COSO The Committee of Sponsoring Organizations of the Treadway Commission

Enterprise Risk Management Framework

➢ Executive Summary

DRAFT

Committee of Sponsoring
Organizations of the
Treadway Commission

Exposure Draft for Public Comment

To submit comments on this document, please visit
www.erm.coso.org

[This page intentionally left blank]

Committee of Sponsoring Organizations of the Treadway Commission (COSO)

Oversight	**Representative**
Committee of Sponsoring Organizations of the Treadway Commission	John J. Flaherty, Chair
American Institute of Certified Public Accountants	Alan W. Anderson
The Institute of Internal Auditors	William G. Bishop, III
Financial Executives International	John P. Jessup
Institute of Management Accountants	Frank C. Minter Dennis L. Neider
American Accounting Association	Larry E. Rittenberg

Project Advisory Council to COSO

Guidance

Tony Maki, Chair
Partner
Moss Adams LLP

Mark S. Beasley
Associate Professor
North Carolina State University

Jerry W. DeFoor
VP and Controller
Protective Life Corporation

James W. DeLoach
Managing Director
Protiviti Inc.

Andrew J. Jackson
Assistant General Auditor
General Motors

Steven E. Jameson
Lead Auditing Specialist
World Bank

John P. Jessup
VP Finance and Controller
E. I. DuPont de Nemours & Company

Tony M. Knapp
Senior VP and Controller
Motorola, Inc.

Douglas F. Prawitt
Associate Professor
Brigham Young University

PricewaterhouseCoopers LLP

Author

Principal Contributors

Richard M. Steinberg
Past Partner, Corporate Governance Leader

Frank J. Martens
Senior Manager
Vancouver, Canada

Miles E.A. Everson
Partner
New York

Lucy E. Nottingham
Manager
Boston

[This page intentionally left blank]

EXECUTIVE SUMMARY

Managements of some companies and other entities have developed processes to identify and manage risk across the enterprise, and many others have begun development or are considering doing so. While considerable information on enterprise risk management is available, including much published literature, no common terminology exists, and there are few if any widely accepted principles that can be used by management as a guide in developing an effective risk management architecture.

Recognizing the need for definitive guidance on enterprise risk management, The Committee of Sponsoring Organizations of the Treadway Commission (COSO) initiated a project to develop a conceptually sound framework providing integrated principles, common terminology and practical implementation guidance supporting entities' programs to develop or benchmark their enterprise risk management processes. A related objective is for this resulting framework to serve as a common basis for managements, directors, regulators, academics and others to better understand enterprise risk management, its benefits and limitations, and to effectively communicate about enterprise risk management issues.

This Executive Summary sets out key elements of the *Enterprise Risk Management Framework*, including the definition, components and underlying principles of enterprise risk management, as well as its benefits and limitations and roles and responsibilities of various parties. This summary also highlights the relevance of enterprise risk management and its relationship to COSO's *Internal Control – Integrated Framework*. Those parties desiring more in-depth knowledge are referred to the full *Enterprise Risk Management Framework* document.

Relevance of Enterprise Risk Management

The underlying premise of enterprise risk management is that every entity, whether for-profit, not-for-profit, or a governmental body, exists to provide value for its stakeholders. All entities face uncertainty, and the challenge for management is to determine how much uncertainty the entity is prepared to accept as it strives to grow stakeholder value. Uncertainty presents both risk and opportunity, with the potential to erode or enhance value. Enterprise risk management provides a framework for management to effectively deal with uncertainty and associated risk and opportunity and thereby enhance its capacity to build value.

Uncertainty

Enterprises operate in environments where factors such as globalization, technology, regulation, restructurings, changing markets, and competition create uncertainty. Uncertainty emanates from an inability to precisely determine the likelihood that potential events will occur and the associated outcomes.

Value

Value is created, preserved or eroded by management decisions ranging from strategy setting to operating the enterprise day-to-day. Inherent in decisions is recognition of risk and opportunity, requiring that management[1] considers information about internal and external environments, deploys precious resources and recalibrates enterprise activities to changing circumstances.

Entities realize value when stakeholders derive recognizable benefits that they in turn value. For companies, shareholders realize value when they recognize value creation from share-value growth. For governmental entities, value is realized when constituents recognize receipt of valued services at an acceptable cost. Stakeholders of not-for-profit entities realize value when they recognize receipt of valued social benefits. Enterprise risk management facilitates management's ability to both create sustainable value and communicate the value created to stakeholders.

Benefits of Enterprise Risk Management

No entity operates in a risk-free environment, and enterprise risk management does not create such an environment. Rather, enterprise risk management enables management to operate more effectively in environments filled with risks.

Enterprise risk management provides enhanced capability to:

- **Align risk appetite and strategy –** Risk appetite is the degree of risk, on a broad-based level, that a company or other entity is willing to accept in pursuit of its goals. Management considers the entity's risk appetite first in evaluating strategic alternatives, then in setting objectives aligned with the selected strategy and in developing mechanisms to manage the related risks.
- **Link growth, risk and return –** Entities accept risk as part of value creation and preservation, and they expect return commensurate with the risk. Enterprise risk management provides an enhanced ability to identify and assess risks, and establish acceptable levels of risk relative to growth and return objectives.
- **Enhance risk response decisions –** Enterprise risk management provides the rigor to identify and select among alternative risk responses – risk avoidance, reduction, sharing and acceptance. Enterprise risk management provides methodologies and techniques for making these decisions.
- **Minimize operational surprises and losses –** Entities have enhanced capability to identify potential events, assess risk and establish responses, thereby reducing the occurrence of surprises and related costs or losses.

[1] While the term "management" is used in this and later discussions, many enterprise risk management activities are performed by non-management personnel.

- **Identify and manage cross-enterprise risks –** Every entity faces a myriad of risks affecting different parts of the organization. Management needs to not only manage individual risks, but also understand interrelated impacts.
- **Provide integrated responses to multiple risks –** Business processes carry many inherent risks, and enterprise risk management enables integrated solutions for managing the risks.
- **Seize opportunities –** Management considers potential events, rather than just risks, and by considering a full range of events, management gains an understanding of how certain events represent opportunities.
- **Rationalize capital –** More robust information on an entity's total risk allows management to more effectively assess overall capital needs and improve capital allocation.

Enterprise risk management is not an end in itself, but rather an important means. It cannot and does not operate in isolation in an entity, but rather is an enabler of the management process. Enterprise risk management is interrelated with corporate governance by providing information to the board of directors on the most significant risks and how they are being managed. And, it interrelates with performance management by providing risk-adjusted measures, and with internal control, which is an integral part of enterprise risk management.

Enterprise risk management helps an entity achieve its performance and profitability targets, and prevent loss of resources. It helps ensure effective reporting. And, it helps ensure that the entity complies with laws and regulations, avoiding damage to its reputation and other consequences. In sum, it helps an entity get to where it wants to go and avoid pitfalls and surprises along the way.

Enterprise Risk Management Defined

Enterprise risk management is defined as follows:

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

This definition reflects certain fundamental concepts. Enterprise risk management:

- Is a *process* – it's a means to an end, not an end in itself
- Is *effected by people* – it's not merely policies, surveys and forms, but involves people at every level of an organization
- Is *applied in strategy setting*

- Is *applied across the enterprise,* at every level and unit, and includes taking an entity-level portfolio view of risks
- Is designed to identify events potentially affecting the entity and manage risk within its *risk appetite*
- Provides *reasonable assurance* to an entity's management and board
- Is geared to the *achievement of objectives* in one or more separate but overlapping categories.

This definition is purposefully broad for several reasons. It captures key concepts fundamental to how companies and other organizations manage risk, providing a basis for application across different types of organizations, industries and sectors. It focuses directly on achievement of entity objectives. And, the definition provides a basis for defining enterprise risk management effectiveness. The fundamental concepts outlined above are discussed in the following paragraphs.

A Process

Enterprise risk management is not one event or circumstance, but a series of actions that permeate an entity's activities. These actions are pervasive and inherent in the way management runs the business.

Enterprise risk management is different from the perspective of some observers who view it as something added on to an entity's activities, or as a necessary burden. That is not to say effective enterprise risk management does not require incremental effort. For instance, risk assessment may require incremental effort to develop needed models and make necessary analysis and calculations. However, these and other enterprise risk management mechanisms are intertwined with an entity's operating activities and exist for fundamental business reasons. Enterprise risk management is most effective when these mechanisms are built into the entity's infrastructure and are part of the essence of the enterprise. By building in enterprise risk management, an entity can directly affect its ability to implement its strategy and achieve its vision or mission.

Building in enterprise risk management also has important implications for cost containment, especially in the highly competitive marketplaces many companies face. Adding new procedures separate from existing ones adds costs. By focusing on existing operations and their contribution to effective enterprise risk management, and integrating risk management into basic operating activities, an enterprise can avoid unnecessary procedures and costs. And, a practice of building enterprise risk management into the fabric of operations helps identify new opportunities for management to seize in growing the business.

Effected by People

Enterprise risk management is effected by a board of directors, management and other personnel. It is accomplished by the people of an organization, by what they do and say.

People establish the entity's mission/vision, strategy and objectives and put enterprise risk management mechanisms in place.

Similarly, enterprise risk management affects people's actions. Enterprise risk management recognizes that people do not always understand, communicate or perform consistently. Each individual brings to the workplace a unique background and technical ability, and has different needs and priorities.

These realities affect, and are affected by, enterprise risk management. Each person has a unique point of reference which influences how they identify, assess and respond to risk. Enterprise risk management provides the mechanisms needed to help people understand risk in the context of the entity's objectives. People must know their responsibilities and limits of authority. Accordingly, a clear and close linkage needs to exist between people's duties and the way in which they are carried out, as well as with the entity's strategy and objectives.

An organization's people include the board of directors, as well as management and other personnel. Although directors primarily provide oversight, they also provide direction and approve strategy and certain transactions and policies. As such, boards of directors are an important element of enterprise risk management.

Applied in Setting Strategy

An entity sets out its mission or vision and establishes strategic objectives, which are the high-level goals that align with and support its vision or mission. An entity establishes a strategy for achieving its strategic objectives. It also sets related objectives it wants to achieve, flowing from the strategy, cascading to business units, divisions and processes. In setting strategy, management considers risks relative to alternative strategies.

Applied Across the Enterprise

To successfully apply enterprise risk management, an entity must consider its entire scope of activities. Enterprise risk management considers activities at all levels of the organization, from enterprise-level activities such as strategic planning and resource allocation, to business unit activities such as marketing and human resources, to business processes such as production and new customer credit review. Enterprise risk management also applies to special projects and new initiatives that might not yet have a designated place in the entity's hierarchy or organization chart.

Enterprise risk management requires an entity to take a *portfolio view* of risk. This might involve each manager responsible for a business unit, function, process or other activity developing an assessment of risk for the unit. The assessment may be quantitative or qualitative. With a composite view at each succeeding level of the organization, senior management is positioned to make a determination whether the entity's overall risk profile is commensurate with its risk appetite.

Management considers interrelated risks from an entity-level portfolio perspective. Interrelated risks need to be identified and acted upon to bring the entirety of risk within the entity’s risk appetite. Risks for individual units of the entity may be within the units’ risk tolerances, but taken together may exceed the risk appetite of the entity as a whole. The overall risk appetite is reflected downstream in an entity through risk tolerances established for specific objectives.

Risk Appetite

Risk appetite is the amount of risk an entity is willing to accept in pursuit of value. Entities often consider risk appetite qualitatively, with such categories as high, moderate or low, or they may take a quantitative approach, reflecting and balancing goals for growth, return and risk.

Risk appetite is directly related to an entity’s strategy. It is considered in strategy setting, where the desired return from a strategy should be aligned with the entity’s risk appetite. Different strategies will expose the entity to different risks. Enterprise risk management, applied in strategy setting, helps management select a strategy consistent with the entity’s risk appetite.

The entity’s risk appetite guides resource allocation. Management allocates resources across business units with consideration of the entity’s risk appetite and individual business units’ strategy for generating a desired return on invested resources. Management considers its risk appetite as it aligns its organization, people and processes, and designs infrastructure necessary to effectively respond to and monitor risks.

Risk tolerances are the acceptable level of variation relative to the achievement of objectives. In setting specific risk tolerances, management considers the relative importance of the related objectives and aligns risk tolerances with its risk appetite. Operating within risk tolerances provides management greater assurance that the entity will remain within its risk appetite and, in turn, provides a higher degree of comfort that the entity will achieve its objectives.

Provides Reasonable Assurance

Well-designed and operated enterprise risk management can provide management and the board of directors reasonable assurance regarding achievement of an entity's objectives. As a result of enterprise risk management determined to be effective, in each of the categories of entity objectives, the board of directors and management gain reasonable assurance that:

- They understand the extent to which the entity’s strategic objectives are being achieved,
- They understand the extent to which the entity's operations objectives are being achieved,

- The entity's reporting is reliable, and
- Applicable laws and regulations are being complied with.

Reasonable assurance reflects the notion that uncertainty and risk relate to the future, which no one can predict with certainty. Limitations also result from the realities that human judgment in decision making can be faulty, decisions on risk responses and establishing controls need to consider the relative costs and benefits, breakdowns can occur because of human failures such as simple errors or mistakes, controls can be circumvented by collusion of two or more people, and management has the ability to override enterprise risk management decisions. These limitations preclude a board and management from having absolute assurance that objectives will be achieved.

Achievement of Objectives

Effective enterprise risk management can be expected to provide reasonable assurance of achieving objectives relating to the reliability of reporting and to compliance with laws and regulations. Achievement of those categories of objectives is within the entity's control and depends on how well the entity's related activities are performed.

However, achievement of strategic and operations objectives is not always within the entity's control. For these objectives, enterprise risk management can provide reasonable assurance only that management, and the board in its oversight role, are made aware, in a timely manner, of the extent to which the entity is moving toward achievement of the objectives.

Components of Enterprise Risk Management

Enterprise risk management consists of eight interrelated components. These are derived from the way management runs a business, and are integrated with the management process. The components are:

Internal Environment

The entity's internal environment is the foundation for all other components of enterprise risk management, providing discipline and structure. The internal environment influences how strategy and objectives are established, business activities are structured and risks are identified, assessed and acted upon. It influences the design and functioning of control activities, information and communication systems, and monitoring activities. The internal environment comprises many elements, including an entity's ethical values, competence and development of personnel, management's operating style and how it assigns authority and responsibility. A board of directors is a critical part of the internal environment and significantly influences other internal environment elements. As part of the internal environment, management establishes a risk management philosophy, establishes the entity's risk appetite, forms a risk culture and integrates enterprise risk management with related initiatives.

An enterprise risk management philosophy that is understood by all personnel facilitates employees' ability to recognize and effectively manage risk. The philosophy – the entity's beliefs about risk and how it chooses to conduct its activities and deal with risk – reflects the value the entity seeks from enterprise risk management and influences how enterprise risk management components will be applied. Management communicates its enterprise risk management philosophy to employees through policy statements and other communications. Importantly, management reinforces the philosophy not only with words but with everyday actions as well.

Risk appetite, established by management and reviewed by the board of directors, is a guidepost in strategy setting. Usually any of a number of different strategies can be designed to achieve desired growth and return goals, each having different associated risks. Enterprise risk management, applied in strategy setting, helps management select a strategy consistent with its risk appetite. Management looks to align the organization, people, processes and infrastructure to facilitate successful strategy implementation and enable the entity to stay within its risk appetite.

Risk culture is the set of shared attitudes, values and practices that characterize how an entity considers risk in its day-to-day activities. For many companies, the risk culture flows from the entity's risk philosophy and risk appetite. For those entities that do not explicitly define their risk philosophy, the risk culture may form haphazardly, resulting in significantly different risk cultures within an enterprise or even within a particular business unit, function or department.

Objective Setting

Within the context of the established mission or vision, management establishes strategic objectives, selects strategy and establishes related objectives, cascading through the enterprise and aligned with and linked to the strategy. Objectives must exist before management can identify events potentially affecting their achievement. Enterprise risk management ensures that management has a process in place to both set objectives and align the objectives with the entity's mission/vision and are consistent with the entity's risk appetite.

Entity objectives can be viewed in the context of four categories:

- **Strategic –** relating to high-level goals, aligned with and supporting the entity's mission/vision.
- **Operations –** relating to effectiveness and efficiency of the entity's operations, including performance and profitability goals. They vary based on management's choices about structure and performance.

- **Reporting –** relating to the effectiveness of the entity's reporting. They include internal and external reporting and may involve financial or non-financial information.
- **Compliance –** relating to the entity's compliance with applicable laws and regulations.

This categorization of entity objectives allows management and the board to focus on separate aspects of enterprise risk management. These distinct but overlapping categories – a particular objective can fall under more than one category – address different entity needs and may be the direct responsibility of different executives. This categorization also allows distinguishing between what can be expected from each category of objectives.

Some entities use another category of objectives, "safeguarding of resources," sometimes referred to as "safeguarding of assets." Viewed broadly, these deal with prevention of loss of an entity's assets or resources, whether through theft, waste, inefficiency or what turns out to be simply bad business decisions - such as selling product at too low a price, failing to retain key employees or prevent patent infringement, or incurring unforeseen liabilities. This broad-based safeguarding of assets category may be narrowed for certain reporting purposes, where the safeguarding concept applies only to the prevention or timely detection of unauthorized acquisition, use, or disposition of the entity's assets.

Event Identification

Management recognizes that uncertainties exist – that it cannot know with certainty whether and when an event will occur, or its outcome should it occur. As part of event identification, management considers external and internal factors that affect event occurrence. External factors include economic, business, natural environment, political, social and technological factors. Internal factors reflect management's choices and include such matters as infrastructure, personnel, process and technology.

An entity's event identification methodology may comprise a combination of techniques together with supporting tools. Event identification techniques look to both the past and the future. Techniques that focus on past events and trends consider such matters as payment default histories, changes in commodity prices and lost-time accidents. Techniques that focus on future exposures consider such matters as shifting demographics, new markets and competitor actions.

It may be useful to group potential events into categories. By aggregating events horizontally across an entity and vertically within operating units, management develops an understanding of the interrelationships between events, gaining enhanced information as a basis for risk assessment.

Events potentially have a negative impact, a positive impact or both. Events that have a potentially negative impact represent risks, which require management's assessment and response. Accordingly, risk is defined as the possibility that an event will occur and adversely affect the achievement of objectives.

Events with a potentially positive impact represent opportunities or offset the negative impact of risks. Events representing opportunities are channeled back to management's strategy or objective-setting processes, so that actions can be formulated to seize the opportunities. Events potentially offsetting the negative impact of risks are considered in management's risk assessment and response.

Risk Assessment

Risk assessment allows an entity to consider how potential events might affect the achievement of objectives. Management assesses events from two perspectives: likelihood and impact.

Likelihood represents the possibility that a given event will occur, while impact represents its effect should it occur. Estimates of risk likelihood and impact often are determined using data from past observable events, which may provide a more objective basis than entirely subjective estimates. Internally generated data based on an entity's own experience may reflect less subjective personal bias and provide better results than data from external sources. However, even where internally generated data are a primary input, external data can be useful as a checkpoint or to enhance the analysis. Users must be cautious when using past events to make predictions about the future, as factors influencing events may change over time.

An entity's risk assessment methodology normally comprises a combination of qualitative and quantitative techniques. Management often uses qualitative assessment techniques where risks do not lend themselves to quantification or when sufficient credible data required for quantitative assessments either are not practicably available or obtaining or analyzing data are not cost-effective. Quantitative techniques typically bring more precision and are used in more complex and sophisticated activities to supplement qualitative techniques. An entity need not use common assessment techniques across all business units. Rather, the choice of techniques should reflect the need for precision and the culture of the business unit. In any event, the methods used by individual business units should facilitate the entity's assessment of risks across the entity.

Management often uses performance measures in determining the extent to which objectives are being achieved. It may be useful to use the same unit of measure when considering the potential impact of a risk to the achievement of a specified objective.
Management may assess how events correlate, where sequences of events combine and interact to create significantly different probabilities or impacts. While the impact of a single

event might be slight, a sequence of events might have more significant impact. Where potential events are not directly related, management assesses them individually; where risks are likely to occur within multiple business units, management may assess and group identified events into common categories.

There is usually a range of possible results associated with a potential event, and management considers them as a basis for developing a risk response. Through risk assessment, management considers the positive and negative consequences of potential events, individually or by category, across the entity.

Because risks are assessed in the context of an entity's strategy and objectives, management often tends to focus on risks with short- to mid-term time horizons. However, some elements of strategic direction and objectives extend to the longer term. As a result, management needs to be cognizant of the longer timeframes, and not ignore risks that might be further out.

Risk assessment is applied first to inherent risk – the risk to the entity in the absence of any actions management might take to alter either the risk's likelihood or impact. Once risk responses have been developed, management then uses risk assessment techniques in determining residual risk – the risk remaining after management's action to alter the risk's likelihood or impact.

Risk Response

Management identifies risk response options and considers their effect on event likelihood and impact, in relation to risk tolerances and costs versus benefits, and designs and implements response options. The consideration of risk responses and selecting and implementing a risk response are integral to enterprise risk management. Effective enterprise risk management requires that management select a response that is expected to bring risk likelihood and impact within the entity's risk tolerance.

Risk responses fall within the categories of risk avoidance, reduction, sharing and acceptance. Avoidance responses take action to exit the activities that give rise to the risks. Reduction responses reduce the risk likelihood, impact, or both. Sharing responses reduce risk likelihood or impact by transferring or otherwise sharing a portion of the risk. Acceptance responses take no action to affect likelihood or impact. As part of enterprise risk management, for each significant risk an entity considers potential responses from a range of response categories. This gives sufficient depth to response selection and also challenges the "status quo."

Having selected a risk response, management recalibrates the risk on a residual basis. Management considers risk from an entity-wide, or portfolio**,** perspective. Management may take an approach in which the manager responsible for each department, function or business unit develops a composite assessment of risks and risk responses for that unit. This view reflects the risk profile of the unit relative to its objectives and risk tolerances. With a view of risk for individual units, the most senior manager of the enterprise is positioned to take a portfolio view, to determine whether the entity's risk profile is commensurate with its overall risk appetite relative to its objectives.

Management should recognize that some level of residual risk will always exist, not only because resources are limited, but also because of inherent future uncertainty and limitations inherent in all activities.

Control Activities

Control activities are the policies and procedures that help ensure risk responses are properly executed. Control activities occur throughout the organization, at all levels and in all functions. Control activities are part of the process by which an enterprise strives to achieve its business objectives. They usually involve two elements: a policy establishing what should be done and procedures to effect the policy.

With widespread reliance on information systems, controls are needed over significant systems. Two broad groupings of information systems control activities can be used. The first is general controls, which apply to many if not all application systems and help ensure their continued, proper operation. The second is application controls, which include computerized steps within application software to control the technology application. Combined with other manual process controls where necessary, these controls ensure completeness, accuracy and validity of information.

General controls include controls over information technology management, information technology infrastructure, security management and software acquisition, development and maintenance. These controls apply to all systems – from mainframe to client/server to desktop computing environments. General controls include information technology management controls addressing the information technology oversight process, monitoring and reporting information technology activities, and business improvement initiatives.

Application controls are designed to ensure completeness, accuracy, authorization and validity of data capture and transaction processing. Individual applications may rely on effective operation of controls over information systems to ensure that interface data are generated when needed, supporting applications are available and interface errors are detected quickly.

Because each entity has its own set of objectives and implementation approaches, there will be differences in objectives, structure and related control activities. Even if two entities had identical objectives and structures, their control activities would likely be different. Each entity is managed by different people who use individual judgments in effecting internal control. Moreover, controls reflect the environment and industry in which an entity operates, as well as the complexity of its organization, its history and its culture.

Information and Communication

Pertinent information – from internal and external sources – must be identified, captured and communicated in a form and timeframe that enable personnel to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across and up the entity. There is also effective communication and exchange of relevant information with external parties, such as customers, suppliers, regulators and shareholders.

Information is needed at all levels of an organization to identify, assess and respond to risks, and to otherwise run the entity and achieve its objectives. An array of information is used, relevant to one or more objectives categories. Information comes from many sources – internal and external, and in quantitative and qualitative forms – and allows enterprise risk management responses to changing conditions in real time. The challenge for management is to process and refine large volumes of data into actionable information. This challenge is met by establishing an information systems infrastructure to source, capture, process, analyze and report relevant information. These information systems – usually computerized but also involving manual inputs or interfaces – often are viewed in the context of processing internally generated data relating to transactions.

Information systems have long been designed and used to support business strategy. This role becomes critical as business needs change and technology creates new opportunities for strategic advantage.

To support effective enterprise risk management, an entity captures and uses historical and current data. Historical data allow the entity to track actual performance against targets, plans and expectations. It provides insights into how the entity performed under varying conditions, allowing management to identify correlations and trends and to forecast future performance. Historical data also can provide early warning of potential events that warrant management attention.

Present or current state data allow an entity to assess its risks at a specific point in time and remain within established risk tolerances. Current state data allow management to take a real-time view of existing risks inherent in a process, function or unit and to identify variations from expectations. This provides a view of the entity's risk profile, enabling management to alter activities as necessary to calibrate to its risk appetite.

Information is a basis for communication, which must meet the expectations of groups and individuals, enabling them to effectively carry out their responsibilities. Among the most critical communications channels is that between top management and the board of directors. Management must keep the board up-to-date on performance, developments, risks and the functioning of enterprise risk management, and other relevant events and issues. The better the communication, the more effective the board will be in carrying out its oversight responsibilities, in acting as a sounding board on critical issues and in providing advice, counsel and direction. By the same token, the board should communicate to management what information it needs and provide feedback and direction.

Management provides specific and directed communication addressing behavioral expectations and the responsibilities of personnel. This includes a clear statement of the entity's enterprise risk management philosophy and approach and delegation of authority. Communication about processes and procedures should align with, and underpin, the desired risk culture. In addition, communication should be appropriately "framed" – the presentation of information can significantly affect how it is interpreted and how the associated risks or opportunities are viewed.

Communication should raise awareness about the importance and relevance of effective enterprise risk management, communicate the entity's risk appetite and risk tolerances, implement and support a common risk language, and advise personnel of their roles and responsibilities in effecting and supporting the components of enterprise risk management.

Communications channels also should ensure personnel can communicate risk-based information across business units, processes or functional silos. In most cases, normal reporting lines in an organization are the appropriate channels of communication. In some circumstances, however, separate lines of communication are needed to serve as a fail-safe mechanism in case normal channels are inoperative. In all cases, it is important that personnel understand that there will be no reprisals for reporting relevant information.

External communications channels can provide highly significant input on the design or quality of products or services. Management considers how its risk appetite and risk tolerances align with those of its customers, suppliers and partners, ensuring that it does not inadvertently take on too much risk through its business interactions. Communication from external parties often provides important information on the functioning of enterprise risk management.

Monitoring

Enterprise risk management is monitored – a process that assesses both the presence and functioning of its components and the quality of their performance over time. Monitoring can be done in two ways: through ongoing activities or separate evaluations. Ongoing and separate monitoring ensures that enterprise risk management continues to be applied at all levels and across the entity.

Ongoing monitoring is built into the normal, recurring operating activities of an entity. Ongoing monitoring is performed on a real-time basis, reacts dynamically to changing conditions and is ingrained in the entity. As a result, it is more effective than separate evaluations. Since separate evaluations take place after the fact, problems often will be identified more quickly by ongoing monitoring routines. Many entities with sound ongoing monitoring activities nonetheless conduct separate evaluations of enterprise risk management.

The frequency of separate evaluations is a matter of management's judgment. In making that determination, consideration is given to the nature and degree of changes, from both internal and external events, and their associated risks; the competence and experience of the personnel implementing risk responses and related controls; and the results of the ongoing monitoring. Usually, some combination of ongoing monitoring and separate evaluations will ensure that enterprise risk management maintains its effectiveness over time.

The extent of documentation of an entity's enterprise risk management varies with the entity's size, complexity and similar factors. The fact that elements of enterprise risk management are not documented does not mean that they are not effective or that they cannot be evaluated. However, an appropriate level of documentation usually makes monitoring more effective and efficient. Where management intends to make a statement to external parties regarding enterprise risk management effectiveness, it should consider developing and retaining documentation to support the statement.

All enterprise risk management deficiencies that affect an entity's ability to develop and implement its strategy and to achieve its established objectives should be reported to those positioned to take necessary action. The nature of matters to be communicated will vary depending on individuals' authority to deal with circumstances that arise and on the oversight activities of superiors. The term "deficiency" refers to a condition within the enterprise risk management process worthy of attention. A deficiency, therefore, may represent a perceived, potential or real shortcoming, or an opportunity to strengthen the process to increase the likelihood that the entity's objectives will be achieved. Information generated in the course of operating activities usually is reported through normal channels. Alternative communications channels also should exist for reporting sensitive information such as illegal or improper acts.

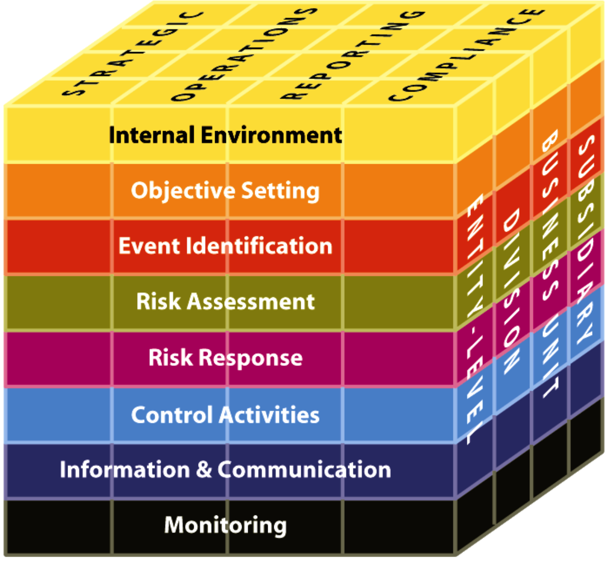
Providing needed information on enterprise risk management deficiencies to the right party is critical. Protocols should be established to identify what information is needed at a particular level for effective decision making. Such protocols reflect the general rule that a manager should receive information that affects actions or behavior of personnel under his or her responsibility, as well as information needed to achieve specific objectives.

Relationship of Objectives and Components

There is a direct relationship between objectives, which are what an entity strives to achieve, and the enterprise risk management components, which represent what is needed to achieve them. Exhibit 1 depicts the relationship in a three-dimensional matrix.

Exhibit 1

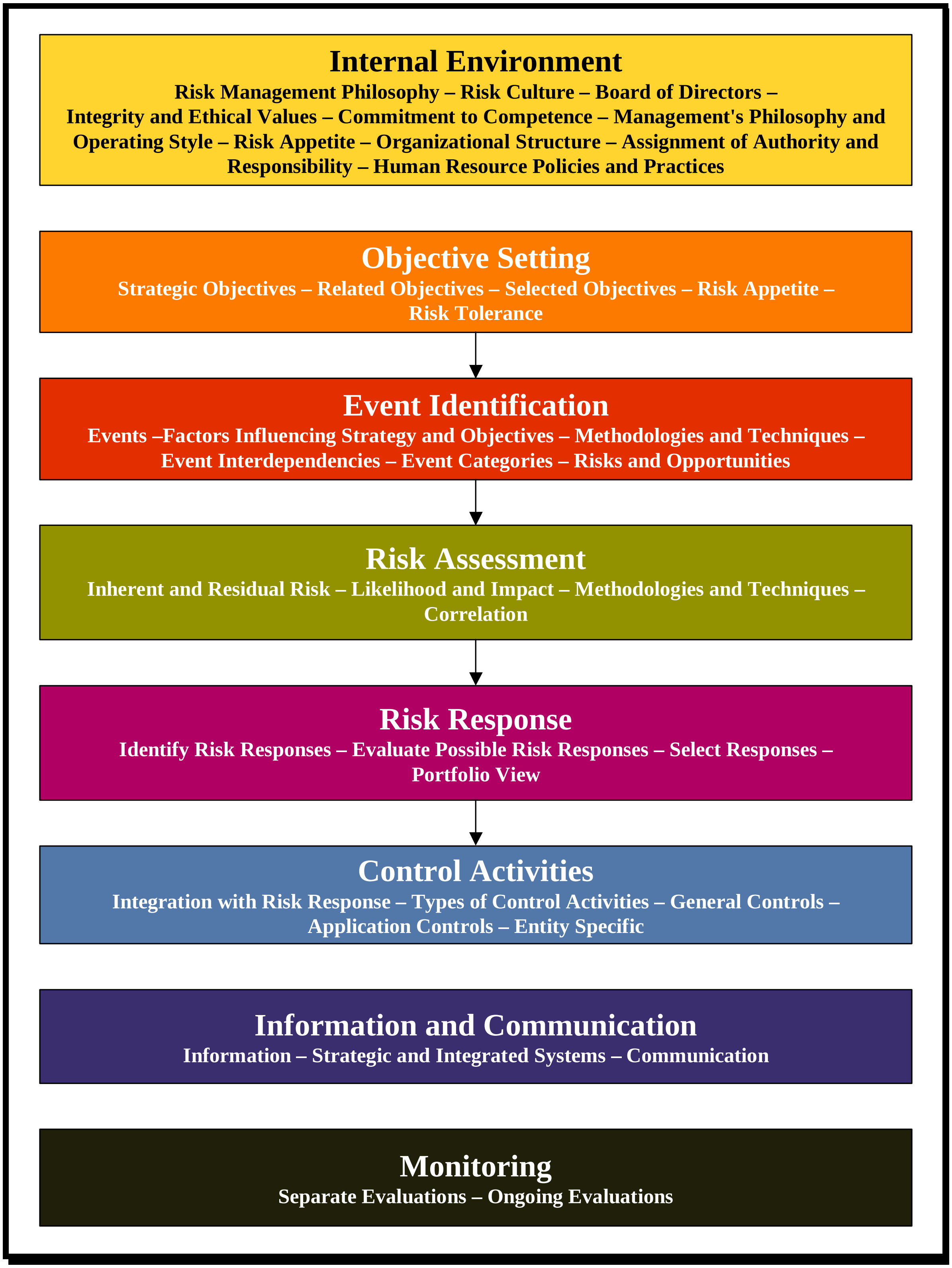
- The four objectives categories – strategic, operations, reporting and compliance – are represented by the vertical columns.
- The eight components are represented by horizontal rows.
- The entity and its organizational units are depicted by the third dimension of the matrix.



It should be recognized that the four columns represent categories of an entity's objectives, not parts or units of the entity. Accordingly, when considering the category of objectives related to reporting, for example, knowledge of a wide array of information about the entity's operations is needed. But in that case focus is on the right-middle column of the model – the reporting objectives – rather than the operations objectives category.

Exhibit 2 expands the component rows of the cube to show the key elements of each component, as well as which components represent a process flow.

Exhibit 2



Internal Environment

Risk Management Philosophy – Risk Culture – Board of Directors – Integrity and Ethical Values – Commitment to Competence – Management's Philosophy and Operating Style – Risk Appetite – Organizational Structure – Assignment of Authority and Responsibility – Human Resource Policies and Practices

Objective Setting

Strategic Objectives – Related Objectives – Selected Objectives – Risk Appetite – Risk Tolerance

Event Identification

Events –Factors Influencing Strategy and Objectives – Methodologies and Techniques – Event Interdependencies – Event Categories – Risks and Opportunities

Risk Assessment

Inherent and Residual Risk – Likelihood and Impact – Methodologies and Techniques – Correlation

Risk Response

Identify Risk Responses – Evaluate Possible Risk Responses – Select Responses – Portfolio View

Control Activities

Integration with Risk Response – Types of Control Activities – General Controls – Application Controls – Entity Specific

Information and Communication

Information – Strategic and Integrated Systems – Communication

Monitoring

Separate Evaluations – Ongoing Evaluations

Effectiveness

While enterprise risk management is a process, its effectiveness is a state or condition at a point in time. Determining whether enterprise risk management is “effective" is a subjective judgment resulting from an assessment of whether all eight components are present and functioning properly.

To be deemed effective, all eight components must be present and functioning. However, this does not mean that each component should function identically, or even at the same level, in different entities, and trade-offs may exist between components. Because enterprise risk management techniques can serve a variety of purposes, techniques applied relative to one component can serve the purpose of those that normally might be present in another. Additionally, risk responses can differ in the degree to which they address a particular risk, so that complementary risk responses, each with limited effect, together may be satisfactory.

The concepts discussed here apply to all entities, regardless of size. While some small and mid-size entities may implement component factors differently than large ones, they still can have effective enterprise risk management. The methodology for each component is likely to be less formal and less structured in smaller entities than in larger ones, but the basic concepts outlined should be present in every entity, regardless of size.

Enterprise risk management may be considered in the context of an enterprise as a whole, or one or more individual units. When considering enterprise risk management for a particular business unit, all eight components must be used as the benchmark.

A company may have joint ventures, partnerships or other investments, the operations of which are not under the company’s direct control. In considering the effectiveness of the company’s enterprise risk management, one would look at the extent to which the company and the investment vehicle together have adequately applied each of the eight components, in light of the company’s strategy and related objectives.

Encompasses Internal Control

Internal control is an integral part of enterprise risk management. This enterprise risk management framework encompasses internal control, forming a more robust conceptualization and tool for management. Internal control is defined and described in *Internal Control – Integrated Framework.* Because *Internal Control – Integrated Framework* is the basis for existing rules, regulations and laws, that document remains in place as the definition of and framework for internal control. The entirety of *Internal Control – Integrated Framework* is incorporated by reference into this framework.

Limitations of Enterprise Risk Management

Effective enterprise risk management helps management achieve objectives. But enterprise risk management, no matter how well designed and operated, does not ensure an entity's success.

The achievement of objectives is affected by limitations inherent in all management processes. Shifts in government policy or programs, competitors' actions or economic conditions can be beyond management's control. Human decision making can be faulty, and breakdowns can occur because of such human failures as simple error or mistake. Enterprise risk management cannot change an inherently poor manager into a good one. Additionally, controls can be circumvented by the collusion of two or more people, and management has the ability to override the enterprise risk management process, including risk responses and controls.

The design of enterprise risk management must reflect the reality of resource constraints, and the risk management benefits must be considered relative to their costs. Thus, while enterprise risk management can help management achieve its objectives, it is not a panacea.

Roles and Responsibilities

Everyone in an organization has responsibility for enterprise risk management.

- *Board of Directors* – Management is accountable to the board of directors, which provides governance, guidance and oversight. By selecting management, the board has a major role in defining what it expects in integrity and ethical values and can confirm its expectations through oversight activities. Similarly, by reserving authority in certain key decisions, the board plays a role in setting strategy, formulating high-level objectives and broad-based resource allocation.

  The board of directors provides oversight with regard to enterprise risk management by:

  - Knowing the extent to which management has established effective enterprise risk management in the organization
  - Being aware of and concurring with the entity’s risk appetite
  - Reviewing the entity’s portfolio view of risks and considering it against the entity’s risk appetite
  - Being apprised of the most significant risks and whether management is responding appropriately

The board is part of the internal environment component and must have the requisite composition and focus for enterprise risk management to be effective.

- *Management* – The chief executive officer is ultimately responsible for and should assume "ownership" of enterprise risk management. More than any other individual, the chief executive sets the "tone at the top" that affects integrity and ethics and other factors of the internal environment. In a large company, the chief executive fulfills this duty by providing leadership and direction to senior managers and reviewing the way they manage the business. Senior managers, in turn, assign responsibility for establishment of more specific risk management policies and procedures to personnel responsible for individual units' functions. In a smaller entity, the influence of the chief executive, often an owner-manager, is usually more direct. In any event, in a cascading responsibility, a manager is effectively a chief executive of his or her sphere of responsibility. Also significant are leaders of staff functions such as compliance, finance, human resources and information technology, whose monitoring and control activities cut across, as well as up and down, the operating and other units of an enterprise.
- *Risk Officer* – A risk officer – referred to in some organizations as the chief risk officer or risk manager – works with other managers in establishing and maintaining effective risk management in their areas of responsibility. The risk officer also may have responsibility for monitoring progress and for assisting other managers in reporting relevant risk information up, down and across the entity, and may be a member of an internal risk management committee.
- *Internal Auditors* – Internal auditors play an important role in the monitoring of enterprise risk management and the quality of performance as part of their regular duties or upon special request of senior management or subsidiary or divisional executives. They may assist both management and the board or audit committee by monitoring, examining, evaluating, reporting on and recommending improvements to the adequacy and effectiveness of management's enterprise risk management processes.
- *Other Personnel* – Enterprise risk management is, to some degree, the responsibility of everyone in an entity and therefore should be an explicit or implicit part of everyone's job description. Virtually all personnel produce information used in enterprise risk management or take other actions needed to manage risks. Also, all personnel are responsible for communicating upward risks such as problems in operations, non-compliance with the code of conduct, other policy violations or illegal actions.

A number of external parties often contribute to achievement of an entity's objectives. External auditors, bringing an independent and objective view, contribute directly through the financial statement audit and internal control examinations, and indirectly by providing additional information useful to management and the board in carrying out their responsibilities. Others providing information to the entity useful in effecting enterprise risk management are regulators, customers and others transacting business with the enterprise, financial analysts, bond raters and the news media. External parties, however, are not responsible for the entity's enterprise risk management.

Use of this Report

Actions that might be taken as a result of this report depend on the position and role of the parties involved:

- *Board Members* – Members of the board of directors should discuss with senior management the state of the entity's enterprise risk management and provide oversight as needed. The board should ensure that the entity’s enterprise risk management mechanisms provide it with an assessment of the most significant risks relative to strategy and objectives, including what actions management is taking and how it is engaged in monitoring the enterprise risk management framework. The board should seek input from the internal auditors, external auditors and advisors.
- *Senior Management* – This study suggests that the chief executive assess the organization’s enterprise risk management capabilities. Using this framework, a CEO, together with key operating and financial executives, can focus attention where needed. Under one approach, the chief executive could bring together business unit heads and key functional staff to discuss an initial assessment of enterprise risk management capabilities and effectiveness. Whatever its form, an initial assessment should determine whether there is a need for, and how to proceed with, a broader, more in-depth evaluation. It also should ensure that ongoing monitoring processes are in place. Time spent in evaluating enterprise risk management represents an investment, but one with a high return.
- *Other Entity Personnel* – Managers and other personnel should consider how their enterprise risk management responsibilities are being conducted in light of this framework, and discuss with more-senior personnel ideas for strengthening enterprise risk management. Internal auditors should consider the breadth of their focus on enterprise risk management.
- *Regulators* – Expectations for enterprise risk management vary widely in two respects. First, they differ regarding what these mechanisms can accomplish. Some observers believe enterprise risk management will, or should, prevent economic loss, or at least prevent companies from going out of business. Second, even when there is agreement about what enterprise risk management can and can't do, and about the “reasonable assurance” concept, there can be disparate views of what that concept means and how it will be applied. To help gain a shared view of enterprise risk

management and what it can do, there should be agreement on a common enterprise risk management framework, including its limitations. This framework may be looked to in that regard.

- *Professional Organizations* – Rule-making and other professional organizations providing guidance on financial management, auditing and related topics should consider their standards and guidance in light of this framework. To the extent that diversity in concepts and terminology is eliminated, all parties will benefit.
- *Educators* – This framework should be the subject of academic research and analysis, to see where future enhancements can be made. With the presumption that this report becomes accepted as a common ground for understanding, its concepts and terms should find their way into university curricula.

Organization of this Report

This *Executive Summary* and the *Framework* document together comprise the *Enterprise Risk Management Framework*. This *Executive Summary* provides a high-level overview directed to the chief executive and other senior executives, board members and regulators. The *Framework* document provides a broader and deeper discussion of the definition, principles and concepts of enterprise risk management framework, providing direction for all levels of management in business other organizations to use in determining how to enhance their enterprise risk management, and to management and others to use in evaluating the effectiveness of an entity's enterprise risk management.

COSO

The Committee of Sponsoring Organizations of the Treadway Commission

Enterprise Risk Management Framework

➢ Framework

Committee of Sponsoring
Organizations of the
Treadway Commission

[This page intentionally left blank]

Committee of Sponsoring Organizations of the Treadway Commission (COSO)

Oversight	**Representative**
Committee of Sponsoring Organizations of the Treadway Commission	John J. Flaherty, Chair
American Institute of Certified Public Accountants	Alan W. Anderson
The Institute of Internal Auditors	William G. Bishop, III
Financial Executives International	John P. Jessup
Institute of Management Accountants	Frank C. Minter Dennis L. Neider
American Accounting Association	Larry E. Rittenberg

Project Advisory Council to COSO

Guidance

Tony Maki, Chair
Partner
Moss Adams LLP

Mark S. Beasley
Associate Professor
North Carolina State University

Jerry W. DeFoor
VP and Controller
Protective Life Corporation

James W. DeLoach
Managing Director
Protiviti Inc.

Andrew J. Jackson
Assistant General Auditor
General Motors

Steven E. Jameson
Lead Auditing Specialist
World Bank

John P. Jessup
VP Finance and Controller
E. I. DuPont de Nemours & Company

Tony M. Knapp
Senior VP and Controller
Motorola, Inc.

Douglas F. Prawitt
Associate Professor
Brigham Young University

PricewaterhouseCoopers LLP

Author

Principal Contributors

Richard M. Steinberg
Past Partner, Corporate Governance Leader

Frank J. Martens
Senior Manager
Vancouver, Canada

Miles E.A. Everson
Partner
New York

Lucy E. Nottingham
Manager
Boston

[This page intentionally left blank]

Table of Contents

Appendices

[This page intentionally left blank]

1. RELEVANCE OF ENTERPRISE RISK MANAGEMENT

Chapter Summary: Enterprise risk management is applied in strategy setting and across an entity's activities. It enables management to identify, assess and manage risks in the face of uncertainty, and supports value creation and preservation. Enterprise risk management provides enhanced capabilities to align risk appetite and strategy, link risk with growth and return, enhance risk response decisions, minimize operational surprises and losses, identify and manage cross-enterprise risks, provide integrated responses to multiple risks, seize opportunities, and rationalize capital.

The underlying premise of enterprise risk management is that every entity, whether for-profit, not-for-profit or a governmental body, exists to provide value for its stakeholders. All entities face uncertainty, and the challenge for management is to determine how much uncertainty the entity is prepared to accept as it strives to grow stakeholder value. Uncertainty presents both risk and opportunity, with the potential to erode or enhance value. Enterprise risk management provides a framework for management to effectively deal with uncertainty and associated risk and opportunity and thereby enhance its capacity to build value.

Uncertainty

Enterprises operate in environments where factors such as globalization, technology, regulation, restructurings, changing markets, and competition create uncertainty. Uncertainty emanates from an inability to precisely determine the likelihood that potential events will occur and the associated outcomes. Uncertainty also is presented and created by the entity's strategic choices. For example, an entity has a growth strategy based on expanding operations to another country. This chosen strategy presents risks and opportunities associated with the stability of the country's political environment, resources, markets, channels, workforce capabilities and costs.

Value

Value is created, preserved or eroded by management decisions in all activities, from strategy setting to operating the enterprise day-to-day. Inherent in decisions is recognition of risk and opportunity, requiring that management[1] considers information about internal and external environments, deploys precious resources and recalibrates enterprise activities to changing circumstances.

Value creation occurs through deploying resources, including people, capital, technology and brand, so that the benefit derived is greater than resources used. Entities preserve value by focusing on people, processes, systems and actions to create sustained value, including, among other things, product quality, production capacity and customer satisfaction. Value

[1] While the term "management" is used in this and later discussions, many enterprise risk management activities are performed by non-management personnel..

can be eroded by acting on incomplete or otherwise inadequate information about risk and opportunity, or by poor strategy or execution.

Value is maximized when management's strategy and objectives strike an optimal balance between growth and return objectives and the related risks, and the efficient and effective deployment of resources in pursuit of the entity's objectives. Enterprise risk management facilitates identification of market needs, inefficiencies and other events that pose either opportunities to create value or risks to strategies and achievement of the entity's goals.

Entities realize value when stakeholders derive recognizable benefits that they in turn value. For companies, shareholders realize value when they recognize value creation from share-value growth. For governmental entities, value is realized when constituents recognize receipt of valued services at acceptable cost. Stakeholders of not-for-profit entities realize value when they recognize receipt of valued social benefits. Enterprise risk management facilitates management's ability both to create sustainable value and communicate the value created to stakeholders.

Measures of Entity Value

A measure of value is relative worth, utility or importance of the entity to its stakeholders. Many company managements are accustomed to thinking about value in terms of financial measures such as economic profit, shareholder value added, risk-adjusted return on capital or total shareholder return. These financial measures share a basic premise that cost of capital must be covered before value is created. However, financial measures need not always be used as the sole proxy for value. Measures of value for a not-for-profit organization may be linked to the social benefit they seek to provide. For instance, a not-for-profit organization that provides advocacy to senior citizens measures value in terms of access to affordable high-quality, long-term health care.

Benefits of Enterprise Risk Management

No entity operates in a risk-free environment, and enterprise risk management does not create such an environment. Rather, enterprise risk management enables management to operate more effectively in environments filled with risks.

Enterprise risk management provides enhanced capability to:

- **Align risk appetite and strategy** – Risk appetite is the degree of risk, on a broad-based level, that a company or other entity is willing to accept in pursuit of its goals. Management considers the entity's risk appetite first in evaluating strategic alternatives, then in setting objectives aligned with the selected strategy and in developing mechanisms to manage the related risks. For example, a pharmaceutical company has a low risk appetite relative to its brand value. Accordingly, to protect its brand, it maintains extensive protocols to ensure product safety and regularly invests significant resources in early stage research and development to support brand-value creation.

- **Link growth, risk and return** – Entities accept risk as part of value creation and preservation, and they expect return commensurate with the risk. Enterprise risk management provides an enhanced ability to identify and assess risks, and establish acceptable levels of risk relative to growth and return objectives. For instance, an insurance company's management in strategic planning brings together business unit plans with growth and return projections. Risks to achievement are identified and considered, responses are selected, business unit plans are modified and capital is allocated based on individual business unit and company-wide objectives.
- **Enhance risk response decisions –** Enterprise risk management provides the rigor to identify and select among alternative risk responses – risk avoidance, reduction, sharing and acceptance. For example, management of a company that uses company-owned and operated vehicles recognizes risks inherent in its delivery process, including vehicle damage and personal injury costs. Available alternatives include reducing the risk through effective driver recruiting and training, avoiding the risk by outsourcing delivery, transferring the risk via insurance or simply accepting the risk. Enterprise risk management provides methodologies and techniques for making these decisions.
- **Minimize operational surprises and losses –** Entities have enhanced capability to identify potential events, assess risk and establish responses, thereby reducing the occurrence of surprises and related costs or losses. For example, a manufacturing company tracks production parts and equipment failure rates and deviation around averages. The company assesses the impact of failures using multiple criteria, including time to repair, inability to meet customer demand, safety of employees and cost of scheduled versus unscheduled repairs, and responds by setting maintenance schedules accordingly.
- **Identify and manage cross-enterprise risks –** Every entity faces a myriad of risks affecting different parts of the organization. Management needs to not only manage individual risks, but also understand interrelated impacts. For example, a bank faces a variety of risks in trading activities across the enterprise, and management developed an information system that analyses transaction and market data from other internal systems and, together with relevant externally generated information, provides an aggregate view of risks across all trading activities. The information system allows drilldown capability to department, customer or counterparty, trader and transaction levels, and quantifies the risks relative to risk tolerances in established categories. The information system enables the bank to tie together once-disparate data to respond more effectively to risks using aggregated as well as targeted views.

- **Provide integrated responses to multiple risks –** Business processes carry many inherent risks, and enterprise risk management enables integrated solutions for managing the risks. For instance, a wholesale distributor faces risks of over- and undersupply positions, tenuous supply sources and unnecessarily high purchase prices. Management identified and assessed risk in the context of the company's strategy, objectives and alternative responses, and developed a far-reaching inventory control system. The system integrates with suppliers, sharing sales and inventory information and enabling strategic partnering, and avoiding stock-outs and unneeded carrying costs, with longer-term sourcing contracts and enhanced pricing. Suppliers are positioned to take responsibility for replenishing stock, generating further cost reductions.
- **Seize opportunities –** By considering a full range of potential events, rather than just risks, management gains an understanding of how certain events represent opportunities. For example, a food company considered potential events likely to affect its sustainable revenue growth objective. In evaluating the events, management determined that the company's primary consumers were increasingly health conscious and changing their dietary preferences, indicating a decline in future demand for the company's current products. In determining its response, management identified ways to apply its existing capabilities to developing new products, enabling the company not only to preserve the revenue from existing customers, but also to create additional revenue by appealing to a broader consumer base.
- **Rationalize capital –** More robust information on risk allows management to more effectively assess overall capital needs and improve capital allocation. For example, a financial institution was apprised of new regulatory rules that would increase capital requirements unless management calculated credit and operational risk levels and related capital needs with greater specificity. The company assessed the risk in terms of system development cost versus additional capital costs, and made an informed decision to deal with the risk. With existing, readily modifiable software, the bank developed the more precise calculations, avoiding a need for additional capital sourcing.

Enterprise risk management is not an end in itself, but rather an important means to achieving its objectives. It does not operate in isolation in an entity, but rather is an enabler of the management process. Enterprise risk management is interrelated with corporate governance by providing information to the board of directors on the most significant risks and how they are being managed. And it interrelates with performance management by providing risk-adjusted measures, and with internal control, which is an integral part of enterprise risk management.

Enterprise risk management helps an entity achieve its performance and profitability targets and prevent loss of resources. It helps ensure effective reporting. And it helps ensure that the entity complies with laws and regulations, avoiding damage to its reputation and other consequences. In sum, it helps an entity get to where it wants to go and avoid pitfalls and surprises along the way.

2. FRAMEWORK OVERVIEW

Chapter Summary: Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within the entity's risk appetite, to provide reasonable assurance regarding the achievement of entity objectives. The definition is broad, relating to all aspects of a business. Enterprise risk management consists of eight interrelated components, which complement the way management runs the enterprise and are integrated with other management processes. The components are linked and serve as criteria for determining whether enterprise risk management is effective.

A key objective of this framework is to help managements of businesses and other entities better deal with risk inherent in achieving an entity's objectives. But enterprise risk management means different things to different people. The wide variety of labels and meanings prevents a common understanding of enterprise risk management. An important goal, then, is to integrate various risk management concepts into a framework in which a common definition is established and components identified. This framework is designed to accommodate most viewpoints and provide a starting point for individual entities' assessments and enhancement of enterprise risk management, for future initiatives of rule-making bodies and for education.

Events and Risks

A myriad of events from internal or external sources has the potential to affect strategy implementation and achievement of objectives. Events potentially have a negative impact, a positive impact or a combination of both. Events with a potentially negative impact represent risks. Accordingly, risk is the possibility that an event will occur and adversely affect the achievement of objectives. Events with a potentially positive impact may offset negative impacts or they may represent opportunities. Management channels opportunities back to its strategy or objective-setting processes, so that actions can be formulated to seize the opportunities. Management assesses risks to implementing strategy and achieving objectives by considering the potential impacts of the underlying events.

Definition of Enterprise Risk Management

Enterprise risk management is defined as follows:

> *Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in 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 reflects certain fundamental concepts. Enterprise risk management:

- Is *a process* – it's a means to an end, not an end in itself
- Is *effected by people* – it's not merely policies, surveys and forms, but involves people at every level of an organization
- Is *applied in strategy setting*
- Is *applied across the enterprise,* at every level and unit, and includes taking an entity-level portfolio view of risk
- Is designed to identify events potentially affecting the entity and manage risk within its *risk appetite*
- Provides *reasonable assurance* to an entity's management and board
- Is geared to the *achievement of objectives* in one or more separate but overlapping categories.

This definition is purposefully broad for several reasons. It captures key concepts fundamental to how companies and other organizations manage risk, providing a basis for application across different types of organizations, industries and sectors. It focuses directly on achievement of objectives established by a particular entity. And, the definition provides a basis for defining enterprise risk management effectiveness, discussed later in this chapter. The fundamental concepts outlined above are discussed in the following paragraphs.

A Process

Enterprise risk management is not one event or circumstance, but a series of actions that permeate an entity's activities. These actions are pervasive and inherent in the way management runs the business.

Enterprise risk management is different from the perspective of some observers who view it as something added on to an entity's activities, or as a necessary burden. That is not to say that effective enterprise risk management does not require incremental effort. For instance, in considering credit and currency risks, incremental effort may be required to develop needed models and make necessary analysis and calculations. However, these enterprise risk management mechanisms are intertwined with an entity's operating activities and exist for fundamental business reasons. Enterprise risk management is most effective when these mechanisms are built into the entity's infrastructure and are part of the essence of the enterprise. By building in enterprise risk management, an entity can directly affect its ability to implement its strategy and achieve its vision or mission.

Building in enterprise risk management also has important implications for cost containment, especially in the highly competitive marketplaces many companies face. Adding new procedures separate from existing ones adds costs. By focusing on existing operations and their contribution to effective enterprise risk management, and integrating risk management into basic operating activities, an enterprise can avoid unnecessary procedures and costs.

And, a practice of building enterprise risk management into the fabric of operations helps identify new opportunities for management to seize in growing the business.

Effected by People

Enterprise risk management is effected by a board of directors, management and other personnel. It is accomplished by the people of an organization, by what they do and say. People establish the entity's vision, mission, strategy and objectives and put enterprise risk management mechanisms in place.

Similarly, enterprise risk management affects people's actions. Enterprise risk management recognizes that people do not always understand, communicate or perform consistently. Each individual brings to the workplace a unique background and technical ability, and has different needs and priorities.

These realities affect, and are affected by, enterprise risk management. Each person has a unique point of reference which influences how they identify, assess and respond to risk. Enterprise risk management provides the mechanisms needed to help people understand risk in the context of the entity's objectives. People must know their responsibilities and limits of authority. Accordingly, a clear and close linkage needs to exist between people's duties and the way in which they are carried out, as well as with the entity's strategy and objectives.

An organization's people include the board of directors, as well as management and other personnel. Although directors primarily provide oversight, they also provide direction and approve strategy and certain transactions and policies. As such, boards of directors are an important element of enterprise risk management.

Applied in Setting Strategy

An entity sets out its mission or vision and establishes strategic objectives, which are the high-level goals that align with and support its vision or mission. An entity establishes a strategy for achieving its strategic objectives. It also sets related objectives it wants to achieve, flowing from the strategy, cascading to entity business units, divisions and processes.

Enterprise risk management is applied in strategy setting, in which management considers risks relative to alternative strategies. For instance, one alternative may be to acquire other companies in order to grow market share. Another may be to cut sourcing costs in order to realize higher gross margin percentage. Each of these strategic choices poses a number of risks. If management selects the first strategy, it may have to expand into new and unfamiliar markets, competitors may be able to gain share in the company's existing markets or the company might not have the capabilities to effectively implement the strategy. With the second choice, risks include having to use new technologies or suppliers, or form new alliances. Enterprise risk management techniques must be applied at this level in determining the entity's strategy.

Applied Across the Enterprise

To successfully apply enterprise risk management, an entity must consider its entire scope of activities. Enterprise risk management considers activities at all levels of the organization, from enterprise-level activities such as strategic planning and resource allocation, to business unit activities such as marketing and human resources, to business processes such as production and new customer credit review. Enterprise risk management also applies to special projects and new initiatives that might not yet have a designated place in the entity's hierarchy or organization chart.

Enterprise risk management requires an entity to take a *portfolio view* of risk. This might involve each manager responsible for a business unit, function, process or other activity developing an assessment of risk for the unit. The assessment may be quantitative or qualitative. With a composite view at each succeeding level of the organization, senior management is positioned to make a determination whether the entity's overall risk portfolio is commensurate with its risk appetite.

Management considers interrelated risks from an entity-level portfolio perspective. Interrelated risks need to be identified and acted upon to bring the entirety of risk within the entity's risk appetite. Risks for individual units of the entity may be within the units' risk tolerances, but taken together may exceed the risk appetite of the entity as a whole. The overall risk appetite is reflected downstream in an entity through risk tolerances established for specific objectives.

In compiling this portfolio view, management considers potential events, rather than just risks. By considering events, management gains an understanding of how certain events may have offsetting effects. For example, a decline in interest rates may positively affect an entity's cost of capital, but negatively impact revenue derived from interest-earning assets.

Where interrelationships between events exist, management may find it useful to group events into categories, facilitating consideration of the related risks and opportunities.

Risk Appetite

Risk appetite is the amount of risk an entity is willing to accept in pursuit of value. Entities often consider risk appetite qualitatively, with such categories as high, moderate or low, or they may take a quantitative approach, reflecting and balancing goals for growth, return and risk.

Risk appetite is directly related to an entity's strategy. It is considered in strategy setting, where the desired return from a strategy should be aligned with the entity's risk appetite.

Different strategies will expose the entity to different risks. Enterprise risk management helps management select a strategy consistent with the entity’s risk appetite.

The entity’s risk appetite guides resource allocation. Management allocates resources across business units with consideration of the entity’s risk appetite and individual business units’ strategy for generating a desired return on invested resources. Management considers its risk appetite as it aligns its organization, people and processes, and designs infrastructure necessary to effectively respond to and monitor risks.

Provides Reasonable Assurance

Well-designed and operated enterprise risk management can provide management and the board of directors reasonable assurance regarding achievement of an entity's objectives. As a result of enterprise risk management determined to be effective, as discussed later in this chapter, in each of the categories of entity objectives, the board of directors and management gain reasonable assurance that:

- They understand the extent to which the entity’s strategic objectives are being achieved,
- They understand the extent to which the entity's operations objectives are being achieved,
- The entity’s reporting is reliable, and
- Applicable laws and regulations are being complied with.

Reasonable assurance reflects the notion that uncertainty and risk relate to the future, which no one can predict with certainty. Limitations also result from the realities that human judgment in decision making can be faulty, decisions on responding to risk and establishing controls need to consider the relative costs and benefits, breakdowns can occur because of human failures such as simple errors or mistakes, controls can be circumvented by collusion of two or more people, and management has the ability to override enterprise risk management decisions. These limitations preclude a board and management from having absolute assurance that objectives will be achieved.

Achievement of Objectives

Within the context of the established mission or vision, management establishes strategic objectives, selects strategy and establishes other objectives cascading through the enterprise and aligned with and linked to the strategy. Although many objectives are specific to a particular entity, some are widely shared. For example, objectives common to virtually all entities are achieving and maintaining a positive reputation within the business and consumer communities, providing reliable reporting to stakeholders and operating in compliance with laws and regulations.

This framework views entity objectives in the context of four categories:

- **Strategic –** relating to high-level goals, aligned with and supporting the entity’s mission.
- **Operations** – relating to effective and efficient use of the entity's resources.
- **Reporting** – relating to the reliability of the entity’s reporting.
- **Compliance** – relating to the entity's compliance with applicable laws and regulations.

This categorization of entity objectives allows a board and management to focus on separate aspects of enterprise risk management. These distinct but overlapping categories – a particular objective can fall under more than one category – address different entity needs and may be the direct responsibility of different executives. This categorization also allows distinguishing between what can be expected from each category of objectives.

Some entities use another category of objectives, “safeguarding of resources,” sometimes referred to as “safeguarding of assets.” Viewed broadly, these deal with prevention of loss of an entity’s assets or resources, whether through theft, waste, inefficiency or what turns out to be simply bad business decisions - such as selling product at too low a price, failing to retain key employees or prevent patent infringement, or incurring unforeseen liabilities. These are primarily operations objectives, although certain aspects of safeguarding can fall under the other categories. Where legal or regulatory requirements apply, these become compliance issues. On the other hand, properly reflecting asset losses in the entity’s financial statements represents a reporting objective. When used in conjunction with public reporting, a narrower definition of safeguarding of assets often is used, dealing with prevention or timely detection of unauthorized acquisition, use or disposition of an entity’s assets.

Enterprise risk management can be expected to provide reasonable assurance of achieving objectives relating to the reliability of reporting, and compliance with laws and regulations. Achievement of those categories of objectives is within the entity’s control and depends on how well the entity’s related activities are performed.

However, achievement of strategic objectives, such as attaining a specified market share, and operations objectives – such as successfully launching a new product line– is not always within the entity's control. While enterprise risk management cannot prevent bad judgments or decisions, or external events that can cause a business to fail to achieve operations goals, it does enhance the likelihood that management will make better decisions. For these objectives, enterprise risk management can provide reasonable assurance that management, and the board in its oversight role, are made aware, in a timely manner, of the extent to which the entity is moving toward achievement of the objectives.

Components of Enterprise Risk Management

Enterprise risk management consists of eight interrelated components. These are derived from the way management runs a business, and are integrated with the management process. These components are:

- **Internal Environment –** Management sets a philosophy regarding risk and establishes a risk appetite. The internal environment sets the foundation for how risk and control are viewed and addressed by an entity's people. The core of any business is its people – their individual attributes, including integrity, ethical values and competence – and the environment in which they operate. They are the engine that drives the entity and the foundation on which everything rests.
- **Objective Setting –** Objectives must exist before management can identify events potentially affecting their achievement. Enterprise risk management ensures that management has a process in place to set objectives and that the chosen objectives support and align with the entity's mission/vision and are consistent with the entity's risk appetite.
- **Event Identification –** Potential events that might have an impact on the entity must be identified. Event identification includes identifying factors – internal and external – that influence how potential events may affect strategy implementation and achievement of objectives. It includes distinguishing between potential events that represent risks, those representing opportunities and those that may be both. Management identifies interrelationships between potential events and may categorize events in order to create and reinforce a common risk language across the entity and form a basis for considering events from a portfolio perspective.
- **Risk Assessment –** Identified risks are analyzed in order to form a basis for determining how they should be managed. Risks are associated with related objectives that may be affected. Risks are assessed on both an inherent and a residual basis, and the assessment considers both risk likelihood and impact. A range of possible results may be associated with a potential event, and management needs to consider them together.
- **Risk Response –** Management selects an approach or set of actions to align assessed risks with the entity's risk appetite, in the context of the strategy and objectives. Personnel identify and evaluate possible responses to risks, including avoiding, accepting, reducing and sharing risk.
- **Control Activities –** Policies and procedures are established and executed to help ensure that the risk responses management selected are effectively carried out.
- **Information and Communication –** Relevant information is identified, captured and communicated in a form and timeframe that enable people to carry out their responsibilities. Information is needed at all levels of an entity for identifying,

assessing and responding to risk. Effective communication also must occur in a broader sense, flowing down, across and up the entity. Personnel need to receive clear communications regarding their role and responsibilities.

- **Monitoring** – The entire enterprise risk management process must be monitored, and modifications made as necessary. In this way, the system can react dynamically, changing as conditions warrant. Monitoring is accomplished through ongoing management activities, separate evaluations of the enterprise risk management processes or a combination of the two.

These enterprise risk management components and their linkages are depicted in a model, presented in Exhibit 2.1.

Enterprise risk management is a dynamic process. For example, the assessment of risks drives risk response and may influence control activities and highlight a need to reconsider information and communication needs or the entity's monitoring activities. Thus, enterprise risk management is not a serial process, where one component affects only the next. It is a multidirectional iterative process in which almost any component can and will influence another.

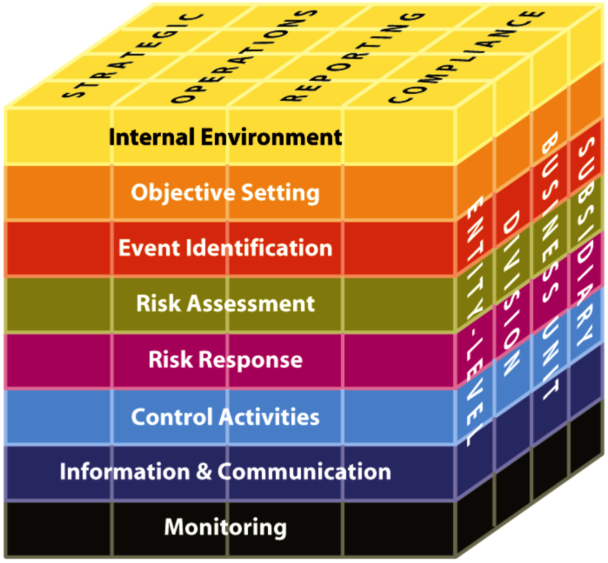
No two entities will, or should, apply enterprise risk management in the same way. Companies and their enterprise risk management capabilities and needs differ dramatically by industry and size, and by culture and management philosophy. Thus, while all entities need each of the components to maintain control over their activities, one company's application of the enterprise risk management framework – including the tools and techniques employed and the assignment of roles and responsibilities for enterprise risk management – often will look very different from another's.

Relationship of Objectives and Components

There is a direct relationship between objectives, which are what an entity strives to achieve, and the enterprise risk management components, which represent what is needed to achieve them. The relationship is depicted in a three-dimensional matrix, in the shape of a cube, shown in Exhibit 2.1.

- The four objectives categories – strategic, operations, reporting and compliance – are represented by the vertical columns,
- The eight components are represented by horizontal rows, and
- The entity and its units are depicted by the third dimension of the matrix.

Exhibit 2.1



Each component row "cuts across" and applies to all four objectives categories. For example, financial and non-financial data generated from internal and external sources, which is part of the information and communication component, is needed in strategy setting, and to effectively manage business operations, report effectively and determine that the entity is complying with applicable laws.

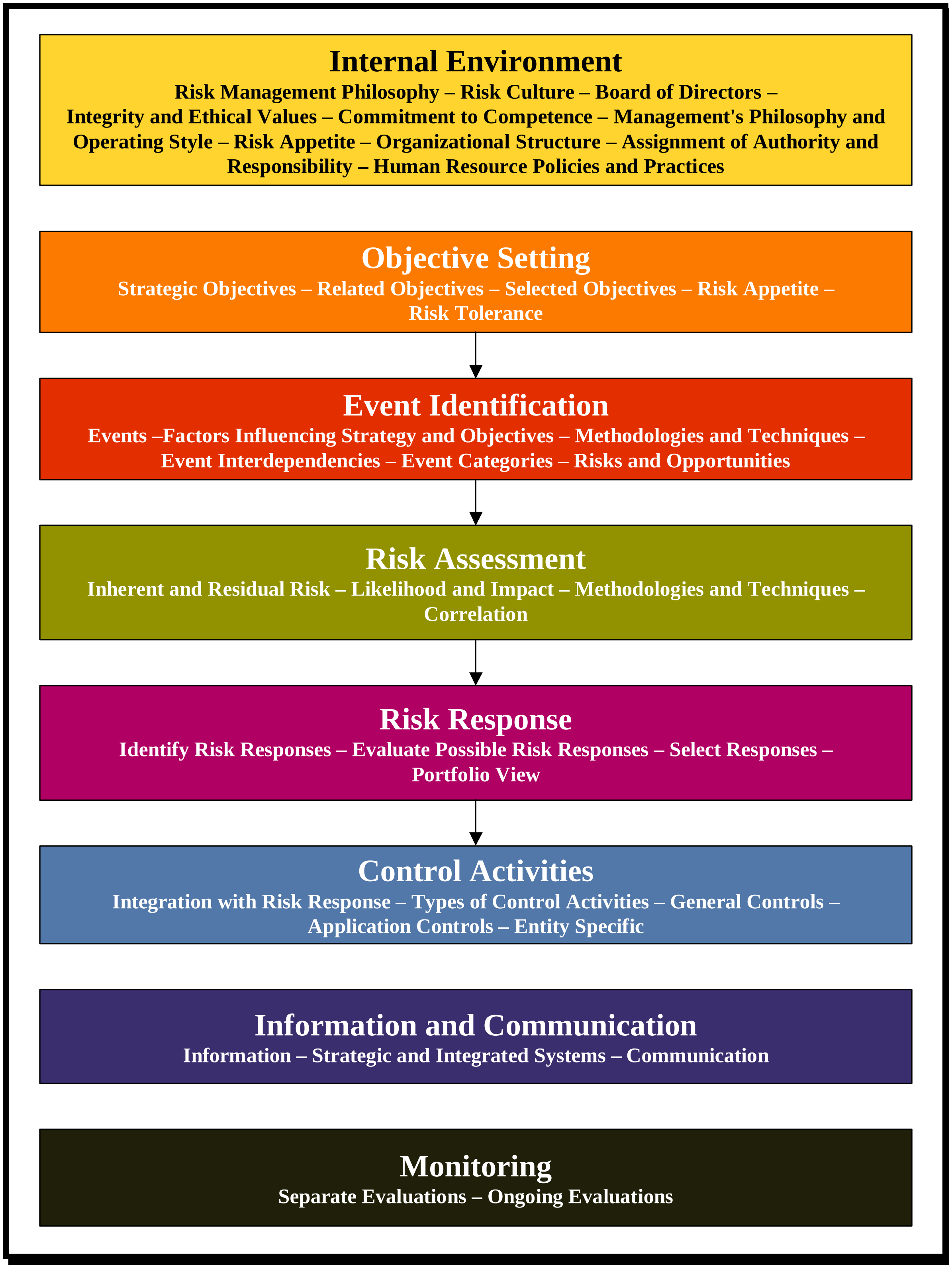
Similarly, looking at the objectives categories, all eight components are relevant to each. Taking one category, effectiveness and efficiency of operations, for example, all eight components are applicable and important to its achievement.

Enterprise risk management is relevant to an entire enterprise or to an individual business unit. This relationship is depicted by the third dimension, which represents subsidiaries, divisions and other business units. Accordingly, one could focus on any one of the matrix's cells. For instance, one could consider the top right back cell, representing the internal environment as it relates to compliance objectives of a particular subsidiary.

It should be recognized that the four columns represent categories of an entity's objectives, not parts or units of the entity. Accordingly, when considering the category of objectives related to reporting, for example, knowledge of a wide array of information about the entity's operations is needed. But in that case focus is on the right-middle column of the model – the reporting objectives – rather than the operations objectives category.

Exhibit 2.2 expands the component rows of the cube to show the key elements of each component as well as which components represent a process flow.

Exhibit 2.2



Internal Environment

Risk Management Philosophy – Risk Culture – Board of Directors – Integrity and Ethical Values – Commitment to Competence – Management's Philosophy and Operating Style – Risk Appetite – Organizational Structure – Assignment of Authority and Responsibility – Human Resource Policies and Practices

Objective Setting

Strategic Objectives – Related Objectives – Selected Objectives – Risk Appetite – Risk Tolerance

Event Identification

Events –Factors Influencing Strategy and Objectives – Methodologies and Techniques – Event Interdependencies – Event Categories – Risks and Opportunities

Risk Assessment

Inherent and Residual Risk – Likelihood and Impact – Methodologies and Techniques – Correlation

Risk Response

Identify Risk Responses – Evaluate Possible Risk Responses – Select Responses – Portfolio View

Control Activities

Integration with Risk Response – Types of Control Activities – General Controls – Application Controls – Entity Specific

Information and Communication

Information – Strategic and Integrated Systems – Communication

Monitoring

Separate Evaluations – Ongoing Evaluations

While the enterprise risk management framework is relevant and applicable to all entities, the manner in which management applies enterprise risk management will vary widely with the nature of the entity and depends on a number of entity-specific factors. These factors include the entity's business model, risk profile, ownership structure, operating environment, size, complexity, industry and degree of regulation, among others. As it considers the entity's specific situation, management will make a series of choices regarding the complexity of processes and methodologies deployed to apply the enterprise risk management framework components. Management may choose to pursue sophisticated methods and techniques in certain business units or processes or enterprise risk management components, but decide to utilize a more basic approach for others.

Effectiveness

While enterprise risk management is a process, its effectiveness is a state or condition at a point in time. Determining whether enterprise risk management is “effective" is a subjective judgment resulting from an assessment of whether the eight components are present and functioning properly.

To be deemed effective, all eight components must be present and functioning. However, this does not mean that each component should function identically, or even at the same level, in different entities, and trade-offs may exist between components. Because enterprise risk management techniques can serve a variety of purposes, techniques applied relative to one component can serve the purpose of those that normally might be present in another. Additionally, risk responses can differ in the degree to which they address a particular risk, so that complementary risk responses, each with limited effect, together may be satisfactory.

The concepts discussed here apply to all entities, regardless of size. While some small and mid-size entities may implement component factors differently than large ones, they still can have effective enterprise risk management. The methodology for each component is likely to be less formal and less structured in smaller entities than in larger ones, but the basic concepts should be present in every entity, regardless of size.

Enterprise risk management may be considered in the context of an enterprise as a whole, or one or more individual units. When considering enterprise risk management for a particular unit of an entity, all eight components must be used as the benchmark. Thus, for example, because having a board of directors with specified attributes is an element of the internal environment, enterprise risk management of a business unit may be judged effective only when the unit has in place a board of directors or similar body (or the entity-level board of directors applies requisite oversight directly to the business unit). Similarly, because the risk response component describes taking a portfolio view of risk, for enterprise risk management to be judged effective, there must be a portfolio view of risk for that business unit.

An entity may have joint ventures, partnerships or other investments, the operations of which are not under the entity's control. In such circumstances, the entity may achieve enterprise risk management if it identifies the potential events that may affect the investment and in turn affect the entity's ability to achieve its objectives; ensures its risk assessment, risk response and control components appropriately address these events; and monitors the mechanisms it has designed to manage the risks associated with the investment.

Alternatively, an entity may achieve effective enterprise risk management if it has monitoring mechanisms to ensure the investment vehicle itself has effective enterprise risk management. However, the investment vehicle may have a risk appetite that differs from the entity's risk appetite. This may occur where the investment vehicle has an independent board or other similar oversight structure. The entity's management needs to assess the consistency between its risk appetite and that of the investment vehicle, to be satisfied that risk to the entity is acceptable.

A mining company has invested in a gold mining joint venture. The mining company has a lower risk appetite regarding earnings volatility than the joint venture. The joint venture's management anticipates a flat or upward movement in gold price and is prepared to accept the risk of a price decline in exchange for anticipated gains from a price increase. It therefore does not hedge gold price movements. The company's management monitors the joint venture's gold production levels and hedges gold price movement in order to manage commodity price risk within the company's risk appetite.

Encompasses Internal Control

Internal control is an integral part of enterprise risk management. This enterprise risk management framework encompasses internal control, forming a more robust conceptualization and tool for management. Internal control is defined and described in *Internal Control – Integrated Framework.* Because *Internal Control – Integrated Framework* is the basis for existing rules, regulations and laws, that document remains in place as the definition of and framework for internal control. The entirety of *Internal Control – Integrated Framework* is incorporated by reference into this framework. Appendix B describes how enterprise risk management is more encompassing than internal control.

Enterprise Risk Management and the Management Process

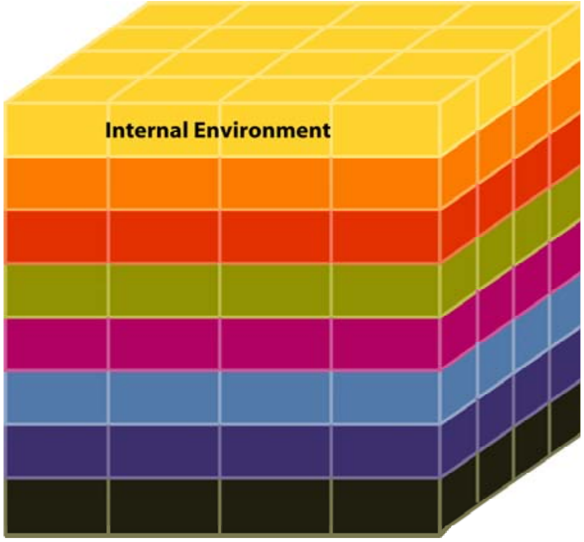
Because enterprise risk management is part of the management process, the enterprise risk management framework components are discussed in the context of what management does in running a business. Not everything management does, however, is an element of enterprise risk management. For example, the process of establishing objectives is a critical component of enterprise risk management, but the particular objectives selected by management, while an important management responsibility and an important link to an entity's strategy, is not part of enterprise risk management. Similarly, responding to risks, based on an assessment of the risks, is a part of enterprise risk management, but which specific risk responses are selected is not. These are a matter of business judgment applied in decision-making, among many decisions and actions by management that are not part of enterprise risk management. Exhibit 2.3 lists common management actions and indicates which are considered part of enterprise risk management. (This listing purports neither to be all-inclusive nor to depict the only way to describe management activities.)

Exhibit 2.3

Management Activities	Management Activities	Enterprise Risk Management
Establish mission, values and strategy	✓	
Apply enterprise risk management in setting strategy	✓	✓
Establish objective-setting processes	✓	✓
Select entity-level and activity-level objectives	✓	
Set performance measures	✓	
Establish internal environment	✓	✓
Establish risk appetite and set risk tolerances	✓	✓
Identify potential events	✓	✓
Assess risk impact and likelihood	✓	✓
Identify and assess risk responses	✓	✓
Select and execute risk response	✓	
Effect control activities	✓	✓
Inform and communicate with internal and external parties	✓	✓
Monitor the presence and functioning of the other components of enterprise risk management	✓	✓

3. INTERNAL ENVIRONMENT

Chapter Summary: The internal environment encompasses the tone of an organization, influencing the risk consciousness of its people, and is the foundation for all other components of enterprise risk management, providing discipline and structure. Internal environment factors include an entity's risk management philosophy; its risk appetite and risk culture; oversight by the board of directors; the integrity, ethical values and competence of the entity's people; management's philosophy and operating style; and the way management assigns authority and responsibility, and organizes and develops its people.



The entity's internal environment is the foundation for all other components of enterprise risk management, providing discipline and structure. The internal environment influences how strategies and objectives are established, business activities are structured and risks are identified, assessed and acted upon. It influences the design and functioning of control activities, information and communication systems, and monitoring activities. In turn, the internal environment is influenced by the entity's history and culture. The internal environment comprises many elements, including an entity's ethical values, competence and development of personnel, management's operating style and how it assigns authority and responsibility. A board of directors is a critical part of the internal environment and significantly influences other internal environment elements.

Although all elements are important, the extent to which each is addressed will vary with the entity. For example, the chief executive of a company with a small workforce and centralized operations might not establish formal lines of responsibility and detailed operating policies. Nevertheless, the company could have an internal environment that provides an appropriate foundation for enterprise risk management.

Risk Management Philosophy

An enterprise risk management philosophy that is understood by all personnel facilitates employees' ability to recognize and effectively manage risk. The philosophy – the entity's beliefs about risk and how it chooses to conduct its activities and deal with risks – reflects the value the entity seeks from enterprise risk management and influences how enterprise risk management components are applied. While some entities may adopt enterprise risk management to satisfy requirements of an external stakeholder, such as a parent company or regulator, more often it's because management recognizes that effective risk management preserves and creates value. Each management team has its own view about what drives value for stakeholders.

Management's enterprise risk management philosophy is reflected in its policy statements and other communications. Importantly, management reinforces the philosophy not only with words but with everyday actions as well.

Risk Appetite

Risk appetite is the amount of risk an entity is willing to accept in pursuit of value. Entities often consider risk appetite qualitatively, with such categories as high, moderate or low, or they may take a quantitative approach, reflecting and balancing goals for growth, return and risk.

Risk appetite is directly related to an entity's strategy. It is considered in strategy setting, where the desired return from a strategy should be aligned with the entity's risk appetite. Different strategies will expose the entity to different risks. Enterprise risk management, applied in strategy setting, helps management select a strategy consistent with the entity's risk appetite.

Risk Culture

Risk culture is the set of shared attitudes, values and practices that characterize how an entity considers risk in its day-to-day activities. For many companies, the risk culture flows from the entity's risk philosophy and risk appetite. For those entities that do not explicitly define their risk philosophy, the risk culture may form haphazardly, resulting in significantly different risk cultures within an enterprise or even within a particular business unit, function or department.

Management considers how its risk culture affects and aligns with other elements of enterprise risk management. Where misalignment exists, management may take steps to re-shape the culture – perhaps by rethinking its risk philosophy and risk appetite – or how it applies enterprise risk management.

A gas pipeline company sought a risk culture where all personnel explicitly considered risk in their day-to-day activities. In support, one step management took was to add a series of risk-focused questions to all employee identification cards. These questions guided employee decision making: What are the risks? Who else will be affected by this event? Who else needs to be informed? The questions encouraged employees to consider the impact of potential events on other units and on the entity as a whole.

Risk Subcultures

Individual business units, functions and departments will have slightly different risk cultures. Managers of some are prepared to take more risk, while others are more conservative, and these different cultures sometimes work at cross-purposes. For example, one function may focus more on making a sale, without careful attention to regulatory compliance matters. Another function's shared values may demand that its personnel focus significant attention to ensuring compliance with all relevant regulations. Separately, these different subcultures may adversely affect the entity. But if these functions work together, complementing one another, the different cultures may collectively reflect the entity's desired risk appetite and philosophy.

Recognizing the Risk Reality

An entity that historically has not suffered losses and has no obvious significant risk exposure should not succumb to the myth that an event with adverse consequences "couldn't happen here." While a company may have competent employees, effective processes and reliable technology, many variables in both the external and internal environments can quickly change. Management should recognize that even a well-run operation is vulnerable.

Board of Directors

An entity's board of directors is a critical part of the internal environment and significantly influences other internal environment elements. The board's independence from management, experience and stature of its members, extent of its involvement and scrutiny of activities, and appropriateness of its actions all play a role. Other factors include the degree to which difficult questions are raised and pursued with management regarding strategy, plans and performance, and interaction the board or audit committee has with internal and external auditors.

An active and involved board of directors, board of trustees or comparable body should possess an appropriate degree of management, technical and other expertise coupled with the mind-set necessary to perform its oversight responsibilities. This is critical to an effective enterprise risk management environment. And, because the board must be prepared to question and scrutinize management's activities, present alternative views and act in the face of obvious wrongdoing, the board must include outside directors.

Members of top management may be effective board members, bringing knowledge of the company to the table. But there must be a sufficient number of independent outside directors not only to provide sound advice, counsel and direction, but also to serve as a necessary check and balance on management. For the internal environment to be effective, the board must have at least a majority of independent outside directors.

Integrity and Ethical Values

An entity's strategy and objectives and the way they are implemented and achieved are based on preferences, value judgments and management styles. Management's integrity and commitment to ethical values influence these preferences and value judgments, which are translated into standards of behavior. Because an entity's good reputation is so valuable, the standard of behavior must go beyond mere compliance with law. Managers of well-run enterprises increasingly have accepted the view that ethics pays and ethical behavior is good business.

Management integrity is a prerequisite for ethical behavior in all aspects of an entity’s activities. The effectiveness of enterprise risk management cannot rise above the integrity and ethical values of the people who create, administer and monitor entity activities. Integrity and ethical values are essential elements of the environment, affecting the design, administration and monitoring of other enterprise risk management components.

Establishing ethical values is often difficult because of the need to consider the concerns of several parties. Management values must balance the concerns of the enterprise, employees, suppliers, customers, competitors and the public. Balancing these concerns can be complex and frustrating because interests are often at odds. For example, providing an essential product (petroleum, lumber or food) may cause environmental concerns.

Ethical behavior and management integrity are by-products of the corporate culture, which encompasses ethical and behavioral standards and how they are communicated and reinforced. Official policies specify what the board and management want to happen. Corporate culture determines what actually happens, and which rules are obeyed, bent or ignored. Top management – starting with the CEO – plays a key role in determining the corporate culture. As the dominant personality in an entity, the CEO often sets the ethical tone.

Certain organizational factors also can influence the likelihood of fraudulent and questionable financial reporting practices. Those same factors also are likely to influence ethical behavior. Individuals may engage in dishonest, illegal or unethical acts simply because the entity gives them strong incentives or temptations to do so. Undue emphasis on results, particularly in the short term, can foster an inappropriate internal environment. Focusing solely on short-term results can hurt even in the short term. Concentration on the bottom line – sales or profit at any cost – often evokes unsought actions and reactions. High-pressure sales tactics, ruthlessness in negotiations or implicit offers of kickbacks, for instance, may evoke reactions that can have immediate (as well as lasting) effects.

Incentives cited for engaging in fraudulent or questionable reporting practices and, by extension, other forms of unethical behavior include rewards highly dependent on reported financial performance, particularly for short-term results, and upper and lower cutoffs on bonus plans.

Removing or reducing inappropriate incentives and temptations can go a long way toward eliminating undesirable behavior. As suggested, this can be achieved by following sound and profitable business practices. For example, performance incentives – accompanied by appropriate controls – can be a useful management technique as long as the performance targets are realistic. Setting realistic performance targets is a sound motivational practice; it reduces counterproductive stress as well as the incentive for fraudulent reporting. Similarly, a well-controlled reporting system can serve as a safeguard against temptation to misstate performance.

Another cause of questionable practices is ignorance. Ethical values must be not only communicated but also accompanied by explicit guidance regarding what is right and wrong. Formal codes of corporate conduct are important to and the foundation of an effective ethics program. Codes address a variety of behavioral issues, such as integrity and ethics, conflicts of interest, illegal or otherwise improper payments, and anticompetitive arrangements. Upward communications channels where employees feel comfortable bringing relevant information also are important.

Existence of a written code of conduct, documentation that employees received and understand it, and an appropriate communications channel does not ensure the code is being followed. Compliance with ethical standards, whether or not embodied in a written code of conduct, is best ensured by top management's actions and examples. Of particular importance are resulting penalties to employees who violate such codes, mechanisms that exist to encourage employee reporting of suspected violations, and disciplinary actions against employees who fail to report violations. Employees are likely to develop the same attitudes about right and wrong – and about risks and control – as those shown by top management. Messages sent by management's actions in these situations quickly become embodied in the corporate culture. And, knowledge that the CEO has “done the right thing” ethically when faced with a tough business decision sends a powerful message throughout the entity.

Commitment to Competence

Competence reflects the knowledge and skills needed to perform assigned tasks. Management decides how well these tasks need to be accomplished weighing the entity's strategy and objectives against plans for strategy implementation and achievement of the objectives. A trade-off often exists between competence and cost – it is not necessary, for instance, to hire an electrical engineer to change a light bulb.

Management specifies the competency levels for particular jobs and translates those levels into requisite knowledge and skills. The necessary knowledge and skills in turn may depend on individuals' intelligence, training and experience. Factors considered in developing knowledge and skill levels include the nature and degree of judgment to be applied to a specific job. Often a trade-off can be made between the extent of supervision and the requisite competence level of the individual.

Management's Philosophy and Operating Style

Management's philosophy and operating style affect the way the enterprise is managed, including the kinds of risks accepted. A company that has been successful accepting significant risks may have a different outlook on enterprise risk management than one that has faced harsh economic or regulatory consequences as a result of venturing into dangerous territory. An informally managed company may control operations largely by face-to-face contact with key managers. A more formally managed one may rely more on written policies, standards of behavior, performance indicators and exception reports.

Other elements of management's philosophy and operating style include preference for conservative or aggressive accounting principles, conscientiousness and conservatism with which accounting estimates are developed and attitudes toward financial reporting, information technology, business processes and personnel.

The attitude and daily operating style of top management affect the extent to which actions are aligned with risk philosophy and appetite. For example, an undisciplined operating style often is associated with – and might encourage – an appetite for high risk. An effective environment does not require that risks be avoided; rather it reinforces the need to be knowledgeable about the risks associated with strategic choices and the entity's operating environment, both internal and external. An effective environment encourages people to pursue business opportunities that align with the entity's risk appetite.

Organizational Structure

An entity's organizational structure provides the framework to plan, execute, control and monitor its activities. A relevant organizational structure includes defining key areas of authority and responsibility and establishing appropriate lines of reporting. For example, an internal audit function should be structured in a manner that achieves organizational objectivity and permits full and unrestricted access to top management and the audit committee of the board, and the chief audit executive should report to a level within the organization that allows the internal audit activity to fulfill its responsibilities.

An entity develops an organizational structure suited to its needs. Some are centralized, others decentralized. Some have direct reporting relationships, others are more of a matrix organization. Some entities are organized by industry or product line, by geographical location or by a particular distribution or marketing network. Other entities, including many state and local governmental units and not-for-profit institutions, are organized by function.

The appropriateness of an entity's organizational structure depends, in part, on its size and the nature of its activities. A highly structured organization with formal reporting lines and responsibilities, may be appropriate for a large entity that has numerous operating divisions, including foreign operations. However, such a structure could impede the necessary flow of information in a small entity. Whatever the structure, an entity should be organized to enable effective enterprise risk management, and to carry out its activities so as to achieve its objectives.

Assignment of Authority and Responsibility

Assignment of authority and responsibility involves the degree to which individuals and teams are authorized and encouraged to use initiative to address issues and solve problems, as well as limits to their authority. It also includes the establishment of reporting relationships and authorization protocols. And it pertains to policies that describe appropriate business practices, knowledge and experience of key personnel, and resources provided for carrying out duties.

Some entities have pushed authority downward to bring decision making closer to front-line personnel. A company may take this tack to become more market-driven or quality-focused – perhaps to eliminate defects, reduce cycle time or increase customer satisfaction. Alignment of authority and accountability often is designed to encourage individual initiatives, within limits. Delegation of authority, or “empowerment,” means surrendering central control of certain business decisions to lower echelons – to the individuals who are closest to everyday business transactions. This may involve empowerment to sell products at discount prices; negotiate long-term supply contracts, licenses or patents; or enter alliances or joint ventures.

A critical challenge is to delegate only to the extent required to achieve objectives. This means ensuring that risk acceptance is based on sound practices for risk identification and assessment, including sizing risks and weighing potential losses versus gains in arriving at good business decisions.

Another challenge is ensuring that all personnel understand the entity's objectives. It is essential that individuals know how their actions interrelate and contribute to achievement of the objectives.

Increased delegation sometimes is intentionally accompanied by or the result of streamlining or “flattening” the organizational structure. Purposeful structural change to encourage creativity, initiative and faster response times can enhance competitiveness and customer satisfaction. This increased delegation may carry an implicit requirement for a higher level of employee competence, as well as greater accountability. It also requires effective procedures for management to monitor results so that decisions can be overruled or accepted as necessary. Along with better, market-driven decisions, empowerment may increase the number of undesirable or unanticipated decisions. For example, if a district sales manager decides that authorization to sell at 35% off list price justifies a temporary 45% discount to gain market share, management may need to know so that it can overrule or accept such decisions going forward.

The internal environment is greatly influenced by the extent to which individuals recognize that they will be held accountable. This holds true all the way to the chief executive, who, with board oversight, has ultimate responsibility for all activities within an entity.

Human Resource Policies and Practices

Human resource practices pertaining to hiring, orientation, training, evaluating, counseling, promoting, compensating and taking remedial actions send messages to employees regarding expected levels of integrity, ethical behavior and competence. For example, standards for hiring the most qualified individuals, with emphasis on educational background, prior work experience, past accomplishments and evidence of integrity and ethical behavior, demonstrate an entity's commitment to competent and trustworthy people. The same is true when recruiting practices include formal, in-depth employment interviews and informative and insightful presentations on the entity's history, culture and operating style. Training policies can reinforce expected levels of performance and behavior by communicating prospective roles and responsibilities and by including such practices as training schools and seminars, simulated case studies and role-play exercises. Transfers and promotions driven by periodic performance appraisals demonstrate the entity's commitment to the advancement of qualified employees. Competitive compensation programs that include bonus incentives serve to motivate and reinforce outstanding performance. Disciplinary actions send a message that violations of expected behavior will not be tolerated.

It is essential that employees be equipped to tackle new challenges as issues and risks throughout the entity change and become more complex – driven in part by rapidly changing technologies and increasing competition. Education and training, whether classroom instruction, self-study or on-the-job training, must help personnel keep pace and deal effectively with the evolving environment. Hiring competent people and providing one-time training are not enough. The education process is ongoing.

Differences in Environment and Their Implications

The internal environment of an entity's autonomous subsidiaries, divisions and other units can vary widely due to differences in senior operating management's preferences, value judgments and management styles. Since operating units often are managed in different ways, it is unlikely their internal environments will be the same. It is important, therefore, to recognize the effect that varying internal environments can have on other enterprise risk management framework components.

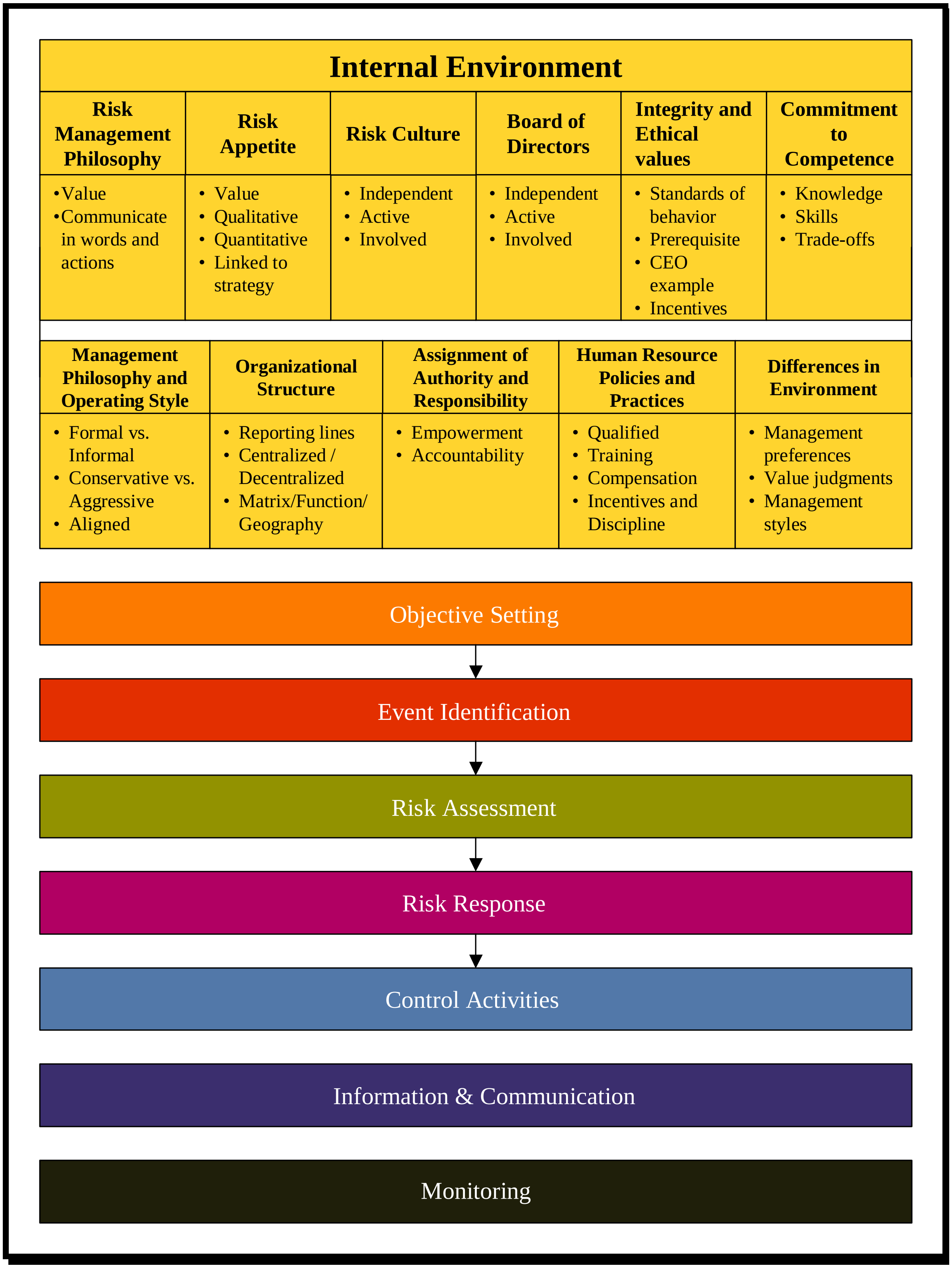
The impact of an ineffective internal environment could be far-reaching, possibly resulting in financial loss, a tarnished public image or a business failure.

An energy company generally was thought to have effective enterprise risk management since it had high-powered and respected senior managers, a prestigious board of directors, an innovative strategy, well-designed information systems and control activities, extensive policy manuals prescribing risk and control functions, and comprehensive reconciling and supervisory routines. Its internal environment, however, was significantly flawed. Management participated in highly questionable business practices, and the board turned a "blind-eye" to these practices. The company was found to have misreported financial results and suffered a loss of shareholder confidence, a liquidity crisis, and destruction of entity value. Ultimately the company went into one of the largest bankruptcies in history.

The attitude and concern of top management for effective enterprise risk management must permeate the organization. It is not sufficient to say the right words. An attitude of "do as I say, not as I do" will only bring about an ineffective environment.

Exhibit 3.1 depicts the key elements of *Internal Environment* as described in this chapter.

Exhibit 3.1



Internal Environment

Risk Management Philosophy	Risk Appetite	Risk Culture	Board of Directors	Integrity and Ethical values	Commitment to Competence
•Value •Communicate in words and actions	• Value • Qualitative • Quantitative • Linked to strategy	• Independent • Active • Involved	• Independent • Active • Involved	• Standards of behavior • Prerequisite • CEO example • Incentives	• Knowledge • Skills • Trade-offs

Management Philosophy and Operating Style	Organizational Structure	Assignment of Authority and Responsibility	Human Resource Policies and Practices	Differences in Environment
• Formal vs. Informal • Conservative vs. Aggressive • Aligned	• Reporting lines • Centralized / Decentralized • Matrix/Function/ Geography	• Empowerment • Accountability	• Qualified • Training • Compensation • Incentives and Discipline	• Management preferences • Value judgments • Management styles

Objective Setting

Event Identification

Risk Assessment

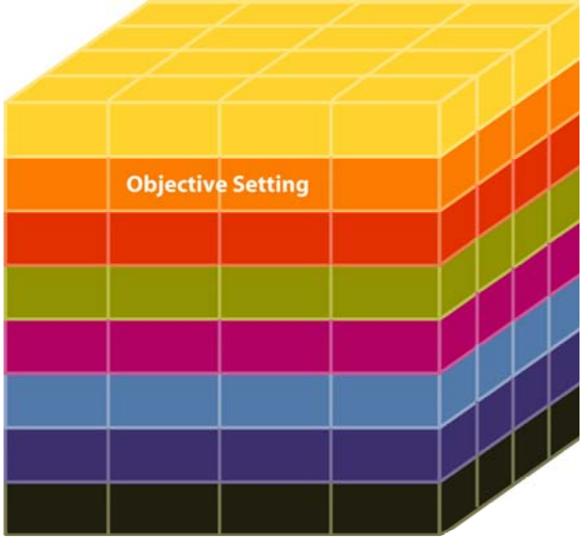
Risk Response

Control Activities

Information & Communication

Monitoring

4. OBJECTIVE SETTING



Chapter Summary: Every entity faces a variety of risks from external and internal sources, and a precondition to effective event identification, risk assessment and risk response is establishment of objectives, linked at different levels and internally consistent. Objectives are set at the strategic level, establishing a basis for operations, reporting, and compliance objectives. Objectives are aligned with the entity's risk appetite, which drives risk tolerance levels for the entity's activities.

Objective setting is a precondition to event identification, risk assessment, and risk response. There must first be objectives before management can identify risks to their achievement and take necessary actions to manage the risks.

Strategic Objectives

An entity's mission sets out in broad terms what the entity aspires to achieve. Whatever term is used, such as "mission," "vision," or "purpose," it is important that management – with board oversight – explicitly establishes the entity's broad-based reason for being. From this, management sets its strategic objectives, formulates strategy and establishes related objectives for the organization. While an entity's mission and strategic objectives are generally stable, its strategy and related objectives are more dynamic and are adjusted for changing internal and external conditions.

Strategic objectives are high-level goals, aligned with and supporting the entity's mission/vision. Strategic objectives reflect management's choice as to how the entity will seek to create value for its stakeholders.

In considering alternative strategies to achieve its strategic objectives, management identifies risks associated with a range of strategy choices and considers their implications. Various event identification and risk assessment techniques, discussed below and in later chapters, can be used in the strategy-setting process. In this way, enterprise risk management techniques are used in setting strategy and objectives.

Exhibit 4.1 provides an example of a company's mission and selected strategic and related objectives.

Exhibit 4.1

Mission	- *To provide high-quality, accessible and affordable community-based health care.*
Strategic Objectives	- *Be the first- or second-largest, full-service health care provider in mid-size metropolitan markets.* - *Rank in the top quartile in quality for our core medical services.* - *Be recognized in the local marketplaces as quality/price leaders.*
Strategies	- *Align with stand-alone hospitals in the target markets in which we do not currently have a presence.* - *Acquire high-quality under-performing service providers in target markets where feasible. Otherwise, consider lesser programs to revamp and rebuild.* - *Develop ownership participation or profit-sharing programs to attract top local medical talent.* - *Develop tailored, targeted marketing programs for large and middle market businesses in target markets.* - *Bring our state-of-the-art infrastructure systems to provide effective management and cost control.* - *Achieve leading track record of compliance with all healthcare and other applicable laws and regulations.*
Related Objectives	
- Operations	- *Initiate dialogue with leadership of 10 top under-performing hospitals and negotiate agreements with two this year.* - *Target 10 other programs in key target markets and execute agreements with five this year.* - *Identify needs and motivations of leading practitioners in major markets and structure alternative model terms.* - *Ensure at least one top medical talent is on board in each core discipline in at least five major markets this year.* - *Hold focus groups with business leaders in key markets to determine program needs.* - *Develop alternative model programs for business customers* - *Develop methodologies for quick-start implementation of information and operational systems in acquired/rebuilt hospitals.*

	- Set protocols for migration from existing systems. *- Implement new systems in one new location to serve as model going forward.*
- Reporting	*- Install our foundation systems in newly acquired facilities to provide management reports on key performance measures, with exception and trend line analysis, within four working days of month-end.* *- Ensure all facilities accurately and timely report compliance performance and issues for management review* *- Establish uniform reporting system/accounts for assembly of accurate and complete information required for external reporting*
- Compliance	*- Establish compliance office with charter, leadership and staffing centrally, providing support to local units.* *- Ensure line recognizes its primary compliance responsibilities, building into HR objectives and performance assessments.* *- Develop company-wide protocols for medical procedures, drug storage and dispensing, staffing assignments and schedules, and all aspects of patient care.* *- Review privacy policies and practices and benchmark against federal requirements and best practices.*

Related Objectives

Establishing the right objectives that support and are aligned with the selected strategy, relative to all entity activities, is critical to success. By focusing first on strategic objectives and strategy, an entity is positioned to develop related objectives at operational levels, achievement of which will create and preserve value. Each set of objectives is linked to and integrated with more specific objectives that cascade through the organization to sub-objectives established for various activities, such as sales, production and engineering, and infrastructure functions.

By setting objectives at the entity and activity levels, an entity can identify critical success factors. These are key things that must go right if goals are to be attained. Critical success factors exist for an entity, a business unit, a function, a department or an individual. By setting objectives, management can identify measurement criteria for performance, with a focus on critical success factors.

Where objectives are consistent with prior practice and performance, the linkage among activities is known. However, where new objectives depart from an entity's past practices, management must address the linkages or run increased risks. In such cases, the need for business unit objectives or sub-objectives that are consistent with the new direction is even more important.

Objectives need to be readily understood and measurable. Enterprise risk management requires that personnel at all levels have a requisite understanding of the entity's objectives as they relate to the individual's sphere of influence. All employees must have a mutual understanding of what is to be accomplished and a means of measuring what is being accomplished.

Categories of Related Objectives

Despite the diversity of objectives across entities, certain broad categories can be established:

- **Operations Objectives –** These pertain to the effectiveness and efficiency of the entity's operations, including performance and profitability goals and safeguarding resources against loss. They vary based on management's choices about structure and performance.
- **Reporting Objectives –** These pertain to the reliability of reporting. They include internal and external reporting and may involve financial or non-financial information.
- **Compliance Objectives –** These pertain to adherence to relevant laws and regulations. They are dependent on external factors, such as environmental regulation, and tend to be similar across all entities in some cases and across an industry in others.

Certain objectives follow from the business an entity is in. A mutual fund must value its holdings daily, whereas another business might do this quarterly. All publicly traded businesses must make certain filings with the SEC. These externally imposed objectives are established by law or regulation, and fall in the category of compliance, and as well as external financial reporting.

Conversely, operations objectives, as well as those for internal management reporting, are based more on preferences, judgments and management style. They vary widely among entities simply because informed, competent and honest people may select different objectives. Regarding product development, for example, one entity might choose to be an early adapter, another a quick follower, and yet another a slow lagger. These choices will affect the structure, skills, staffing and controls of the research and development function. Consequently, no one formulation of objectives can be optimal for all entities.

Operations Objectives

Operations objectives relate to the effectiveness and efficiency of the entity's operations. They include related sub-objectives for operations, directed at enhancing operating effectiveness and efficiency in moving the enterprise toward its ultimate goal.

Operations objectives need to reflect the particular business, industry and economic environments in which the entity functions. The objectives need, for example, to be relevant to competitive pressures for quality, reduced cycle times to bring products to market or changes in technology. Management must ensure that objectives reflect reality and the demands of the marketplace, and are expressed in terms that allow meaningful performance measurements. A clear set of operations objectives, linked to sub-objectives, is fundamental to success. Operations objectives provide a focal point for directing allocated resources; if an entity's operations objectives are not clear or well conceived, its resources may be misdirected.

Reporting Objectives

Reliable reporting provides management with accurate and complete information appropriate for its intended purpose. It supports management's decision making and monitoring of the entity's activities and performance. Examples of such reports may include results of marketing programs, daily sales flash reports, production quality, and employee and customer satisfaction results. Reliable reporting provides management reasonable assurance of preparation of reliable reports for external dissemination. Such reporting includes financial statements and footnote disclosures, management's discussion and analysis, and reports filed with regulatory agencies.

Compliance Objectives

Entities must conduct their activities, and often take specific actions, in accordance with relevant laws and regulations. These requirements may relate to markets, pricing, taxes, the environment, employee welfare and international trade. Applicable laws and regulations establish minimum standards of behavior, which the entity integrates into its compliance objectives. For example, occupational safety and health regulations might cause a company to define its objective as, "Package and label all chemicals in accordance with regulations." In this case, policies and procedures would deal with communication programs, site inspections and training. An entity's compliance record can significantly – either positively or negatively – affect its reputation in the community and marketplace.

Overlap of Objectives

An objective in one category may overlap or support an objective in another. The category in which an objective falls sometimes depends on circumstances. For example, providing reliable information to business unit management to manage and control production activities may serve to achieve both operations and reporting objectives. And, to the extent the information is used for reporting environmental data to the government, it serves compliance objectives.

Some entities use another category of objectives, “safeguarding of resources,” sometimes referred to as “safeguarding of assets,” which overlaps with the other categories of objectives. Viewed broadly, safeguarding of assets deals with prevention of loss of an entity’s assets or resources, whether though theft, waste, inefficiency or what turns out to be simply bad business decisions – such as selling product at too low a price, failing to retain key employees or prevent patent infringement, or incurring unforeseen liabilities. These are primarily operations objectives, although certain aspects of safeguarding can fall under the other categories. Where legal or regulatory requirements apply, these become compliance objectives. On the other hand, properly reflecting asset losses in the entity’s financial statements represents a reporting objective.

When used in conjunction with public reporting, a narrower definition of safeguarding of assets often is used, dealing with prevention or timely detection of unauthorized acquisition, use or disposition of an entity’s assets. For further discussion of this category of objectives reference should be made to *Internal Control – Integrated Framework,* including the *Addendum to Reporting to External Parties* module.

Achievement of Objectives

Establishing objectives is a component of enterprise risk management. Although objectives provide the measurable targets toward which the entity moves in conducting its activities, they may have differing degrees of importance and priority. Although an entity should have reasonable assurance that certain objectives are achieved, that may not be the case for all objectives.

Effective enterprise risk management provides reasonable assurance that an entity’s reporting objectives are being achieved. Similarly, there should be reasonable assurance that compliance objectives are being achieved. Achieving reporting and compliance objectives is largely within the entity’s control. That is, once the objectives have been determined, the entity has control over its ability to do what’s needed to meet them.

But there is a difference when it comes to operations objectives, for a number of reasons. An entity may perform as intended, yet be outperformed by a competitor. It is subject to external events – such as a change in government, poor weather and the like – where an occurrence is beyond its control. It may even have considered some of these events in its objective-setting process and treated them as having a low likelihood, with a contingency plan in case they occurred. However, such a plan only mitigates the impact of external events. It does not ensure that the objectives are achieved.

Enterprise risk management over operations focuses primarily on: developing consistency of objectives and goals throughout the organization; identifying key success factors and risks; assessing the risks and making informed responses; implementing appropriate risk responses; establishing needed controls; and timely reporting of performance and expectations. For these objectives, enterprise risk management can provide reasonable assurance that management and, in its oversight role, the board are made aware, in a timely manner, of the extent to which the entity is moving toward these objectives.

Selected Objectives

As part of enterprise risk management, management ensures that the entity has selected objectives and considered how they support the entity's strategy and mission/vision. Entity objectives also should align with the entity's risk appetite. Misalignment could result in an entity not accepting enough risk to achieve its objectives or, conversely, accepting undue risks. Effective enterprise risk management does not dictate which objectives the board and management should choose, but that management has a process that aligns objectives with the entity's mission and strategy and that the chosen objectives are consistent with the entity's risk appetite.

Risk Appetite

Risk appetite, established by management and reviewed by the board of directors, is a guidepost in strategy setting. Companies may express risk appetite as the acceptable balance between growth, risk and return, or as risk-adjusted shareholder value-added measures. Not-for-profit entities may express risk appetite as the level of risk they will accept in providing value to their stakeholders.

There is a relationship between an entity's risk appetite and its strategy. Usually any of a number of different strategies can be designed to achieve desired growth and return goals, each having different risks. Enterprise risk management, applied in strategy setting, helps management select a strategy consistent with its risk appetite. If the risk associated with a strategy is inconsistent with the entity's risk appetite, the strategy is revised. This may occur where management initially formulates a strategy that exceeds the entity's risk appetite, or where the strategy does not embrace sufficient risk to allow the entity to achieve its vision/mission.

The entity's risk appetite is reflected in entity strategy, which in turn guides resource allocation. Management allocates resources across business units with consideration of the entity's risk appetite and individual business units' strategic plans to generate a desired return on invested resources. Management looks to align the organization, people, processes and infrastructure to facilitate successful strategy implementation and enable the entity to stay within its risk appetite.

Risk Tolerances

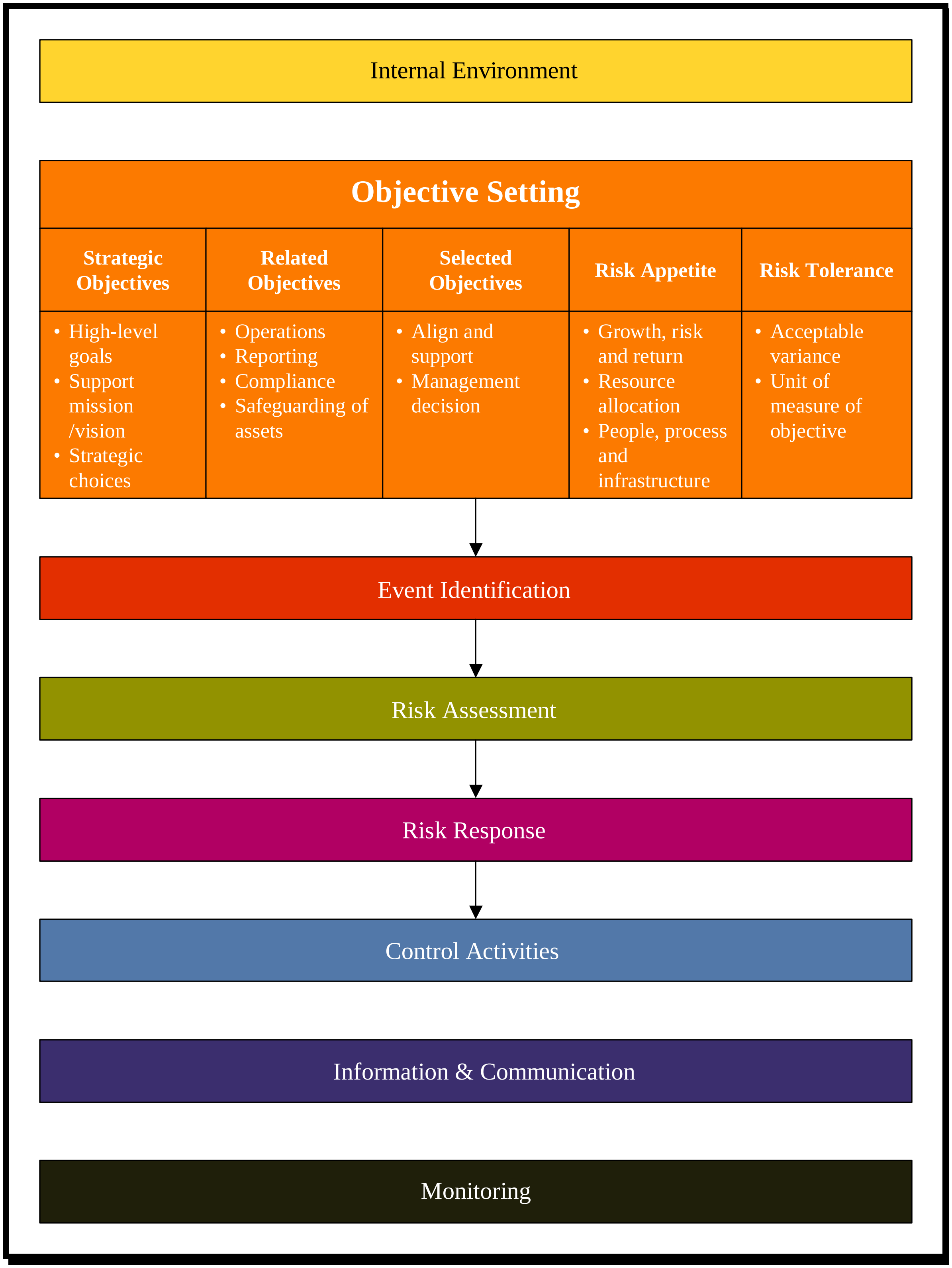
Risk tolerances are the acceptable levels of variation relative to the achievement of objectives. Risk tolerances can be measured, and often are best measured in the same units as the related objectives.

Performance measures are aligned to help ensure that actual results will be within the acceptable risk tolerances. In setting risk tolerances, management considers the relative importance of the related objectives and aligns risk tolerances with risk appetite. Operating within risk tolerances provides management greater assurance that the entity remains within its risk appetite and, in turn, provides a higher degree of comfort that the entity will achieve its objectives.

A company targets on-time delivery at 98%, with acceptable level of variation in the range of 97%–100% of the time; targeting training with a pass rate of 90%, with acceptable performance variation being a pass rate of at least 75%; and expecting staff to respond to all customer complaints within 24 hours, but accepting that up to 25% of these complaints may receive a response within 24 –36 hours.

Exhibit 4.2 depicts the key elements of *Objective Setting* as described in this chapter.

Exhibit 4.2



Internal Environment

Objective Setting

Strategic Objectives	**Related Objectives**	**Selected Objectives**	**Risk Appetite**	**Risk Tolerance**
• High-level goals • Support mission /vision • Strategic choices	• Operations • Reporting • Compliance • Safeguarding of assets	• Align and support • Management decision	• Growth, risk and return • Resource allocation • People, process and infrastructure	• Acceptable variance • Unit of measure of objective

Event Identification

Risk Assessment

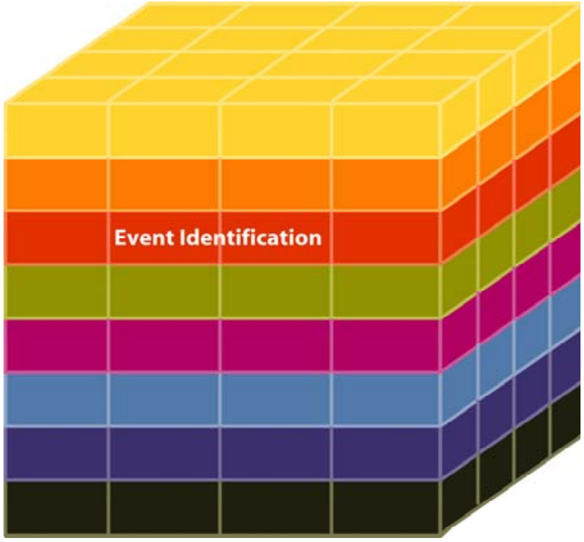
Risk Response

Control Activities

Information & Communication

Monitoring

5. EVENT IDENTIFICATION



Chapter Summary: Management identifies potential events affecting an entity's ability to successfully implement strategy and achieve objectives. Events with a potentially negative impact represent risks, which require management's assessment and response. Events with a potentially positive impact may offset negative impacts or represent opportunities. Management channels opportunities back into the strategy and objective-setting processes. A variety of internal and external factors give rise to events. When identifying potential events, management considers the full scope of the organization. Management considers the context within which the entity operates and its risk tolerances.

Events

An event is an incident or occurrence emanating from internal or external sources that could affect implementation of strategy or achievement of objectives. Events may have positive or negative impacts, or both.

As part of event identification, management recognizes that uncertainties exist, but does not know when an event may occur, or its outcome should it occur. Management initially considers a range of potential events – affected by both internal and external factors – without necessarily focusing on whether the potential impact is positive or negative.

Potential events range from the obvious to the obscure, and the potential effects from the significant to the insignificant. To avoid overlooking relevant events, identification is best made apart from the assessment of the likelihood of the event occurring, which is the topic of *Risk Assessment*. However, practical limitations exist, and it is often difficult to know where to draw the line. But even potential events with relatively remote possibility of occurrence should not be ignored at the event identification stage if the potential impact on achieving an important objective is great.

Factors Influencing Strategy and Objectives

A myriad of external and internal factors influences how events could potentially affect strategy implementation and achievement of objectives. As part of enterprise risk management, personnel recognize the importance of understanding external and internal factors and the type of events that can emanate there from. Management considers current factors, as well as those that may occur in the future. External factors include:

- Economic and Business – Related events might include emerging competition and market movements. Management considers both macroeconomic conditions, such as general price movements, and microeconomic conditions, such as competition in terms of emerging competitors with new product substitutes.
- Natural environment – Events might include such natural disasters as flood, fire or earthquake, and sustainable development.
- Political – Events might include newly elected government officials, political agendas and new legislation and regulations.
- Social – Events might include changing demographics, new food harvesting and preparation methods, and shifting family structures and work/life priorities.
- Technological – Events might include evolving electronic commerce, expanded availability of data and reductions in infrastructure costs.

Events also stem from choices management makes about how it will function. The entity's capability and capacity reflect previous choices, influence future events and affect management decisions. Internal factors include:

- Infrastructure – Events might include unexpected repair costs, or equipment incapable of supporting production demand.
- Personnel – Events might include increase in number of on-the-job accidents, increased human error or propensity for fraudulent behavior.
- Process – Events might include product quality deficiencies, unexpected downtime, or service delays.
- Technology – Events might include inability to maintain adequate uptime, handle increased volumes, deliver requisite data integrity, or incorporate needed system modifications.

Identifying external and internal factors that influence events is useful to effective event identification. Once the major contributing factors have been identified, management can consider their significance and, where possible, link the internal and external factors to the identification of potential events that impact objectives.

A manufacturer and importer of footwear established a vision of becoming an industry leader in high-quality footwear. To achieve this, it set out to manufacture shoes that combine durability and comfort, using the most advanced techniques, together with highly selective import sourcing. The company reviewed its external operating environment and identified social factors and related events such as an aging consumer market and changing trends in work attire. Economic factors identified foreign currency fluctuations. Internal technology factors pointed to outdated distribution management systems, and personnel factors to inadequate marketing training.

In most instances, for any stated or implied objective, different factors and related events may be identified. In addition to identifying events at the entity level, events also should be identified at the activity level. This helps focus risk assessment (the subject of the next chapter) on major business units or functions, such as sales, production, marketing, technology development, and research and development. Assessing activity-level events also contributes to maintaining alignment between the entity's risk profile and risk appetite.

Event Identification Methodology and Techniques

An entity's event identification methodology may comprise a combination of techniques, together with supporting tools. For instance, management may use interactive group workshops as part of its event identification methodology, with a facilitator employing a variety of technology-based tools to assist participants.

Event identification techniques look to both the past and the future. Techniques that focus on past events and trends consider such matters as payment default histories, changes in commodity prices and lost time accidents. Techniques that focus on future exposures consider such matters as exposure to shifting demographics, new market conditions and competitor actions.

Techniques vary widely in level of sophistication. While many of the more sophisticated techniques are industry-specific, most are derived from a common approach. For example, both the financial services and health and safety industries use loss event tracking techniques. Although these techniques start with a focus on common historical events, the more basic approaches look at potential events based on internal staff perceptions, while more advanced techniques are based on factual sources of observable events – and then feed the data into sophisticated projection models. Companies more advanced in enterprise risk management will employ a combination of techniques that consider both past and potential future events.

Techniques also vary in where they are used within an entity. Some focus on detailed data analysis and create a bottom-up view of events, while others focus from the top down. Exhibit 5.1 provides examples of event identification techniques.

Exhibit 5.1

- ***Event inventories*** *– These are detailed listings of potential events common to companies within a particular industry, or to a particular process or activity common across industries. Software products can generate relevant lists and the associated risks. Some entities use such generic lists as a starting point for event identification activities. For example, a company undertaking a software development project may draw on an inventory detailing generic events related to software development projects.*
- ***Internal analysis*** *– This may be done as part of a routine business planning cycle process, typically via a business unit's staff meetings. Internal analysis sometimes utilizes information from other stakeholders (customers, suppliers, other business units) or subject matter expertise outside the unit (internal or external functional experts or internal audit staff). For example, a company considering introduction of a new product utilizes its own historical experience, along with external market research identifying events that have impacted the success of competitors' products.*
- ***Escalation or threshold triggers*** *– These triggers alert management to potential areas of concern by comparing current transactions, or events, to predefined criteria. Once triggered, an event may require further assessment or an immediate response. For example, management may monitor sales volume in markets targeted for new marketing or advertising programs and redirect resources based on results. Or, management may track competitors' pricing structures and consider changes in its own prices when a specified threshold is met.*
- ***Facilitated workshops and interviews*** *– These techniques identify events by drawing on accumulated knowledge and experience of management, staff and other stakeholders through structured discussions. The facilitator or interviewer leads a discussion about events that may impact achievement of entity or unit objectives. For example, a financial controller may facilitate a workshop with members of the accounting team to identify events that have an impact on the entity's external financial reporting objectives. By combining the knowledge and experience of team members, important potential events are identified that otherwise might be missed.*

- ***Leading event indicators*** *– By monitoring data correlated to events, entities identify the existence of conditions that could give rise to an event – often referred to as leading event indicators. For example, financial institutions have long recognized the correlation between late loan payments and eventual loan default, and the positive effect of early intervention. Monitoring payment patterns enables the potential for default to be mitigated by timely action.*
- ***Loss event data methodologies*** *– Repositories of data on past individual loss events are a useful source of information for identifying trends and root causes. Once a root cause has been identified, management may find that assessment and treatment of it is a more effective solution than addressing individual events. For example, a company operating a large fleet of automobiles maintains a database of accident claims and through analysis, finds that a disproportionate percentage of accidents, in number and monetary amount, are linked to staff drivers in particular units, geographies and age bracket. This analysis equips management to identify root causes of events and take necessary action.*
- ***Process flow analysis*** *– This technique considers the combination of inputs, tasks, responsibilities and outputs that combine to form a process. By considering the internal and external factors that affect inputs, or activities within a process, an entity identifies events that could affect achievement of process objectives. For example, a medical laboratory maps its processes for receipt and testing of blood samples. Using process maps, the entity considers the range of factors that could affect inputs, tasks and responsibilities, identifying exposures related to sample labeling, handoffs within the process and personnel shift changes.*

Depth, breadth, timing and discipline in event identification vary among entities. Management selects methodologies that fit its risk culture and ensures that the entity develops needed event identification capabilities and that supporting techniques and tools are in place. Overall, the event identification methodology needs to be robust, as it forms the basis for risk assessment and risk response components.

Event Interdependencies

Events do not occur in isolation. One event can trigger another, and events can occur concurrently. In event identification, management should understand how events interrelate. By assessing the interrelationships, one can determine where risk management efforts are best directed. For example, a change to a central bank interest rate affects foreign exchange rates and, in turn, a company's currency transaction gains and losses. A decision to curtail capital investment defers an upgrade to distribution management systems, causing additional downtime and increased operating costs. A decision to expand marketing training may increase frequency and volume of repeat customer orders.

Event Categories

It may be useful to group potential events into categories. By aggregating events horizontally across an entity and vertically within operating units, management develops an understanding of the interrelationships between events, gaining enhanced information as a basis for risk assessment. By grouping together similar potential events, management can better determine potential opportunities and risks.

Event categorization also allows management to consider the completeness of its event identification efforts. For instance, a company may have categorized potential events related to creditor collections into a single category called creditor defaults. By examining the potential events in this category, management can gauge whether it has identified all significant potential events related to creditor defaults.

Furthermore, event categorization can reinforce an entity-level portfolio view of events across the entity.

Some companies have developed event categories based on categorization of their objectives, using a hierarchy that begins with high-level objectives and then cascades down to objectives relevant to organizational units, functions or business processes.

Exhibit 5.2 illustrates one approach that classifies events based on internal and external factors. The broad headings in this exhibit represent internal and external factors, which can lead to the listed types of illustrative events.

Exhibit 5.2

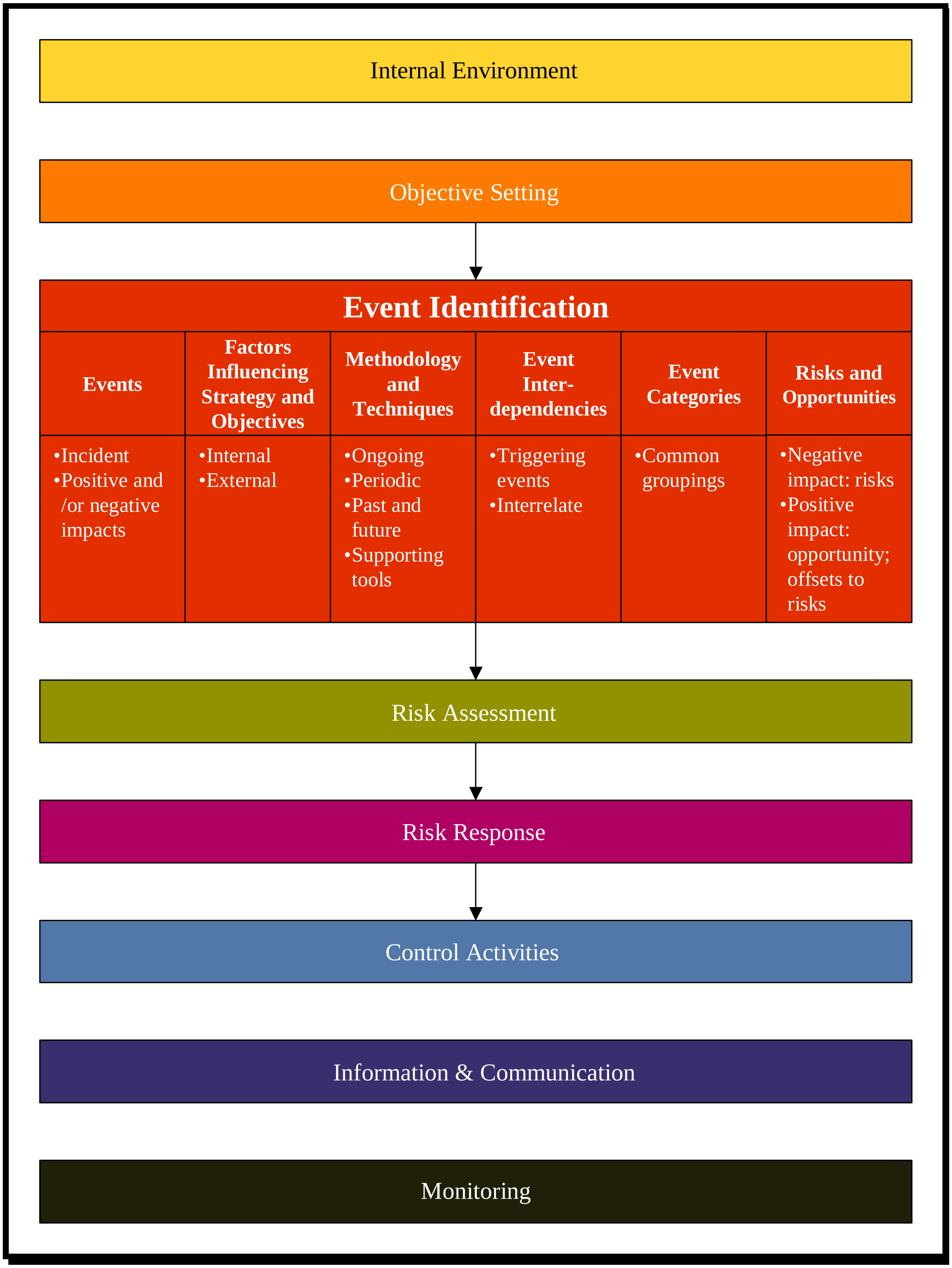
Event Categories		
Internal Factors	**External Factors**	
Infrastructure • Availability of assets • Capability of assets • Access to capital • Complexity • Mergers/ acquisitions **Personnel** • Employee capability • Fraudulent activity • Health and safety • Judgment • Malfeasance • Security practices • Sales practices **Process** • Capacity • Design • Execution • Suppliers/ dependencies **Technology** • Data – Acquisition – Maintenance – Distribution – Confidentiality – Integrity • Data and system availability • Capacity • System – Selection – Development – Deployment – Reliability	**Economic** • Capital availability • -Credit – Issuance – Default – Concentration • Liquidity – Market – Funding – Cash flow • Market – Commodity prices – Interest rate – Unemployment – Indices – Exchange rate – Equity valuation – Real estate values **Business** • Brand/ trademark • Competition • Consumer behavior • Counterparty • Fraud • Industry standards • Ownership structure • Publicity • Product relevance	**Technological** • Electronic commerce • External data • Emerging technology **Natural Environment** • Biodiversity • Emissions, effluents and waste • Energy • Fire • Natural disaster (earthquake, flood, etc.) • Sustainable development • Transport • Water **Political** • Governmental changes • Legislation • Public policy • Regulation **Social** • Demographics • Corporate citizenship • Environmental stewardship • Privacy •

Distinguishing Risks and Opportunities

Events may have a negative impact, a positive impact or both. Events with a potentially negative impact represent risks, which require management's assessment and response. Accordingly, risk is the possibility that an event will occur and adversely affect the achievement of objectives. Events with a potentially positive impact represent opportunities, or offset the negative impact of risks. Events representing opportunities are channeled back to management's strategy or objective-setting processes, so that actions can be formulated to seize the opportunities. Events potentially offsetting the negative impact of risks are considered in management's risk assessment and response.

Exhibit 5.3 depicts the key elements of *Event Identification* as described in this chapter.

Exhibit 5.3



Internal Environment

Objective Setting

Event Identification

Events	**Factors Influencing Strategy and Objectives**	**Methodology and Techniques**	**Event Inter-dependencies**	**Event Categories**	**Risks and Opportunities**
•Incident •Positive and /or negative impacts	•Internal •External	•Ongoing •Periodic •Past and future •Supporting tools	•Triggering events •Interrelate	•Common groupings	•Negative impact: risks •Positive impact: opportunity; offsets to risks

Risk Assessment

Risk Response

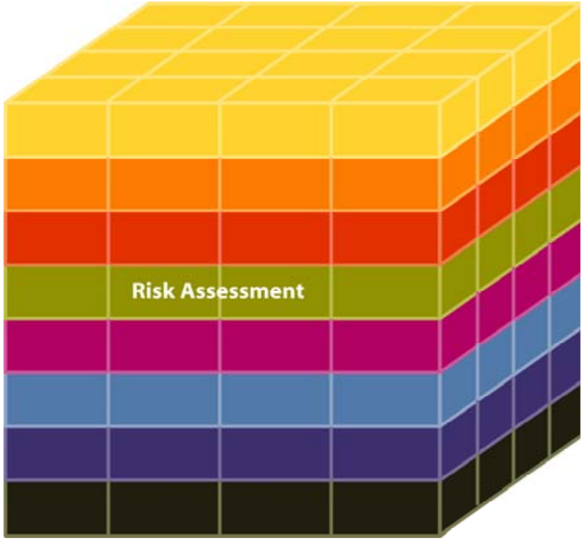
Control Activities

Information & Communication

Monitoring

6. RISK ASSESSMENT

Chapter Summary: Risk assessment allows an entity to consider the extent to which potential events might have an impact on achievement of objectives. Management should assess events from two perspectives – likelihood and impact– and normally uses a combination of qualitative and quantitative methods. The positive and negative impacts of potential events should be examined, individually or by category, across the entity. Potentially negative events are assessed on both an inherent and a residual basis.



Context for Risk Assessment

External and internal factors influence which events may occur, as discussed in the previous chapter, and to what extent the events will affect an entity's achievement of objectives. Although some factors are common to companies in an industry, many are unique to a particular entity, because of its established objectives and past choices. In risk assessment, management considers the mix of potential future events relevant to the entity and its activities. This entails examining factors – including entity size, complexity of operations and degree of regulation over its activities – that shape the entity's risk profile and influence the methodology it uses to assess risks.

Inherent and Residual Risk

Management considers both inherent and residual risk. Inherent risk is the risk to an entity in the absence of any actions management might take to alter either the risk's likelihood or impact. Residual risk is the risk that remains after management responds to the risk.

In assessing risk, management considers the impact of expected and unexpected potential events. Many events are routine and recurring, and they are already addressed in management programs and operating budgets. Others are unexpected, often having a low likelihood of occurrence but may have a significant potential impact. Unexpected events usually are responded to separately. However, uncertainty exists with respect to both expected and unexpected potential events, and each has the potential to affect strategy implementation and achievement of objectives. Accordingly, management assesses the risk of all potential events that are likely to have a significant impact on the entity. Risk assessment is applied first to inherent risks. Once risk responses have been developed, management then uses risk assessment techniques in determining residual risk.

Estimating Likelihood and Impact

Uncertainty of potential events is evaluated from two perspectives – likelihood and impact. Likelihood represents the possibility that a given event will occur, while impact represents its effect. Likelihood and impact are commonly used terms, although some entities use terms such as probability, and severity or consequence. Sometimes the words take on more specific connotations, with "likelihood" indicating the possibility that a given event will occur in qualitative terms such as high, medium and low, or other judgmental scales, whereas "probability" may be used to express a quantitative measure as a percentage, frequency of occurrence, or other numerical metric.

Management may choose to express potential likelihood and impact in terms such as an estimate of expected or worst-case value, or a range or distribution. It may describe identified and assessed risks in words or portray them in graphs. One example is risk mapping, which depicts risks by event category, organizational objective or other grouping. This facilitates reporting risks at multiple levels, including organizational, business unit, function or process.

Determining how much attention should be given to assessing the array of risks an entity faces is difficult and challenging. Management recognizes that a risk with a low likelihood of occurrence and little potential impact generally does not warrant further consideration. On the other hand, a risk with high likelihood of occurrence and significant potential impact demands considerable attention. Circumstances in between these extremes usually require difficult judgments. It is important that the analysis be rational and careful.

Because risks are assessed in the context of an entity's strategy and objectives, management naturally tends to focus on risks with short- to mid-term time horizons. However, some elements of strategic direction and objectives extend to the longer term. As a result, management needs to be cognizant of the longer timeframes, and not ignore risks that might be further out.

A company operating in California may consider the risk of an earthquake disrupting its business operations. Without a specified risk assessment time horizon, the likelihood of an earthquake exceeding 6.0 on the Richter scale is high, perhaps virtually certain. On the other hand, the likelihood of such an earthquake occurring within two years is substantially lower. By establishing a time horizon, the entity gains greater insight into the relative importance of the risk and an enhanced ability to compare multiple risks.

Management often uses performance measures in determining the extent to which objectives are being achieved and normally uses the same unit of measure when considering the potential impact of a risk to the achievement of a specified objective. A company, for example, with an objective of maintaining a specified level of customer service will have devised a rating or other measure for that objective – such as a customer satisfaction index, number of complaints or measure of repeat business. When assessing the impact of a risk that might affect customer service – such as the possibility that the company's web site might be unavailable for a time period – impact is best determined using the same measures.

Using Observable Data

Estimates of risk likelihood and impact often are determined using data from past observable events, which may provide a more objective basis than entirely subjective estimates. Internally generated data based on an entity's own experience may reflect less subjective personal bias and provide better results than data from external sources. However, even where internally generated data are a primary input, external data can be useful as a checkpoint or to enhance the analysis. Caution should be exercised when using past events to make predictions about the future, as factors influencing events may change over time.

Management assessing the risk of production stoppages because of equipment failure looks first at frequency and impact of previous parts failures of its own manufacturing equipment. It then supplements that data with industry benchmarks. This allows a more precise estimate of likelihood and impact of failure, enabling more effective preventive maintenance scheduling.

Qualitative and Quantitative Methodology and Techniques

An entity's risk assessment methodology comprises a combination of qualitative and quantitative techniques. Management often uses qualitative assessment techniques where risks do not lend themselves to quantification or when sufficient credible data required for quantitative assessments either are not practicably available or obtaining or analyzing data is not cost-effective. Quantitative techniques typically bring more precision and are used in more complex and sophisticated activities to supplement qualitative techniques.

Quantitative assessment techniques usually require a higher degree of effort and rigor, sometimes using mathematical models. Quantitative techniques are dependent on the quality of the supporting data and assumptions, and are most relevant for exposures that have a known history and frequency of variability and allow reliable forecasting. Exhibit 6.1 provides examples of quantitative risk assessment techniques.

Exhibit 6.1

- ***Benchmarking –*** *A collaborative process among a group of entities, benchmarking focuses on specific events or processes, compares measures and results using common metrics, and identifies improvement opportunities. Data on events, processes and measures are developed to compare performance. Some companies use benchmarking to assess the impact and likelihood of potential events across an industry.*
- ***Probabilistic Models –****Probabilistic models associate a range of events and the resulting impact with the likelihood of those events based on certain assumptions. Likelihood and impact are assessed based on historical data or simulated outcomes reflecting assumptions of future behavior. Examples of probabilistic models include value at risk, cash flow at risk, earnings at risk and the development of credit and operational loss distributions. Probabilistic models may be used with different time horizons to estimate such outcomes as the range of values of financial instruments over time. Probabilistic models also may be used to assess expected or average impacts versus extreme or unexpected impacts.*
- ***Non-probabilistic Models*** *– Non-probabilistic models use subjective assumptions in estimating the impact of events without quantifying an associated likelihood. Assessing the impact of events is based on historical or simulated data and assumptions of future behavior. Examples of non-probabilistic models include sensitivity measures, stress tests and scenario analyses.*

To gain consensus on likelihood and impact using qualitative assessment techniques, entities may employ the same approach they use in identifying events, such as interviews and workshops. A risk self-assessment process captures participants' views on the potential likelihood and impact of future events, using either descriptive or numerical scales.

An entity need not use common assessment techniques across all business units. Rather, the choice of techniques should reflect the need for precision and the culture of the business unit. However, the methods used by individual business units should facilitate the entity's assessment of risks across the entity.

One business unit uses self-assessment questionnaires to identify and assess risks at a process level. Another unit uses workshops to identify and assess risks at a process level. The risks are assessed on an inherent and residual basis, and then organized and grouped by risk categories and objectives for both business units.

Management is able to derive an entity-wide quantitative impact measure of an event when all of its individual risk assessments for that event are expressed in quantitative terms. For example, the impact on gross margin of a change in energy prices is computed across business units and entity-wide impact is determined. Where there is a blend of qualitative and quantitative measures, management develops a qualitative assessment across both the qualitative and quantitative measures, with the resulting composite assessment expressed in qualitative terms. Establishing common likelihood and impact terms across an entity and common risk categories for qualitative measures facilitates these composite assessments of risk.

Correlation of Events

Management may assess how events correlate, where sequences of events combine and interact to create significantly different probabilities or impacts. While the impact of a single event might be slight, a sequence of events might have more significant impact. Management may use stress testing to assess the impact of extreme events and use scenario analysis to assess the effects of multiple events. Where potential events are not directly related, management assesses them individually. For example, a company with business units with exposure to different price fluctuations – such as pulp prices and energy prices – would assess the risks relative to market movements separately. This assessment may be presented as a distribution graph, a range of potential probabilities and impacts, or in some other form.

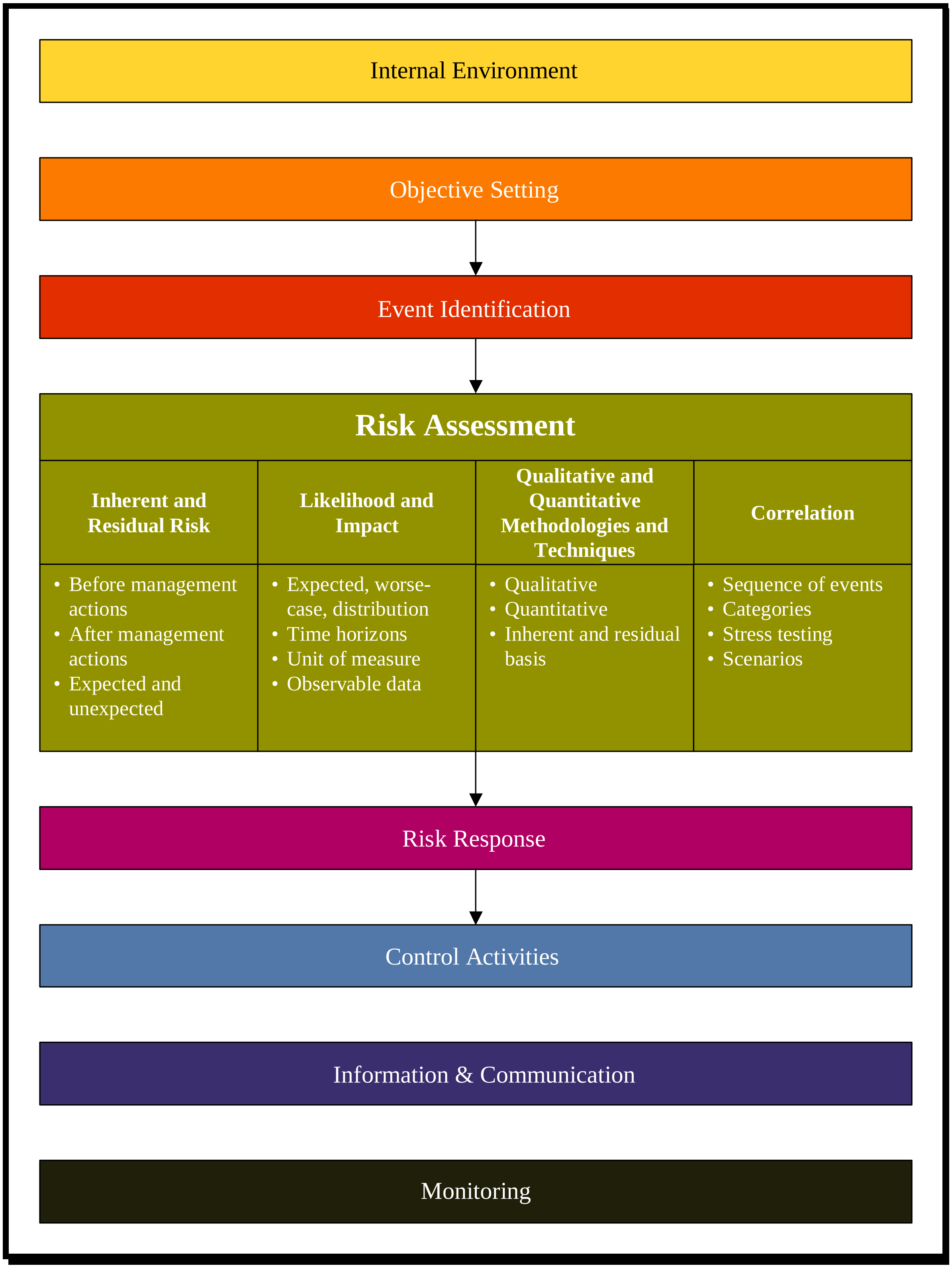
Where risks are likely to occur within multiple business units, management may assess and group identified events into common event categories. An example is a change in government interest rates that affects multiple business units of a financial services company.

An old valve on a propane tank in a garage allows propane to leak; the garage door is closed to keep heat in adjoining offices; a garage door remote control device is pressed by a truck driver pulling into the driveway. Together, the presence of gas and a spark in the garage-opener motor results in an explosion. These distinct events interrelate and result in a significant risk.

Looking at interrelationships of risk likelihood and impact is an important management responsibility. Effective enterprise risk management requires that risk assessment be done with respect to both inherent risk, and risk following risk response, as discussed in the next chapter.

Exhibit 6.2 illustrates the key elements of *Risk Assessment* as described in this chapter.

Exhibit 6.2



Internal Environment

Objective Setting

Event Identification

Risk Assessment

Inherent and Residual Risk	**Likelihood and Impact**	**Qualitative and Quantitative Methodologies and Techniques**	**Correlation**
• Before management actions • After management actions • Expected and unexpected	• Expected, worse-case, distribution • Time horizons • Unit of measure • Observable data	• Qualitative • Quantitative • Inherent and residual basis	• Sequence of events • Categories • Stress testing • Scenarios

Risk Response

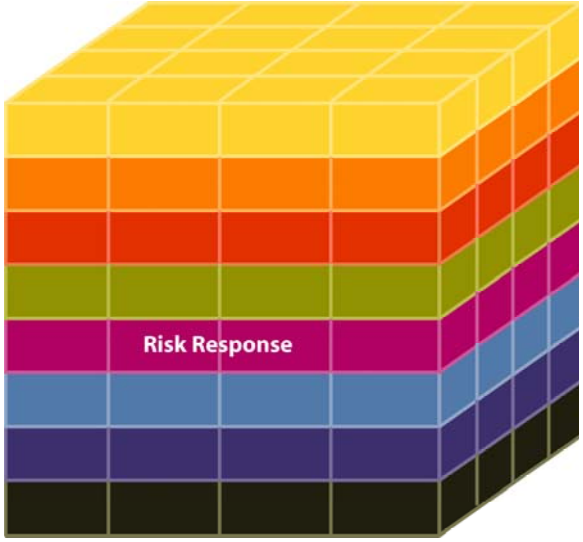
Control Activities

Information & Communication

Monitoring

7. RISK RESPONSE

Chapter Summary: Having assessed relevant risks, management determines how it will respond. Responses include risk avoidance, reduction, sharing and acceptance. In considering its response, management considers costs and benefits, and selects a response that brings expected likelihood and impact within the desired risk tolerances.



Identifying Risk Responses

Risk responses fall within the following categories:

- **Avoidance** – Action is taken to exit the activities giving rise to risk. Risk avoidance may involve exiting a product line, declining expansion to a new geographical market, or selling a division.
- **Reduction** – Action is taken to reduce the risk likelihood or impact, or both. This may involve any of a myriad of everyday business decisions.
- **Sharing** – Action is taken to reduce risk likelihood or impact by transferring or otherwise sharing a portion of the risk. Common risk-sharing techniques include purchasing insurance products, pooling risks, engaging in hedging transactions, or outsourcing an activity.
- **Acceptance** – No action is taken to affect likelihood or impact.

Exhibit 7.1 provides examples of risk responses within the above categories.

Exhibit 7.1

***Avoidance** – A not-for-profit organization identified and assessed risks of providing direct medical services to its members and decided not to accept the associated risks. It decided instead to provide a referral service.*

Reduction – *A stock-clearing corporation identified and assessed the risk of its systems not being available for more than three hours and concluded that it would not accept the impact of such an occurrence. The company invested in technology with enhanced self-detecting failure and back-up systems to reduce the likelihood of system unavailability.*
Sharing – *A university identified and assessed the risk associated with managing its student dorms and concluded that it did not have the requisite in-house capabilities to effectively manage large residential properties. The university outsourced the dorm management to a property management company better able to reduce the impact and likelihood of property-related risks.*
Acceptance – *A government agency identified and assessed the risks of fire to its infrastructure across diverse geographical regions and assessed the cost of sharing the impact of its risk through insurance coverage. It concluded that the incremental cost of insurance and related deductibles exceeded the likely cost of replacement and decided to accept this risk.*

The avoidance response suggests that either the cost of other responses would exceed the desired benefit, or no response option was identified that would reduce the impact and likelihood to an acceptable level. Reduction and sharing responses reduce residual risk to a level that is in line with an entity’s risk tolerances, while an acceptance response suggests that inherent risk is already in line with risk tolerances.

For many risks, appropriate response options are obvious and well accepted. For instance, a response option appropriate for the loss of computing availability is the development of a business continuity plan. For other risks, available options may not be readily apparent, requiring more extensive identification activities. For instance, response options relevant to mitigating the effect of competitor activities on brand value might require market research testing and analysis.

As part of enterprise risk management, for significant risks an entity typically considers potential responses from a range of response categories. This gives sufficient depth to response selection and also challenges the “status quo.”

A large software developer considered insuring its building against fire damage. In analyzing risks relative to the loss of the building, it concluded that the most significant impact of a fire was not the financial loss of the building, but displacement of its employees and interruption of operations. The company determined it had the capital capacity to reconstruct its building and concluded it did not need fire insurance for the building. It was willing to accept the risk of financial loss of the building, instead choosing to reallocate its resources to address how it would deploy and equip staff following a loss.

In determining potential responses, management should consider such things as:

- Evaluating effects of potential risk responses on risk likelihood and impact – and which response options align with the entity's risk tolerances,
- Assessing the costs versus benefits of potential risk responses, and
- Possible opportunities to achieve entity objectives going beyond dealing with the specific risk.

Evaluating Possible Risk Responses

Inherent risks are analyzed and responses evaluated with the intent of achieving a residual risk level aligned with the entity's risk tolerances. Any of several responses may bring residual risk in line with risk tolerances, and sometimes a combination of responses provides the optimum result. Similarly, certain responses will affect the risk of multiple potential events. Because risk responses may address multiple risks, management may discover that additional actions are not warranted. Existing procedures may be sufficient or may need to be performed better. Accordingly, management considers how individual responses, or combinations of responses, interact to affect potential events.

Evaluating Effect of Response on Likelihood and Impact

In evaluating response options, management considers the effect on both risk likelihood and impact, and understands that a response might affect likelihood and impact differently.

> *A business continuity plan for a computer center, while effective in mitigating the impact of disasters such as an earthquake, has no effect on the likelihood that an earthquake will occur. Conversely, while the choice to relocate a company's computer center to a more seismic-stable region reduces the likelihood an earthquake will affect the building, it does not affect the impact should an earthquake of comparable severity occur.*

The potential response to assessment of likelihood and impact may consider past events and trends, and potential future scenarios. In evaluating alternative responses, management determines their potential effect typically using the same units of measure for the objective and associated risks as established in the risk assessment component.

Assessing the Costs Versus Benefits

Resources always have constraints, and entities must consider the relative costs and benefits of alternative risk response options. Cost and benefit measurements for implementing risk response options are made with different levels of precision. Generally, it is easier to deal with the cost side of the equation, which, in many cases, can be quantified fairly precisely. All direct costs associated with instituting a response, and the indirect costs where practically measurable, usually are considered. Some entities also include opportunity costs associated with use of resources.

In other cases, however, it may be more difficult to quantify costs. It may be difficult to quantify time and effort, or to manage certain internal factors, such as management's commitment to ethical values or the competence of employees who perform event identification and risk assessments. It also may be difficult to capture external information, such as market intelligence on evolving customer preferences.

The benefit side may involve an even more subjective valuation. For example, the benefits of effective training programs are usually apparent, but difficult to quantify. Nevertheless, certain internal factors can be considered in assessing potential benefits: the likelihood of the undesired event occurring, the nature of the event, and the potential financial or operating effect the event might have on an entity.

While challenges in assessing costs and benefits exist, cost–benefit analyses should be performed at a level sufficient to evaluate risk responses on an individual risk or portfolio basis. Some entities may choose to assess risk responses in such terms as additional capital required – for example, return on investment or capital at risk – and may consider such matters as inflation, discount rates and sensitivity analysis.

Looking at risks as interrelated allows an entity to pool its risk reduction and risk sharing responses. For instance, when sharing risk via insurance, it may be beneficial to combine risks under one policy since pricing usually is reduced when larger exposures are insured under one financing arrangement.

Opportunities in Response Options

Event identification describes how enterprise risk management identifies events that affect achievement of entity objectives, either positively or negatively. Events with positive potential impacts represent opportunities, and are channeled back to the strategy or objective-setting processes.

Similarly, opportunities with the potential for significant upside results may be identified when considering risk response. Management may identify innovative responses, which while fitting within the response categories described earlier in this chapter, may be entirely new to the entity or even an industry. Such opportunities may surface when existing risk response options are reaching the limit of effectiveness, and when further refinements are likely to provide only marginal changes to a risk impact or likelihood. An example is the creative response by an automobile insurance company to the high number of accidents at certain road intersections – it decided to fund enhancements to traffic signal lights, reducing accident claims and enhancing margins.

Selected Responses

Once the effects of alternative risk responses have been evaluated, management decides how to manage the risk. Effective enterprise risk management requires that management select a response or combination of responses that brings anticipated risk likelihood and impact within risk tolerances.

Once management selects a response, it may need to develop an implementation plan to execute the response and recalibrate the risk on a residual basis. Additionally, procedures are needed to enable management to ensure effective implementation of the actions. Those procedures represent *Control Activities.*

Management recognizes that some level of residual risk will always exist, not only because resources are limited, but also because of inherent future uncertainty and limitations inherent in all activities.

Iterative Process

Evaluating alternative responses to inherent risk requires consideration of risks that might result from the response itself. This may prompt an iterative process where before management finalizes a decision, it considers risks resulting from the response, including those that might not be immediately evident.

In response to risk of increases in the price of natural gas used in power generation, an electric utility company considered structuring arrangements with customers such that much of the impact of price volatility would flow through to the customers. With this response, the company would share gas price volatility with its customers. However, adverse movements in gas prices would result in higher customer billings, along with potential customer dissatisfaction and defection. These new risks were factored into the risk response analysis.

Portfolio View

Management considers risk from an entity-wide, or portfolio, perspective. Management may take an approach in which the manager responsible for each department, function or business unit develops a composite assessment of risks and risk responses for that unit. This view reflects the risk profile of the unit relative to its objectives and risk tolerances.

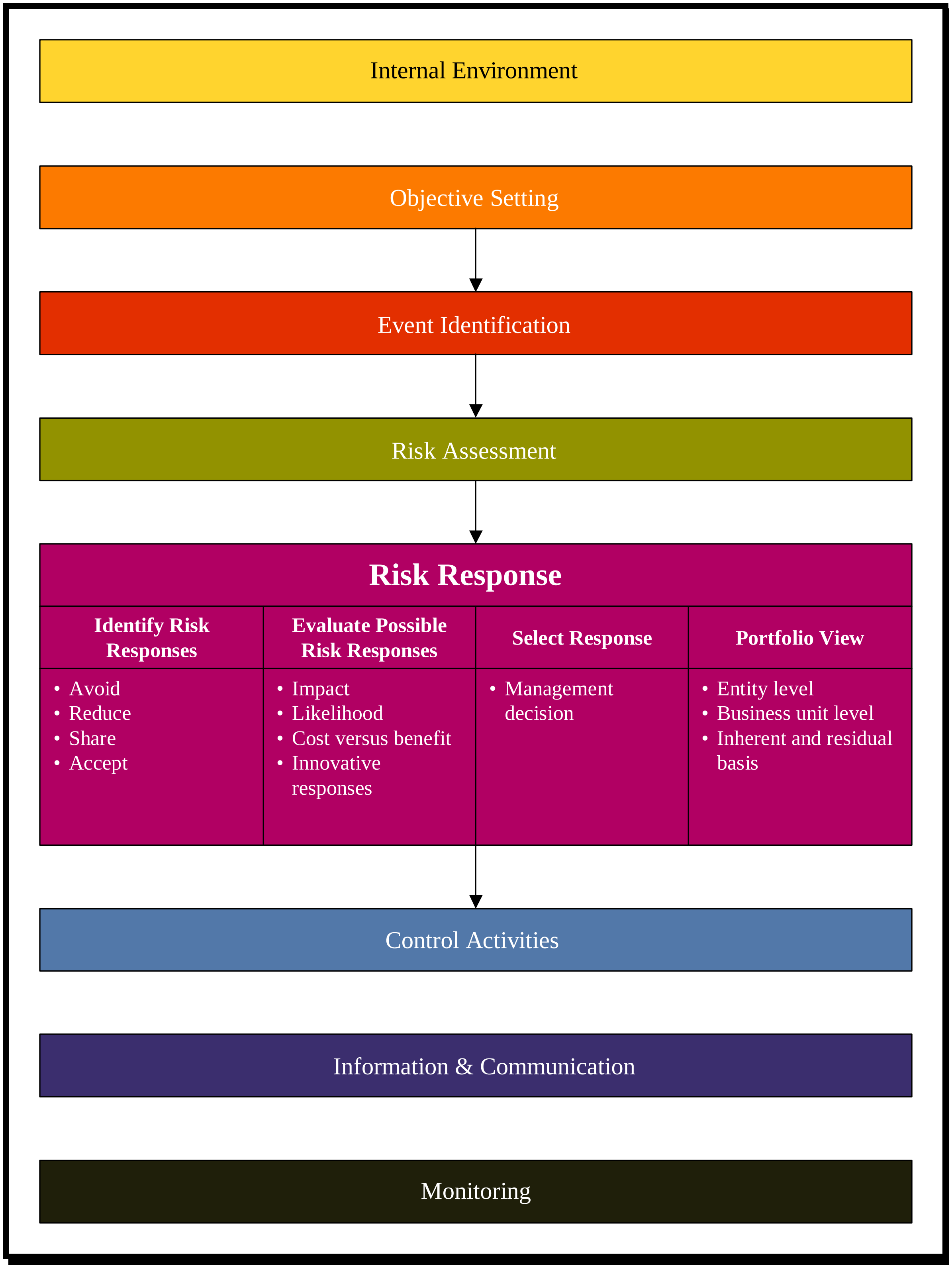
With a view of risk for individual units, the senior management of the enterprise is positioned to take a portfolio view, to determine whether the entity’s risk profile is commensurate with its overall risk appetite relative to its objectives. Risk may exist in different units that are within the risk tolerances of the individual units. But taken together, the risk might exceed the risk appetite of the entity as a whole, in which case additional or different risk response is needed. Conversely, risks may naturally offset across the entity, or individual units may be relatively risk averse. Where the portfolio of risk is considerably less than the entity’s risk appetite, management may decide to motivate individual business unit managers to accept greater risk in targeted areas to enhance the entity’s overall growth and return.

In establishing a portfolio view of risk responses, management will recognize the diversity of responses selected and the effect of multiple responses on the entity's risk tolerances. Where potential events are not directly related, management may assess the effect of its risk response on these events individually and then form a composite, or portfolio view. Where similar risks exist within multiple business units, management may decide to assess the effect of its risk responses on the particular type or category of events, and then take a portfolio view. The portfolio view would typically reflect any offsets – events representing opportunities or events that would mitigate the negative effect of other events – that exist within the portfolio, as well as the cumulative effect of all responses.

A company with business units with exposure to different price fluctuations – the prices of manufacturing supplies from diverse product suppliers – assesses its risk response relative to market movements within each business unit. It then reports a composite view, presented as a distribution graph depicting the range of potential probabilities and impacts. Another company with multiple business units – each with exposure to gold price fluctuations – aggregates the effect of its risk responses to potential shifts in the price of gold into a single measure showing the net effect of a $1/ounce shift in gold on its total gold inventory.

Exhibit 7.2 depicts the key elements of *Risk Response* as described in this chapter.

Exhibit 7.2



Internal Environment

Objective Setting

Event Identification

Risk Assessment

Risk Response

Identify Risk Responses	Evaluate Possible Risk Responses	Select Response	Portfolio View
• Avoid • Reduce • Share • Accept	• Impact • Likelihood • Cost versus benefit • Innovative responses	• Management decision	• Entity level • Business unit level • Inherent and residual basis

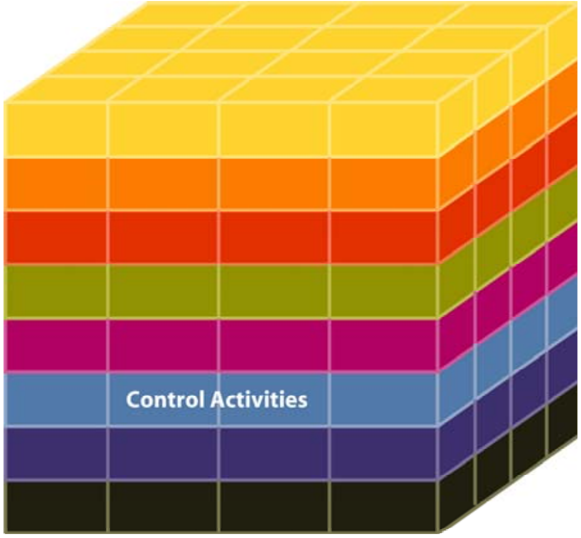
Control Activities

Information & Communication

Monitoring

8. CONTROL ACTIVITIES

Chapter Summary: Control activities are the policies and procedures that help ensure that management's risk responses are carried out. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities – as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.



Control activities are policies and procedures, which are the actions of people to implement the policies, to help ensure that management's risk responses are carried out. Control activities are applied with respect to each of the four categories of objectives – strategic, operations, reporting and compliance.

Although some control activities relate solely to one area, there is often overlap. Depending on circumstances, a particular control activity could help satisfy entity objectives in more than one of the categories. Operations controls also can help ensure reliable reporting, reporting control activities can serve to effect compliance, and so on.

In a retail chain, the completeness of credits issued for merchandise returned by customers is controlled electronically by the numerical sequence of documents and then summarized for reporting purposes. This summarization also provides an analysis by product for merchandise managers' use in future buying decisions and for inventory control. In this case, control activities established primarily for reporting also serve operations objectives.

Although these categories are helpful in discussing control, the particular category in which a control happens to be placed is not as important as the role it plays in achieving a particular activity's objectives.

Integration with Risk Response

Risk responses serve to focus attention on control activities needed to help ensure that the risk responses are carried out properly and in a timely manner. Control activities are part of the process by which an enterprise strives to achieve its business objectives.

An illustration of the link between objectives, risk responses and controls is the following: For the objective, "Meet or exceed sales targets," risks include having insufficient knowledge of external factors such as current and potential customers' needs. To reduce the likelihood of occurrence and impact of the risk, management establishes buying histories of existing customers and undertakes new market research initiatives. These actions serve as focal points for the establishment of control activities. Control activities might include tracking progress of the development of customer buying histories against established timetables, and taking steps to ensure the accuracy of reported data. In this sense, control activities are built directly into the management process.

In selecting control activities, management considers how they interrelate. A company might rely on a single control activity to address multiple risk responses. For instance, a performance indicator that measures staff turnover may provide evidence of the effectiveness of management's response to such risks as competitor recruiting, and lack of effectiveness of staff incentive and training and development programs. When establishing new risk responses, management considers existing control activities that may be sufficient to ensure that new responses are executed effectively. On the other hand, it might be necessary to consider multiple control activities relative to a risk response.

Control activities are an important part of the process by which an enterprise strives to achieve its business objectives. Control activities are not performed simply for their own sake or because it seems to be the "right or proper" thing to do. In the example above, management needs to take steps to ensure that sales targets are met. Control activities serve as mechanisms for managing the achievement of that objective and often are built directly into the management process.

Types of Control Activities

Many different descriptions of types of control activities have been put forth, including preventive controls, detective controls, manual controls, computer controls and management controls. Control activities can be typed by specified control objectives, such as ensuring completeness and accuracy of data processing.

In Exhibit 8.1 are commonly used control activities. These are just a very few among many procedures performed every day that serve to enforce adherence to established action plans and to keep entities on track toward achieving their objectives. They are presented to illustrate the range and variety of control activities, not to suggest any particular categorization.

Exhibit 8.1

- *Direct functional or activity management – Managers running functions or activities review performance reports. A manager responsible for a bank's consumer loans reviews reports by branch, region and loan (collateral) type, checking summarizations and identifying trends, and relating results to economic statistics and targets. In turn, branch managers receive data on new business by loan-officer and local-customer segment. Branch managers also focus on compliance issues, reviewing reports required by regulators on new deposits over specified amounts. Reconciliations are made of daily cash flows, with net positions reported centrally for overnight transfer and investment.*
- *Information processing – A variety of controls are performed to check accuracy, completeness and authorization of transactions. Data entered is subject to on-line edit checks or matching to approved control files. A customer's order, for example, is accepted only after reference to an approved customer file and credit limit. Numerical sequences of transactions are accounted for; exceptions are followed up and reported to supervisors. Development of new systems and changes to existing ones are controlled, as is access to data, files and programs.*
- *Physical controls – Equipment, inventories, securities, cash and other assets are secured physically and periodically counted and compared with amounts shown on control records.*
- *Performance indicators – Relating different sets of data – operating or financial – to one another, together with analyses of the relationships and investigative and corrective actions, serves as a control activity. Performance indicators include, for example, staff turnover rates by functional unit. By investigating unexpected results or unusual trends, management identifies circumstances where an insufficient capacity to complete key processes may mean that objectives have a lower likelihood of being achieved. How managers use this information – for operating decisions only, or to also follow up on unexpected results reported by external financial reporting systems – determines whether analysis of performance indicators serves operational purposes alone or external financial reporting control purposes as well.*

Policies and Procedures

Control activities usually involve two elements: a policy establishing what should be done and procedures to effect the policy. For example, a policy might call for review of customer trading activities by a securities dealer's retail branch manager. The procedure is the review itself, performed in a timely manner and with attention given to factors set forth in the policy, such as the nature and volume of securities traded and their relation to customer net worth and age.

Many times, policies are communicated orally. Unwritten policies can be effective where the policy is a long-standing and well-understood practice, and in smaller organizations where communications channels involve only limited management layers and close interaction with and supervision of personnel. But regardless of whether a written policy exists, it must be implemented thoughtfully, conscientiously and consistently. A procedure will not be useful if performed mechanically and without a sharp, continuing focus on conditions to which the policy is directed. Further, it is essential that conditions identified as a result of the procedure be investigated and appropriate corrective actions taken. Follow-up actions might vary depending on the size and organizational structure of an enterprise. They could range from formal reporting processes in a large company – where business units state why targets were not met and what actions are being taken to prevent recurrence – to an owner-manager of a small business walking down the hall to speak with the plant manager about what went wrong and what needs to be done.

Controls over Information Systems

With widespread reliance on information systems, controls are needed over significant systems. Two broad groupings of information systems control activities can be used. The first is general controls, which apply to many if not all application systems and help ensure their continued, proper operation. The second is application controls, which include computerized steps within application software to control the technology application. Combined with other manual process controls where necessary, these controls ensure completeness, accuracy and validity of information.

General Controls

General controls include controls over information technology management, information technology infrastructure, security management and software acquisition, development and maintenance. These controls apply to all systems – from mainframe to client/server to desktop computer environments.

Exhibit 8.2 provides examples of common controls within these categories.

Exhibit 8.2

- *Information technology management – A steering committee provides oversight, monitoring, and reporting of information technology activities and improvement initiatives.*
- *Information technology infrastructure – Controls apply to system definition, acquisition, installation, configuration, integration and maintenance. Controls may include service level agreements that establish and reinforce system performance, business continuity planning that maintains system availability, tracking network performance for operational failures and scheduling of computer operations. The system software component of information technology infrastructure may include such controls as management or steering committee review and approval of significant new acquisitions, restricting access to system configuration and operating system software, automated reconciliations of data accessed through middleware software and parity bit detection for communications errors. System software controls include incidents tracking, system logging, and review of reports detailing usage of data-altering utilities.*
- *Security management – Protect against inappropriate access and unauthorized use. Logical access controls such as secure passwords restrict access at the network, database and application levels. User accounts and related access privilege controls help restrict authorized users to only applications or application functions needed to do their jobs. Internet firewalls and virtual private networks protect data from unauthorized external access.*
- *Software acquisition, development and maintenance – Controls over software acquisition and implementation are incorporated into an established process for managing change, including documentation requirements, user acceptance testing, stress testing and project risk assessments. Access to source codes is controlled via code library. Software developers work only in segregated development/test environments and do not have access to production environment. Controls over system changes include required authorization of change requests, review of the changes, approvals, documentation, testing, implications of changes on other information technology components, stress testing results and implementation protocols.*

Information technology-led improvement efforts often help build controls into the operations of an organization. Such initiatives may include business process improvement, total quality management and defect identification and management.

Application Controls

Application controls are designed to ensure completeness, accuracy, authorization and validity of data capture and processing. Individual applications may rely on effective operation of controls over information systems to ensure that data is captured or generated when needed, supporting applications are available and interface errors are detected quickly.

One of the most significant contributions of computers is the ability to prevent errors from entering the system, as well as detecting and correcting them once they are present. To do this, application controls depend on computerized edit checks. These consist of format, existence, reasonableness and other checks on the data that are built into an application during development. When properly designed, they can provide control over entered data.

Exhibit 8.3 provides examples of application controls. These are just a few among a myriad of application controls performed every day that serve to prevent and detect inaccurate, incomplete, inconsistent or improper data capture and processing through calculation and logical comparison.

Exhibit 8.3

- *Balancing control activities – Detect data capture errors by reconciling amounts captured either manually or automatically to a control total. A company automatically balances the total number of transactions processed and passed from its on-line order entry system to the number of transactions received in its billing system.*
- *Check digits – Calculations to validate data. A company's part numbers contain a check digit to detect and correct inaccurate ordering from its suppliers.*
- *Predefined data listings – Provide the user with predefined lists of acceptable data. A company's intranet site includes drop-down lists of products available for purchase.*
- *Data reasonableness tests – Compare data captured to a present or learned pattern of reasonableness. An order to a supplier by a home renovation retail store for an unusually large number of board feet of lumber may trigger a review.*
- *Logic tests – Include the use of ranges limits or value or alphanumeric tests. A government agency detects potential errors in social security numbers by checking that all entered numbers are nine digits.*

Entity Specific

Because each entity has its own set of objectives and implementation approaches, there will be differences in risk responses and related control activities. Even if two entities had identical objectives and made similar decisions on how they should be achieved, their control activities would likely be different. Each entity is managed by different people who use individual judgments in effecting internal control. Moreover, controls reflect the environment and industry in which an entity operates, as well as the complexity of its organization, its history and its culture.

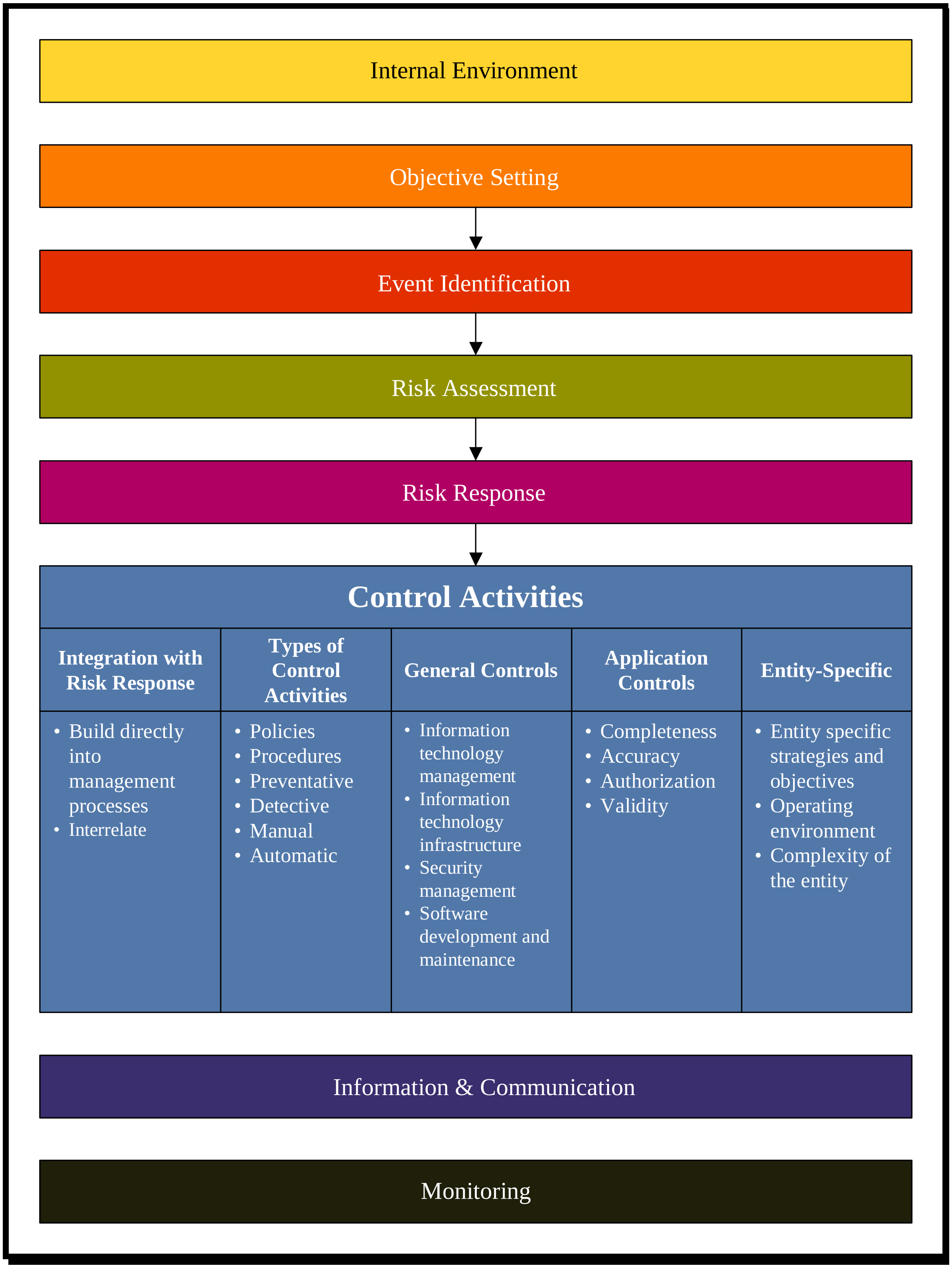
The environment in which an entity operates affects the risks to which it is exposed and may present unique reporting objectives or special legal or regulatory requirements. A chemicals manufacturer, for example, must manage greater environmental risks than those facing a typical service company.

The complexity of an entity, and the nature and scope of its activities, affect its control activities. Complex organizations with diverse activities may face more difficult control issues than simple organizations with less varied activities. An entity with decentralized operations and an emphasis on local autonomy and innovation presents different control circumstances than a highly centralized one. Other factors that influence an entity's complexity and therefore the nature of its controls include location and geographical dispersion, the extensiveness and sophistication of operations, and information processing methods.

All these factors affect an entity's control activities, which need to be designed accordingly to contribute to the achievement of the entity's objectives.

Exhibit 8.4 provides the key elements of *Control Activities* as described in this chapter.

Exhibit 8.4



Internal Environment

Objective Setting

Event Identification

Risk Assessment

Risk Response

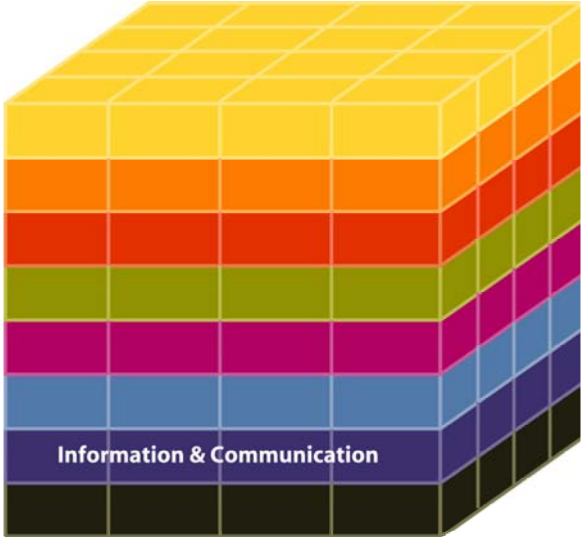
Control Activities

Integration with Risk Response	Types of Control Activities	General Controls	Application Controls	Entity-Specific
• Build directly into management processes • Interrelate	• Policies • Procedures • Preventative • Detective • Manual • Automatic	• Information technology management • Information technology infrastructure • Security management • Software development and maintenance	• Completeness • Accuracy • Authorization • Validity	• Entity specific strategies and objectives • Operating environment • Complexity of the entity

Information & Communication

Monitoring

9. INFORMATION AND COMMUNICATION



Chapter Summary: Pertinent information is identified, captured and communicated in a form and timeframe that enable people to carry out their responsibilities. Information systems use internally generated data, and information about external events, activities and conditions, providing information for managing enterprise risks and making informed decisions relative to objectives. Effective communication also occurs, flowing down, across and up the organization. All personnel receive a clear message from top management that enterprise risk management responsibilities must be taken seriously. They understand their own role in enterprise risk management, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There is also effective communication with external parties.

Every enterprise identifies and captures information – financial and non-financial, relating to external as well as internal events and activities – relevant to managing the entity. This information is delivered to personnel in a form and timeframe that enable them to carry out their enterprise risk management and other responsibilities.

Information

Information is needed at all levels of an organization to identify, assess and respond to risks, and to otherwise run the entity and achieve its objectives. An array of information is used, relevant to one or more objectives categories. Financial information, for instance, is used not only in developing financial statements for external dissemination, but also for operating decisions, such as monitoring performance and allocating resources. Reliable financial information is fundamental to planning, budgeting, pricing, evaluating vendor performance, assessing joint ventures and alliances, and a range of other management activities.

Similarly, operating information is essential for developing financial reports. This includes the routine – purchases, sales and other transactions – as well as information on competitors' product releases or economic conditions, which can affect inventory and receivables valuations. Operating information from internal and external sources, both financial and non-financial, is relevant to all business objectives. For example, information on airborne particle emissions or personnel data may be needed to achieve both compliance and external reporting objectives.

Information comes from many sources – internal and external, and in quantitative and qualitative forms – and facilitates responses to changing conditions. The challenge for management is to process and refine large volumes of data into actionable information. This challenge is met by establishing an information systems infrastructure to source, capture, process, analyze and report relevant information. These information systems – usually computerized but also involving manual inputs or interfaces – often are viewed in the context of processing internally generated data. But information systems have a much broader application. They also deal with information about external events, activities and conditions, for example, market- or industry-specific economic data that signals changes in demand for a company’s products or services; data on goods and services for production processes; market intelligence on evolving customer preferences or demands; information on competitors' product development activities; and legislative or regulatory initiatives.

Some systems provide continual surveillance of customer transactions, integrating with rules-based workflow applications to mitigate risk in day-to-day operations. Other systems capture information on customer satisfaction, identifying and reporting sales by product and location, customer gains and losses, returns and requests for allowances, application of product warranty provisions and customer feedback. This information may be supplemented with market, technical or service-related information obtained through survey questionnaires, interviews, market demand studies or focus groups.

Information systems can be formal or informal. Conversations with customers, suppliers, regulators and personnel often provide critical information needed to identify risks and opportunities. Similarly, attendance at professional or industry seminars and memberships in trade and other associations can provide valuable information.

Keeping information consistent with needs is particularly important when an entity faces fundamental industry changes, highly innovative and quick-moving competitors, or significant customer demand shifts. Information systems must change as needed to support new objectives. Information systems must not only identify and capture needed financial and non-financial information, they must also process and report this information in a timeframe and way that are useful in controlling the entity's activities.

Strategic and Integrated Systems

As enterprises have become more collaborative and integrated with customers, business partners and regulators, the division between an entity's information systems architecture and that of external parties is increasingly blurred. As a result, data processing and data management often become a shared responsibility of multiple entities. In such cases, an organization's information systems architecture must be sufficiently flexible and agile to effectively integrate with new customers and business partners.

The design of an information systems architecture and acquisition of technology are important aspects of entity strategy, and choices regarding technology can be critical to achieving objectives. Decisions about technology selection and implementation depend on many factors, including organizational goals, marketplace needs and competitive requirements. While information systems are fundamental to effective enterprise risk management, risk management techniques can assist in making technology decisions.

Systems Support Strategic Initiatives

Information systems have long been designed and used to support business strategy. This role becomes critical as business needs change and technology creates new opportunities for strategic advantage. In some cases, changes in technology have reduced the advantage gained in initial deployment, driving new strategic direction. For instance, airline reservation systems that gave travel agents easy access to flight information have moved to customer-facing Internet reservation systems, significantly reducing or eliminating involvement of the traditional travel agent.

Integration with Operations

Information systems often are fully integrated into most aspects of operations. Web and web-based systems are common, with many companies having enterprise-wide information systems such as enterprise resource planning (ERP). These applications facilitate access to information previously trapped in functional or departmental silos and not practically available for widespread management use.

Many companies use fully integrated information systems, where transactions are recorded and tracked in real time, enabling managers to immediately access financial and operating information more effectively to control business activities.

A construction company dealing in multiple large-scale projects uses an integrated, extranet-based system to meet marketplace and efficiency expectations. The system provides information that helps managers track customer-supplied inventory and parts, identify over- or short-supply material at multiple job sites, obtain cost savings with suppliers of common materials or combine with similar organizations to obtain volume discounts, and oversee the *activities of subcontractors. It also allows employees to seamlessly share current drawings with architects and engineers, customers, subcontractors and regulators, while maintaining drawings version control. Additionally, the system encompasses knowledge management capabilities that allow company employees to share innovative solutions throughout the organization.*

To support effective enterprise risk management, an entity captures and uses historical and present data. Historical data allow the entity to track actual performance against targets, plans and expectations. It provides insights into how the entity performed under varying conditions, allowing management to identify correlations and trends, and to forecast future performance. Historical data also can provide early warning of potential events that warrant management attention.

Present or current state data allow an entity to determine its risk profile at a specific point in time and remain within established risk tolerances. Such data allow management to take a real-time view of existing risks inherent in a process, function or unit and to identify variations from expectations.

Entities also use data to assess the likelihood and impact of potential future events, allowing management to weigh the potential impact on objectives. This provides a view of the entity's risk profile, enabling management to alter activities as necessary to calibrate the risk profile to its risk appetite.

Management uses historical dollar sales-per-salesperson by category, matched with current state data on numbers in sales force categories and in the recruiting/orientation pipeline, and maps the result against targeted revenue. The resulting analysis, against objectives and risk tolerances, drives decisions on recruiting, training, marketing and related issues.

Information that supports enterprise risk management is captured and developed as part of management's ongoing processes. The flow of information for enterprise risk management is integrated with existing information used to manage the entity. For instance, financial information is used not only in developing financial statements for external distribution, but also for internal reporting and monitoring performance.

Developments in information systems have improved the ability of many organizations to measure and monitor performance and present analytical information at an enterprise level. System complexity and integration continue, with organizations utilizing new technology capabilities as they emerge. However, the growing reliance on information systems at the strategic and operational level bring about new risks – such as information security breaches or cyber-crimes – that must be integrated into the entity's enterprise risk management process.

Depth and Timeliness of Information

The information infrastructure sources and captures data in a timeframe and at a depth consistent with an entity's need to identify, assess and respond to risk, and remain within its risk tolerance. Timeliness of information flow needs to be consistent with the rate of change in the entity and its internal and external environments.

The importance of depth of data is illustrated by looking at different events that potentially affect a brokerage firm located in a city susceptible to floods. For business continuity planning, management maintains a general awareness of potential flood conditions and is positioned to advise personnel when to move to established back-up facilities. Information captured at this high level is sufficient to allow the firm to adequately manage the risk. In contrast, as a brokerage, the firm sources and continuously captures changes in stock, bond and commodity prices to several decimal points. This level of data timeliness and detail is consistent with the firm's need to respond immediately to stock price changes that may precipitate risks, such as an overexposure to a particular market sector or security inconsistent with the firm's risk appetite.

The information infrastructure converts raw data into relevant information that assists personnel in carrying out their enterprise risk management and other responsibilities. Information is provided in a form and timeframe that are actionable, reasonably easy to use and linked to defined accountabilities.

Advances in data collection, processing and storage have resulted in exponential growth in data volume. With much more data available – often in real time – to more people in an organization, the challenge is to avoid "information overload" by ensuring the flow of the right information, in the right form, at the right level of detail, to the right people at the right time. In developing the information infrastructure, consideration should be given to the distinct information requirements of individual users and departments, and to the summary level information needed by different levels of management.

Information Quality

With increasing dependence on sophisticated information systems and data-driven automated decision systems and processes, data reliability is critical. Inaccurate data can result in unidentified risks or poor assessments and bad management decisions.

The quality of information includes ascertaining whether:

- Content is appropriate – Is it at the right level of detail?
- Information is timely – Is it there when required?
- Information is current – Is it the latest available?
- Information is accurate – Is the data correct?

- Information is accessible – Is it easy to obtain by those who need it?

To ensure data quality, entities establish enterprise-wide data management programs, encompassing acquisition, maintenance and distribution of data and management information. Without such programs, information systems might not provide the information management and other personnel require.
Challenges are many: Conflicting functional needs, system constraints and non-integrated processes can inhibit data acquisition and its effective use. To meet these challenges, management establishes a strategic plan with clear accountability and responsibilities for data integrity, and performs regular data quality assessments.

Often, the data management strategy must extend beyond the entity itself. Through expansion of e-business, the flow of information about an entity's performance now includes supply chain partners, vendors, customers and others. There is often a great deal of operational, financial and compliance data sharing and transparency with key strategic partners. The information necessary for enterprise risk management may reside both internally and externally to the entity, and must move seamlessly back and forth between often disparate systems.

Having the right information, on time and at the right place is essential to effecting risk management and control. That is why information systems, while a component of enterprise risk management, also must be controlled.

Communication

Communication is inherent in information systems. As discussed above, information systems must provide information to appropriate personnel so that they can carry out their operating, financial reporting and compliance responsibilities. But communication also must take place in a broader sense, dealing with expectations, responsibilities of individuals and groups, and other important matters.

Internal

Management provides specific and directed communication that addresses behavioral expectations and the responsibilities of personnel. This includes a clear statement of the entity's enterprise risk management philosophy and approach and a clear delegation of authority. Communication about processes and procedures should align with, and underpin, the desired risk culture.

Communication should effectively:

- Ensure awareness about the importance and relevance of effective enterprise risk management.

- Communicate the entity's risk appetite and risk tolerances.
- Implement and support a common risk language.
- Advise personnel of their role and responsibilities in effecting and supporting the components of enterprise risk management.

All personnel, particularly those with important operating or financial management responsibilities, need to receive a clear message from top management that enterprise risk management must be taken seriously. Both the clarity of the message and the effectiveness with which it is communicated are important.

Personnel should know that when the unexpected occurs, attention is to be given not only to the event itself, but also to its cause. In this way, a potential weakness in the system can be identified and action taken to prevent a recurrence. For example, finding out about unsalable inventory should result not only in an appropriate write-down in financial reports, but also in a determination of why the inventory became unsalable in the first place.

Personnel also need to know how their activities relate to the work of others. This knowledge will help them recognize a problem or determine its cause and corrective action. And, they need to know what is deemed acceptable and unacceptable behavior. There have been well-publicized instances of fraudulent reporting in which managers, under pressure to meet budgets, misrepresented operating results. In a number of these instances no one had told these individuals that such misreporting could be illegal or otherwise improper. This underscores the critical nature of how messages are communicated within an organization. A manager who instructs subordinates, "Meet the budget – I don't care how you do it, just do it," can unwittingly send the wrong message.

Front-line employees who deal with critical operating issues every day are often in the best position to recognize problems as they arise. For example, sales representatives or account managers may learn of important customer product design needs; production personnel may become aware of costly process deficiencies; and purchasing personnel may be confronted with improper incentives from suppliers.

For such information to be reported upstream, there must be open channels of communication and a clear-cut willingness to listen. Personnel must believe their superiors truly want to know about problems and will deal with them effectively. Most managers recognize intellectually that they should avoid "shooting the messenger." But when caught up in everyday pressures, they can be unreceptive to people bringing them legitimate problems. Personnel are quick to pick up on spoken or unspoken signals that a superior doesn't have the time or interest to deal with problems they have uncovered. Compounding such problems, the unreceptive manager is the last to know that the communications channel has been effectively shut down.

Communications channels also should ensure personnel can communicate risk-based information across business units, processes or functional silos. For example, an increase in customer complaints about a product monitored by a customer service group may need to be flagged for the product design and development team. Communication breakdowns can occur when individuals or units are discouraged or do not have a vehicle to provide information important to others. Personnel may be aware of significant risks, but unwilling or unable to report them.

In most cases, normal reporting lines in an organization are the appropriate channels of communication. In some circumstances, however, separate lines of communication are needed to serve as a fail-safe mechanism in case normal channels are inoperative.

Some companies provide a channel directly to a senior officer, the chief internal auditor or legal counsel. Without both open communications channels and a willingness to listen, the upward flow of information might be blocked.

In all cases, it is important that personnel understand that there will be no reprisals for reporting relevant information. A clear message is sent by the existence of mechanisms that encourage employees to report suspected violations of an entity's code of conduct and by the treatment of reporting personnel.

Among the most critical communications channels is that between top management and the board of directors. Management must keep the board up to date on performance, developments, risk and the functioning of enterprise risk management, and other relevant events or issues. The better the communications, the more effective a board will be in carrying out its oversight responsibilities, in acting as a sounding board on critical issues and in providing advice, counsel and direction. By the same token, the board should communicate to management what information it needs and provide feedback and direction.

External

With open external communications channels, customers and suppliers can provide highly significant input on the design or quality of products or services, enabling a company to address evolving customer demands or preferences. Open communication about the entity’s risk appetite and risk tolerances is important, particularly for entities linked with others in supply chains or e-business enterprises. In such instances, management considers how its risk appetite and risk tolerances align with those of its partners, ensuring that it does not inadvertently take on too much risk through its partners.

Communication from external parties often provides important information on the functioning of enterprise risk management. External auditors' understanding of an entity's strategy, operations and related business issues and control systems provides management and the board important risk and control information.

Results of compliance reviews or examinations by state banking or insurance authorities highlight risks and control weaknesses. Customer complaints or inquiries about shipments, receipts, billings or other activities often point to operating problems. Management should be ready to recognize implications of such circumstances, investigate and take necessary corrective actions.

Communication with stakeholders, regulators, financial analysts and other external parties provides information relevant to their needs, so they can readily understand the circumstances and risks the entity faces. Such communication should be meaningful, pertinent and timely, and conform to legal and regulatory requirements.

Management's commitment to communication with external parties – whether open and forthcoming and serious in follow-up, or otherwise – also sends messages throughout the organization.

Means of Communication

Communication can take such forms as policy manuals, memoranda, e-mails, bulletin board notices, webcasts and videotaped messages. Where messages are transmitted orally – in large groups, smaller meetings or one-on-one sessions – tone of voice and body language emphasize what is being said.

How information is presented or "framed" can significantly affect how the information is interpreted and how the associated risks or opportunities are viewed.

Individuals have different responses to potential losses compared to potential gains. How a risk is framed – focusing on the upside (a potential gain) or downside (a potential loss) – often will influence the response. Prospect theory, which explores human decision making, says that individuals are not risk neutral; rather, a response to loss tends to be more extreme than a response to gain. And with this comes a tendency to misinterpret probabilities and best solution reactions. To illustrate, an individual is confronted with two sets of choices:

1. *A sure gain of $240, or*
   a 25 percent chance to gain $1,000 and a 75 percent chance to gain nothing.

2. *A sure loss of $760, or*
   a 75 percent chance to lose $1,000 and a 25 percent chance to lose nothing.

In the first set of choices, most people select a "sure gain of $240," due to tendencies to be risk averse concerning gain and positively framed questions. In contrast, most people select a "75 percent chance to lose $1,000," due to a tendency to be risk seeking concerning losses and negatively framed questions. Prospect theory holds that people do not want to put at *risk what they already have or think they can have, but they will have higher risk tolerances when they think they can minimize losses.*

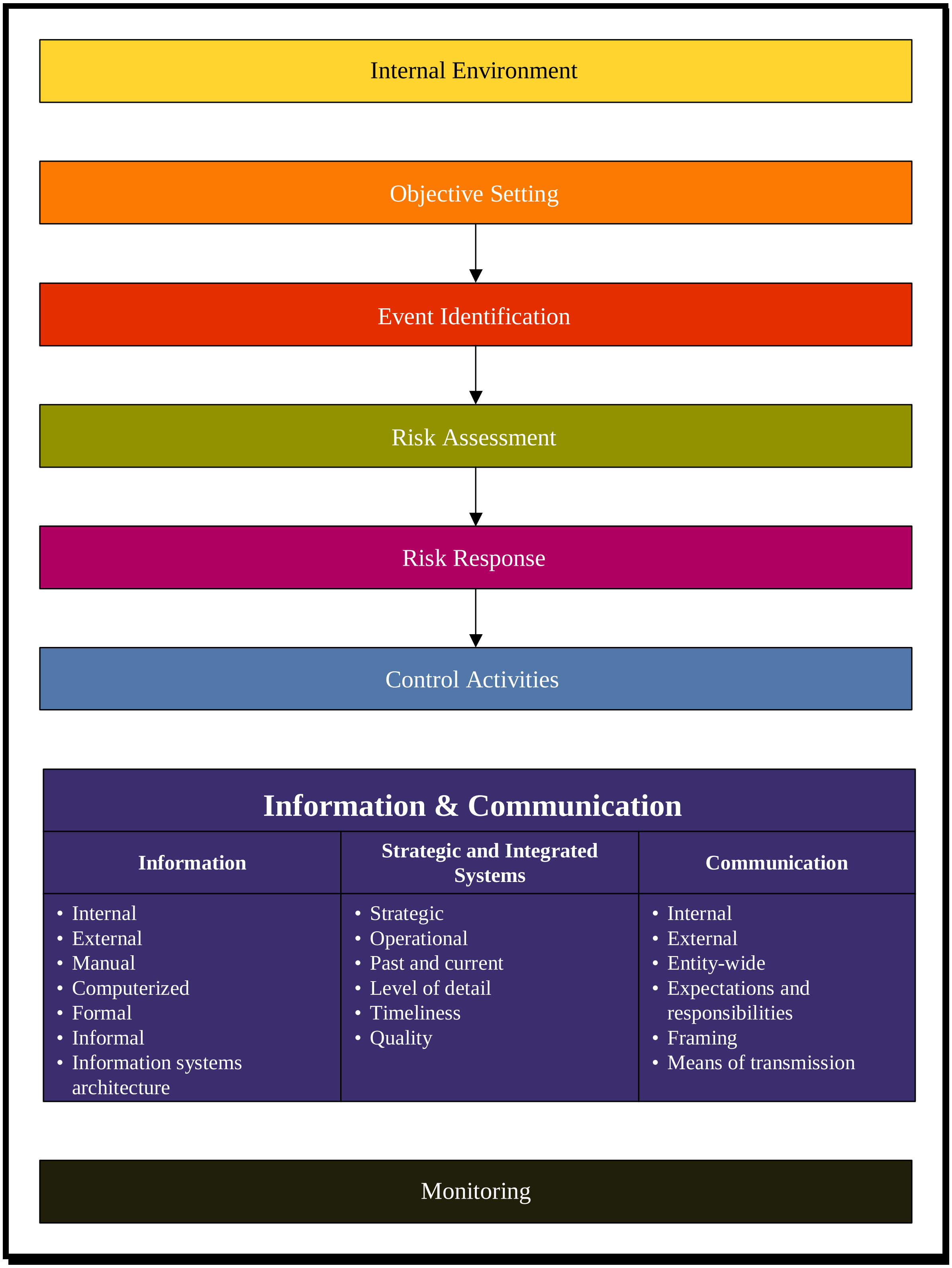
Human tendencies around decision making are exhibited across business units, functions and activities. For example, some personnel are more accustomed to taking riskier options in pursuit of gains, while others may seek to minimize losses. By recognizing these human tendencies, managers can frame information to reinforce the risk appetite and behavior throughout the entity.

Another powerful communication tool can be found in the way management deals with subordinates. Managers should remember that actions speak louder than words. Their actions are, in turn, influenced by the history and culture of the entity, drawing on past observations of how their superiors dealt with similar situations.

An entity with a history of operating with integrity, and whose culture is well understood by people throughout the organization, will likely find little difficulty in communicating its message. An entity without such a tradition will need to put more effort into the way messages are communicated.

Exhibit 9.1 provides the key elements of *Information and Communication* as described in this chapter.

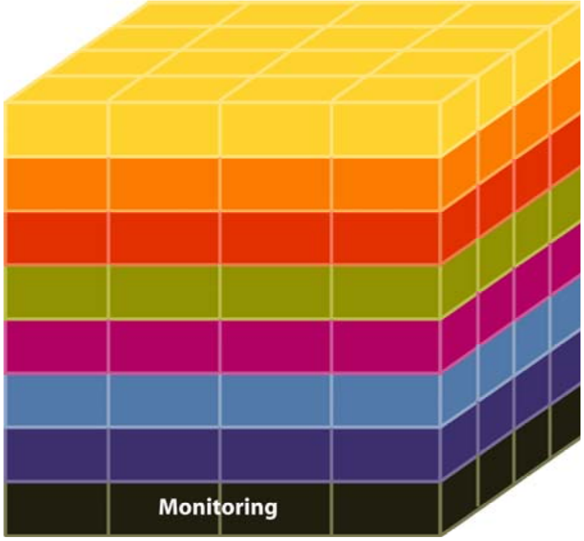
Exhibit 9.1



Information	Strategic and Integrated Systems	Communication
• Internal • External • Manual • Computerized • Formal • Informal • Information systems architecture	• Strategic • Operational • Past and current • Level of detail • Timeliness • Quality	• Internal • External • Entity-wide • Expectations and responsibilities • Framing • Means of transmission

10. MONITORING

Chapter Summary: Enterprise risk management is monitored – a process that assesses the presence and functioning of its components over time. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two. Ongoing monitoring occurs in the normal course of management activities. The scope and frequency of separate evaluations will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures. Enterprise risk management deficiencies are reported upstream, with serious matters reported to top management and the board.



An entity's enterprise risk management changes over time. Risk responses that were once effective may become irrelevant; control activities may become less effective, or no longer be performed; or entity objectives may change. This can be due to the arrival of new personnel, changes in entity structure or direction, or the introduction of new processes. In the face of such changes, management needs to determine whether the functioning of each enterprise risk management component continues to be effective.

Monitoring can be done in two ways: through ongoing activities or separate evaluations. Enterprise risk management mechanisms usually are structured to monitor themselves on an ongoing basis, at least to some degree. The greater the degree and effectiveness of ongoing monitoring, the less need for separate evaluations. The frequency of separate evaluations necessary for management to have reasonable assurance about the effectiveness of enterprise risk management is a matter of management's judgment. In making that determination, consideration is given to the nature and degree of changes occurring, from both internal and external events, and their associated risks; the competence and experience of the personnel implementing risk responses and related controls; and the results of the ongoing monitoring. Usually, some combination of ongoing monitoring and separate evaluations will ensure that enterprise risk management maintains its effectiveness over time.

Ongoing monitoring is built into the normal, recurring operating activities of an entity. Ongoing monitoring is performed on a real-time basis, reacts dynamically to changing conditions and is ingrained in the entity. As a result, it is more effective than separate evaluations. Since separate evaluations take place after the fact, problems often will be identified more quickly by ongoing monitoring routines. Many entities with sound ongoing monitoring activities nonetheless conduct separate evaluations of enterprise risk management. An entity that perceives a need for frequent separate evaluations should focus on enhancing ongoing monitoring activities by "building in" versus "adding on" such activities.

Ongoing Monitoring Activities

Many activities serve to monitor the effectiveness of enterprise risk management in the ordinary course of running the business. These include regular management and supervisory activities, variance analysis, stress testing, comparisons, reconciliations and other routine actions.

Exhibit 10.1 includes examples of ongoing monitoring activities.

Exhibit 10.1

- *Operating reports are integrated or reconciled with reporting systems and used to manage operations on an ongoing basis, and significant inaccuracies or exceptions to anticipated results are likely to be spotted quickly. For example, managers of sales, purchasing and production at divisional, subsidiary and corporate levels who are in touch with operations can question reports that differ significantly from their knowledge of operations. Timely and complete reporting and resolution of these exceptions enhance effectiveness of the process.*
- *Value-at-risk models are used to evaluate the impacts of potential market movements on an entity's financial position. These models can serve as effective tools in determining whether business units or functions are staying within identified risk tolerances.*
- *Communications from external parties corroborate internally generated information or indicate problems. Customers implicitly corroborate billing data by paying their invoices. Conversely, customer complaints about billings could indicate system deficiencies in the processing of sales transactions. Similarly, reports from investment managers on securities gains, losses and income can corroborate or signal problems with the entity's (or the manager's) records. An insurance company's review of safety policies and practices provides information on the functioning of enterprise risk management, from both operational safety and compliance perspectives, thereby serving as a monitoring technique.*
- *Regulators may also communicate with the entity on compliance or other matters that reflect on the functioning of the enterprise risk management process.*

- *Internal and external auditors and advisors regularly provide recommendations to strengthen enterprise risk management. Auditors may focus considerable attention on assessing the key risks of the enterprise or unit, the risk response selections and the related design of control activities, and on testing their effectiveness. Potential weaknesses may be identified, and alternative actions recommended to management, accompanied by information useful in making cost-benefit determinations. Internal auditors or personnel performing similar review functions can be particularly effective in monitoring an entity's activities.*
- *Training seminars, planning sessions and other meetings provide important feedback to management on whether enterprise risk management is effective. In addition to particular problems that may indicate risk issues, participants' risk and control consciousness often becomes apparent.*
- *Personnel are asked periodically to state explicitly whether they understand and comply with the entity's code of conduct. Operating and financial personnel may be similarly requested to state whether certain control procedures, such as reconciling specified amounts, are regularly performed. Such statements may be verified by management or internal audit personnel.*

Separate Evaluations

While ongoing monitoring procedures usually provide important feedback on the effectiveness of other enterprise risk management components, it may be useful to take a fresh look from time to time, focusing directly on enterprise risk management effectiveness. This also provides an opportunity to consider the continued effectiveness of the ongoing monitoring procedures.

Scope and Frequency

Evaluations of enterprise risk management vary in scope and frequency, depending on the significance of risks and importance of the risk responses and related controls in managing the risks. Higher-priority risk areas and responses tend to be evaluated more often. Evaluation of the entirety of enterprise risk management – which generally will be needed less frequently than the assessment of specific parts – may be prompted by a number of reasons: major strategy or management change, major acquisitions or dispositions, significant change in economic or political conditions, or significant changes in operations or methods of processing information. When a decision is made to undertake a comprehensive evaluation of an entity's enterprise risk management, attention should be directed to addressing its application in strategy setting as well as with respect to significant activities. The evaluation scope also will depend on which objectives categories – strategic, operations, reporting and compliance – are to be addressed.

Who Evaluates

Often, evaluations take the form of self-assessments, where persons responsible for a particular unit or function determine the effectiveness of enterprise risk management for their activities.

The chief executive of a division directs the evaluation of its enterprise risk management activities. He personally assesses the risks associated with strategic choices and high-level objectives as well as the internal environment component, and individuals in charge of the division's various operating activities assess the risk to achieving the division's established objectives and the effectiveness of other components. Line managers focus on operations and compliance objectives, and the divisional controller focuses on reporting objectives. The division's assessments are then considered by senior management, along with evaluations of the company's other divisions.

Internal auditors normally perform evaluations as part of their regular duties, or at the specific request of senior management, the board or subsidiary or divisional executives. Similarly, management may utilize input from external auditors in considering the effectiveness of enterprise risk management. A combination of efforts may be used in conducting whatever evaluative procedures management deems necessary.

The Evaluation Process

Evaluating enterprise risk management is a process in itself. While approaches or techniques vary, a discipline should be brought to the process, with certain basics inherent in it.

The evaluator must understand each of the entity activities and each of the components of enterprise risk management being addressed. It may be useful to focus first on how enterprise risk management purportedly functions – this is sometimes referred to as the system or process design.

The evaluator must determine how the system actually works. Procedures designed to operate in a particular way may be modified over time to operate differently or may no longer be performed. Sometimes new procedures are established but are not known to those who described the process and are not included in available documentation. A determination as to actual functioning can be accomplished by holding discussions with personnel who perform or are affected by enterprise risk management, by examining records on performance or a combination of procedures.

The evaluator analyzes the enterprise risk management process design and the results of tests performed. The analysis is conducted against the backdrop of management's established standards for each component, with the ultimate goal of determining whether the process provides reasonable assurance with respect to the stated objectives.

Methodology

A variety of evaluation methodologies and tools are available, including checklists, questionnaires and flowcharting techniques.

As part of their evaluation methodology, some companies compare or benchmark their enterprise risk management process against those of other entities. An entity may, for example, measure its process against those of companies with reputations for having particularly good enterprise risk management. Comparisons might be done directly with another company or under the auspices of trade or industry associations. Other organizations may provide comparative information, and peer review functions in some industries can help a company evaluate its process against those of its peers. A word of caution is needed. When conducting comparisons, consideration must be given to differences that always exist in objectives, facts and circumstances. And all eight individual enterprise risk management components, as well as the inherent limitations of enterprise risk management, need to be kept in mind.

Documentation

The extent of documentation of an entity’s enterprise risk management varies with the entity's size, complexity and similar factors. Larger organizations usually have written policy manuals, formal organization charts, written job descriptions, operating instructions, information system flowcharts, and so forth. Smaller entities typically have considerably less documentation. Many aspects of enterprise risk management are informal and undocumented, yet are regularly performed and highly effective. These activities may be tested in the same ways as documented activities. The fact that elements of enterprise risk management are not documented does not mean that they are not effective or that they cannot be evaluated. However, an appropriate level of documentation usually makes monitoring more effective and efficient.

The evaluator may decide to document the evaluation process itself. He or she usually will draw on existing documentation of the entity's enterprise risk management. Typically, this will be supplemented with additional documentation, along with descriptions of the tests and analyses performed in the evaluation process.

Where management intends to make a statement to external parties regarding enterprise risk management effectiveness, it should consider developing and retaining documentation to support the statement. Such documentation may be useful if the statement is subsequently challenged.

Reporting Deficiencies

Deficiencies in an entity’s enterprise risk management may surface from many sources, including the entity's ongoing monitoring procedures, separate evaluations and external parties.

The term “deficiency” refers to a condition within the enterprise risk management process worthy of attention. A deficiency, therefore, may represent a perceived, potential or real shortcoming, or an opportunity to strengthen the process to increase the likelihood that the entity’s objectives will be achieved.

Sources of Information

One of the best sources of information on enterprise risk management deficiencies is enterprise risk management itself. Ongoing monitoring activities of an enterprise, including managerial activities and everyday supervision of employees, generate insights from those who are directly involved in the entity's activities. These insights are gained in real time and can provide quick identification of deficiencies. Other sources of deficiencies are the separate evaluations of enterprise risk management. Evaluations performed by management, internal auditors or other functions can highlight areas in need of improvement.

External parties frequently provide important information on the functioning of an entity's enterprise risk management. These include customers, vendors and others doing business with the entity, external auditors and regulators. Reports from external sources should be carefully considered for their implications for enterprise risk management, and appropriate corrective actions should be taken.

What Is Reported

What should be reported? Although a universal answer is not possible, certain parameters can be drawn.

All enterprise risk management deficiencies that affect an entity’s ability to develop and implement its strategy and to achieve its established objectives should be reported to those positioned to take necessary action. The nature of matters to be communicated will vary depending on individuals' authority to deal with circumstances that arise and on the oversight activities of superiors.

In considering what needs to be communicated, it is necessary to look at the implications of findings. It is essential not only that the particular transaction or event be reported, but also that potentially faulty procedures be re-evaluated.

A salesperson points out that earned sales commissions were computed incorrectly. Payroll department personnel investigate and find that an outdated price for a particular product was used, resulting in under-computation of commissions as well as under-billings to customers. Action taken may include recalculation of all salespersons' commissions and billings since the price change went into effect. However, this action still may not address a number of important related questions: Why wasn't the new price used in the first place? What procedures exist to identify this risk and the actions required to ensure price increases are entered into the information system correctly and on time? Is there a problem with the computer programs that compute sales commissions and customer billings? If so, are controls over software development or changes to software in need of attention? Would another part of the enterprise risk management process have identified the problem on a timely basis had the salesperson not pointed out the error?

It can be argued that no problem is so insignificant as to make investigation of its implications unwarranted. An employee taking a few dollars from a petty cash fund for personal use, for example, would not be significant in terms of that particular event, and probably not in terms of the amount of the entire petty cash fund. Thus, investigating it might not be worthwhile. However, such apparent condoning of personal use of the entity's money might send the wrong message to employees.

To Whom to Report

Information generated in the course of operating activities usually is reported through normal channels to immediate superiors. The supervisor in turn may communicate upstream or laterally in the organization, so that the information ends up with personnel who can and should act on it. Alternative communications channels also should exist for reporting sensitive information such as illegal or improper acts. Findings of enterprise risk management deficiencies usually should be reported not only to the individual responsible for the function or activity involved, but also to at least one level of management above that person. This higher level of management provides needed support or oversight for taking corrective action and is positioned to communicate with others in the organization whose activities may be affected. Where findings cut across organizational boundaries, the reporting should cross over as well and be directed to a sufficiently high level to ensure appropriate action.

Reporting Directives

Providing needed information on enterprise risk management deficiencies to the right party is critical. Protocols should be established to identify what information is needed at a particular level for effective decision making.

Such protocols reflect the general rule that a manager should receive information that affects actions or behavior of personnel under his or her responsibility, as well as information needed to achieve specific objectives. A chief executive normally would want to be apprised, for example, of serious infractions of policies and procedures. He or she also would want supporting information on matters that could have significant financial impacts or strategic implications or that could affect the entity's reputation.

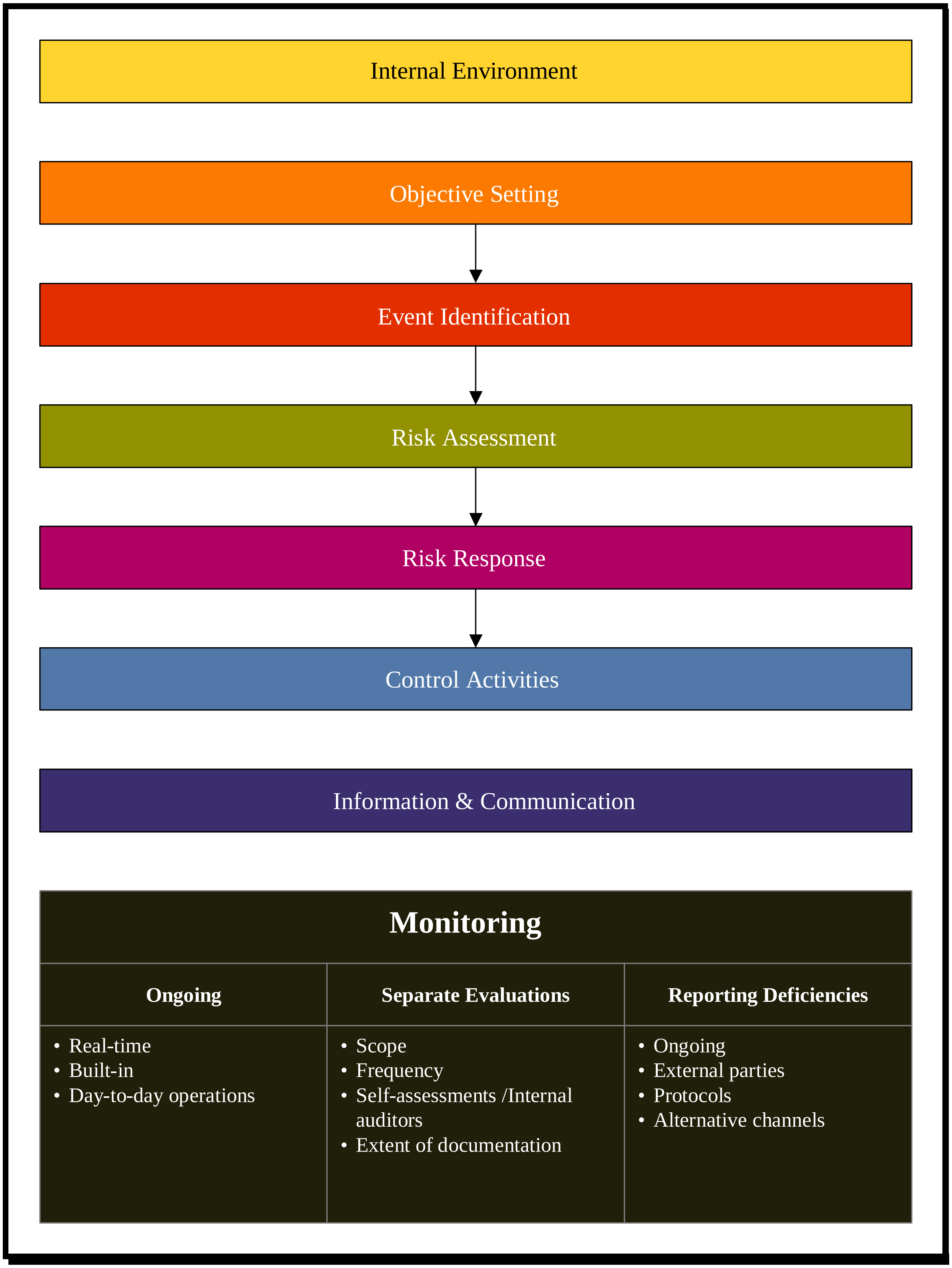
Senior managers should be apprised of risk and control deficiencies affecting their units. Examples include circumstances where assets with a specified monetary value are at risk, where the competence of employees is lacking or where important financial reconciliations are not performed correctly. Managers should be informed of deficiencies in their units in increasing levels of detail as one moves down the organizational structure.

Supervisors define reporting protocols for subordinates. The degree of specificity will vary, usually increasing at lower levels in the organization. While reporting protocols can inhibit effective reporting if too narrowly defined, they can enhance the reporting process if sufficient flexibility is provided.

Parties to whom deficiencies are to be communicated sometimes provide specific directives regarding what should be reported. A board of directors or audit committee, for example, may ask management or internal or external auditors to communicate only those deficiencies meeting a specified threshold of seriousness or importance.

Exhibit 10.2 provides the key elements of *Monitoring* as described in this chapter.

Exhibit 10.2



Internal Environment

Objective Setting

Event Identification

Risk Assessment

Risk Response

Control Activities

Information & Communication

Monitoring

Ongoing	**Separate Evaluations**	**Reporting Deficiencies**
• Real-time • Built-in • Day-to-day operations	• Scope • Frequency • Self-assessments /Internal auditors • Extent of documentation	• Ongoing • External parties • Protocols • Alternative channels

11. LIMITATIONS OF ENTERPRISE RISK MANAGEMENT

Chapter Summary: Effective enterprise risk management, no matter how well designed and operated, provides only reasonable assurance to management and the board of directors regarding achievement of an entity's objectives. Achievement of objectives is affected by limitations inherent in all management processes. These include the realities that human judgment in decision-making can be faulty and that breakdowns can occur because of such human failures as simple error or mistake. Additionally, controls can be circumvented by the collusion of two or more people, and management has the ability to override the enterprise risk management process, including risk response decisions and control activities. Another limiting factor is the need to consider the relative costs and benefits of risk responses.

To some observers, enterprise risk management, with embedded internal control, ensures that an entity will not fail – that is, the entity will always achieve its objectives. This view is misguided.

In considering limitations of enterprise risk management, three distinct concepts must be recognized:

- First, risk relates to the future, which is inherently uncertain.
- Second, enterprise risk management – even effective enterprise risk management – operates at different levels with respect to different objectives. For strategic and operations objectives, enterprise risk management can help ensure that management, and the board in its oversight role, is aware, in a timely manner, only of the extent to which the entity is moving toward achievement of these objectives. But it cannot provide even reasonable assurance that the objectives themselves will be achieved. .
- Third, enterprise risk management cannot provide absolute assurance with respect to any of the objectives categories.

The first limitation acknowledges that no one can predict the future with certainty. The second acknowledges that certain events are simply outside management's control. The third has to do with the reality that no process will always do what it's intended to do.

Reasonable assurance does not imply that enterprise risk management will frequently fail. Many factors, individually and collectively, reinforce the concept of reasonable assurance. The cumulative effect of risk responses that satisfy multiple objectives and the multipurpose nature of internal controls reduce the risk that an entity may not achieve its objectives. Furthermore, the normal everyday operating activities and responsibilities of people functioning at various levels of an organization are directed at achieving the entity's objectives. Indeed, among a cross-section of well-controlled entities, it is likely that most will be apprised regularly of movement toward their strategic and operations objectives, will achieve compliance objectives regularly, and consistently will produce – period after period, year after year – reliable reports. However, an uncontrollable event, a mistake or an improper reporting incident can occur. In other words, even effective enterprise risk management can experience a failure. Reasonable assurance is not absolute assurance.

Judgment

The effectiveness of enterprise risk management is limited by the realities of human frailty in making business decisions. Decisions must be made with human judgment in the time available, based on information at hand and under the pressures of the conduct of business. With the clairvoyance of hindsight, some decisions later may be found to produce less than desirable results and may need to be changed.

Breakdowns

Well-designed enterprise risk management can break down. Personnel may misunderstand instructions. They may make judgment mistakes. Or, they may commit errors due to carelessness, distraction or fatigue. An accounting department supervisor responsible for investigating exceptions might simply forget or fail to pursue the investigation far enough to be able to make appropriate corrections. Temporary personnel executing control duties for vacationing or sick employees might not perform correctly. System changes may be implemented before personnel have been trained to react appropriately to signs of incorrect functioning.

Collusion

The collusive activities of two or more individuals can result in enterprise risk management failures. Individuals acting collectively to perpetrate and conceal an action from detection often can alter financial data or other management information in a manner that cannot be identified by enterprise risk management process. For example, there may be collusion between an employee performing an important control function and a customer, supplier or another employee. On a different level, several layers of sales or divisional management might collude in circumventing controls so that reported results meet budgets or incentive targets.

Costs Versus Benefits

There are always resource constraints, and entities must consider the relative costs and benefits of decisions, including those related to risk response and control activities.

In determining whether a particular action should be taken or control established, the risk of failure and the potential effect on the entity are considered along with the related costs. For example, it may not pay for a company to install sophisticated inventory controls to monitor levels of raw material if the cost of the raw material used in a production process is low, the material is not perishable, ready supply sources exist and storage space is readily available.

Cost and benefit measurements for implementing event identification and risk assessment capabilities and related response and control activities are done with different levels of precision. Generally, it is easier to deal with the incremental cost side of the equation, which in many cases can be quantified in a fairly precise manner. All direct costs associated with establishing a capability or instituting a control, and indirect costs where practically measurable, are usually considered. And as companies become more mature, they may begin to quantify the direct and indirect cost of losses and resulting cost of remediation actions, including opportunity costs associated with use of resources. Also difficult to quantify on the cost side are the time and effort related to certain internal environment factors, such as management's commitment to ethical values or the competence of personnel; and capturing certain external information such as market intelligence on evolving customer preferences.

The benefit side may require even more subjective valuation. For example, if a loss is averted due to effective enterprise risk management, the benefit often goes unnoticed, or the benefits of risk responses such as effective training programs are usually readily apparent, but difficult to quantify. Nevertheless, certain factors can be considered in assessing potential benefits: the likelihood of the undesired condition occurring, the nature of the activities, and the potential financial or operating effect the event might have on the entity.

Cost-benefit determinations vary considerably depending on the nature of the entity. The challenge is to find the right balance. Just as limited resources should not be allocated to less significant risks, excessive control is costly and counterproductive. Customers placing telephone orders will not tolerate order acceptance procedures that are too cumbersome or time-consuming. A bank that makes creditworthy potential borrowers “jump through hoops” will not book many new loans. Too little control, on the other hand, presents undue risk of bad debts. An appropriate balance is needed in a highly competitive environment. And, despite the difficulties, cost-benefit decisions will continue to be made.

Management Override

Enterprise risk management can be only as effective as the people who are responsible for its functioning. Even in effectively managed and controlled entities – those with generally high levels of integrity and risk and control consciousness, and an active and informed board with appropriate governance process – a manager might be able to override enterprise risk management processes. No management or control system is infallible, and those with criminal intent will seek to break systems. However, effective enterprise risk management will improve the entity’s capacity to prevent and detect override activities.

The term “management override” is used here to mean overruling prescribed policies or procedures for illegitimate purposes – such as personal gain or an enhanced presentation of an entity's financial condition or compliance status. A manager of a division or unit, or a member of top management, might override the enterprise risk management process for many reasons: to increase reported revenue to cover an unanticipated decrease in market share; to enhance reported earnings to meet unrealistic budgets; to boost the market value of the entity prior to a public offering or sale; to meet sales or earnings projections to bolster bonus pay-outs tied to performance or value of stock options; to appear to cover violations of debt covenant agreements; or to hide lack of compliance with legal requirements. Override practices include deliberate misrepresentations to bankers, lawyers, auditors and vendors, and intentionally issuing false documents such as purchase orders and sales invoices.

Management override should not be confused with management intervention, which represents management's actions to depart from prescribed policies or procedures for legitimate purposes. Management intervention is necessary to deal with non-recurring and non-standard transactions or events that otherwise might be handled inappropriately. Provision for management intervention is necessary in all enterprise risk management processes because no process can be designed to anticipate every risk and every condition. Management's actions to intervene are generally overt and commonly documented or otherwise disclosed to appropriate personnel. Actions to override usually are not documented or disclosed, with an intent to cover up the actions.

12. ROLES AND RESPONSIBILITIES

Chapter Summary: Everyone in an entity has some responsibility for enterprise risk management. The chief executive officer is ultimately responsible and should assume "ownership." Other managers must support the risk philosophy, promote compliance with the risk appetite and manage the effective functioning of all enterprise risk management components within their spheres of responsibility consistent with the risk culture. Other personnel are responsible for executing in accordance with established enterprise risk management directives and protocols. The board of directors provides important oversight to enterprise risk management. A number of external parties often provide information useful in effecting enterprise risk management. However, these external parties are not responsible for the effectiveness of the entity's enterprise risk management.

Enterprise risk management is effected by a number of parties, each with important responsibilities. The board of directors (directly or through its committees), management, internal auditors and other personnel all make important contributions to effective risk management. Other parties, such as external auditors and regulatory bodies, are sometimes associated with risk assessments and internal control. However, a distinction exists between those who are part of an entity's enterprise risk management process and those who are not, but whose actions nonetheless can affect the process or otherwise help achieve the entity's objectives. Directly or indirectly helping an entity achieve its objectives, however, does not make an external party a part of or responsible for the entity's enterprise risk management.

Responsible Parties

The board of directors, management, chief risk officers, financial officers, internal auditors and indeed every individual within an entity contributes to effective enterprise risk management.

Board of Directors

Management is accountable to the board of directors or trustees, which provides guidance and direction. By selecting management, the board has a major role in defining what it expects in integrity and ethical values, and can confirm its expectations through its oversight activities. Similarly, by reserving authority in certain key decisions, the board plays a role in setting strategy, formulating high-level objectives and broad-based resource allocation.

The board provides oversight with regard to enterprise risk management by:

- Knowing the extent to which management has established effective enterprise risk management in the organization.
- Being aware of and concurring with the entity's risk appetite.

- Reviewing the entity’s portfolio view of risk and considering it against the entity’s risk appetite.
- Being apprised of the most significant risks and whether management is responding appropriately.

The board is part of the internal environment component and must have the requisite composition and focus for enterprise risk management to be effective.

Effective board members are objective, capable and inquisitive. They have a working knowledge of the entity's activities and environment and commit the time necessary to fulfill their board responsibilities. They utilize resources as needed to conduct special investigations and have open and unrestricted communications with internal auditors, external auditors and legal counsel.

Boards of directors may use board committees in carrying out certain of their duties. The use and focus of committees vary from one entity to another, although common committees are nominating/governance, compensation and audit committees, with each focusing attention on elements of enterprise risk management. The audit committee, for example, has a direct role in the reliability of external reporting, and the nominating committee identifies and considers qualifications of prospective board members. As such, the board and its committees are an important part of enterprise risk management.

Management

Management is directly responsible for all activities of an entity, including enterprise risk management. Naturally, management at different levels will have different enterprise risk management responsibilities. These will differ, often considerably, depending on the entity's characteristics.

In any entity, “the buck stops” with the chief executive officer. He or she has ultimate ownership responsibility for enterprise risk management. One of the most important aspects of this responsibility is ensuring that a positive internal environment exists. More than any other individual or function, the CEO sets the tone at the top that influences internal environmental factors and other components of enterprise risk management. A CEO also can influence the board of directors, through whatever influence he or she has on identifying new members, and in setting an example and serving to attract, or deter, candidates for the board. Increasingly, candidates for board seats look closely at top management's integrity and ethical values in determining whether to accept a nomination. Potential directors also focus on whether the entity’s enterprise risk management has the necessary critical underpinnings of integrity and ethical values to enable its effectiveness.

The chief executive's responsibilities include seeing that all components of enterprise risk management are in place. The CEO generally fulfills this duty by:

- Providing leadership and direction to senior managers. Together with them, the CEO shapes the values, principles and major operating policies that form the foundation of the entity's enterprise risk management. The CEO and key senior managers set strategy and formulate entity-wide objectives. They also set broad-based policies and develop the entity’s risk appetite and culture. They take actions concerning the entity's organizational structure, content and communication of key policies, and the type of planning and reporting systems the entity will use.
- Meeting periodically with senior managers responsible for major functional areas – sales, marketing, production, procurement, finance, human resources – to review their responsibilities, including how they manage risk. The CEO gains knowledge of risks inherent in their operations, risk responses and control improvements required, and the status of efforts under way. To discharge this responsibility, the CEO must clearly define the information he or she needs.

Senior managers in charge of organizational units have responsibility for managing risks related to their units' objectives. They convert strategy into operations, identify and assess risks, and effect risk responses. Managers guide the application of enterprise risk management components within their spheres of responsibility, ensuring application is consistent with risk tolerances. In this sense, a cascading responsibility exists, where each executive is effectively a CEO for his or her sphere of responsibility.

Senior managers usually assign responsibility for specific enterprise risk management procedures to managers in specific functions or departments. Accordingly, these managers usually play a more hands-on role in devising and executing particular risk procedures that address unit objectives, such as techniques for event identification and risk assessment, and in determining responses such as developing authorization procedures for purchasing raw materials or accepting new customers. They also make recommendations on related control activities, monitor their application and meet with upper-level managers to report on the control activities' functioning.

This may involve investigating external events or conditions, data entry errors or transactions appearing on exception reports, looking into reasons for departmental expense budget variances and following up on customer back orders or product inventory positions. Significant matters, whether pertaining to a particular transaction or an indication of a larger concern, are communicated upward in the organization.

Each manager's responsibilities should entail both authority and accountability. Each manager should be accountable to the next higher level for his or her portion of enterprise risk management, with the CEO ultimately accountable to the board.

Although different management levels have distinct enterprise risk and control responsibilities and functions, their actions should coalesce in the entity's enterprise risk management.

Staff functions, such as human resources, compliance or legal, also have important supporting roles in designing or shaping effective enterprise risk management components. The human resources function may design and help implement training programs on the entity’s code of conduct and other broad policy issues, often rolled out with business unit leadership. The legal function provides information to line managers on new laws and regulations that affect operating policies. And compliance officers often provide critical information on whether planned transactions or protocols conform to legal and ethical requirements.

Risk Officer

Some companies have established a centralized coordinating point to facilitate enterprise risk management. A risk officer – referred to in some organizations as the chief risk officer or risk manager – works with other managers in establishing effective risk management in their areas of responsibility. Established by and with authority of the chief executive, the risk officer has the resources to help effect enterprise risk management across subsidiaries, businesses, departments, functions and activities. The risk officer may have responsibility for monitoring progress and for assisting other managers in reporting relevant risk information up, down and across the entity. The risk officer also may serve as a supplementary reporting channel.

Some companies assign this role to another senior officer, such as chief financial officer, general counsel, chief audit executive or chief compliance officer; others have found that the importance and breadth of scope of this function require separate assignment and resources.

Companies have found this role most successful when set up with clarity around its responsibility as a staff function – providing support and facilitation to line management. For enterprise risk management to be effective, line managers must assume primary responsibility and have accountability for managing risk within their respective areas.

Responsibilities of a risk officer may include:

- Establishing enterprise risk management policies, including defining roles and responsibilities and participating in setting goals for implementation.
- Framing accountability and authority for enterprise risk management in the business units.
- Promoting an enterprise risk management competence throughout the entity, including facilitating development of technical enterprise risk management expertise and helping managers align risk responses with the entity’s risk tolerances.

- Guiding integration of enterprise risk management with other business planning and management activities.
- Establishing a common risk management language that includes common measures around likelihood and impact, and common risk categories.
- Overseeing development of entity-wide and business unit-specific risk tolerances and working with managers to establish control activities and recommending corrective action where needed.
- Facilitating managers' developing of reporting protocols, including quantitative and qualitative thresholds, and monitoring the reporting process.
- Reporting to the chief executive on progress and outliers and recommending action as needed.

Financial Officers

Of particular significance to enterprise risk management activities are finance and controllership officers and their staffs, whose activities cut across, up and down all operating and business units. These financial executives often are involved in developing entity-wide budgets and plans, and they track and analyze performance, often from an operations, compliance and reporting perspective. These activities are usually part of an entity's central or "corporate" organization, but commonly they also have "dotted line" responsibility for monitoring division, subsidiary or other unit activities. As such, the chief financial officer, chief accounting officer, controller and others in the financial function are central to the way management exercises enterprise risk management. The financial officer plays an important role in preventing and detecting fraudulent reporting, as emphasized in the Treadway Commission report "As a member of top management, the chief accounting officer helps set the tone of the organization's ethical conduct; is responsible for the financial statements; generally has primary responsibility for designing, implementing and monitoring the company's external financial reporting system; and is in a unique position regarding identification of unusual situations caused by fraudulent external reporting." The report notes that the chief financial officer or controller may perform functions of a chief accounting officer.

When looking at the components of enterprise risk management, it is clear that the chief financial (accounting) officer and his or her staff play critical roles. This person is a key player when objectives are established, strategies decided, risks analyzed and decisions made on how changes affecting the entity will be managed. He or she provides valuable input and direction and is positioned to focus on monitoring and following up on the actions decided.

As such, the chief financial (accounting) officer should come to the table an equal partner with the other functional heads. Any attempt by management to have him or her more narrowly focused – limited to principally areas of financial reporting and treasury, for example – could severely limit the entity's ability to succeed.

Internal Auditors

Internal auditors play a key role in evaluating the effectiveness of – and recommending improvements to – enterprise risk management. Standards established by the Institute of Internal Auditors specify that the scope of internal auditing should encompass risk management and control systems. This includes evaluating the reliability of reporting, reviewing the effectiveness and efficiency of operations, safeguarding assets and ensuring compliance with laws, regulations and contracts.

The internal audit function does not – as some people believe – have primary responsibility for establishing or maintaining enterprise risk management. That, as noted, is the responsibility of the CEO, along with designated responsibilities to key managers. Internal auditors should assist both management and the audit committee by monitoring, examining, evaluating, reporting on and recommending improvements to the adequacy and effectiveness of management's enterprise risk management processes.

All activities within an entity are potentially within the scope of the internal auditors' responsibility. In some entities, the internal audit function is heavily involved with controls over operations. For example, internal auditors may periodically monitor production quality, test the timeliness of shipments to customers or evaluate the efficiency of plant layout. In other entities, the internal audit function may focus primarily on compliance or external reporting-related activities.

The Institute of Internal Auditors also identifies standards that state, among other things, – that internal auditors should be objective with regard to the activities they audit. This objectivity should be reflected by their position and authority within the entity.

Organizational position and authority involve such matters as a reporting line to an individual who has sufficient authority to ensure appropriate audit coverage, consideration and response; selection and dismissal of the chief audit executive only with concurrence of the board of directors or audit committee; internal auditor access to the board or audit committee; and internal auditor authority to follow up on findings and recommendations.

Internal auditors are objective when not placed in a position of subordinating their judgment on audit matters. The primary protection for this objectivity is appropriate internal auditor staff assignments. These assignments should avoid potential and actual conflicts of interest and bias. Staff assignments should be rotated periodically and internal auditors should not assume operating responsibilities. Similarly, they should not be assigned to audit activities with which they were involved recently in prior operating assignments.

Other Entity Personnel

Enterprise risk management is, to some degree, the responsibility of everyone in an entity, and therefore it should be an explicit or implicit part of everyone's job description. This is true from two perspectives:

- Virtually all personnel play some role in effecting risk management. They may produce information used in identifying or assessing risks, or take other actions needed to effect enterprise risk management. The care with which those activities are performed directly affects the effectiveness of an entity's enterprise risk management.
- All personnel are responsible for supporting information and communication flows inherent in enterprise risk management. This includes communicating to a higher organizational level any problems in operations, non-compliance with the code of conduct or other violations of policy or illegal actions. Enterprise risk management relies on checks and balances, including segregation of duties, and on personnel not "looking the other way." Personnel should understand the need to resist pressure from superiors to participate in improper activities, and channels outside of normal reporting lines should be available to permit reporting of such circumstances.

Enterprise risk management is everyone's business, and roles and responsibilities of all personnel should be well defined and effectively communicated.

External Parties

A number of external parties can contribute to achievement of an entity's objectives, sometimes by actions that parallel those taken within the entity. In other cases, external parties may provide information useful to the entity in its enterprise risk management activities.

External Auditors

Public accountants provide management and the board of directors a unique, independent and objective view that can contribute to an entity's achievement of its external financial reporting objectives, as well as other objectives.

In a financial statement audit, the auditor expresses an opinion on the fairness of the financial statements in conformity with generally accepted accounting principles, thereby contributing to the entity's external financial reporting objectives. While enterprise risk management can provide a degree of assurance regarding the fair presentation of the entity's financial statements, the independent auditor brings assurance to a higher level. The auditor, in addition, often provides information to management useful in conducting enterprise risk management responsibilities.

People have different perceptions of the attention given during a financial statement audit to an entity's enterprise risk management, particularly internal control. Some believe that an auditor who expresses a standard, unqualified, "clean" opinion on the financial statements has concluded that the entity's internal control over published financial statements is effective. Others believe that, at the very least, the auditor has conducted a sufficiently thorough review of risks and controls to identify all or most significant weaknesses. Neither of these views is accurate.

To put a financial statement audit in perspective, it helps to recognize that while an entity can have ineffective enterprise risk management and ineffective internal control related to external financial reporting, an auditor may still be able to issue an opinion that the financial statements are "fairly presented." This is because an auditor focuses audit attention directly on the financial statements. If corrections to the financial statements are needed, they can be made, in which case a "clean" opinion may be rendered.

Under generally accepted auditing standards, the auditor gives an opinion on the financial statements, not the internal control system. Inadequate enterprise risk management and internal control may affect the audit and make it more costly, due to the need for the auditor to perform more extensive tests of financial statement balances before forming an opinion. An auditor must gain sufficient knowledge of an entity's internal control over financial reporting in order to plan the audit. The extent of attention given to internal control varies from audit to audit. In some cases, considerable attention is given, and in others, relatively little attention is given. But even in the former case, an auditor usually would not be in a position to identify all internal control weaknesses that might exist.

In many cases, auditors conducting a financial statement audit do, in fact, provide information useful to management in carrying out their risk management related responsibilities:

- By communicating audit findings, analytical information and recommendations for use in taking actions necessary to achieve established objectives.
- By communicating findings regarding deficiencies in risk management and control that come to their attention, and recommendations for improvement.

This information frequently will relate not only to financial reporting but to operations and compliance activities as well, and can make important contributions to an entity's achievement of its objectives in each of these areas. The information is reported to management and, depending on its significance, to the board of directors or audit committee.

On the other hand, where law and regulation require the auditor to evaluate a company's assertions related to internal control over financial reporting and the supporting basis for those assertions, the scope of the examination directed at those areas will be extensive.

Legislators and Regulators

Legislators and regulators affect the enterprise risk management of many entities, either through requirements to establish internal controls or through examinations of particular entities. Many of the relevant laws and regulations deal primarily with financial reporting risks and controls. However, some – particularly those that apply to government organizations – also can deal with operations and compliance objectives. Many entities have long been subject to legal requirements for internal control. For example, public companies have been required to establish and maintain internal accounting control systems that satisfy specified objectives. More-recent legislation requires that senior executives of publicly listed companies certify to the effectiveness of the companies' internal control over financial reporting, together with auditor attestation.

Several regulatory agencies directly examine entities for which they have oversight responsibility. For example, federal and state bank examiners conduct examinations of banks and often focus on aspects of the banks' risk management and internal control systems. These agencies make recommendations and take enforcement action.

Therefore, legislators and regulators affect entities' enterprise risk management in two ways: They establish rules that provide the impetus for management to ensure that risk management and control systems meet the minimum statutory and regulatory requirements; and, pursuant to examination of a particular entity, they provide information used by the entity to apply enterprise risk management, and recommendations and sometimes directives to management regarding needed improvements.

Parties Interacting with the Entity

Customers, vendors, business partners and others who conduct business with an entity are an important source of information used in enterprise risk management activities.

- *A customer informs a company about shipping delays, inferior product quality or failure to otherwise meet the customer's needs for product or service. Or a customer may be more proactive and work with an entity in developing needed product enhancements.*
- *A vendor provides statements or information regarding completed or open shipments and billings, which is used in identifying and correcting discrepancies and reconciling balances.*
- *A business partner highlights emerging trends in technology affecting market demand for product or service.*

These parties provide information that, in some cases, can be extremely important to an entity in achieving its strategic, operations, reporting and compliance objectives. The entity must have mechanisms in place to receive such information and to take appropriate action. Appropriate action includes not only addressing the particular situation reported, but also investigating the underlying source of the problem and fixing it.

In addition to customers and vendors, other parties, such as creditors, can provide oversight regarding achievement of an entity's objectives. A bank, for example, may request reports on an entity's compliance with certain debt covenants. It also may recommend performance indicators or other desired targets or controls.

Outsource Service Providers

Many organizations outsource a non-core business function, delegating its day-to-day management to outside providers. Administrative, finance and internal operations sometimes are outsourced, with the objective of obtaining access to enhanced capabilities and lower cost of services. A financial institution may outsource its loan review process to a third party; a technology company may outsource the operation and maintenance of its information technology processing; and a retail company may outsource its internal audit function. While these external parties execute activities for or on behalf of the entity, management cannot abdicate its responsibility to manage the associated risks. Management should implement an oversight program to monitor those activities.

Financial Analysts, Bond Rating Agencies and the News Media

Financial analysts and bond rating agencies consider many factors relevant to an entity's worthiness as an investment. They analyze management's objectives and strategies, historical financial statements and prospective financial information, actions taken in response to conditions in the economy and marketplace, potential for success in the short and long term, and industry performance and peer group comparisons. The print and broadcast media, particularly financial journalists, also may undertake similar analyses.

The investigative and monitoring activities of these parties can provide insights on how others perceive the entity's performance, industry and economic risks the entity faces, innovative operating or financing strategies that may improve performance, and industry trends. This information sometimes is provided in face-to-face meetings between the parties and management, or indirectly in analyses for investors, potential investors and the public. In either case, management should consider the observations and insights of financial analysts, bond rating agencies and the news media that may enhance enterprise risk management.

13. WHAT TO DO

Actions that might be taken as a result of this report depend on the position and role of the parties involved.

:

- *Board Members* – Members of the board of directors should discuss with senior management the state of the entity's enterprise risk management and provide oversight as needed. The board also should ensure that the entity's enterprise risk management mechanisms provide it with an assessment of the most significant risks relative to strategy and objectives, including what actions management is taking and how it is engaged in monitoring the enterprise risk management framework. The board should seek input from the internal auditors, external auditors and advisors.
- *Senior Management* – This study suggests that the chief executive should assess the entity's enterprise risk management capabilities. Using this framework, a CEO, together with key operating and financial executives, can focus attention where needed. Under one approach, the chief executive could bring together business unit heads and key functional staff to discuss an initial assessment of enterprise risk management capabilities and effectiveness. Whatever its form, an initial assessment should determine whether there is a need for, and how to proceed with, a broader, more in-depth evaluation. It also should ensure that ongoing monitoring processes are in place. Time spent in evaluating enterprise risk management represents an investment, but one with a high return.
- *Other Entity Personnel* – Managers and other personnel should consider how their enterprise risk management responsibilities are being conducted in light of this framework and discuss with more senior personnel ideas for strengthening enterprise risk management. Internal auditors should consider the breadth of their focus on enterprise risk management.
- *Regulators* – Expectations for enterprise risk management vary widely in two respects. First, they differ regarding what these mechanisms can accomplish. Some observers believe enterprise risk management will, or should, prevent economic loss, or at least prevent companies from going out of business. Second, even when there is agreement about what enterprise risk management can and can't do, and about the "reasonable assurance" concept, there can be disparate views of what that concept means and how it will be applied. Executives have expressed concern regarding how some regulators view the capability of enterprise risk management, especially in hindsight after an alleged failure has occurred. To help gain a shared view of enterprise risk management and what it can do, there should be agreement on a common enterprise risk management framework, including its limitations. This framework may be looked to in that regard.

- *Professional Organizations* – Rule-making and other professional organizations providing guidance on financial management, auditing and related topics should consider their standards and guidance in light of this framework. To the extent diversity in concept and terminology is eliminated, all parties will benefit.
- *Educators* – This framework should be the subject of academic research and analysis, to see where future enhancements can be made. With the presumption that this report becomes accepted as a common ground for understanding, its concepts and terms should find their way into university curricula.

We believe this report offers a number of benefits. With this foundation for mutual understanding, all parties will be able to speak a common language and communicate more effectively. Business executives will be positioned to assess enterprise risk management processes against a standard, and strengthen the process and move their enterprises toward established goals. Future research can be leveraged off an established base. Legislators and regulators will be able to gain an increased understanding of enterprise risk management, its benefits and limitations. With all parties utilizing a common internal control framework, these benefits will be realized.

[This page intentionally left blank]

A. Objectives and Methodology

In Fall 2001, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) launched a landmark study designed to provide guidance in helping organizations manage risk. Despite an abundance of literature on the subject, COSO concluded there was a need for this study to design and build a framework and application guidance. PricewaterhouseCoopers was engaged to lead this project.

The framework defines risk and enterprise risk management, and provides a foundational definition, conceptualizations, objectives categories, components, principles and other elements of a comprehensive risk management framework. It provides direction for companies and other organizations in determining how to enhance their risk management architectures, providing context for and facilitating application in the real world. This document also is designed to provide criteria for companies' use in determining whether their enterprise risk management is effective and, if not, what is needed to make it so.

The application guidance links directly to the framework. The guidance provides practical "how to" information that can be applied by companies and other organizations at various levels – enterprise, line of business and individual function or process – and in support of incremental or transformational decisions. The guidance enables entities to build effective programs to identify, assess and respond to risks.

Because of readers' diverse needs, input was obtained from corporate executives of organizations of varying sizes, both public and private, in different industries. The executives included corporate chief executives, chief financial officers, chief risk officers, controllers, and internal auditors, as well as legislators, regulators, lawyers, external auditors, consultants, academicians and others.

Throughout the project, the project team received advice and counsel from an Advisory Council to the COSO Board. The Advisory Council, composed of individuals in senior financial management, internal and external audit, and academia, met periodically with the project team and members of the COSO Board to review the project plan, progress and drafts of the framework and to take up related matters. At important project milestones, the Advisory Council communicated with the full COSO Board.

The methodology employed in this study was designed to produce a report meeting the stated objectives. The project consisted of five phases:

I. Assessing

The project team assessed the current state of risk management models through review of literature, a survey and workshops, for the purpose of capturing relevant information across the full spectrum of risk management. This phase encompassed analyzing the information, comparing and contrasting conceptual and practical risk management philosophies and protocols, understanding user needs and identifying critical issues and concerns.

II. Envisioning
The team created a working risk management framework conceptual model and developed a preliminary inventory of tools as a basis for the application guidance. Using customized input solicitation techniques, the team tested the concepts with key user and stakeholder groups and, based on feedback, refined the conceptual model.

III. Building and Designing
Using the refined conceptual model as a blueprint, the team developed the framework, with all related elements – definitions, objectives categories, components, principles, infrastructure and management context, along with related discussion. This phase encompassed designing the application guidance. Both the draft framework and implementation guidance design were reviewed with key user and stakeholder groups, and reactions and suggestions for enhancement were obtained.

IV. Preparing for Public Exposure
In this phase the team refined and fine-tuned the framework document. During this phase the team further developed the application guidance and reviewed the key concepts with executives from several companies who provided feedback on their value and utility.

V. Finalizing
This phase encompasses issuing the document for public exposure for a 90-day comment period, and field testing the framework with several companies. Upon receipt of comments, the team will review and analyze them, together with input received from the field tests, and identify needed modifications. The team will then finalize the framework document and the application guidance and provide the final manuscripts to the COSO Advisory Council and the COSO Board for review and acceptance.

As one might expect, many different and sometimes contradictory opinions were expressed on fundamental issues – within a project phase and between phases. The project team, with COSO Advisory Council and Board oversight, carefully considered the merits of the positions put forth, both individually and in the context of related issues, embracing those facilitating development of a relevant, logical and internally consistent framework. The Advisory Council and COSO Board are entirely supportive of the framework resulting from this process.

Acknowledgments

The COSO Board, Advisory Council and PricewaterhouseCoopers LLP gratefully acknowledge the many individuals, including executives, legislators, regulators, auditors, academics and others, who gave their time and energy in participating in and contributing to various aspects of the study.

The following PricewaterhouseCoopers partners provided important input to this framework: Dick Anderson, Jeffery Boyle, Glen Brady, Michael Bridge, John Bromfield, Gary Chamblee, Nicholas Chipman, John Copley, Michael de Crespigny, Steven Del Vecchio, Scott Dillman, P. Gregory Garrison, Bruno Gasser, Susan Kenney, Brian Kinman, Robert Lamoureux, James LaTorre, Mike Maali, Jorge Manoel, Cathy McKeon, Juan Pujadas, Richard Reynolds, Mark Stephen, Robert Sullivan, Jeffrey Thompson and Shyam Venkat.

The following individuals also contributed to this study: Michael Haubenstock, Director, Enterprise Risk Management , Capital One Finance Corporation; Adrienne Willich, Manager of Operational Risk, Capital One Finance Corporation; and Daniel Mudge, President and Chief Operating Officer, OpVantage. Richard A. Scott, William G. Shenkir and Paul L. Walker from the University of Virginia conducted preliminary research leading to this study.

Special acknowledgement goes to Robert G. Eccles, President, Advisory Capital Partners, Inc. and former Harvard Business School Professor, for his extensive contributions to this enterprise risk management framework.

[This page intentionally left blank]

B. Relationship Between Enterprise Risk Management Framework and Internal Control – Integrated Framework

In 1992, the Committee of Sponsoring Organizations of the Treadway Commission issued *Internal Control – Integrated Framework*, which established a framework for internal control and provided evaluation tools which business and other entities could use to evaluate their control systems. The framework identified and described five interrelated components necessary for effective internal control.

Internal Control – Integrated Framework defined internal control as a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations;
- Reliability of financial reporting; and
- Compliance with applicable laws and regulations.

Internal control is encompassed within and an integral part of enterprise risk management. Enterprise risk management is broader than internal control, expanding and elaborating on internal control to form a more robust conceptualization focusing more fully on risk. *Internal Control – Integrated Framework* remains in place for entities and others looking at internal control by itself. This appendix highlights the key areas where the enterprise risk management framework expands on internal control.

Categories of Objectives

Internal Control – Integrated Framework specifies three categories of objectives – operations, financial reporting and compliance. Enterprise risk management also specifies three similar objectives categories – operations, reporting and compliance – and while two are defined in the same way as in the internal control framework, one is different. The reporting category in the internal control framework is defined as relating to the reliability of published financial statements. In the enterprise risk management framework, the reporting category is significantly expanded, to cover all reports developed by the entity, disseminated both internally and externally. These include reports used internally by management and those issued to external parties, including regulatory filings and reports to other stakeholders. And, the scope expands from financial statements to cover not just financial information, but non-financial information as well.

Another category of objectives has been added, namely, strategic objectives, which operate at a higher level than the others. These objectives flow from an entity's mission or vision, and the operations, reporting and compliance objectives should be aligned with them. Enterprise risk management is applied in strategy setting, as well as in working toward achievement of objectives in the other three categories.

Portfolio View

A concept not contemplated in the internal control framework is a portfolio view of risk. In addition to focusing on risk in considering achievement of entity objectives on an individual basis, it is necessary to consider risk in the aggregate, from a "portfolio" perspective.

Environment

In discussing the environment component, the enterprise risk management framework focuses more directly and broadly on how risk shapes, either explicitly or implicitly, an entity's risk culture, which is the set of shared attitudes, values, goals and practices that characterize how an entity considers risks. The framework encompasses the concept of an entity's risk appetite, or the broad-based conceptualization of the amount of risk it is willing to accept to achieve its goals. The risk appetite is supported by more specific risk tolerances that reflect the degree of acceptable variation in executing business activities.

Event Identification

Enterprise risk management and internal control acknowledge that risks occur at every level of the entity and result from a variety of internal and external factors. Both frameworks consider risk identification in the context of the potential impact on the achievement of objectives.

The enterprise risk management framework discusses the concept of potential events, defining an event as an incident or series of incidents emanating from internal or external sources that could affect the implementation of strategy and achievement of objectives. Events with potentially positive impact represent opportunities, while events with potentially negative impact represent risks. Enterprise risk management involves identifying events using a combination of techniques that consider both past and potential future events as well as emerging trends, and considering what it is that triggers the events.

Risk Assessment

While both the internal control and enterprise risk management frameworks call for assessment of risk in terms of the likelihood that a given risk will occur and its potential impact, the enterprise risk management framework suggests viewing risk assessment through a sharper lens. Risks are considered on an inherent and residual basis, with impact analyzed using a single mean, worst-case value or distribution of events, preferably expressed in the same unit of measure established for the objectives to which the risks relate. Time horizons should be consistent with an entity's strategies and objectives, and, where possible, observable data. The enterprise risk management framework also calls attention to interrelated risks, describing how a single event may create multiple risks.

As noted above, enterprise risk management encompasses the need for management to develop an entity-level portfolio view. With managers responsible for business unit, function, process or other activities having developed a composite assessment of risk for individual units, entity-level management considers interrelated and aggregate risk from an entity-wide perspective.

Risk Response

The enterprise risk management framework identifies four categories of risk response – avoid, reduce, share and accept. As part of enterprise risk management, management considers potential responses from these categories and considers these responses with the intent of achieving a residual risk level aligned with the entity's risk tolerances. Having considered responses to risk on an individual or a group basis, management considers the aggregate effect of its risk responses across the entity.

Information and Communication

The enterprise risk management framework expands on the information and communication component, considering data derived from past, present and potential future events. Historical data allows the entity to track actual performance against targets, plans and expectations and provides insights into how the entity performed in past periods under varying conditions. Present or current state data provides important additional information, and data on potential future events and underlying factors completes the information analysis. The information infrastructure sources and captures data in a timeframe and at a depth of detail consistent with entity's need to identify, assess and respond to risks and remain within its risk appetite.

Roles and Responsibilities

Both frameworks focus attention on the roles and responsibilities of various parties that are a part of, or provide important information to, internal control and enterprise risk management. The enterprise risk management framework describes the role and responsibilities of risk officers and expands on the role of an entity's board of directors.

[This page intentionally left blank]

C. Selected Bibliography

American Institute of Certified Public Accountants and The Canadian Institute of Chartered Accountants, *Managing Risk in the New Economy*, 2000.

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Internal Control – Integrated Framework*, 1992.

CFO, *A High Level of Intolerance*, Russ Banham, April 2000.

Conference Board of Canada, *A Conceptual Framework for Integrated Risk Management*, Lucy Nottingham, 1997.

Conference Board of Canada, *A Composite Sketch of Chief Risk Officer*, Karen Thiessen, 2001.

Conference Board of Canada, *Don't Gamble with Goodwill – The Value of Effectively Communicating Risks*, Karen Thiessen, 2000.

Economist Intelligence Unit, *Managing Business Risk – An Integrated Approach*, in cooperation with Arthur Andersen & Co, 1995.

Economist Intelligence Unit, *Enterprise Risk Management – Implementing New Solutions*, in cooperation with MCC Enterprise Risk, 1995.

FEI Research Foundation, *Making Enterprise Risk Management Pay Off*, Thomas L. Barton, William G. Shenkir and Paul L. Walker, 2001.

FEI Research Foundation, *Risk Management: An Enterprise Perspective*, in cooperation with Andersen, 2002.

Financial Times, *Enterprise-Wide Risk Management, Strategies for Linking Risk and Opportunity*, James W. DeLoach, 2000.

Institute of Chartered Accountants in England and Wales, *Internal Control Guidance for Directors on the Combined Code*, 1999.

Institute of Directors in Southern Africa, *King Report on Corporate Governance for South Africa 2001*, 2001.

John Wiley & Sons, *Judgement in Managerial Decision Making*, Max H. Bazerman, 2002. (Page 78)

John Wiley & Sons, *Beyond COSO Internal Control to Enhance Corporate Governance*, Stephen J. Root, 1998.

John Wiley & Sons, *Building Public Trust: The Future of Corporate Reporting*, Samuel A. DiPiazza, Jr. and Robert G. Eccles, 2002.

McGraw-Hill, *Risk Management*, Michael Crouhy, Dan Galai and Robert Mark, 2001.

National Commission on Fraudulent Financial Reporting, *Report of the National Commission on Fraudulent Financial Reporting*, 1987, (Page 98).

RMA: PricewaterhouseCoopers, *Operational Risk Management: The Next Frontier*, Michael Haubenstock and John Gontero, 2001.

Risk Management Group of the Basel Committee on Banking Supervision, *Sound Practices for the Management and Supervision of Operational Risk*, 2001.

Risk Management, *The CRO Is Here to Stay*, James Lam, April 2001.

Risk Management, *Executive Perspectives*, September 2001.

Securities Industry News, *Lofty Ambitions for Measuring Global Risk*, Clive Davidson, June 5, 2000.

Standards Australia and Standards New Zealand, *Australian/New Zealand Standard 4360:1999: Risk Management*, 1999.

The Institute of Internal Auditors Research Foundation, *Enterprise Risk Management: Pulling It All Togethe*r, Paul L. Walker, William G. Shenkir and Thomas L. Barton, 2002.

The Institute of Internal Auditors Research Foundation, *Corporate Governance and the Board – What Works Best,* Richard M. Steinberg and Catherine L. Bromilow, 2001.

The RMA Journal, *Creating an Operational Risk-Sensitive Culture*, Miles Everson, March 1, 2002.

Tillinghast–Towers Perrin, *Enterprise Risk Management: Trends and Emerging Practices*, 2001.

D. Consideration of Comment Letters

[To be inserted following public comment period]

[This page intentionally left blank]

E. Glossary

Application Controls – Programmed procedures in application software, and related manual procedures, designed to help ensure the completeness and accuracy of information processing. Examples include computerized edit checks of input data, numerical sequence checks and manual procedures to follow up on items listed in exception reports.

Cause – Underlying internal or external factor that results in an event.

Compliance – Having to do with conforming with laws and regulations applicable to an entity.

Component – One of eight elements of enterprise risk management. The enterprise risk management components are the entity's internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring.

Computer Controls – 1. Controls performed by computer, i.e., controls programmed into computer software. 2. Controls over computer processing of information, consisting of general controls and application controls.

Control – 1. A noun, denoting an item, e.g., existence of a control – a policy or procedure that is part of internal control. A control can exist within any of the eight components. 2. A noun, denoting a state or condition, e.g., to effect control – the result of policies and procedures designed to control; this result may or may not be effective internal control. 3. A verb, e.g., to control – to regulate; to establish or implement a policy that effects control.

Criteria – A set of standards against which enterprise risk management can be measured in determining effectiveness. The eight enterprise risk management components, taken in the context of inherent limitations of enterprise risk management, represent criteria for enterprise risk management effectiveness for each of the four objectives categories.

Deficiency – An enterprise risk management shortcoming, or an opportunity to strengthen enterprise risk management to provide a greater likelihood that the entity's objectives are achieved.

Design – 1. Intent. As used in the definition, enterprise risk management is intended to provide reasonable assurance as to achievement of objectives; when the intent is realized, the system can be deemed effective. 2. Plan; the way a system is supposed to work, contrasted with how it actually works.

Effected – Used with enterprise risk management: devised and maintained.

Effective Enterprise Risk Management – Determining whether enterprise risk management is “effective" is a subjective judgment resulting from an assessment of whether the eight components are present and functioning effectively. As a result of enterprise risk management being judged effective in each of the four categories, respectively, the board of directors and management have reasonable assurance that:

- They understand the extent to which the entity’s strategic objectives are being achieved;
- They understand the extent to which the entity's operations objectives are being achieved;
- The entity’s reporting is reliable; and
- Applicable laws and regulations are being complied with.

Enterprise Risk Management System (or Process, or Architecture) – A synonym for enterprise risk management applied in an entity.

Entity – An organization of any size established for a particular purpose. An entity, for example, may be a business enterprise, not-for-profit organization, government body or academic institution. Other terms used as synonyms include organization and enterprise.

Ethical Values – Moral values that enable a decision maker to determine an appropriate course of behavior; these values should be based on what is “right,” which may go beyond what is legally required.

Event – An incident or occurrence, from sources internal or external to an entity, that could affect the implementation of strategy or achievement of objectives.

Exposure – Portion of the range of possible outcomes of future events for which the entity is susceptible to loss.

General Controls – Policies and procedures that help ensure the continued, proper operation of computer information systems. They include controls over information technology management, information technology infrastructure, security management, and software acquisition, development and maintenance. General controls support the functioning of programmed application controls. Other terms sometimes used to describe general controls are general computer controls and information technology controls.

Impact – Result or effect of an event. There may be a range of possible impacts associated with an event. The impact of an event can be positive or negative relative to the entity’s related objectives.

Inherent Limitations – Those limitations of all enterprise risk management systems. The limitations relate to the limits of human judgment; resource constraints and the need to consider the cost of controls in relation to expected benefits; the reality that breakdowns can occur; and the possibility of management override and collusion.

Inherent Risk – The risk to an entity in the absence of any actions management might take to alter either the risk's likelihood or impact.

Integrity – The quality or state of being of sound moral principle; uprightness, honesty and sincerity; the desire to do the right thing, to profess and live up to a set of values and expectations.

Internal Control – A process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations.
- Reliability of financial reporting.
- Compliance with applicable laws and regulations.

Internal Control System – A synonym for Internal Control, applied in an entity.

Management Intervention – Management's actions to overrule prescribed policies or procedures for legitimate purposes; management intervention is usually necessary to deal with non-recurring and non-standard transactions or events that otherwise might be handled inappropriately by the system (contrast this term with Management Override).

Management Override – Management's overruling of prescribed policies or procedures for illegitimate purposes with the intent of personal gain or an enhanced presentation of an entity's financial condition or compliance status (contrast this term with Management Intervention).

Management Process – The series of actions taken by management to run an entity. Enterprise risk management is a part of and integrated with the management process.

Manual Controls – Controls performed manually, not by computer (contrast with Computer Controls (1)).

Objectives Category – One of four categories of entity objectives – strategic, effectiveness and efficiency of operations, reliability of reporting, and compliance with applicable laws and regulations. The categories overlap, so that a particular objective might fall into more than one category.

Operations – Used with "objectives" or "controls": having to do with the effectiveness and efficiency of an entity's activities, including performance and profitability goals, and safeguarding resources.

Opportunity – Possibility that an event will occur and positively affect the achievement of objectives.

Policy – Management's dictate of what should be done to effect control. A policy serves as the basis for procedures for its implementation.

Procedure – An action that implements a policy.

Reasonable Assurance – The concept that enterprise risk management, no matter how well designed and operated, cannot guarantee that an entity's objectives will be met. This is because of Inherent Limitations in all enterprise risk management systems.

Reporting – Used with "objectives": having to do with the reliability of the entity's reporting, including both internal and external reporting.

Residual Risk – The remaining risk after management has taken action to alter the risk's likelihood or impact.

Risk – The possibility that an event will occur and adversely affect the achievement of objectives.

Risk Appetite – The broad-based amount of risk a company or other entity is willing to accept in pursuit of its mission or vision.

Risk Management – The identification, assessment and response to risk to a specific objective.

Risk Tolerance – The acceptable variation relative to the achievement of objectives.

Stakeholders – Parties that are affected by the entity, such as shareholders, the communities in which the entity operates, employees, customers and suppliers.

Strategic – "Used with objectives": having to do with high-level goals that are aligned with and support the entity's mission.

Uncertainty – Inability to know in advance the exact likelihood or impact of future events.

Value – A measure of worth, utility or importance of an entity to its stakeholders.

Variance – The degree of difference between the expected outcome and actual outcome.

Volatility – Sensitivity of actual outcomes to unexpected changes.