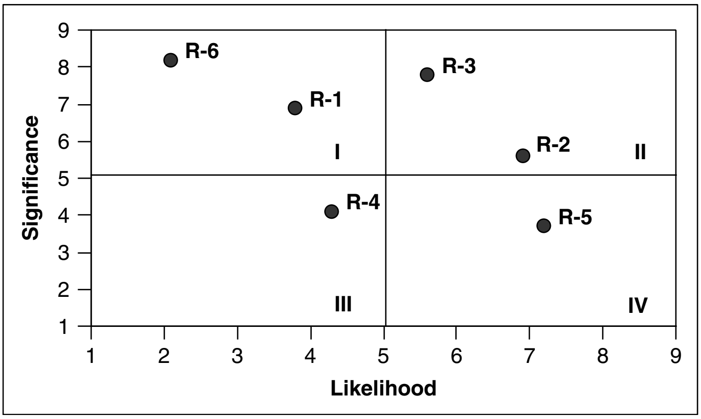

**EXHIBIT 4.2** Risk Assessment Analysis Map

*Source:* Robert R. Moeller, *COSO Enterprise Risk Management: Understanding the New Integrated ERM Framework* (Hoboken, NJ: John Wiley & Sons). Copyright © 2007 John Wiley & Sons. Reprinted with the permission of John Wiley & Sons, Inc.

Questionnaires here should be circulated independently to knowledgeable people to score each of the identified risks per these two measures. As an example, assume that an enterprise has identified six risks, R-1 through R-6, and four managers are asked to separately evaluate each risk in terms of its likelihood and significance. These scores can be averaged by both factors and plotted on a risk assessment analysis chart as shown in Exhibit 4.2. R-1 had an average Likelihood score of about 3.75 and a Significance score of 7.00, and this score is plotted in quadrant I of the chart. For example, R-1 is relatively significant but not that likely to occur. After all identified risks are plotted in this manner, the high-likelihood and more significant risks in quadrant II should receive immediate management attention. This type of chart provides a good qualitative measure to understand some of the significant risks surrounding an enterprise.

This high-risk assessment process works well when an enterprise has identified a relatively small number of risks. It is fairly easy to look at the analysis chart and focus on remediation planning for the high-likelihood and significant risks in the upper left-hand quadrant. Often, however, an enterprise may identify a much larger set of risks, with risk ranges of only 1 to 9 as well as plots on the example chart will not provide sufficient detail. It is often a better approach to express risk significance and impact estimates in terms of two-digit percentage estimates (e.g., 72%) of achieving some risk or as a probability. However, just increasing the number of digits, from a 7% to a full 72%, does not increase the accuracy of the assessment. More attention should be given to better understanding the relationship between probabilities covering independent and related risk events.

Combined estimates of likelihood and significance are key factors in any risk analysis assessment. The combination of two probabilities requires one to go back to some basic mathematical concepts. A basic rule of probability is that we cannot add up independent probability estimates to develop a joint estimate. If the probability of risk A occurring is 60% and the probability of a separate but related risk B is also 60%, we *cannot* say that the probability of both occurring is $0.60 + 0.60 = 1.20$. This 120% does not make sense! Rather, the joint probability of two independent events is the product of the two separate probabilities:

$$\Pr(\text{Event } 1) \times \Pr(\text{Event } 2) = \Pr(\text{Both Events})$$

That is, if Event 1 has a probability of 0.60 and Event 2 is also 0.60, the combined probability of both events occurring is $(0.60) \times (0.60) = 0.36$. In terms of the assessments, if a risk has a 60% significance estimate or we are 60% certain that the risk will occur, and if the impact has been rated at 60%, there is a 36% probability that we will achieve both of those risks. We can also call this the risk score for the individual risk.

An accurate risk assessment process, however, requires more than just top-of-the-head estimates stated in percentage estimates. Enterprise management should take a hard look at identified risks and gather more information, if required. For example, during the risk identification process, one manager may have identified the consequences of a new tariff law as a serious risk. However, responsible managers may want to better understand its actual consequences. Perhaps the law is not applicable to the unit in question, or it often does not go in to effect until some years in to the future. The point here is that all identified risks may need some additional information before they can be assessed accurately.

Risk independencies must always be considered and evaluated throughout the organizational structure. Although any entity should be concerned about risks at all levels of the organization, it really has control over only the risks within its own sphere. The 2002 example of the fall of the major public accounting firm Arthur Andersen in the wake of the Enron collapse is an example. Each city-by-city and country-by-country unit of that once esteemed public accounting firm had its own risk assessment procedures, following firm-wide standards. However, a risk event at one operating office, in Houston, Texas, caused the firm to collapse worldwide. An operating office in another area, such as Toronto, might not have even have fully anticipated such risks in a faraway Houston. The point here is that risks within an enterprise are often very interdependent. Each operating unit is responsible for managing its own risks but may be subject to the consequences of risk events on units above or below it in the organization structure.

The examples used in this chapter show a short list of identified risks, but a typical enterprise will end up with a very long list of potential risks. A next step is to take the established significance and likelihood estimates, calculate risk rankings, and identify the most significant risks across the entity reviewed. Exhibit 4.3 is an example of this type of analysis. Based on the likelihood and significance scores from Exhibit 4.2, the product of these two values gives relative risk rankings. Risks C and G have the highest risk rank scores and would be plotted in the upper right-hand quadrant as the most significant risks in this sample. These risks would be called the risk drivers for this set identified risk. That is, these are the key risk areas requiring attention. An organization should focus its attention going forward on these primary risks. These risk-ranked schedules should be organized on a unit-by-unit basis and adjusted to accommodate all related risks in parallel with as well as above or below the entity being evaluated.

| Identified Risk | Significance Probability | Likelihood Probability | Risk Score (P × I) | Rank |
|---|---|---|---|---|
| A | 0.55 | 0.30 | 0.17 | 8 |
| B | 0.88 | 0.24 | 0.21 | 7 |
| C | 0.79 | 0.66 | 0.52 | 1 |
| D | 0.77 | 0.45 | 0.35 | 4 |
| E | 0.35 | 0.88 | 0.31 | 5 |
| F | 0.54 | 0.49 | 0.26 | 6 |
| G | 0.62 | 0.72 | 0.45 | 2 |
| H | 0.66 | 0.20 | 0.13 | 9 |
| I | 0.90 | 0.45 | 0.41 | 3 |
| J | 0.12 | 0.88 | 0.11 | 10 |

**EXHIBIT 4.3** Risk Scoring Schedule

This analysis requires that a risk management team identify its unit-by-unit assessed risks to make certain that risk likelihood and significance estimates are appropriate throughout. All too often, risk events that occur far away from corporate headquarters can cause major problems. An example from nearly 30 years ago can be drawn from a risk event at Union Carbide, a U.S. corporation. On the night of December 2, 1984, over 40 tons of poisonous gases leaked from a pesticide factory owned by Union Carbide in Bhopal, India, killing more than 20,000 residents.[3] After much legal wrangling, Union Carbide, which had built the plant in 1969, settled a civil suit brought by the Indian government by agreeing to pay US$470 million for damages suffered by the half-million people who were exposed to the gas. The company maintained that this payment was made out of a sense of ''moral'' rather than any ''legal'' responsibility since the plant was operated by a separate Indian subsidiary, Union Carbide India Limited (UCIL), but court proceedings revealed that senior management's cost-cutting measures had effectively disabled safety procedures essential to prevent such disasters or alert employees to problems. Dow Chemical has since taken over Union Carbide and also denies responsibility for this disaster. However, because of the tremendous loss of life in Bhopal and because Dow Chemical is much larger than what Union Carbide and its UCIL subsidiary had been, ongoing actions haunted Dow Chemical over many years.

The Bhopal gas leak is an example of how a risk event at a distant and relatively small unit can have disastrous consequences for a major corporation. The risk identification and assessment rules outlined in this chapter would not have accounted for a catastrophe of this magnitude, and each unit in an enterprise needs to recognize the likelihood and consequences of risks at individual unit levels. As noted, a risk event at a small foreign subsidiary can bring down the entire enterprise. Risk management at all levels should recognize that catastrophes can happen, although we never can predict risks of this major consequence; an enterprise should always be aware of the worst disaster that can happen.

This Bhopal incident was much more than an IT-related matter; we have cited it as the type of a major risk that can impact an enterprise. Risk assessment at all levels should be based on two estimates: the relative significance probability and the likelihood of the risk event occurring.

## QUANTITATIVE RISK ANALYSIS TECHNIQUES

There is little value in identifying significant risks unless an enterprise has at least some preliminary plans in place for the action steps necessary if one of the risks is incurred. The idea is to estimate the cost impact of incurring some identified risk and then to apply that cost to a risk factor probability to derive an expected value or cost of the risk. Often this exercise that does not require detailed cost studies with lots of supporting historical trends and estimates. Rather, expected cost estimates should be performed by front-line people at various levels of the enterprise who have a good level of knowledge of the area or risk implications.

The idea here is to go through each of the identified risks—or, if time is limited, only the key risks—and estimate the costs of incurring the risk. Because the kinds of risks discussed involve such matters as the failure of an IT hardware component, the drop in market share, or the impact of a new government regulation, typically they are not the types of costs that one can just look up in a current vendor catalog. Some typical risks, arbitrarily labeled A, B, and C, illustrate this type of thinking:

**Risk A: Loss of up to x% market share due to changing consumer tastes**

- Estimate the reduction in sales and loss of profits due to the x% drop.
- Estimate how much will it cost to begin to restore the lost market position.

**Risk B: Temporary loss of major manufacturing facility for zz days due to major database failure**

- Estimate the best- and worst-case costs to get the database temporarily repaired and back in operation within zz days.
- Estimate the extra labor and production costs incurred during the interim.

**Risk C: Loss of information systems for two days due to pernicious IT network virus**

- Estimate the business and profitability loss during the down period.
- Estimate the cost to transfer operations to the business continuity site.

The above factor examples illustrate the type of thinking needed to estimate the costs of recovering from some risk event. It is often difficult to determine what it would cost to recover from these risks. There is no need to perform detailed, time-consuming analyses. Knowledgeable people who understand the risk area often can provide good estimates on the basis of:

1. What is the best-case cost estimate if it is necessary to incur the risk? This is an assumption that there will be only limited impact if the risk occurs.

2. What would a sample of knowledgeable people estimate for the cost? For Risk A mentioned earlier, the director of marketing might be asked to supply an estimate.
3. What is the expected value or cost of incurring the risk? This is the type of risk that might include some base costs as well as other factors, such as additional labor requirements.
4. What is the worst-case cost of incurring the risk? This is a what-if-everything-goes-wrong type of estimate.

We have suggested using four estimates as an idea of the ranges of costs. However, one best-guess estimate should be selected from the four estimates—usually something between estimates 2 and 3. These estimates and supporting work should be documented, with the selected cost estimate entered as the cost impact on the risk response planning schedule in Exhibit 4.4. These are the same risks that were identified in Exhibit 4.3, but here they are ordered by risk rank. This reordering is important when an enterprise has a long list of identified risks.

The expected value or cost values in Exhibit 4.4 are just the products of the cost impacts and their risk scores. Exhibit 4.4 shows an estimate of what it would cost an enterprise to incur some risk. Although the numbers selected for these samples are very arbitrary, they show how a risk management specialist should interpret this type of analysis. Risk C, for example, has a high likelihood and significance as well as fairly high expected cost to correct. This is the type of risk that management should identify as a candidate for corrective actions. However, the next risk on the schedule, Risk G, also belongs in the upper left-hand quadrant but with a relatively low cost to implement. Management may decide to accept this risk or to develop some other form of remediation plan. Risk H is an example of another risk with a high cost to accept that risk, with its fairly high significance and a low likelihood of occurrence. The numbers shown for Risk H are the kinds where management frequently decides to hope for the best and live with the risk. It will be expensive if management incurs the risk, but it also would be expensive to install corrective action facilities.

| Identified Risk | Significance Probability | Likelihood Probability | Risk Score (P × I) | Rankings | Cost Impact | Expect Cost (Cost × Score) |
|---|---|---|---|---|---|---|
| C | 0.79 | 0.66 | 0.52 | 1 | $ 120,600 | $ 62,881 |
| G | 0.62 | 0.72 | 0.45 | 2 | $ 785,000 | $350,424 |
| I | 0.90 | 0.45 | 0.41 | 3 | $ 15,000 | $ 6,075 |
| D | 0.77 | 0.45 | 0.35 | 4 | $ 27,250 | $ 9,442 |
| E | 0.35 | 0.88 | 0.31 | 5 | $ 52,350 | $ 16,124 |
| F | 0.54 | 0.49 | 0.26 | 6 | $ 1,200 | $ 318 |
| B | 0.88 | 0.24 | 0.21 | 7 | $ 12,650 | $ 2,672 |
| A | 0.55 | 0.30 | 0.17 | 8 | $ 98,660 | $ 16,279 |
| H | 0.66 | 0.20 | 0.13 | 9 | $1,200,980 | $158,529 |
| J | 0.12 | 0.88 | 0.11 | 10 | $ 88,600 | $ 9,356 |

**EXHIBIT 4.4** Risk Ranking Expected Cost Estimate

## IIA AND ISACA RISK MANAGEMENT INTERNAL AUDIT GUIDANCE

Risk management and understanding risks are important elements in both the standards and supporting guidance materials released by the IIA for all internal auditors and ISACA, with its more IT audit focus. Chapter 3 reviewed many of the internal audit standards. This section examines the levels of guidance available to assist IT auditors in their risk-related reviews. Each of these important IT audit professional organizations provides both standards and supporting guidance to help IT auditors to consider risks in their IT audit review activities.

Which standards should the IT audit professional follow? This question was answered somewhat in Chapter 3. The IIA International and ISACA IT Audit Standards are not in conflict with each other and are very similar with regard to risk management. Some chief audit executives (CAEs) and audit committee members are more familiar with the IIA offerings, and that will dictate the standards selection approach. However, if the enterprise has selected *C*ontrol *Ob*jectives for *I*nformation and related *T*echnology (CobiT) as its guidance framework for SOx compliance work, the ISACA standards are the better approach.

### IIA Risk-Related International Standards and Management Guidance

The need to understand and assess risks has been part of the IIA International Standards going back to their earliest versions. Risk concepts are part of both the IIA's Attribute and Performance Standards. For example, the supporting Attribute assurance standard 1220.A3, titled Risk Identification, states:

> Internal auditors must be alert to the significant risks that might affect objectives, operations, or resources. However, assurance procedures alone, even when performed with due professional care, do not guarantee that all significant risks will be identified.

The problem with this standard, however, is that it really does not give much guidance on what is meant by a "significant risk." This lack of definition is one of those issues that has led to the COSO ERM framework and its definition of risk management. Without a clear and consistent understanding, internal auditors may miss key areas of audit risk in their review work.

As discussed in Chapter 3, the IIA International Standards for the Professional Practice of Internal Auditing consist of Attribute Standards that define areas of internal audit activity at a high level and Performance Standards that define minimum requirements for performing all levels of internal audits. There is a full Performance Standard, 2120, along with several assurance and consulting substandards on risk management.

International Professional Practice Standard 2120 on risk management says: "The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes." With a bit more guidance than Assurance substandard 1220.A3, this risk-related IIA International Standard is supported by two Assurance and three Consulting Standards related to risk management:

**2120.A1.** The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the:

- Reliability and integrity of financial and operational information;
- Effectiveness and efficiency of operations;
- Safeguarding of assets; and
- Compliance with laws, regulations, and contracts.

**2120.A2.** The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.

**2120.C1.** During consulting engagements, internal auditors must address risk consistent with the engagement's objectives and be alert to the existence of other significant risks.

**2120.C2.** Internal auditors must incorporate their knowledge of risks gained from consulting engagements into their evaluation of the organization's risk management processes.

**2120.C3.** When assisting management in establishing or improving risk management processes, internal auditors must refrain from assuming any management responsibility by actually managing risks.

The Assurance substandard A1 gives a broader picture of the areas an internal auditor should review and consider with regard to risks. Whether the review is IT related or in other areas, an internal auditor should take a wide view regarding risk exposures. Substandard A2 on fraud risks is the only place where the topic of fraud appears in the IIA international standards. IT audit fraud detection and prevention issues are discussed in Chapter 21.

Chapter 3 discussed the mix of IIA mandatory and strongly recommended guidance materials. One of the recommended guidance materials is an IIA publication in their Guides to the Assessment of IT (GAIT) series titled *GAIT for Business and IT Risk*.[4] This useful guide is available to IIA members. Many of its concepts appear later in this chapter on considering risk when auditing IT-related controls.

## ISACA Audit Risk-Related Standards and Management Guidance

With its focus more on IT audit-related issues, ISACA has taken a stronger position on considering risk issues through its CobiT framework, discussed in Chapter 2, and the ISACA IT Audit Standards. Exhibit 4.5 is the ISACA Audit Standard S11 on the use of risk assessment in audit planning. The exhibit shows the full standard with only a few minor changes (American versus English spelling). It also follows the ISACA format where standards items in bold type are considered to be mandatory for ISACA member IT auditors.

Similar to the IIA International Standards, this standard says that IT auditors should follow a consistent risk evaluation process to plan areas for their audit reviews. ISACA also has a companion audit guideline, G13, with the same title. A fairly detailed guide, it advises that there are many risk assessment methodologies available from which the IT auditor may choose. These range from simple classifications of high, medium, and low, based on the IS auditor's judgment, to complex calculations to

**Introduction**

01 ISACA IT Auditing Standards contain the basic principles and essential procedures, identified in bold type, that are mandatory, together with related guidance.

02 The purpose of this standard is to establish standards and provide guidance regarding the use of risk assessment in audit planning.

**Standard**

**03 The IT auditor should use an appropriate risk assessment technique or approach in developing the overall IT audit plan and in determining priorities for the effective allocation of IT audit resources.**

**04 When planning individual reviews, the IT auditor should identify and assess risks relevant to the area under review.**

**Commentary**

05 Risk assessment is a technique used to examine auditable units in the IS audit universe and select areas for review to include in the IT annual plan that have the greatest risk exposure.

06 An auditable unit is defined as a discrete segment of every organization and its systems.

07 Determination of the IT audit universe should be based on knowledge of the organization's IT strategic plan, its operations, and discussions with responsible management.

08 Risk assessment exercises to facilitate the development of the IT audit plan should be carried out and documented at least on an annual basis. Organizational strategic plans, objectives, and the enterprise risk management framework should be considered as part of the risk assessment exercise.

09 The use of risk assessment in the selection of audit projects allows the IT auditor to quantify and justify the amount of IT audit resources needed to complete the IT audit plan or a particular review. Also, the IT auditor can prioritize scheduled reviews based on perceptions of risk and contribute toward the documentation of risk management frameworks.

10 An IT auditor should carry out a preliminary assessment of the risks relevant to the area under review. IT audit engagement objectives for each specific review should reflect the results of such a risk assessment.

11 Following the completion of the review, the IT auditor should ensure that the organization's enterprise risk management framework or risk register is updated, if one has been developed, to reflect findings and recommendations of the review and subsequent activity.

12 The IT auditor should refer to IT auditing guideline G13, Use of Risk Assessment in Audit Planning, and the IS auditing procedure P1, IS Risk Assessment Measurement.

**EXHIBIT 4.5** ISACA Standard S11 Use of Risk Assessment in Audit Planning

*Source: IT Standards, Guidelines, and Tools and Techniques for Audit Assurance and Control Professionals.* © 2005 ISACA. All rights reserved. Used by permission.

provide numeric risk ratings. IT auditors should consider the level of complexity and detail appropriate for the activity being audited.

IT auditors should include, at a minimum, an analysis, within their methodology, of the risks to the enterprise resulting from the loss of and controls supporting system availability, data integrity, and business information confidentiality. In developing an appropriate risk assessment methodology, IT auditors should consider such things as:

- The type of information required to be collected and the extent to which the information required is already available
- The cost of software licenses required to use the methodology

- The amount of additional information required to be collected before reliable output can be obtained, and the cost of collecting this information (including the time required to be invested in the collection exercise)
- The opinions of other users of the methodology, and their views of how well it has assisted them in improving the efficiency and/or effectiveness of their audits
- The willingness of management to accept the methodology as the means of determining the type and level of audit work carried out

No single risk assessment methodology can be expected to be appropriate in all situations, but IT auditors should reevaluate the appropriateness of their chosen risk assessment methodologies and make changes the can justify as appropriate.

## COSO ERM: ENTERPRISE RISK MANAGEMENT

COSO ERM is a framework to help enterprises have a consistent definition of their risks. It is also an important tool for understanding and improving SOx internal controls. COSO ERM was launched in a manner similar to the development of the COSO internal control framework, as discussed in Chapter 1. Just as there had been no consistent definition of internal controls, industry accounting professionals felt there had been no consistent enterprise-level definition of risk. For example, assessing risks by their likelihood and probability of occurrence is important for IT auditors and other professions, but this method was not universally accepted elsewhere. Similarly, our discussion of IIA and ISACA standards for considering risk really do not fully define what is meant by this concept of enterprise-wide risk for IT auditors and others.

Until recently, there was no commonly accepted definition of *risk management* and no comprehensive framework outlining how the process should work, which made risk communication among board members and management difficult and sometimes frustrating.[5] Similar to the manner in which the COSO internal controls framework was developed, COSO developed an enterprise risk management framework. It was first published just after the enactment of SOx in September 2004. Just as the COSO internal controls framework started by proposing a consistent definition of its subject, the COSO ERM framework document starts by defining enterprise risk management:

> Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in a strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

This definition is rather academic sounding. Professionals should consider the key points supporting this COSO ERM framework definition, including:

- **ERM is a process.** An often misused word, the dictionary definition of a *process* is a "set of actions designed to achieve a result." Although this definition does not provide much help for IT audit professionals, the idea here is that a process is not a static procedure, such as the use of an employee badge to allow only certain authorized persons to enter a locked IT server facility. Such a badge procedure—like a key to a lock—only either allows or does not allow someone entry to the facility. A process tends to be a more flexible arrangement. In a credit approval process, for example, acceptance rules are established with options to alter them, given other considerations. An enterprise might bend the credit rules for an otherwise good credit customer that is experiencing a short-term problem. ERM is that type of process. An enterprise often cannot define its risk management rules through a small, tightly organized rule book. Rather, there should be a series of documented steps to review and evaluate potential risks and to take action based on a wide range of factors across the entire enterprise.

- **ERM process is implemented by people in the enterprise.** An ERM will not be effective if it is implemented only through a set of rules sent in to an operating unit from a distant corporate headquarters, where the people who drafted the rules may have little understanding of the various decision factors that arise. The risk management process must be managed by people who are close enough to the risk situation to understand the various factors surrounding and implications of that risk.
- **ERM is applied through the setting of strategies across the overall enterprise.** Every enterprise is constantly faced with alternative strategies regarding a vast range of potential future actions. Should the entity acquire another complementary business to expand growth or just build internally? Should it adopt a new technology in its manufacturing processes or stick with the tried and true? An effective ERM set of processes should play a major role in helping to establish those alternative strategies. Since many enterprises are large with varied operating units, ERM should be applied across that entire enterprise using a portfolio type of approach that blends a mix of high- and low-risk activities.
- **Concept of risk appetite must be considered.** A newer concept for many, risk appetite is the amount of risk, on a broad level, that an enterprise and its individual managers are willing to accept in their pursuit of value. Risk appetite can be measured in a qualitative sense by looking at risks in such categories as high, medium, or low; alternatively, it can be defined in a qualitative manner. The basic idea behind risk appetite is that every manager and, collectively, every enterprise has some appetite for risk. Some will accept risky ventures that promise potentially high returns while others prefer a more guaranteed-return, low-risk approach. One can think of this appetite for risk concept in terms of an example of two investors. One may prefer to invest in very-low-risk but typically low-return money market or index funds; another may invest in low-cap start-up technology stocks with expectations of very high returns. That latter investor can be described as having a high appetite for risk. As another example, on a street intersection with a Walk or Don't Walk crossing lights, the person who keeps crossing the intersection when the light begins to flash "Walk," meaning it will soon change to "Don't Walk," has a higher appetite for risk.
- **ERM provides only reasonable, not positive, assurance on objective achievements.** The idea here is that an ERM, no matter how well thought out or implemented, cannot provide management or others with any assured

guarantee of outcomes. A well-controlled enterprise, with people at all levels consistently working toward understood and achievable goals, may achieve those objectives period after period, even over multiple years. However, an unintentional human error, an unexpected action by another, or even a natural disaster can occur. Despite an effective ERM process, an enterprise can experience a major and totally unexpected catastrophic event. Reasonable assurance does not provide absolute assurance.

- **ERM is designed to help attain the achievement of objectives.** An enterprise, through its management, should work to establish high-level common objectives that can be shared by all stakeholders. Examples here include such matters as achieving and maintaining a positive reputation within an enterprise's business and consumer communities, providing reliable financial reporting to all stakeholders, and operating in compliance with laws and regulations. The overall ERM program for an enterprise should help it to achieve those objectives.

ERM-related goals and objectives are of little value unless they can be organized and modeled together in a way that management can look at the various aspects of the task and understand—at least sort of—how they interact and relate in a multidimensional manner. This is a real strength of the COSO internal controls framework. It describes, for example, how an enterprise's compliance with regulations impacts all levels of internal controls, from monitoring processes to the control environment, and how that compliance is important for all enterprise entities or units. The COSO ERM framework provides some common definitions of risk management and can help to achieve SOx internal control objectives as well as better risk management processes throughout the enterprise.

Although COSO ERM is designed to provide guidance to the total enterprise, auditors should consider its concepts when performing reviews and assessments at multiple levels. The next sections describe the COSO ERM framework in greater detail. The ERM framework looks very similar to the COSO internal controls framework discussed in Chapter 1, but it has different objectives.

## Key Elements

The COSO internal control framework, has become a worldwide model for describing and defining internal controls and has been the basis for establishing SOx Section 404 compliance. Perhaps because some of the same team members were involved with both COSO internal controls and ERM, the COSO ERM framework—at first glance—looks very similar to the COSO internal controls framework. The COSO ERM framework is also shown in Exhibit 4.6 as a three-dimensional cube with the components of:

- Four vertical columns representing the strategic objectives of enterprise risk.
- Eight horizontal rows or risk components.
- Multiple levels to describe any enterprise, from a ''headquarters'' entity level to individual subsidiaries. Depending on organization size, there can be many ''slices'' of the model here.

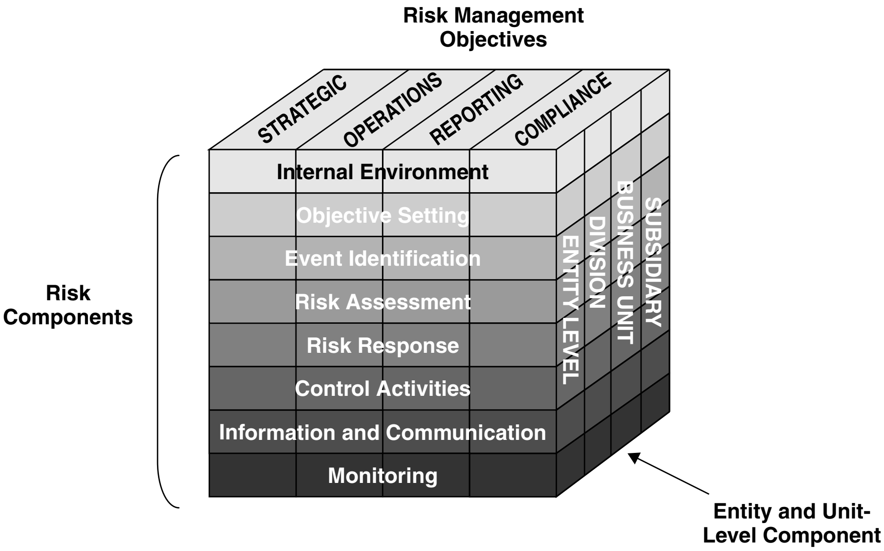

**EXHIBIT 4.6** COSO ERM Framework
*Source:* Robert R. Moeller, *COSO Enterprise Risk Management: Understanding the New Integrated ERM Framework* (Hoboken, NJ: John Wiley & Sons). Copyright © 2007, John Wiley & Sons. Used with permission of John Wiley & Sons.

This section focuses on the front-facing horizontal components of COSO ERM, with brief discussions on COSO ERM's other two dimensions and how they all relate to one another. The concept behind the ERM framework is to provide a model for enterprises to consider and understand their risk-related activities at all levels as well as how these risk components impact one another. An objective of this chapter is to help internal auditors at all levels—from from the CAE to staff IT auditors—to better understand COSO ERM and learn how it can help manage a wide range of risks facing enterprises.

Because the COSO ERM framework diagram looks very similar to the COSO internal controls framework, some have incorrectly viewed COSO ERM as just a new update to their familiar COSO internal controls framework. However, COSO ERM has different objectives and uses. *COSO ERM should not be considered just a new and improved or revised version of the COSO internal control framework.* It is much more. The next sections outline this framework from a risk components perspective.

- **Internal environment component.** Looking at the front of the COSO ERM cube, there are eight levels, with the internal environment component located at the top of ERM framework. The internal environment may be thought of as the capstone to COSO ERM. It holds the framework together. This capstone component is similar to the box at the top of an organization chart that lists the CEO as the designated head of a function. This level defines the basis for all other components in an enterprise's ERM model, influencing how strategies and objectives should be established, how risk-related business activities are structured, and how risks are identified and acted on. The COSO ERM internal environment component consists of these elements:

- **Risk management philosophy.** These are the shared attitudes and beliefs that characterize how the enterprise should consider risk in everything it does. More than a message in a code of conduct, a risk management philosophy is the attitude that should allow stakeholders at all levels to respond to high-risk proposals with an answer along the lines of "No, that's not the kind of venture our company will be interested in."
- **Risk appetite.** Appetite is the amount of risk an enterprise is willing to accept in the pursuit of its objectives. An appetite for risk can be measured in either quantitative or qualitative terms, but all levels of management should have a general understanding of their enterprise's overall risk appetite. The term *appetite* was not often used by internal auditors prior to COSO ERM, but it is a useful expression that describes an overall risk philosophy.
- **Board of director attitudes.** The board and its committees have a very important role in overseeing and guiding an enterprise's risk environment. The independent, outside directors in particular should closely review management actions, ask appropriate questions, and serve as a check and balance control for the enterprise.
- **Integrity and ethical values.** This ERM element requires more than just a published code of conduct and includes a well-thought-out mission statement and integrity standards. There should be a strong corporate culture to guide the enterprise, at all levels, in helping to make risk-based decisions. This area should be an essential component in every ERM framework today.
- **Commitment to competence.** *Competence* refers to the knowledge and skills necessary to perform assigned tasks. Management decides how these critical tasks will be accomplished by developing strategies and assigning the proper people to perform them. With a strong commitment to competence, managers at all levels should take steps to achieve their promised goals.
- **Organization structure.** An enterprise should develop an organization structure with clear lines of authority, responsibility, and appropriate reporting. Every professional has seen situations where an organization does not allow for appropriate lines of communication. There can be many situations in which the organization structure needs improvement to achieve effective ERM.
- **Assignments of authority and responsibility.** This ERM component refers to the degree to which authority and responsibility is assigned or delegated. The trend in many enterprises today is to flatten organizations by eliminating middle management levels. These structures usually encourage employee creativity, faster response times, and greater customer satisfaction. However, this type of customer-facing organization requires strong procedures and rules for the staff as well as ongoing management processes so that lower-level staff decisions can be overruled if necessary. All individuals should know how their actions interrelate and contribute to the overall objectives of the enterprise.

- **Human resource (HR) standards.** Practices regarding employee hiring, training, compensating, promoting, disciplining, and all other actions send messages to staff regarding what is favored, tolerated, or forbidden. When management winks at or ignores some gray-area activities rather than taking a strong stand, that message is usually informally and quickly communicated to others. Strong standards are needed to ensure that HR rules are both communicated to all stakeholders and are enforced.

Other COSO ERM guidance materials include examples of the components necessary to build an effective internal environment. Many refer to the standards and approaches an enterprise should implement to accept and manage various levels of risk; others refer to just good business practices. No matter whether an enterprise has a high or low appetite for risk, it needs to establish control environment practices to manage those risks. For example, the enterprise can give its sales force rather free rein to do deals without much management supervision and approval. Yet everyone should know the legal, ethical, and management policy limits of those free-rein practices. Processes should be in place such that if anyone steps over the line regarding these limits, swift remedial actions are taken and communicated.

The COSO ERM internal environment components of the enterprise's risk management philosophy and its relative appetite for risk feed other elements of the COSO ERM framework. A risk management philosophy is often defined by the board of directors' attitudes and their policies, and the concept risk appetite is often a softer measure, where an enterprise has determined that it will accept some risks but reject others in terms of their likelihood and impact. Exhibit 4.7 shows a risk appetite map illustrating where an enterprise should recognize the range in which it is willing to accept risks in terms of their likelihood and impact. This exhibit says an enterprise may be willing to get involved in a high-negative-impact project if there is a low likelihood of an occurrence. There is a third dimension to this chart as well. An enterprise sometimes will have a greater appetite for a more risky endeavor if there is a higher potential return.

### *Objective-Setting Components*

Ranked below the internal environment in the COSO ERM framework, objective setting outlines important conditions to help management create an effective ERM process. This emphasizes that an enterprise mission statement is a crucial element for setting objectives; it is a general, formal statement of purpose and a building block for the development of specific functional strategies. COSO ERM calls for an enterprise to formally define its goals with a direct linkage to its mission statement, along with measurement criteria to assess whether it is achieving these risk management objectives.

The COSO ERM's objective-setting component should formally define the enterprise's risk appetite in terms of risk tolerance and guidelines whether to accept these risks or not. Establishing and enforcing risk tolerances can be very difficult, if these rules are not clearly defined, well understood, and strictly enforced. An enterprise should

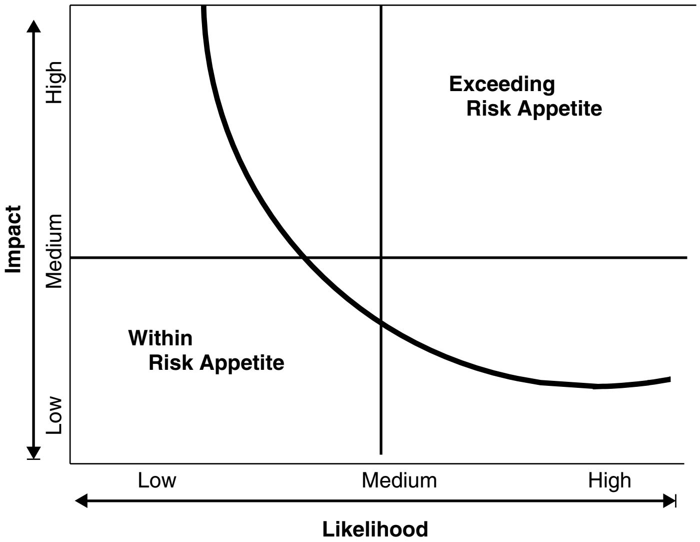

**EXHIBIT 4.7** Risk Appetite Map

*Source:* Robert R. Moeller, *COSO Enterprise Risk Management: Understanding the New Integrated ERM Framework* (Hoboken, NJ: John Wiley & Sons, 2007). Copyright © 2007, John Wiley & Sons. Used with permission of John Wiley & Sons.

establish tolerable ranges of acceptable risks in many areas. For example, products coming off production lines might have acceptable preestablished error rates of no greater than 0.005%. That is an acceptably low error rate in many areas, and production management here would accept the risk of any product warranty claims or damage to the enterprise's reputation if there were errors within that relatively narrow limit. Of course, today's quality assurance emphasis on six sigma programs, as discussed in Chapter 28, brings those tolerance limits much tighter.[6]

The point here is that an enterprise should define its risk-related strategies and objectives and should decide on its appetite and tolerances for these risks. That is, it should determine the level of risks it is willing to accept and, given those risk tolerance rules, how far it is willing to deviate from these preestablished measures. In order to manage and control risks at all levels, an enterprise needs set its objectives and define its tolerances for engaging in risky practices and for adherence to these rules. Things will not work if the enterprise establishes some risk-related objectives but then proceeds to ignore them.

### *Event Identification*

Events are enterprise incidents or occurrences—external or external—that affect the implementation of an ERM strategy and the achievement of its objectives. Although our tendency is to think of events in a negative sense—determining what went wrong—they can be positive as well. Many enterprises today have strong performance monitoring tools in place, monitoring costs, budgets, quality assurance, compliance, and the like. However, going beyond activities on a production assembly line, monitoring processes should include external economic, natural environmental, and political events.

An enterprise needs to clearly define its significant risk events and then have processes in place to monitor them in order to take any necessary appropriate actions. This is a forward-thinking type of process that is often difficult to recognize in many enterprises. Looking at these internal and external potential risk events and deciding which ones require further attention can be a difficult process. Some are immediate needs, and others very future directed. An enterprise should establish processes to review potentially significant risks and then take action.

### *Risk Assessments*

While the internal environment component is COSO ERM's cornerstone, risk assessment processes allow an enterprise to consider the extent to which these potential risk-related events may be considered as part of an enterprise's achievement of its objectives. These risks should be assessed from the likelihood of the risk occurring and its potential impact. A key part of this risk assessment process, however, is the need to consider the inherent and residual risks, as discussed previously.

These two concepts imply that an enterprise will always face some risks. After management has addressed the risks that came out of its risk identification process, some residual risks to remedy still will exist. In addition, there are always some inherent risks where management can do little. As mentioned previously in our discussion of inherent risk, Wal-Mart can take some steps to reduce its inherent risks related to market dominance but can do essentially nothing regarding the inherent risk of a major earthquake.

Risk likelihood and impact are two other key components necessary for performing risk assessments. *Likelihood* is the probability or possibility that a risk will occur. In many instances, this can be a key management assessment stated in the terms of a high, medium, or low likelihood of the risk occurring. There are also some good quantitative tools to develop likelihood estimates, but it does little good to estimate the likelihood of a risk occurring unless there is strong supporting data.

Estimating the *impact* if a risk event occurs is a bit easier. Examples include, for IT-related risks, the impact of a data server and network center catastrophic loss or failure. An enterprise can develop some relatively accurate estimates such as the cost of replacing facilities and equipment, the cost of restoring systems, and the cost of lost business due to the failure. However, the whole concept behind ERM is not to develop precise, actuarial-level calculations regarding these risks but to gain some measure to provide for an effective risk management framework. Those detailed calculations can be delegated to insurance estimators and others.

Risk likelihoods and potential impacts can be analyzed through a series of quantitative and qualitative measures. The idea, however, is to assess all of the identified risks and to rank them in terms of likelihood and impact in a consistent manner. That is, each identified risk can be ranked on an overall relative scale of perhaps 1 to 10, with consideration given to the impact and likelihood of each. Then one can identify the risks that should receive the most thorough management attention.

Overall approaches to reviewing these various likelihood and impact risks need to be considered. Risk assessment is a key component of the COSO ERM framework.

This is where an enterprise evaluates all of the identified risks that might impact its various objectives, considers their potential likelihoods and impacts, considers their interrelationship on a unit-by-unit or total enterprise basis, and then develops strategies for appropriate responses. In some respects, this COSO ERM risk assessment process is not too different from the classic risk assessment techniques that have been used over the years. What is unique is that COSO ERM suggests that an enterprise should take a total approach, across all units and covering all major strategic concerns, to identify its risks in a consistent and thorough manner.

### *Risk Response Strategies*

Having assessed and identified its more significant risks, COSO ERM risk response calls for measured actions to these various identified risks. There should be a careful review of estimated risk likelihoods and potential impacts, with consideration given to associated costs and benefits, to develop appropriate risk response strategies. These risk responses can be handled in any of four basic approaches:

1. Risk **Avoidance.** This is a strategy of walking away from a risk—such as selling a business unit that gives rise to a risk, exiting from a risky geographic area, or dropping a product line. The problem is that enterprises often do not drop a product line or walk away until *after* the risk event has occurred with its associated costs. Unless an enterprise has a very low appetite for risk, it is difficult to walk away from an otherwise successful business area or product line on the basis of a potential future risk. Avoidance can be a costly strategy if investments were made to get into an area with a subsequent pull-out to avoid the risk.

   A collective lessons-learned understanding of past activities often can help with this strategy. If the enterprise had been involved in some area in the past with unfavorable consequences, this may be a good way to avoid the risk once again. With the tendency of constant changes and short employment tenures, this collective history is too often lost and forgotten. An enterprise's well-understood and communicated appetite for risk is perhaps the most important consideration when deciding if a risk avoidance strategy is appropriate.
2. Risk **Reduction.** A wide range of business decisions may be able to reduce certain risks. Product line diversification may reduce the risk of too strong of a reliance on one key product line, or splitting IT operations into two geographically separate locations will reduce the risk of some catastrophic failure. There exists a wide range of often-effective strategies to reduce risks at all levels, going down to the obvious and mundane, such as cross-training employees to reduce the risk of someone departing unexpectedly.
3. Risk **Sharing.** Virtually all enterprises regularly share some of their risks through the purchase of insurance, but other risk-sharing techniques are available as well. For financial transactions, an enterprise can engage in hedging operations to protect from possible price fluctuations, or an enterprise can share potential business risks and rewards through corporate joint venture share-the-risk agreements. The idea is to have another party accept some of a potential risk as well as to share in any resultant rewards.

4. Risk **Acceptance.** This is a strategy of taking no action, such as when an enterprise self-insures by taking no action to reduce a potential risk. Essentially, an enterprise should look at a risk's likelihood and impact in light of its established risk tolerance and then decide whether to accept that risk or not. Acceptance is often an appropriate strategy for some of the risks that an enterprise faces.

Management must develop a general response strategy for each of its risks using an approach built around one or a mixture of the risk avoidance strategies. In doing so, it should consider the costs versus benefits of each potential risk response as well as strategies that best align with the enterprise's overall risk appetite. For example, an enterprise's recognition that the impact of a given risk is relatively low would be balanced against a low risk tolerance that suggests that insurance should be purchased to provide a potential risk response. For many risks, appropriate responses are obvious and almost universally understood. An IT operation, for example, spends the time and resources to back up its key data files and implements a business continuity plan. There are typically no questions regarding the need for these basic approaches, but various levels of management may question the frequency of backup processes or how often the continuity plan needs to be tested. That is, they may question the extent and cost of planned risk prevention measures.

An enterprise should go back to its established risk objectives as well as the tolerance ranges for those objectives. Then it should readdress both the likelihoods and impacts associated with each to develop an overall set of the planned risk responses. This is perhaps the most difficult step in building an effective COSO ERM program. It is comparatively easy to identify a 5% likelihood risk that there will be a fire in the scrap materials bin and then to establish a risk response remedy to install a nearby fire extinguisher. However, responses to most risks are much more complex and require fairly detailed planning and analysis. If there is a risk that an enterprise could lose an entire manufacturing operation due to a key but old equipment plant production failure, potential risk responses might include:

- Acquire backup production equipment to serve as spare parts for cannibalization.
- Shut down the manufacturing production line with plans to move it elsewhere.
- Arrange for a specialized shop to rebuild/reconstruct the old equipment.
- Reengineer the manufactured product along with plans for new product introduction.

Developing risk responses requires a significant amount of planning and strategic thinking. For example, one of the response strategies just mentioned is to acquire a set of backup equipment. If that is to be the approved strategy, action must be taken to acquire the backup equipment before this activity can even be identified as an actual risk response strategy. The idea is that all risks listed on such an analysis should be measured against the same impact factors, based on an accept, avoid, share, or reduce risks strategy.

COSO ERM calls for risks to be considered and evaluated on an entity- or portfolio-wide basis. This can be a difficult process in a large, multi-unit, multiproduct enterprise, but it provides a starting point in getting the various risks organized for identification of more significant risks that may impact the enterprise. The idea here is to look at these various potential risks, their probability of occurrence, and the impacts of each. A good analysis here should highlight areas for more detailed attention.

### *Control Activities*

COSO ERM's control activities are the policies and procedures necessary to ensure action on identified risk responses. Although some of these activities may relate to an identified and approved risk response in only one area of the enterprise, they often overlap across multiple functions and units. The control activities component of COSO ERM should be tightly linked with the risk response strategies and actions previously discussed.

Having selected appropriate risk responses, an enterprise should select control activities necessary to ensure that these control activities are executed in a timely and efficient manner. The process of determining if control activities are performing properly is very similar to completing SOx Section 404 internal control assessments, as discussed in Chapter 1. COSO ERM calls for approaches of identifying, documenting, testing, and then validating these risk protection controls. Many control activities under the COSO internal controls framework are fairly easy to identify and test, including these internal control areas:

- **Separation of duties.** Essentially, the person who initiates a transaction should not be the same person who authorizes that transaction. This area is discussed in Chapter 6 on IT general controls.
- **Audit trails.** Processes should be organized such that final results can be easily traced back to the transactions that created them. This area is particularly important for reviews of IT applications, as discussed in Chapter 10.
- **Security and integrity.** Control processes should have appropriate control procedures such that only authorized persons can review or modify them. IT security controls are discussed in Chapter 19.
- **Documentation.** Processes should be appropriately documented. Chapter 12 discusses the importance of IT documentation and records management systems.

These well-recognized control procedures are applicable to all IT internal control processes and apply to many risk-related events. Many IT professionals—whether they have an accounting and auditing background or not—often can easily define some of these key controls, which are necessary in most business processes. For example, if asked to identify the types of internal controls that should be built into an accounts payable system, many would identify the significant control points that checks issued from the system must be authorized by independent persons, that accounting records must be in place to keep track of the checks issued, and that the check-issuing process should be such that only authorized persons can initiate such transactions. These are generally well widely understood internal control procedures. An enterprise often faces a more difficult task in identifying control activities to support its ERM framework. Although there is no accepted or standard set of ERM control activities at this time, the COSO ERM documentation suggests several areas:

- **Top-level reviews.** Senior management should be very aware of the identified risk events within their organizational units and perform regular top-level reviews on the status of identified risks.
- **Direct functional or activity management.** In addition to top-level reviews, supporting unit managers should have a key role in risk control activity monitoring.
- **Information processing.** Whether it is IT systems and processes or softer forms such as paper-based or messages, information processing represents a key component in an enterprise's risk-related control activities. Appropriate control procedures should be established with an emphasis on enterprise IT processes and risks.
- **Physical controls.** Many risk-related concerns involve physical assets, such as IT equipment, inventories, securities, and physical plants. Whether it is dealing with physical inventories, inspections, or plant security procedures, an enterprise should install appropriate risk-based physical control activity procedures.
- **Performance indicators.** The typical enterprise today employs a wide range of financial and operational reporting tools that can also support risk event–related performance reporting. Where necessary, performance tools should be modified to support this important COSO ERM control activity component.
- **Segregation of duties.** Segregation of duties is a classic control activity: The person who initiates certain actions should not be the same person who approves them.

These control activities can be expanded to cover other key areas. Some will be specific to individual units within the enterprise, but each control activity, singly and collectively, should be important components of supporting the enterprise's ERM framework. The next sections describe control activities from many perspectives of IT operations.

### *Information and Communication*

This COSO ERM component links together each of the other components. For example, the risk response component receives residual and inherent risk inputs from risk assessment as well as risk tolerance support from the objective-setting component. COSO ERM risk response then provides risk response and risk portfolio data to control activities as well as feedback to the risk assessment.

Although it is relatively easy to describe how information should be communicated from one COSO ERM component to another in a simple flow diagram, in practice the process is far more complex. Many enterprises have a complex web of operational and financial information systems for their basic processes that often are not very well linked. These linkages become even more complex for many ERM processes, given that many basic enterprise applications do not lend themselves directly to processes for risk identification, assessment, and risk response. Going beyond a comprehensive ERM information application for an enterprise, there is a need to develop risk monitoring and communications systems that link with customers, suppliers, and other stakeholders.

The information half of the ERM information and communication component is normally thought of in terms of IT strategic and operational information systems. ERM communication is the second aspect of this component. It talks about communication beyond just IT applications, such as the need for mechanisms to ensure that all stakeholders receive messages regarding the enterprise's interest in managing its risks abs using a common risk language throughout the enterprise. COSO ERM will be of little value to an enterprise unless the overall message of its importance is communicated to all stakeholders in a common and consistent manner.

### *Monitoring Component*

Placed at the base of the stack of ERM framework model components shown in Exhibit 4.6, monitoring processes are necessary to determine that all installed ERM components work effectively. People in the enterprise change, as do supporting processes and internal and external conditions, but the monitoring component helps ensure that ERM is working effectively on a continuous basis. The monitoring component should include processes to flag exceptions or violations in other components of the ERM process. For example, an IT accounts receivable billing system should identify the overall financial and operational risks if customer bills are not paid on a timely basis. An ongoing—almost real-time—credit collections monitoring tool could provide senior management with day-to-day and trending data on the status of collections. Dashboard monitoring tools, discussed in Chapter 14, are types of ERM monitors that can work on a continuous basis.

Going beyond IT dashboard tools, enterprise management should take an overall responsibility for ERM monitoring. In order to establish an effective ERM framework, monitoring should include ongoing reviews of the overall ERM process, ranging from identified objectives to the progress of ongoing ERM control activities.

Separate or individual evaluation monitoring processes refers to detailed reviews of individual risk processes by a qualified reviewer, such as internal or IT audit. Here the review can be limited to specific areas or cover the entire ERM process for an enterprise unit. Internal audit is often the best internal source to perform such specific ERM reviews. The role of internal audit in the ERM process and its role in monitoring, in particular, is discussed in the next sections.

## Other Dimensions of COSO ERM: Risk Management Objectives

Although much of our COSO ERM discussion here is on the front-facing side of the three-dimensional framework, the two other dimensions—the operational and organizational levels—should always be considered as well. Each component of COSO ERM operates in this three-dimensional space, where each must be considered in terms of the other related categories. The top-facing components of strategic, operations, reporting, and compliance risk objectives are important for understanding and implementing COSO ERM. In addition, although Exhibit 4.6 shows each of these top-facing risk objectives as having the same relative size, the category of operations-level risk objectives is often viewed as a much broader and higher-exposure risk category than the others.

As an example, the top-facing component of the three-dimensional ERM framework, the operations-level risk objective, calls for the identification of risks for each enterprise unit or component. Identification of these risk objectives often requires detailed information gathering and analysis, particularly for a larger enterprise covering multiple geographic areas, product lines, or business processes. Of course, IT operations are usually a major component here. In order to gather more detailed background information on potential operations risks, an internal audit survey of direct on-the-floor members of the enterprise, along with follow-up questions, should survey potential operations risks across all levels of the enterprise. This type of survey is similar to the types of questions often used in other IT audit internal control assessments.

With COSO ERM's portfolio view of risks, an enterprise should avoid rolling things up to too much of a summary level, missing or rounding off important lower-level risks. Managers at all levels should be aware that they are responsible for accepting and managing the risks within their own operational units. Too often, unit managers believe that risk management is of concern only to some senior-level, headquarters type. The importance of COSO ERM and operations risk management should be communicated to all levels of an enterprise. Internal and IT auditors should act as eyes and ears here and report all observed operations risks.

### *Reporting Risk Management Objectives*

This risk objective covers the reliability of an enterprise's reporting, including the internal and external reporting of financial and nonfinancial data. Accurate reporting is critical to an enterprise's success in many dimensions. News reports often relate the discovery of inaccurate corporate financial reporting and the resultant stock market repercussions for the offending entity; that same inaccurate reporting can cause problems in many areas.

No matter what the industry, an enterprise faces major risks from inaccurate reporting. Operating units must make certain that reported results are correct before they are passed up to the next level in the organization, and consolidated numbers must be accurate, whether on financial reports, tax returns, or any of a myriad of other areas. Although good internal controls are necessary to ensure accurate reporting, COSO ERM is concerned about the risk of authorizing and releasing inaccurate reports. Strong internal controls should minimize the risk of errors, and an enterprise should always consider the risks associated with inaccurate reporting. Small errors and discrepancies can be ignored over time until a major error needs to be disclosed. The risk of such inaccurate reporting should be a concern at all levels of the enterprise.

### *Legal and Regulatory Compliance Risk Objectives*

Every enterprise has requirements to comply with a wide range of laws, government-imposed regulations, or industry standards. Although compliance risks can be monitored and recognized, legal risks are sometimes totally unanticipated. In the United States, for example, an aggressive plaintiff legal system can pose a major risk to otherwise well-intentioned enterprises. Asbestos litigation during the 1990s and beyond is an example. A fibrous mineral, asbestos has three extraordinary characteristics: It works as an insulator for heat and electricity; it resists other dangerous chemicals; and, when inhaled, it has been found to cause illnesses that may take decades to develop. Asbestos is a natural insulation material that previously was used extensively in building materials and was considered totally benign. Too much direct contact with asbestos fibers over time, however, can cause severe lung problems and even death. Underground miners extracting asbestos have met that fate. However, in the past, asbestos was used in many products, such as wrappers to insulate heating pipes or as fire protection wall barriers. The risks to persons working or living in a structure with these asbestos-sealed pipes are minimal, but aggressive litigators have brought actions against corporations, claiming that anyone who could have had any contact, no matter how minimal, with a product that used asbestos could be at risk sometime in the future. The result was litigation directed against companies that had manufactured products containing some asbestos, calling for damages based on potential human risks in future years. Because of huge damage awards, virtually all major corporations that once used asbestos have gone bankrupt or out of business, or have had to pay huge court-imposed damage losses. This is the type of legal risk that is very difficult to anticipate but that can be disastrous to an enterprise.

COSO ERM recommends that compliance-related risks be considered for each of the risk framework components, whether in the context of the internal environment, objective setting, or risk monitoring, as well as across the enterprise. The COSO ERM guidance material does not offer much additional material on this compliance objective other than to state that it refers to conformance with applicable laws and regulations. These COSO ERM elements are important components of the risk management framework that need to be communicated and understood.

All enterprises face a wide range of legal and regulatory compliance requirements; some impact virtually all enterprises, and others are related to only single business units in a specialized industry sector. The nature of those compliance risks needs to be communicated and understood through all levels of an enterprise. This is an area where an enterprise may accept a certain level of risk in terms of its concerns regarding legal compliance. Although an enterprise should not deliberately ignore a major law because of a feeling it never will be caught, it should always take a reasoned approach to risks in conjunction with its overall philosophy and risk appetites. For example, many regulatory rules specify that all expenditures over US$25 must be supported by a receipt. Although there usually are no reasonableness guidelines here, another enterprise could decide that "all expenditures" goes down to an employee travel expenses of less than $1.00, while another will require receipts for anything above $25.00. The latter enterprise has made a decision that the costs of documenting small expenditures is greater than any fine it might receive if caught in a regulatory compliance issue. This type of a risk-related decision is similar to the SOx Auditing Standard No. 5 on financial internal controls rules discussed in Chapter 1. In order to manage and establish legal and regulatory risk objectives, the board of directors, the CEO, and members of management need to have an understanding of the nature and extent of all of the regulatory risks the enterprise faces. The legal department, key managers, internal audit, and others can help in assembling this information. There are many regulatory