Enterprise Risk Management – Integrated Framework

➢ Application Techniques

September 2004

Committee of Sponsoring Organizations of the Treadway Commission (COSO)

Oversight	Representative
COSO Chair	John J. Flaherty
American Accounting Association	Larry E. Rittenberg
American Institute of Certified Public Accountants	Alan W. Anderson
Financial Executives International	John P. Jessup Nicholas S. Cyprus
Institute of Management Accountants	Frank C. Minter Dennis L. Neider
The Institute of Internal Auditors	William G. Bishop, III David A. Richards

Project Advisory Council to COSO

Guidance

Tony Maki, Chair
Partner
Moss Adams LLP

James W. DeLoach
Managing Director
Protiviti Inc.

John P. Jessup
Vice President and Treasurer
E. I. duPont de Nemours and Company

Mark S. Beasley
Professor
North Carolina State University

Andrew J. Jackson
Senior Vice President of Enterprise Risk Assurance Services
American Express Company

Tony M. Knapp
Senior Vice President and Controller
Motorola, Inc.

Jerry W. DeFoor
Vice President and Controller
Protective Life Corporation

Steven E. Jameson
Executive Vice President, Chief Internal Audit & Risk Officer
Community Trust Bancorp, Inc.

Douglas F. Prawitt
Professor
Brigham Young University

PricewaterhouseCoopers LLP

Author

Principal Contributors

Richard M. Steinberg
Former Partner and Corporate Governance Leader (Presently Steinberg Governance Advisors)

Miles E.A. Everson
Partner and Financial Services Finance, Operations, Risk and Compliance Leader
New York

Frank J. Martens
Senior Manager, Client Services
Vancouver, Canada

Lucy E. Nottingham
Manager, Internal Firm Services
Boston

Table of Contents

1. INTRODUCTION

Use of This Document

This volume of *Enterprise Risk Management – Integrated Framework* provides practical illustrations of techniques used at various levels of an organization in applying enterprise risk management principles. The organization of this volume parallels that of the *Framework* volume. In order to provide further linkage, passages from the *Framework* volume are included here, in *italics*. Those passages also provide a foundation for the illustrated techniques. To gain the desired benefit from this material, users should be familiar with the *Framework* document.

While it is expected that this material will be useful to those seeking to apply enterprise risk management techniques, it is not a part of the *Framework*. Its presentation here in no way suggests that the illustrated techniques need to be used to effect enterprise risk management, or that their application must be present in determining whether enterprise risk management is effective. There is no suggestion that these descriptions or exhibits are a preferred method, or represent "best practices."

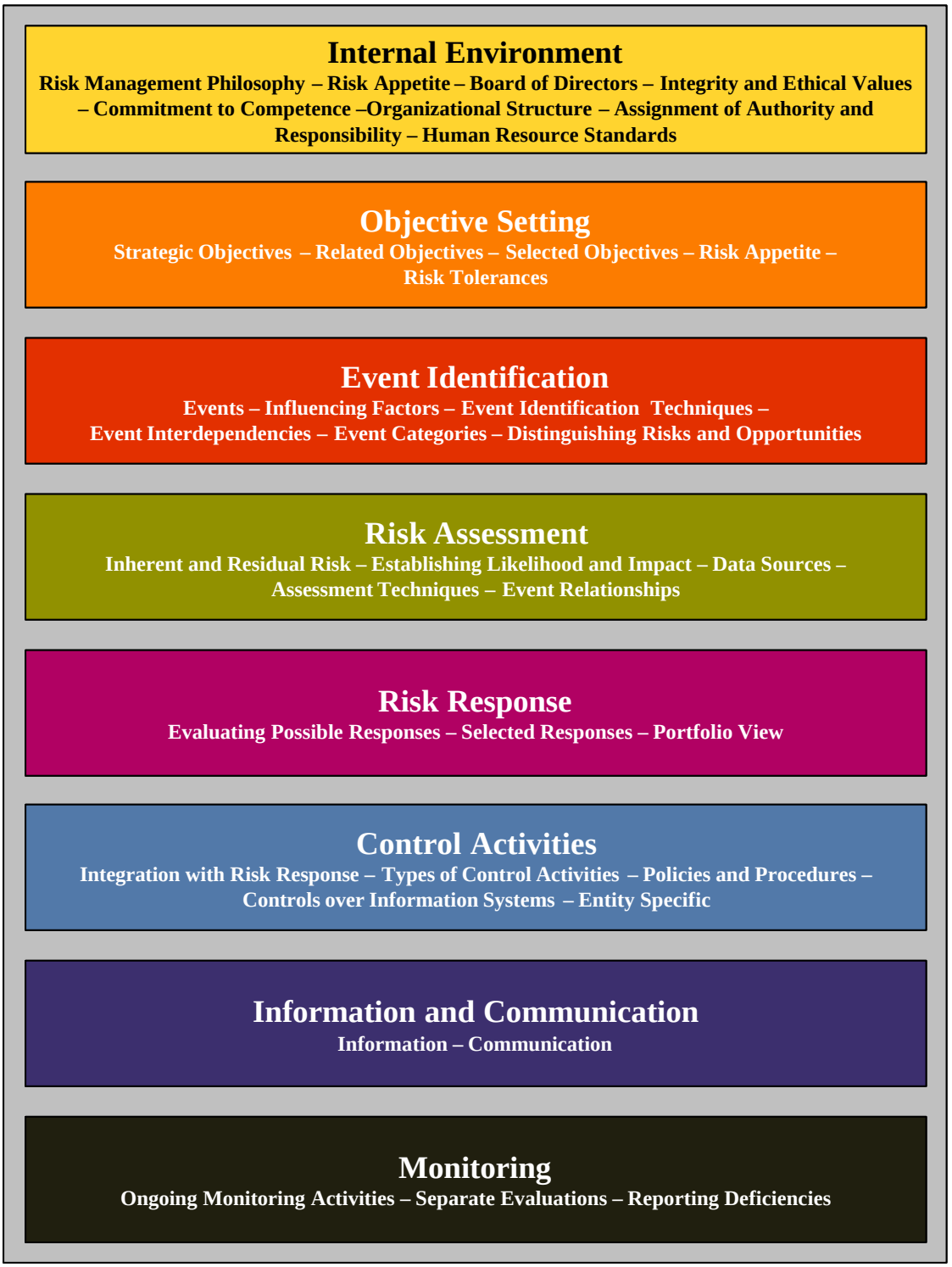
The techniques illustrated in this volume are neither intended to be, nor are they, complete. The exhibits and accompanying discussions relate to only certain elements presented in the *Framework* and depicted in Exhibit 1.1. Some of the techniques are applicable to smaller, non-complex organizations, while others are more relevant to larger, complex entities. A more comprehensive presentation of techniques for applying enterprise risk management that reflects entity size, diversity, and industry is beyond the scope of this project. Over time, we believe that additional guidance will evolve as professional organizations, industry groups, academics, regulators, and others develop material to assist their constituencies.

It is suggested that readers considering enterprise risk management application techniques also refer to the *Evaluation Tools* volume of *Internal Control – Integrated Framework* for additional guidance. It presents tools for use in conducting an evaluation of an entity's internal control system, including a set of blank tools, filled-in tools completed for a hypothetical company, and a reference manual.

Key Elements of Enterprise Risk Management

To provide ready context, Exhibit 1.1 lists key elements of each of the enterprise risk management components.

Exhibit 1.1
Key Elements of Each Component



An Implementation Process

As noted, this volume illustrates a variety of techniques useful in applying specific elements of the enterprise risk management framework. A higher-level, "up front" issue involves what approach management takes when first considering how to implement the framework throughout the organization.

An entity's size, complexity, industry, culture, management style, and other attributes will affect how the framework's concepts and principles are most effectively and efficiently implemented. Because of the array of available approaches and choices, even similar organizations implement enterprise risk management differently – whether applying the framework's concepts and principles for the first time or considering whether their existing enterprise risk management process, which may have been developed ad hoc over time, is truly effective. Experience shows, however, that certain commonalities exist, and provided here is a brief description of common broad-based steps taken by managements that have successfully completed enterprise risk management implementation:

- *Core Team Preparedness* – Establishing a core team, with representation from business units and key support functions, including strategic planning, is an important first step. This team becomes intimately familiar with the framework's components, concepts, and principles. This familiarity provides a common understanding and language, and a foundational basis needed to design and implement an enterprise risk management process that effectively addresses the entity's unique needs.
- *Executive Sponsorship* – While the timing and form of executive sponsorship vary by organization, it is important that executive sponsorship be initiated early and solidified as implementation progresses. Executive leadership articulates the benefits of enterprise risk management, and establishes and communicates the business case for the related investment of resources. CEO support, and usually at least initial direct and visible involvement, drives success.
- *Implementation Plan Development* – An initial plan is created for the next steps, setting out key project phases, including defined work streams, milestones, resources, and timing. Responsibilities are identified, and a project management system put in place. The plan serves as a means to consistently communicate and coordinate with team leadership, and as a basis for communicating and confirming expectations of various units and personnel, and discussing entity-wide changes anticipated from adopting enterprise risk management.
- *Current State Assessment* – This includes an assessment of how enterprise risk management components, concepts, and principles currently are being applied across the entity. This usually involves ascertaining whatever risk management philosophy has evolved within the organization and determining whether there is uniform understanding of the entity's risk appetite. The core team also identifies formal and informal policies, processes, practices, and techniques currently in place, as well as

existing capabilities in the organization for applying the framework's principles and concepts.

- *Enterprise Risk Management Vision* – The core team develops a vision that sets out how enterprise risk management will be used going forward and how it will be integrated within the organization to achieve its objectives – including how the organization focuses its enterprise risk management efforts on aligning risk appetite and strategy, enhancing risk response decisions, identifying and managing cross-enterprise risks, seizing opportunities, and improving deployment of capital.
- *Capability Development* – The current state assessment and the enterprise risk management vision provide insights needed to determine the people, technology, and process capabilities already in place and functioning, as well as new capabilities that need to be developed. This includes defining roles and responsibilities, and modifications to the organizational model, policies, processes, methodologies, tools, techniques, information flows, and technologies.
- *Implementation Plan* – The initial plan is updated and enhanced, adding depth and breadth to cover further assessment, design, and deployment. Additional responsibilities are defined, and the project management system refined as needed. The plan typically embraces general project management disciplines that are a part of any implementation process.
- *Change Management Development and Deployment* – Actions are developed as needed to implement and sustain the enterprise risk management vision and desired capabilities – including deployment plans, training sessions, reward reinforcement mechanisms, and monitoring the remainder of the implementation process.
- *Monitoring* – Management will continually review and strengthen risk management capabilities as part of its ongoing management process.

The following chapters illustrate some of the specific techniques for applying the concepts and principles in each of the components of the enterprise risk management framework.

2. INTERNAL ENVIRONMENT

Framework Chapter Summary: The internal environment encompasses the tone of an organization, influencing the risk consciousness of its people, and is the basis 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; oversight by the board of directors; the integrity, ethical values, and competence of the entity's people; and the way management assigns authority and responsibility, and organizes and develops its people.

This application techniques chapter briefly describes the impact internal environment elements can have on an entity's success or failure, and illustrates statements of risk management philosophy, techniques to evaluate the extent to which the philosophy is integrated into an entity's culture, and tools to promote a culture of integrity and ethics.

Impact

An organization's internal environment has a significant impact on how enterprise risk management is implemented and functions on an ongoing basis. The internal environment is the context in which other components of enterprise risk management are applied, typically with powerful effect, either positive or negative. An example of the latter is presented in Exhibit 2.1.

Exhibit 2.1
Impact of the Internal Environment

The impact of the internal environment is illustrated in findings from the Columbia Accident Investigation Board Report. This board, activated by the National Aeronautics and Space Administration (NASA), investigated the causes of the Columbia Space Shuttle disaster, where the space shuttle broke up on re-entry. The report states: "The organizational causes of the Columbia accident were rooted in the Space Shuttle Program's history and culture. . . . Cultural traits and organizational practices detrimental to safety were allowed to develop, including: reliance on past success as a substitute for sound engineering practices (such as testing to understand why systems were not performing in accordance with requirements); organizational barriers that prevented effective communication of critical safety information and stifled professional differences of opinion; lack of integrated management across program elements; and the evolution of an informal chain of command and decision-making processes that operated outside the organization's rules."

Risk Management Philosophy

An entity's risk management philosophy is the set of shared beliefs and attitudes characterizing how the entity considers risk in everything it does, from strategy development and implementation to its day-to-day activities. . . . [It] is reflected in virtually everything management does in running the entity. It is captured in policy statements, oral and written communications, and decision making. Whether management emphasizes written policies, standards of behavior, performance indicators, and exception reports, or operates more

informally largely through face-to-face contact with key managers, of critical importance is that management reinforces the philosophy not only with words but also with everyday actions.

Managements of some companies articulate elements of their risk management philosophy in writing. Examples of risk management philosophies are presented in Exhibits 2.2 and 2.3.

Exhibit 2.2
Illustrative Statement Describing Risk Management Philosophy

Amidst global growth and cultural expansion, our organization requires a comprehensive approach to corporate risk management that promotes broad strategic thinking and analysis, while fundamentally integrating the Organization's Core Values and Beliefs. To this end, we strive for risk management to become our competitive advantage.

The starting point for our risk management program is an enterprise risk strategy that respects the needs and aspirations of all with whom we have relationships. By facilitating the flow of information and stressing communication across the organization, the risk management program provides a continuous loop risk information model. This model provides information regarding stakeholder needs and expectations to continuously improve our enterprise-wide risk strategy.

To ensure that we fulfill our strategy, our risk management program arms our people with the tools and capabilities to overcome the barriers that arise in striving to exceed expectations. By realizing that risk and control is everyone's job, our people will proactively identify risk in delivering products and services to the market in a more efficient and cost effective manner. Our risk management program allows our people to view the problem from various angles to identify not only the risk mitigation activities, but also to anticipate and act on potential opportunities—therefore challenging conventional wisdom to create better solutions.

A fundamental tenet of our organization is respect and integrity for our employees, customers and shareholders. By incorporating risk management into our daily business practices and by operationalizing the related performance measures, the risk management program ensures that we maintain our highest ethical standards by living our core values.

Exhibit 2.3
Illustrative Statement Describing Risk Management Philosophy

Enterprise risk management will provide our organizations with the superior capabilities to identify, assess and manage the full spectrum of risks and to enable staff at all levels to better understand and manage risk. This will provide us with:

- Responsible acceptance of risk
- Support for Executive and the Board
- Improved outcomes
- Strengthened accountability
- Enhanced stewardship

All staff are expected to demonstrate appropriate standards of behavior in development of strategy and pursuit of objectives. This philosophy is supported by following guiding principles. Management and staff shall:

- Consider all forms of risk in decision-making.
- Create and evaluate business-unit level and Company-level risk profile to consider what's best for their individual business unit and department and what's best for the Company as a whole.
- Support executive management's creation of a Company-level portfolio view of risk.
- Retain ownership and accountability for risk and risk management at the business unit or other point of influence level. Risk management does not defer accountability to others.
- Strive to achieve best practices in enterprise risk management.
- Monitor compliance with policies and procedures and the state of enterprise risk management.
- Lever existing risk management practices, wherever they exist within the Company.
- Document and report all significant risks and enterprise risk management deficiencies.
- Accept that enterprise risk management is mandatory, not optional.

To gain insight into how well the risk management philosophy is integrated into an entity's culture, some companies conduct a risk-related culture survey, which measures the presence and strength of key risk-related attributes. Some of the attributes typically addressed in these surveys are presented in Exhibit 2.4.

Exhibit 2.4
Attributes Measured in a Risk-Related Culture Survey

1. Leadership and Strategy

   Demonstrate Ethics and Values
   Communicate Mission and Objectives

2. People and Communication

   Commitment to Competency
   Share Information and Knowledge

3. Accountability and Reinforcement

   Organizational Structure
   Measure and Reward Performance

4. Risk Management and Infrastructure

   Assess and Measure Risk
   System Access and Security

Some companies survey all staff periodically, such as annually, and a representative sample of staff more frequently, based on desired timing and confidence level. One company deploys these surveys quarterly to allow for greater insight into the ongoing pulse and trends of the organization, especially helpful during times of change. The results of such surveys provide directional indicators of areas of strength and weakness in an organization's culture. An illustration of how results of a risk-related culture survey question are presented and interpreted is shown, in part, in Exhibit 2.5. The results help the entity identify attributes that need strengthening to ensure an effective internal environment.

Exhibit 2.5
Illustrative Risk-Related Culture Survey

#	Question	Attribute	Mean Rating		Std Dev	Count	SD	D	N	A	SA
1	The leaders of my unit set a positive example for ethical conduct	Leadership and Strategy	1.42	Strong	0.71	186	1	3	9	77	96
2	I understand the entity's overall mission and strategy	Leadership and Strategy	1.05	Good	0.69	186	0	7	18	119	42
3	Disciplinary action is taken against those who engage in professional misconduct	Accountability and Reinforcement	0.21	Action Needed	1.20	175	11	55	18	68	23
4	Turnover of personnel has not significantly affected our ability to achieve objectives	People and Communication	0.81	Caution	0.88	145	4	3	39	69	30
5	The leaders of my business unit are receptive to all communications about risk, including bad news	Risk Management and Infrastructure	0.99	Good	0.85	183	2	13	16	106	46

In the example above, each question is ranked using a scale of -2 to +2 as follows: -2 Strongly Disagree (SD); -1 Disagree (D); 0 Neutral (N); +1 Agree (A); +2 Strongly Agree (SA). The assessment, depicted by the color coding, is based on the mean ratings. Additional information is provided by the standard deviation, which is a measure of the respondents' degree of consensus around an issue – the smaller the standard deviation, the greater the respondents' level of agreement on that issue, and the greater the standard deviation, the less agreement.

Integrity and Ethical Values

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 commitment to ethical values start with the individual. Value judgments, attitude, and style are based on individual experiences. Nowhere are integrity and ethical values more important than with the CEO and the senior management team, who set the "tone

at the top" and influence how other entity personnel will conduct themselves. The "right" tone at the top helps:

- The organization's people do the right thing, both legally and morally
- Create a compliance-supporting culture, which is committed to enterprise risk management
- Navigate "gray" areas where no specific compliance rules or guidelines exist
- Promote a willingness to seek assistance and report problems before the point of no return

Organizations support a culture of integrity and ethical values with communications such as a credo or core values statement that sets out the organization's values and priorities, and a code of conduct. A code of conduct provides a connection between the organization's mission or vision and its operating policies and procedures. Not typically an exhaustive conduct guide, or a legal document outlining in detail key organizational protocols, a code of conduct is a proactive statement of an organization's positions on ethics and compliance issues. Codes also can serve as a "user-friendly" guide to the organization's policies on employee and organizational conduct.

An illustration of topics often addressed in a code of conduct is presented in Exhibit 2.6. This structure is derived from the Open Compliance and Ethics Group's pending Foundation Guidelines for an Integrated Compliance and Ethics Program.

Exhibit 2.6
Illustrative Code of Conduct Structure

Code Section	Section Outline
1. Letter from Chief Executive	• Presents top management's message of the importance of integrity and ethics to the organization • Introduces the code of conduct: its purpose and how to use it
2. Goals and Philosophy	• Considers the entity's: – Culture – Business and industry – Geographic locations, domestically and internationally – Commitment to ethical leadership
3. Conflicts of Interest	• Addresses conflicts of interest and forms of self-dealing • Speaks to personnel and other corporate agents and those activities, investments, or interests that reflect on the entity's integrity or reputation
4. Gifts and Gratuities	• Deals with giving of gifts and gratuities, setting forth the entity's policy, typically going well beyond local law • Sets standards and provides guidance regarding gifts and entertainment and their proper reporting
5. Transparency	• Includes provisions dealing with the organization's commitment to complete and understandable social,

Code Section	Section Outline
	environmental, and economic reporting
6. Corporate Resources	• Includes provisions dealing with corporate resources, including intellectual property and proprietary information – whom these belong to and how they are safeguarded
7. Social Responsibility	• Includes the entity's role as a corporate citizen, including its commitment to human rights, environmental sustainability, community involvement, and environmental and economic issues
8. Additional Conduct-Related Topics	• Includes provisions regarding adherence to policies established within specific areas of company activity, for example: – Employment issues such as fair labor practices and antidiscrimination – Governmental dealings such as contracting, lobbying, and political activity – Antitrust and other competitive practices – Good faith and fair dealing with customers/competitors/ suppliers – Confidentiality and security of information – Environmental practices – Product safety/quality

The overview from a professional service firm's code of conduct is presented in Exhibit 2.7.

Exhibit 2.7
Illustrative Overview from Code of Conduct

Our Values

- The best solutions come from working together with colleagues and clients.
- Effective teamwork requires Relationships, Respect and Sharing.
- Delivering what we promise and adding value beyond what is expected.
- We achieve excellence through Innovation, Learning, and Agility.
- Leading with clients, leading with people and thought leadership.
- Leadership demands Courage, Vision and Integrity.

Upholding the [firm] name

- Our clients and colleagues trust [firm name] based on our professional competence and integrity – qualities that underpin our reputation. We uphold that reputation.
- We seek to serve only those clients whom we are competent to serve, who value our service and who meet appropriate standards of legitimacy and integrity.
- When speaking in a forum in which audiences would reasonably expect that we are speaking as a representative of [firm name], we generally state only [firm name] view and not our own.
- We use all assets belonging to [firm name] and to our clients, including tangible, intellectual and electronic assets, in a manner both responsible and appropriate to the business and only for legal and authorized purposes.

Behaving Professionally

- We deliver professional services in accordance with [firm name] policies and relevant technical and professional standards.
- We offer only those services we can deliver and strive to deliver no less than our commitments.
- We compete vigorously, engaging only in practices that are legal and ethical.
- We meet our contractual obligations and report and charge honestly for our services.
- We respect the confidentiality and privacy of our clients, our people and others with whom we do business. Unless authorized, we do not use confidential information for personal use, [firm name's] benefit or to benefit a third party. We disclose confidential information or personal data only when necessary, and when appropriate approval to do so has been obtained, and/or we are compelled to do so by legal, regulatory or professional requirements.
- We aim to avoid conflicts of interest. Where potential conflicts are identified and we believe that the respective parties' interests can be properly safeguarded by the implementation of appropriate procedures, we will implement such procedures.
- We treasure our independence of mind. We protect our clients' and other stakeholders' trust by adhering to our regulatory and professional standards, which are designed to enable us to achieve the objectivity necessary in our work. In doing so, we strive to ensure our independence is not compromised or perceived to be compromised. We address circumstances that impair or could appear to impair our objectivity.
- When faced with difficult issues or issues that place [firm name] at risk, we consult appropriate [firm name] individuals before taking action. We follow our applicable technical and administrative consultation requirements.
- It is unacceptable for us to receive or pay bribes.

Respecting Others

- We treat our colleagues, clients and others with whom we do business with respect, dignity, fairness and courtesy.
- We take pride in the diversity of our workforce and view it as a competitive advantage to be nurtured and expanded.
- We are committed to maintaining a work environment that is free from discrimination or harassment.
- We try to balance work and private life and help others to do the same.
- We invest in the ongoing enhancement of our skills and abilities.
- We provide a safe working environment for our people.

Corporate Citizenship

- We express support for fundamental human rights and avoid participating in business activities that abuse human rights.
- We act in a socially responsible manner, within the laws, customs and traditions of the countries in which we operate, and contribute in a responsible manner to the development of communities.
- We aspire to act in a manner that minimizes the detrimental environmental impacts of our business operations.
- We encourage the support of charitable, educational and community service activities.

- We are committed to supporting international and local efforts to eliminate corruption and financial crime.

To monitor the extent to which employees' actions conform to established standards, some companies periodically use staff focus groups. This feedback, often employing technology, is used to "validate" core values. Technology also can be used to enable sharing and updating information and tracking employee compliance with the code of conduct and related policies, standards, and procedures. Illustrations of how entities are using technology to foster the desired culture are presented in Exhibit 2.8.

Exhibit 2.8
Technology to Support a Culture of Integrity and Ethics

- A direct link from the organization's Internet (or intranet) home page to the values statement and code of conduct, facilitating their use and sending a message about their importance
- Electronically available codes and related information, providing ease of access and eliminating need for paper copies
- Confirmation that staff received the information
- Training venues and e-learning
- Automatic reference to the code or guidance used during completion of tasks
- Automatic reminder to staff of required actions
- Notification to staff's immediate supervisor and above if action is not taken in a timely manner
- Method to obtain certification of compliance
- Audit trail of activities

3. OBJECTIVE SETTING

Framework Chapter Summary: Objectives are set at the strategic level, establishing a basis for operations, reporting, and compliance objectives. 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. Objectives are aligned with the entity's risk appetite, which drives risk tolerance levels for the entity.

This chapter illustrates linking an entity's mission with strategic and related objectives, aligning strategic and related objectives, and depictions of risk appetite and risk tolerances.

Strategic Objectives

In considering alternative ways 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.

Exhibit 3.1 illustrates setting strategic objectives, using risk assessment techniques.

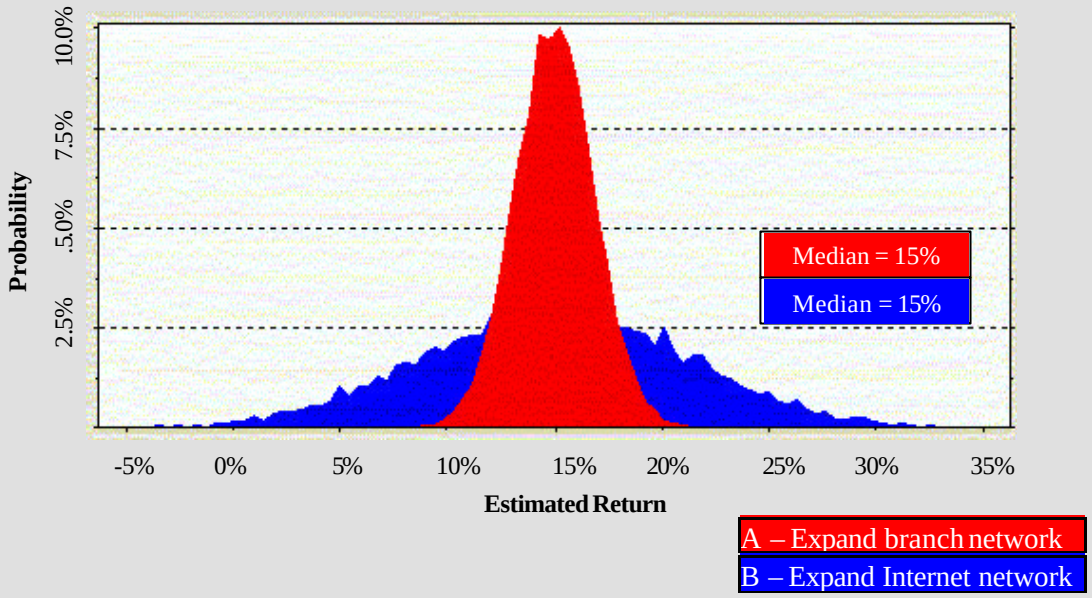
Exhibit 3.1
Setting Strategic Objectives

A community bank considering its options for enhancing customer services identified three strategies:

- Option A – Expand its branch network into new areas matching its target demographics
- Option B – Scale back the branch network to 50% of its current size, and significantly enhance its Internet and call-center capabilities
- Option C – Maintain the branch network, and outsource the existing Internet and call-center operations to a lower-cost company in a foreign country

When considered against the bank's vision, which encompasses contributing to the communities within which it operates, Option C was seen as inconsistent with the vision, given the job losses that would result. Management then focused on Options A and B.

Using scenario analysis, modeling, and stress testing (discussed in the Risk Assessment chapter), management compared the results of each option in relation to the impact on return on capital employed. Management identified the distribution of potential return outcomes given their differing credit and operational risk profiles, and determined that the potential returns on capital employed under the two scenarios, while having similar median outcomes, have markedly different distributions, as shown below.



Based on this analysis, management adopted Option A, deciding to forego the potential upside but avoiding the potential downside of Option B.

Related Objectives

Entity-level objectives are 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.

Linkage of a company's mission with its strategic objectives, strategies, and related objectives is illustrated in Exhibit 3.2.

Exhibit 3.2
Linking Mission/Vision with Strategic and Related Objectives

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 medical 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 ten top under-performing hospitals and negotiate agreements with two this year • Target ten 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 report, accurately and on a timely basis, 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 personnel recognize their primary compliance responsibilities, building into human resource 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

Another example of linkage is illustrated in Exhibit 3.3. Here, the bank referred to in Exhibit 3.1 aligned its vision first with strategic objectives and strategies, and then with objectives in its property unit and human resources function.

Exhibit 3.3
Linking Mission/Vision with Strategic and Related Objectives

Vision	Be the leading and most trusted provider of financial services to families within the region, thereby contributing to the communities within which we operate
Strategic Objectives	• To maintain an annual return on capital employed of 15% • To grow the customer base by 30% within three years through expanding the branch network by 50% over that timeframe
Strategies	• Acquire new property leases in areas that match our target customer demographics • Maintain the current cost structure for the branch network
Property Unit Objectives	• Develop an outsourcing relationship with a qualified real estate company to identify and negotiate suitable leases in accordance with the required growth in the property portfolio • Open 15 new branches in the coming year • Maintain rental cost average of $xx rental per square foot across the property portfolio • Recruit two additional in-house property managers
Human Resources Objectives	• Annual turnover of customer services staff below 10% • Recruit and train 100 customer service staff in the coming year • Develop negotiating position and plan for upcoming negotiations with the trade union regarding treatment of the new employees

Risk Appetite

Risk appetite can be expressed in qualitative or quantitative terms. Exhibit 3.4 provides illustrative questions management might ask when considering its risk appetite.

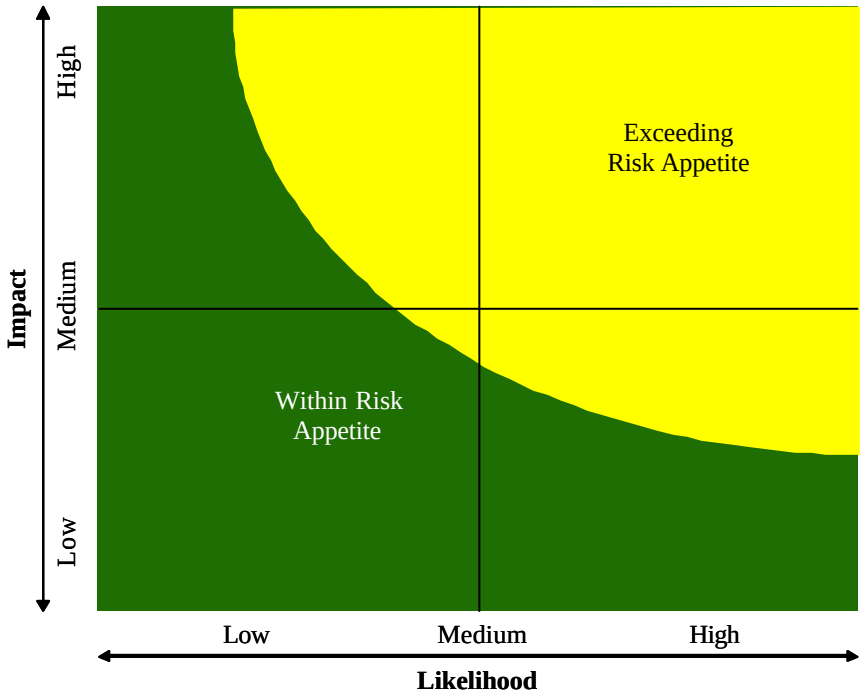
Exhibit 3.4
Considering Risk Appetite

1.	What risks is the company in business to accept and what risks will it not accept – e.g., is the organization prepared to accept minor losses of physical inventory from pilferage but not willing to accept large losses of physical inventory from spoilage, obsolescence, or natural disasters?
2.	Is the company comfortable with the amount of risk accepted, or to be accepted, by each of its businesses?
3.	What levels of risk is the company prepared to accept on new initiatives in order to achieve the company-wide desired return on invested capital of 15%?
4.	Is the entity prepared to accept more risk than it currently is accepting and, if so, what return level would be required?

5.	What level of capital or earnings is the organization willing to put at risk given a particular confidence level – e.g., will management accept 50% of its capital at risk of loss with 95% confidence in this amount?
6.	What percentage of "worst case" risks does the company want to have capital available to cover – based on a scale of likelihood and impact of major risk potentialities? Is it acceptable that an unlikely event could challenge the entity's viability?
7.	Are there specific risks that the organization is not prepared to accept, such as risks that could result in non-compliance with privacy of information laws?
8.	To what extent will the company accept risk to competing objectives, such as risk of lower gross profit margin in return for greater market share?
9.	How does the organization's risk appetite compare with that of peers – how much risk is the organization prepared to accept to move from following competitors in product innovation to trend-setter status?
10.	What are the relative risks, and related comfort levels, in preserving value by maintaining the quality of existing products and services, versus seeking to create new value through new product development?
11.	To what extent is the company prepared to enter into projects with lower likelihood of success but larger potential returns?
12.	Is the organization more comfortable with a qualitative descriptor versus a quantitative one?

Some organizations express risk appetite in terms of a "risk map," as illustrated in Exhibit 3.5. In this exhibit, any significant residual risk in the yellow area exceeds the company's risk appetite, calling for management to take action to reduce the likelihood and/or impact of the risk to bring it within the company's risk appetite.

Exhibit 3.5
Forming Risk Appetite



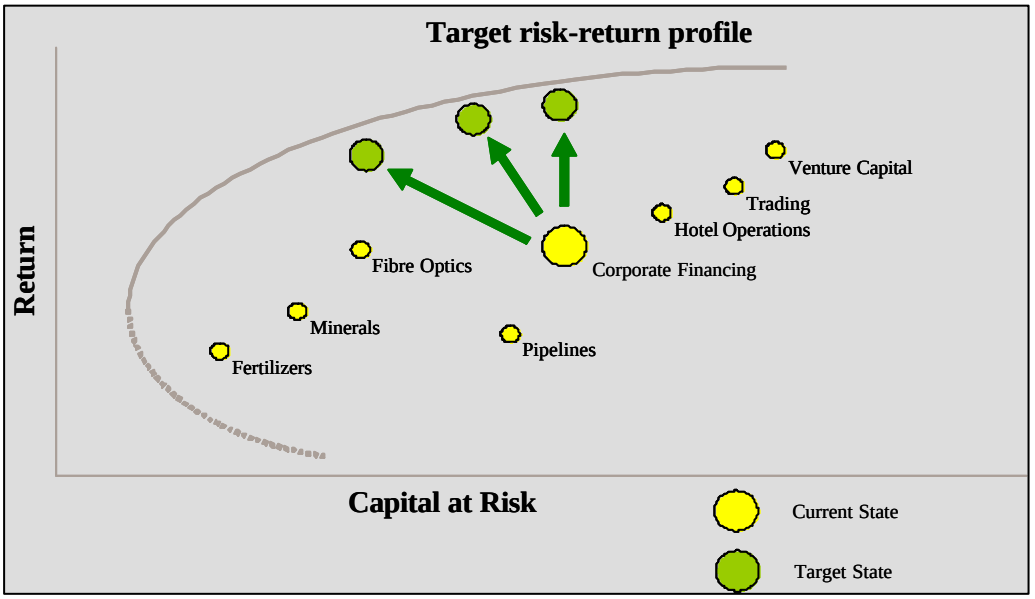
Some industries, especially those in financial services and the oil and gas sector, are able to adopt sophisticated approaches using quantitative techniques to express risk appetite. Advanced entities might express risk appetite using market measures or risk-based capital. Exhibit 3.6 provides an illustration of a statement of risk appetite in terms of market measures.

Exhibit 3.6
Risk Appetite in Terms of Market Measures

A utility company focuses on growing market value capitalization through generating stable cash flows and earnings, and sets risk appetite in those terms. Therefore, all entity-level risks are expressed in relation to the effect on earnings and cash flow volatility. When the trend line in volatility approaches risk appetite, management takes actions as necessary.

Exhibit 3.7 illustrates how a company views capital at risk versus return in relation to risk appetite. The company strives to diversify its portfolio to earn a return that lines up along the target profile, rather than lower down, in the interior of the region.

Exhibit 3.7
Risk Appetite, Return, and Capital at Risk



Determine Risk Tolerances

Risk tolerances are the acceptable levels of variation relative to the achievement of objectives. . . . Operating within risk tolerances provides management greater assurance that the entity remains within its risk appetite, which, in turn, provides a higher degree of comfort that the entity will achieve its objectives.

Development of risk tolerances by an airline related to on-time service is illustrated in Exhibit 3.8.

Exhibit 3.8
Objectives and Risk Tolerances

An airline decided to set an objective around superior on-time service. Management recognized the factors causing flight delays, some of which are within its control, while others are not, and understood well how the various factors affected regulators' public reporting of on-time service. In considering risk tolerances, marketing, customer service, and operations, personnel determined that:

- 85% on-time flight arrival has remained the company's target for many years, which generally has been achieved and is in line with messages in its marketing program
- The industry average for on-time arrival on the relevant routes for the past several years has remained at approximately 80%
- There is minimal effect on the company's customer flight bookings when arrival times temporarily decrease to as low as the industry average
- The cost to achieve more than 87% on-time arrival is uneconomical and cannot be passed through in ticket prices
- The company has been criticized by industry analysts for its inability to keep costs down

Based on this information, management maintained the objective of 85% average on-time arrival, with a tolerance of between 82% and 86%. Looking at the tolerances for other objectives, management is better able to allocate resources to ensure reasonable likelihood of achieving outcomes across multiple objectives.

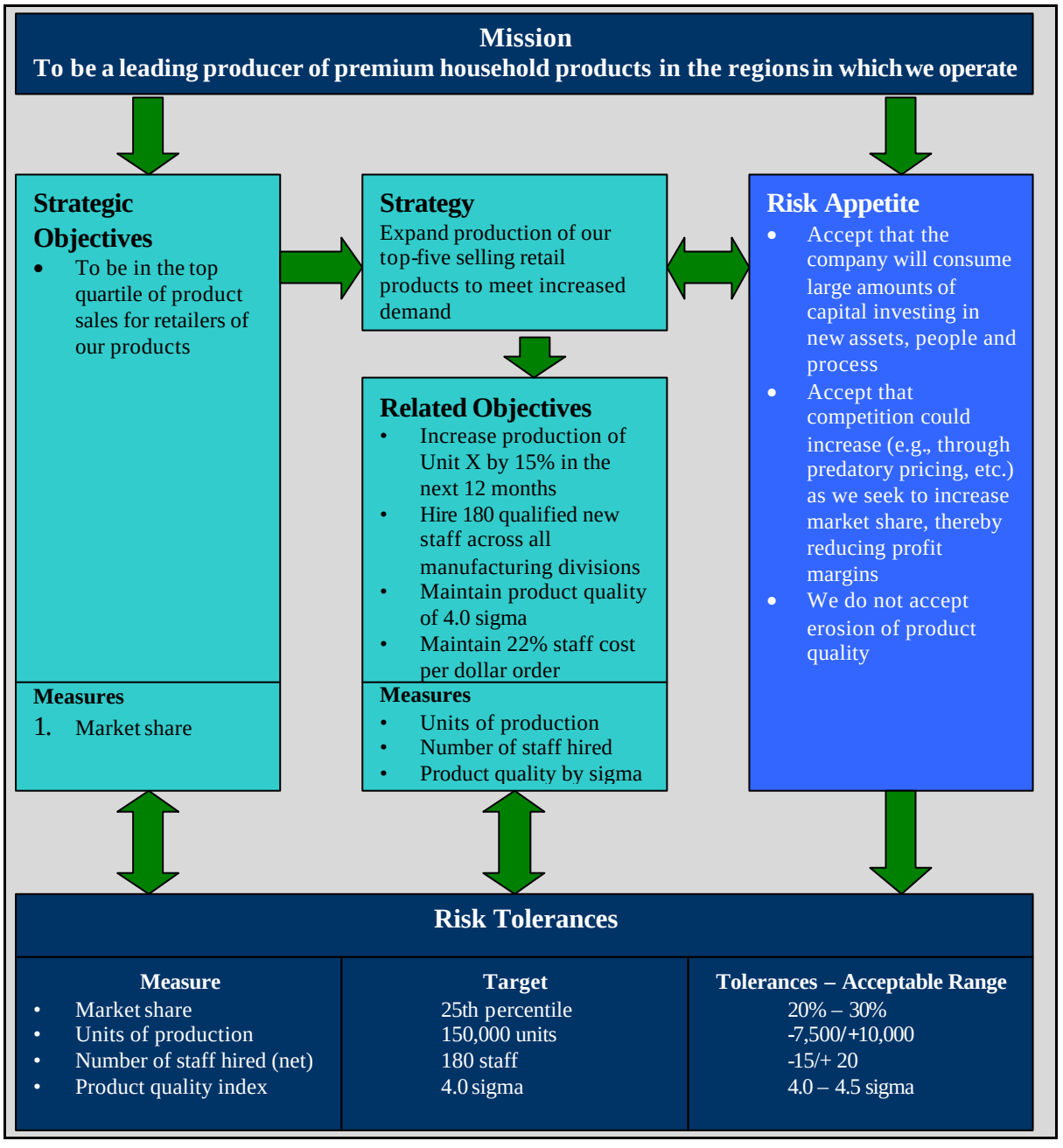
Risk tolerances sometimes are set at the entity level and allocated across business units, as illustrated in Exhibit 3.9.

Exhibit 3.9
Risk Tolerances Across Multiple Business Units

A company set a risk tolerance of no more than 20% of revenue to be derived from alliance partners. When its two business units developed operating and marketing plans for the coming period, both showed a strong dependence on alliance partners, and, when aggregated, the plans reflected such sourced revenue exceeding the 20% threshold. Management decided to allow business unit A to generate up to 40% of revenue from its alliance partner, while business unit B was allowed only 15%, allowing the company's overall plan to retain the 20% tolerance level.

The way in which one organization depicted the relationship between its mission, objectives, appetite, and tolerance is illustrated, in part, in Exhibit 3.10.

Exhibit 3.10
Relating Mission, Objectives, Appetite, and Tolerance



4. EVENT IDENTIFICATION

Framework Chapter Summary: Management identifies potential events that, if they occur, will affect the entity, and determines whether they represent opportunities or whether they might adversely affect the entity's ability to successfully implement strategy and achieve objectives. Events with negative impact represent risks, which require management's assessment and response. Events with positive impact represent opportunities, which management channels back into the strategy and objective-setting processes. When identifying events, management considers a variety of internal and external factors that may give rise to risks and opportunities, in the context of the full scope of the organization.

This chapter illustrates some of the techniques used in event identification. Included are illustrations of how events are linked with objectives; techniques enabling personnel to identify events using event inventories, facilitated workshops, interviews, questionnaires, surveys, and process flow analysis; and identifying events using leading event indicators, escalation triggers, and loss event data tracking. Also illustrated are interrelationships between multiple events, and use of event categories to enhance understanding the relationships.

Linking Events with Objectives

In some circumstances, identifying events related to a specific objective is reasonably straightforward, as illustrated in Exhibit 4.1. In this illustration, building on Exhibit 3.10, potential events and their impacts are identified and related to the objective, associated risk tolerance, and measurement unit. In this example, management determined that increasing staffing levels and maintaining staff costs were two operations objectives (other operations objectives are not presented).

Exhibit 4.1
Identifying Events

Mission	To be the leading producer of premium household products in the regions in which we operate
Strategic objective	To be in the top quartile of product sales for retailers of our products
Related objectives	• Hire 180 new qualified staff across all manufacturing divisions to meet customer demand without overstaffing • Maintain 22% staff cost per dollar order
Objective unit of measure	• Number of new qualified staff hired • Staff cost per dollar order
Tolerance	• 165 – 200 new qualified staff • Staff cost between 20% and 23% per dollar order
Potential events/risks and related impact	• Unexpected slowdown in job market causing more offers being accepted than planned, resulting in excess staff • Unexpected heating up of job market causing fewer offers being accepted, resulting in too few staff • Inadequate needs/specifications descriptions, resulting in hiring unqualified staff

In other circumstances, risk identification is not as immediately evident, and a variety of techniques are used, as discussed in the following paragraphs.

Event Identification Techniques

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.

Management uses any number of techniques to identify potential events affecting achievement of objectives. The techniques are used in identifying risks and opportunities, for example, when implementing a new business process, re-designing an existing one, or evaluating a process. Or, they may be used in connection with strategic or business unit planning, or when considering new initiatives or organizational change. They may be used on a periodic or an ongoing basis.

Application of common event identification techniques is illustrated below.

Event Inventories

Managements use listings of potential events common to a specific industry or functional area. The list is developed by personnel within the entity, or from generic lists generated externally. Such lists of potential events are used, for example, relative to a specific project, process or activity, and can be useful in ensuring a consistent view across similar activities within the organization. If externally developed, the inventory is enhanced and otherwise

tailored to the entity's circumstances, to better relate to the organization's risks, and to be consistent with the organization's common enterprise risk management language. Exhibit 4.2 illustrates use of an externally produced inventory of events potentially affecting a software development project.

Exhibit 4.2
Event Inventories

Before undertaking a software development project, a company reviews an inventory of generic risks inherent in software development projects. The inventory provides a useful way to draw on the accumulated risk knowledge of others experienced in this subject area. Recognizing that the inventory includes risks from companies with different characteristics, management considers the effect of these risks on its own unique circumstances.

Facilitated Workshops

Event identification facilitated workshops typically bring together cross-functional or multi-level individuals for the purpose of drawing on the group's collective knowledge to develop a list of events as they relate, for example, to the company's strategic, business unit, or process objectives. The results of workshops usually depend on the depth and breadth of information the participants bring to the table.

Some organizations in connection with strategy setting hold a workshop of senior management to identify events that could affect achievement of corporate strategic objectives. An approach to the workshop and agenda used by one company to identify potential events relevant to the achievement of specified objectives is outlined in Exhibit 4.3.

Exhibit 4.3
Facilitated Workshop Outline

Prior to the workshop

- Identify experienced facilitator to lead the session, manage group dynamics, and plan how best to capture generated ideas in usable form
- Establish and agree on ground rules at the commencement of the workshop
- Recognize the different participant styles and personality types, considering how to optimize their contribution
- Identify which objectives, category of objectives, and categories of events to focus on
- Invite an appropriate number of workshop participants – normally limit to 15 or fewer
- Set realistic expectations up front with respect to what the workshop is intended to achieve

Agenda

1. **Introduction**
   - Explain background of workshop and why each participant has been invited
   - Explain ground rules
2. **Explain workshop process**
   - Events are to be considered against corporate objectives per business plan

- For each objective, the facilitator will prompt discussion on events emanating from the following factors, and their related effects:

External	**Internal**
Economic	Infrastructure
Natural environment	Personnel
Political	Process
Social	Technology
Technological	

- Describe how and when voting tools and verbal inputs will be used
- Explain how ideas, conclusions will be documented

3. **Explore Objective 1**
   - Identify the objective, its unit of measure, and the related established targets
   - Gain consensus of risk tolerance – the degree of acceptable variation around the unit of measure
   - Discuss internal and external factors that drive potential events relative to the objective
   - Determine which events represent risks to achieving the objective, and which events represent opportunities
   - Consider how multiple risks affecting this objective relate to one another
4. **Next steps and close**
   - Distribute the workshop output to all participants within 48 hours, with action plan for next steps

Interviews

Interviews typically are conducted in a one-on-one setting, or sometimes two-on-one, where the interviewer is accompanied by a colleague taking notes. The purpose is to ascertain the individual's candid views and knowledge of actual past events and potential events. An interview agenda used in focusing on business unit objectives is illustrated in Exhibit 4.4.

Exhibit 4.4
Interview Agenda

Interview Agenda

1. Introduction
2. Provide background on the project and interview process
3. Confirm the person's position, background, and current responsibilities
4. Confirm they received and read any background material provided in advance

Strategies and Objectives

1. Identify the key objectives within the interviewee's business unit/division
2. Determine how the objectives align with and support the entity's strategies and objectives
3. Identify the unit of measure for each objective and the related established targets
4. Determine the established risk tolerances
5. Discuss factors related to potential events relative to the objective
6. Identify potential events creating risks to objectives, and those representing opportunities
7. Consider how the interviewee prioritizes these events, considering likelihood and impact
8. Identify events that have occurred in the past 12 months that impacted the entity that were not identified by management and staff
9. Consider whether risk identification mechanisms need to be enhanced

Questionnaires and Surveys

Questionnaires address a range of issues to be considered by participants, focusing their thinking on internal and external factors that have given rise, or may give rise, to events. Questions can be open-ended or closed, depending on the goal. They can be directed to one or a few individuals, or used in connection with a broader-based survey, either within an entity or directed to customers, suppliers, or other external parties. Use of these techniques is illustrated in Exhibit 4.5.

Exhibit 4.5
Illustrative Questionnaire and Survey

Targeted Questionnaire
A company requires business unit staff to complete a questionnaire before accepting a new vendor. The questionnaire requires the staff person to consider a range of questions exploring the potential vendor's:

- Quality processes
- Risk management processes
- Insurance coverage
- Terms and conditions

In considering the questions, the staff person identified the following potential events to which the company would be exposed if it were to do business with the vendor:

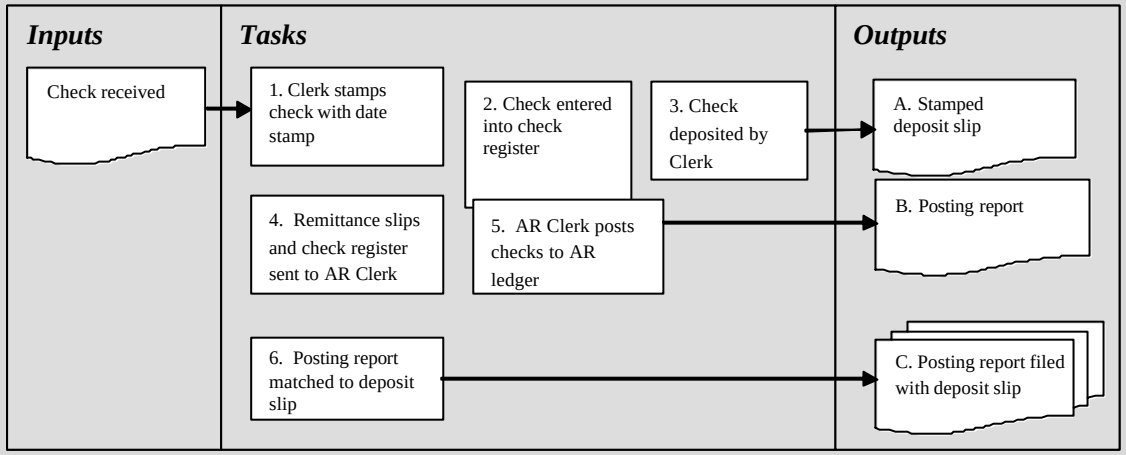
- The vendor's history of inconsistent delivery presents a risk of supply chain disruptions.
- The vendor is not certified to an appropriate quality standard. A risk exists that the materials provided might not meet the company's quality specifications, resulting in production problems, loss of customers, and reputational damage.
- The vendor has inadequate insurance coverage for product defects. A risk exists that the company would not be able to recover associated losses.
- The vendor's terms require a two-year commitment from the company, with an associated risk of changing needs and related economic loss.

Survey
A fast-food company regularly surveys its customers in two areas: changes in their consumption habits/preferences, and satisfaction levels with the service received in its restaurants. A recently completed survey identified a shift in preference toward organic foods and away from genetically modified foods. With this information, management assessed the extent to which the shift in preferences called for modification of strategy and related objectives, including new product offerings and marketing programs. Similarly, management used the survey results – which showed a declining level of satisfaction with service at particular restaurants – in looking at underlying issues related to those units.

Process Flow Analysis

Process flow analysis typically involves the diagrammatic representation of a process, with the goal of better understanding the interrelationships of its component inputs, tasks, outputs, and responsibilities. Once mapped, events can be identified and considered against process objectives. As with other event identification techniques, process flow analysis can be used in looking from a high level within the entity, or at a detailed level. Exhibit 4.6 illustrates the latter, depicting how a company mapped its cash receipts process as a basis for identifying related risks to the objective of depositing and recording all cash receipts on a timely and accurate basis.

Exhibit 4.6
Process Flow Analysis



Tasks	Possible events
1. Clerk stamps check with date stamp	• Clerk fails to stamp check
2. Check entered into check register	• Clerk fails to record check details • Clerk records incorrect check details • Clerk misappropriates check
3. Check deposited by Clerk	• Check lost en route to bank • Check deposited to incorrect bank account • Incorrect amount recorded by bank • Stamped deposit slip lost
4. Remittance slips and check register sent to AR Clerk	• Remittance slips or check register misplaced or lost
5. AR Clerk posts checks to AR ledger	• Checks applied to incorrect accounts • Incorrect amount recorded against customer account • AR Clerk does not post checks
6. Posting report matched to deposit slip	• Details do not match

Leading Event Indicators and Escalation Triggers

Leading event indicators, often called leading risk indicators, are qualitative or quantitative measures that provide insight into potential events – such as the price of fuel, turnover in investor securities accounts, and traffic on an Internet site. To be useful, leading risk indicators must be available to management on a timely basis, which, depending on the information, might be daily, weekly, monthly, or in real time.

Escalation triggers typically focus on day-to-day operations and are reported, on an exception basis, when a pre-established threshold is passed. Companies often have escalation triggers established within business units or departments. To be effective, escalation triggers need to establish when managers are to be notified, with notification timing based on the manager's view of how much time is needed to take action.

Leading risk indicators and escalation triggers are illustrated in Exhibit 4.7.

Exhibit 4.7
Leading Risk Indicators and Escalation Triggers

Business Unit Objective	Measure	Target and Tolerance	Potential Event	Leading Indicator	Escalation Trigger for Business Unit
Develop product promotional campaign with supermarket chain in key region	Number of units sold per month per store	*Target*: 1,000 units of new product sold per month per store during promotional campaign *Tolerance*: 900–1,250 units sold per month per store	Consumer confidence decreases, resulting in decreases in purchases of the company's products	Consumer confidence indicators	Consumer confidence decreases by more than 5%
Create and maintain strong security against external intrusions on systems	Number of successful intrusions	*Target:* 0 per month *Tolerance*: 0 per month	Unauthorized individuals access the company's systems via Internet ports	Detected vulnerabilities in the company's core operating systems published by the vendor/third party; number of unauthorized attempts	New critical vulnerabilities identified by third parties
Comply with standards governing the movements of	Volume of spills of hazardous materials	*Target:* <100 gallons per year *Tolerance:* 0–	Corrosion on barrels causes material to leak from trucks	Age of barrels used to transport hazardous material	Barrels in use for more than 85% of their estimated useful life

Business Unit Objective	Measure	Target and Tolerance	Potential Event	Leading Indicator	Escalation Trigger for Business Unit
hazardous material	transported by company staff	125 gallons	during transport		
Maintain stable high-quality workforce	Turnover of staff rated as high performers	*Target*: Turnover of high performers < 10% *Tolerance*: 2% –12%	High performers resign	Staff morale of high performers	High performers responding as "very" or "somewhat" dissatisfied in annual employee survey

Loss Event Data Tracking

Monitoring relevant data can help an organization identify past events having a negative impact and quantify the associated losses, in order to predict future occurrences. While event data typically are used in risk assessment – based on actual experience with likelihood and impact – they also can be useful in event identification by providing a basis for fact-based discussion, institutionalizing knowledge (particularly helpful where staff turnover is high), and serving as a source for understanding loss event interdependencies and developing predictive and causal models.

Loss event databases developed and maintained by third party service providers are available on a subscription basis. In some industries, such as banking, consortiums have formed to share internal data.

Loss event databases contain information on actual events meeting specified criteria. Information in externally developed event databases can be useful to supplement internally generated information in estimating future event likelihood and impact, particularly for potential events with low likelihood (which a company is unlikely to have experienced in the past) but high impact. One such database, for example, contains loss event data, across industries, on publicly reported operational losses in excess of one million dollars.

Some companies track ranges of external data. Large companies, for example, track a range of leading economic indicators to identify movements suggesting change in demand for their products and services. Similarly, financial institutions monitor changes in world politics to identify leading indicators suggesting modification to future investment strategies and actual events calling for immediate change to investment portfolios.

Use of internally generated data is illustrated in Exhibit 4.8, and externally developed data in Exhibit 4.9.

Exhibit 4.8
Loss Event Tracking Using Internal Data

A manufacturing company tracks production equipment failures, through automated routines that electronically monitor and capture disparate equipment diagnostic information. By tracking the sequence of events, management is positioned to assess the underlying cause of a manufacturing process failure and the costs associated with equipment downtime. Operations managers use the information in real time, diagnosing the cause and quickly making repair decisions. Future maintenance schedules reflect known past equipment failures. Periodically operations management is provided reports determining the effect of the equipment failures on a key unit of measure – production availability – and associated monetized cost.

Equipment	Component	Sub-component	Cause	Downtime Duration	Negative Effect on Production Availability	Cost
Pump #1	Motor	Insulation	Overheating due to deterioration in insulation caused by excessive lead cable lengths	1H: 20M	0.4%	$24,000
Pump #2	Motor	Switch	Product defect	2H: 10M	0.7%	$42,000
Conveyor	Belting	Roller	Contamination in the ball oil	4H: 45M	1.6%	$95,000

Exhibit 4.9
Loss Event Tracking Using External Data

A government agency is tasked with controlling the inflow of illegal drugs and other contraband through its ports. Governments from multiple countries collect and share data, including:

- Port of origin
- Countries traveled through en route
- Ship carried on
- Type of goods carried
- Traditional cargo carried
- Owner of vessel
- Owner of goods
- Receiver of goods
- Value of goods
- Delivery address
- Frequency of trips

The data are measured against predefined threshold triggers in order to more effectively target inspections.

Ongoing Event Identification

The techniques illustrated above typically are applied in particular circumstances, with varying frequency over time. Potential events also are identified on an ongoing basis in connection with routine business activities. Exhibit 4.10 illustrates some of those techniques, which are useful in bringing to light risks and opportunities that may be important to an entity's achieving its objectives. This exhibit demonstrates how one company matches its ongoing event identification mechanisms against external and internal factors that give rise to events, to aid in determining whether there is a need to take further action.

Exhibit 4.10
Illustrative Event Identification Mechanisms

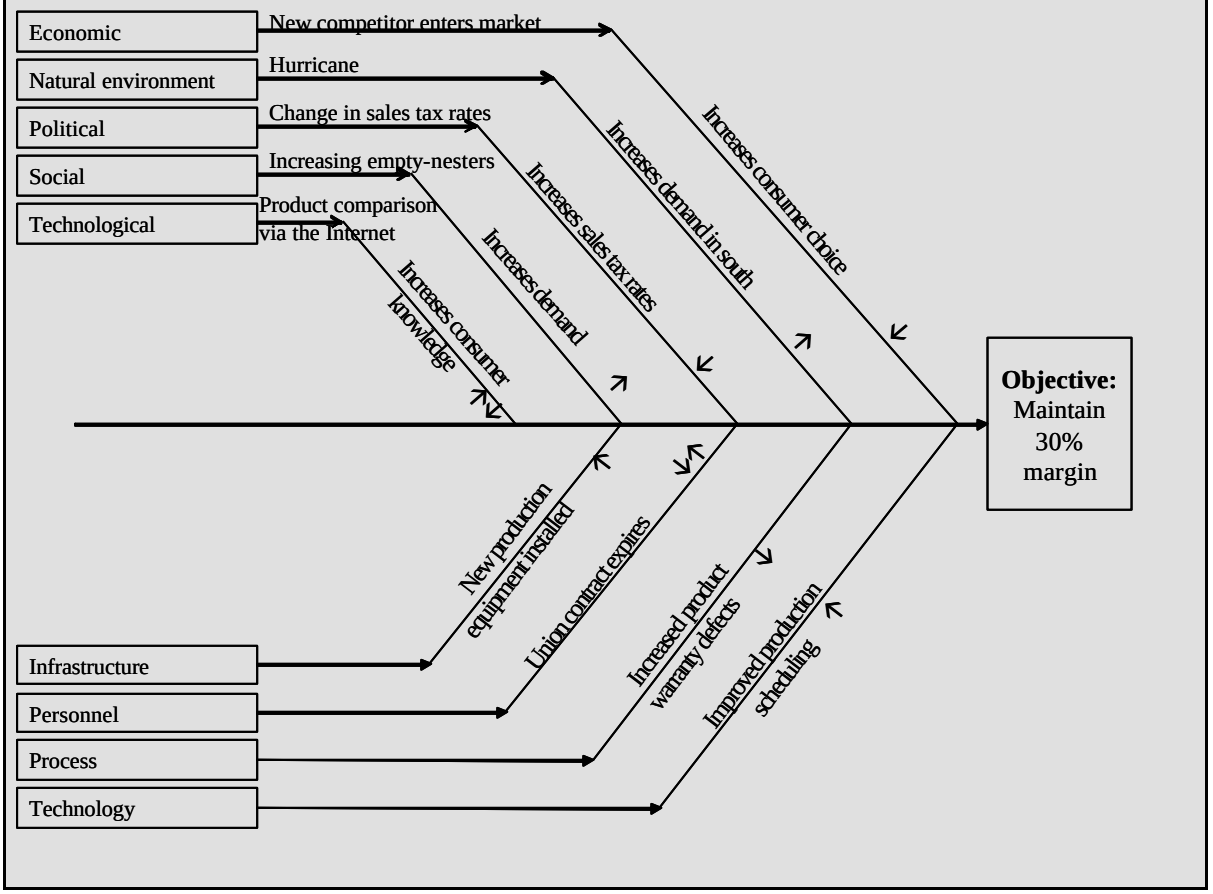
	External Factors					Internal Factors			
Mechanism – Input from	**Economic**	**Natural Environment**	**Political**	**Social**	**Technological**	**Infrastructure**	**Personnel**	**Process**	**Technology**
Industry/technical conferences	✓	✓	✓	✓	✓	✓	✓	✓	✓
Peer company websites and advertising campaigns	✓				✓				
Political lobbyists			✓						
Internal risk management meetings						✓	✓	✓	✓
Benchmarking reports	✓				✓	✓	✓	✓	✓
Competitors' regulatory filings	✓			✓	✓				
Key external indices	✓	✓	✓	✓	✓				
Key internal indices/risk & performance measures/scorecards						✓	✓	✓	✓
New legal decisions	✓		✓	✓					
Media reports	✓	✓	✓	✓	✓				
Monthly management reports						✓	✓	✓	✓
Analyst reports	✓		✓	✓					
Electronic bulletin boards and notification services	✓	✓	✓	✓	✓				
Industry, trade, and professional journals	✓	✓	✓	✓	✓				
Timing of new product launches versus competitors	✓						✓	✓	✓
Profiling calls to customer service	✓				✓			✓	
Real-time feeds of financial market activity	✓								

Interrelationship of Events That May Affect Objectives

In many circumstances multiple events can impact achievement of an objective. To gain an understanding and insight into interrelationships, some companies use event tree diagrams, also known as fishbone diagrams. An event tree diagram provides a means by which to identify and graphically represent uncertainty, generally focusing on one objective and how multiple events affect its achievement. This technique is illustrated in Exhibit 4.11.

Exhibit 4.11
Linking Factors and Potential Events to Objective Unit of Measure

A company that sells mattresses through retail outlets seeks to maintain a 30% margin on sales. It looks to determine which factors and events affect product demand and cost of production – either of which is likely to affect achievement of the 30% margin objective. The objective is shown at the right end of the main "bone." At an angle to this main bone are sub-bones listing events that directly affect the objective. Sub-bone events that positively affect achievement of the objective are depicted by an upward pointing arrow, and those with a negative effect by a downward arrow. The related internal and external factors associated with the sub-bone events are identified at the left.

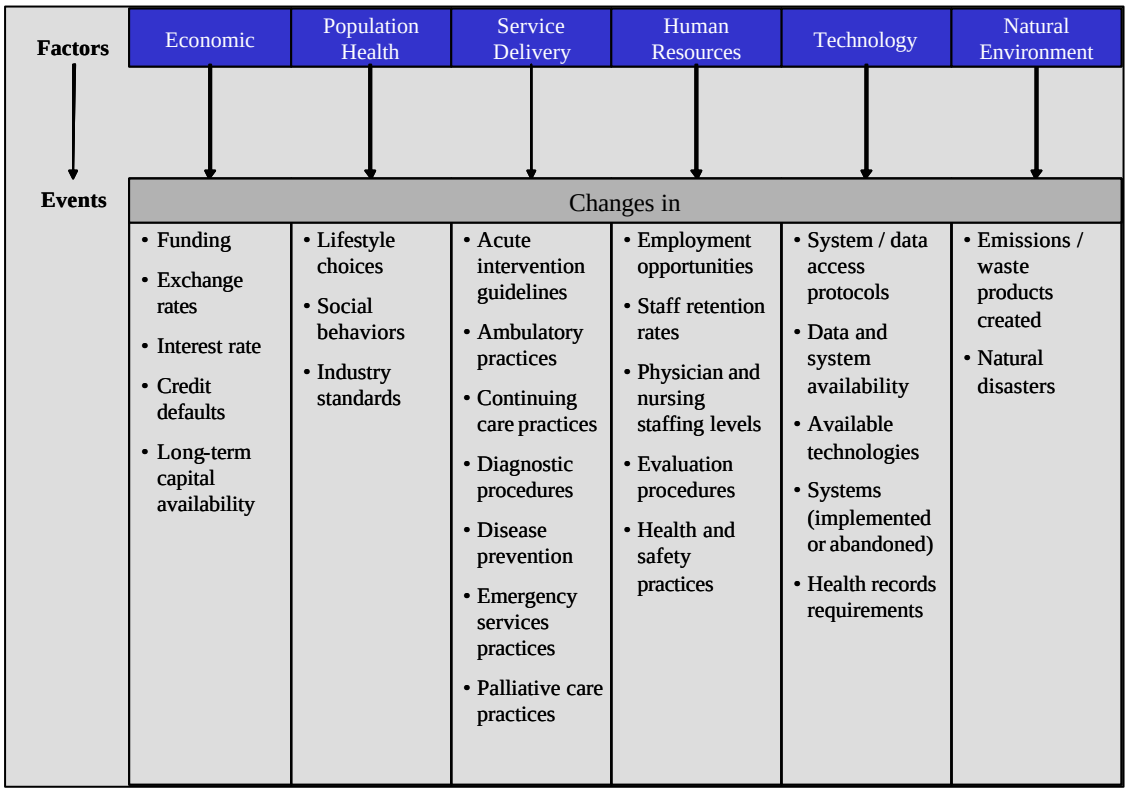


Categorizing Events

By grouping similar potential events, management can better determine opportunities and risks.

Some entities categorize potential events to assist in ensuring event identification efforts are complete. Categorization also can help to subsequently develop a portfolio view of risks. A categorization used by one company, a hospital, is illustrated in Exhibit 4.12.

Exhibit 4.12
Illustrative Event Categorization



5. RISK ASSESSMENT

Framework Chapter Summary: Risk assessment allows an entity to consider the extent to which potential events have an impact on achievement of objectives. Management assesses 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. Risks are assessed on both an inherent and a residual basis.

This chapter illustrates some of the techniques used in risk assessment. Included are illustrations of inherent and residual risk assessments; qualitative techniques including risk ranking and questionnaires; quantitative techniques including such probabilistic techniques as value at risk, market value at risk, loss distributions, and back-testing, and non-probabilistic techniques such as sensitivity analysis, scenario analysis, stress testing, and benchmarking. Also illustrated are techniques for risk and capital attribution used to estimate the amount of capital required for accepted risks; how risks may be portrayed in risk maps, heat maps, or numerical presentations; and techniques for entity-level views of risk.

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.

An example of an inherent risk assessment, linking risks to objectives, is illustrated in Exhibit 5.1 (which builds on Exhibit 4.1).

Exhibit 5.1
Inherent Risk Assessment

Operations objective	Hire 180 new qualified staff across all manufacturing divisions to meet customer demand without overstaffing	
Objective unit of measure	Number of new qualified staff hired	
Tolerance	165–200 new qualified staff, with staff cost between 20% and 23% per dollar order	
Risks	Inherent risk assessment	
	Likelihood	Impact
Insufficient number of qualified candidates available	20%	10% reduction in hiring → 18 unfilled positions
Initial candidate screening filters too stringent	30%	5% reduction in hiring due to poor candidate screenings → 9 unfilled positions

Residual risk is the risk that remains after management's response to the risk.

Residual risk reflects the risk remaining after management's intended actions to mitigate an inherent risk have been effectively implemented. These may include diversification strategies related to customers, products, or other concentrations; policies and procedures providing limits, authorizations, and other protocols; supervisory staff reviewing and acting on performance measures; or automating criteria to standardize and accelerate recurring decisions or transaction approvals. These actions may reduce the likelihood of occurrence of a potential event, the impact of such event, or both.

In the following example, management assesses the inherent risk in changes in foreign currency exchange rates, in terms of the effect on revenue generated by the company's foreign operations. In this case, management considered foreign exchange hedging as a risk response and reassessed the remaining exposure after reflecting the effects of the hedges. The result of the risk assessment is illustrated in Exhibit 5.2.

Exhibit 5.2
Inherent and Residual Risk Assessment

Operations objective	Operating income from foreign operations of $100 million				
Unit of measure	Change in operating income from foreign operations				
Risk	Exchange rate fluctuation adversely affects operating income from foreign operations				
Risk tolerance	Acceptable variation is +/- $10,000,000				
Risk	Inherent risk assessment		Risk response	Residual risk assessment	
	Likelihood	Impact		Likelihood	Impact
Foreign exchange rate moves up 1 percentage point within 90 days	10%	$5,000,000	No response in place	10%	$5,000,000
Foreign exchange rate moves up 1.5 percentage points within 90 days	4%	$10,000,000	Obtain foreign exchange hedge instruments to limit the impact	4%	$5,000,000
Foreign exchange rate moves up 3 percentage points within 90 days	1%	$20,00,000		1%	$8,000,000

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 either sufficient credible data required for quantitative assessments is not practically 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.

Measurement Scales

In estimating likelihood and impact of potential events, whether on an inherent or a residual basis, some form of measurement is applied. For purposes of illustration, there are four general types of measurement, namely, nominal, ordinal, interval, and ratio.

- **Nominal measurement** – This is the simplest form of measurement and involves grouping events by such categories as economic, technology, or natural environment. It does not involve any kind of ranking where one is deemed "more" than another. Numbers assigned in nominal measurement are for identification purposes only – like numbers assigned to baseball players – and items cannot be ordered, ranked, or added.
- **Ordinal measurement** – In this type of measurement events are listed in order of importance, perhaps with such tags as high, medium, or low, or otherwise in rank-order along a scale. Management states that item one is greater than item two. For instance, management may assess the likelihood of a new computer virus disrupting its systems as greater than the likelihood of staff's unauthorized transmittals of confidential information.
- **Interval measurement –** Interval measures use a scale of numerically equal distances. If, for instance, the impact of the loss of production of a key machine is measured as a "three," the impact of a one-hour power outage as a "six," and the effect of 100 vacant positions as a "nine," management can state that the difference in potential impact between losing a machine and the one-hour power outage is the same as the difference between the one-hour power outage and having 100 vacant positions. This does not mean, however, that the impact of the event measured as a "six" is twice as great as the impact of the event measured as a "three."
- **Ratio measurement** – A ratio measurement scale allows one to conclude that if the potential impact of one event is assigned a "three" and another event a "six," the second event has twice the potential impact as the first. This is possible because ratio measurement includes the concept of a true zero, whereas interval measurement does not.

Used here, nominal and ordinal measures are considered "qualitative" techniques, whereas interval and ratio measures are quantitative.

Qualitative Techniques

While some qualitative risk assessments are put forth in subjective terms, and others in more objective ones, the quality of the assessments depends largely on the knowledge and judgment of the individuals involved, their understanding of potential events, and the surrounding context and dynamics.

The following exhibits portray qualitative assessments using ordinal measurement scales. Exhibit 5.3 illustrates a scale of the likelihood of events affecting computer operations. In Exhibit 5.4, rankings are given to the range of potential impacts of the risk of a hazardous materials release.

Exhibit 5.3
Likelihood Risk Ranking Affecting Computer Operations (Next Quarter Timeframe)

Level	Descriptor	Likelihood of Occurrence	Risk
1	Rare	Very low	Technology systems shut down for prolonged periods by terrorist or other intentional action
2	Unlikely	Low	A natural disaster or third party (e.g., utility) event requires invoking the business continuity plan
3	Possible	Moderate	Hackers penetrate our computer security
4	Likely	High	Internal staff use company resources to access inappropriate information from the Internet
5	Almost certain	Very high	Internal staff use company resources for personal messaging

Exhibit 5.4
Impact Risk Ranking of Hazardous Materials Release (One Year Timeframe)

Objective To manage hazardous materials in accordance with state and federal requirements		
Risk		**Units of Measure**
Unplanned release of hazardous material		Production hours lost Containment costs Lost time injuries Compensation and related costs
Level	**Relative Impact**	**Measures**
1	**Insignificant**	• No reportable incidents • Minimal loss of production hours • No injuries
2	**Minor**	• 1–2 reportable incidents • Materials contained on-site by staff • Effect less than 5% of day's production hours • No or minor injuries
3	**Moderate**	• Several reportable incidents • Material contained on-site with outside assistance • Effect between 5% and 20% of day's production hours • Out-patient medical treatment required
4	**Major**	• Major reportable event • Material released into environment, but without real or perceived detrimental effects • Significant loss of production – between 20% and 100% of day's production hours • Limited in-patient care required
5	**Catastrophic**	• Multiple major reportable events or a single catastrophic event • Release into environment with significant detrimental effect, requiring significant third party resources • Substantial loss of production capability – more than two days' production hours • Significant injuries

The questionnaire in Exhibit 5.5 is used by a company in a regulated industry in assessing risks related to implementing new information systems, using categorization and risk ranking of low (green), moderate (yellow), and high (red).

Exhibit 5.5
Risk Assessment for New Systems Implementation

Objective: Implement a new information system to oversee compliance with federal and state legislation			
Risk:	**The project takes longer to complete than expected**		
Category	**Question**	**Response**	
Personnel	What is the experience of personnel on this project?	At least one staff member has successfully implemented such system before	
		At least one staff member has implemented such system before, but with mixed results	
		No team member has done this before, or has with negative results	
Management process	How stable is the management team?	Stable management team with average tenure >2 years	
		Changing management team with average tenure between 1 and 2 years	
		New management team with average tenure < 1 year	
Vendor	How well known is the technology vendor?	Expansion of current services with alliance partner	
		New service with existing vendor	
		New vendor	
Implementation process	How well established is the implementation process?	Proven methodology Existing methodology in place, but used with mixed results	
		New methodology	
Regulatory	How well are regulatory requirements known?	Regulatory requirements are well established	
		Regulatory requirements are unclear or subject to periodic amendment	
		Regulatory requirements are unknown or frequently subject to substantial change	
Continuity plan	How well tested is the continuity plan for this project?	Successfully tested continuity plan for the new application	
		Tested continuity plan for the new application, with significant needed fixes identified	
		No continuity plan in place for the new application	

Quantitative Techniques

Quantitative techniques can be used when enough information exists to estimate risk likelihood or impact using interval or ratio measures. Quantitative methods include probabilistic, non-probabilistic, and benchmarking techniques. An important consideration in quantitative assessment is availability of accurate data, either internally or externally sourced, and one of the challenges in using these techniques is obtaining enough valid data points.

Probabilistic Techniques

Probability-based techniques measure the likelihood and impact of a range of outcomes based on distributional assumptions of the behavior of events. Probabilistic techniques include "at-risk" models (including value at risk, cash flow at risk, and earnings at risk), assessment of loss events, and back-testing.

Value at Risk

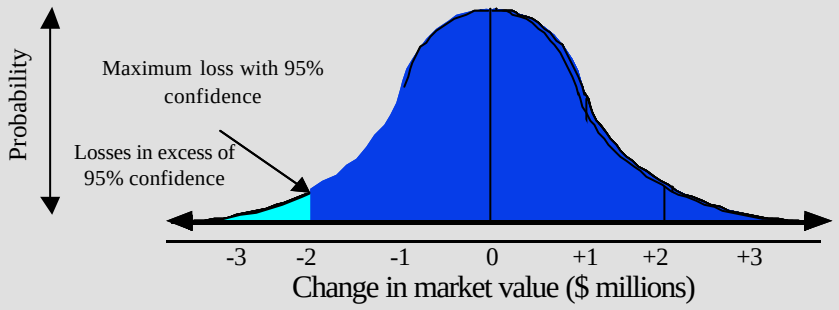
Value-at-risk (VaR) models are based on distributional assumptions about change in the value of an item or group of items, which is not expected to be exceeded with a given confidence level over a defined time period. These models are used to estimate extreme ranges of value change expected to occur infrequently, such as the estimated level of loss that would not be expected to be exceeded with 95% or 99% confidence. Management chooses both the desired confidence and the time horizon over which the risk is assessed, based, in part, on established risk tolerances.

Value-at-risk measures sometimes are used to rationalize capital required for business units by estimating, with high confidence over a specified time horizon, the capital required to cover possible losses. The period for capital measurement is set to coincide with the period of performance assessment.

One application of value at risk is market value at risk, which is used by trading institutions to assess exposures to price changes affecting financial instruments and by some non-trading institutions as well. Market value at risk is defined as the estimated maximum loss on an instrument or portfolio that can be expected over a given time horizon with specified confidence. Exhibit 5.6 provides an example of a market-value-at-risk measure.

Exhibit 5.6
Market-Value-at-Risk Analysis

A financial services company assesses the risk of change in the value of its trading portfolio. It estimates the maximum loss during any one day with 95% confidence, assuming portfolio value changes are represented by a normal distribution, which takes into account all possible scenarios. Value at risk is depicted as follows:



The light blue area represents an estimate of losses that exceed the maximum loss estimated over one day with 95% confidence.

Cash Flow at Risk

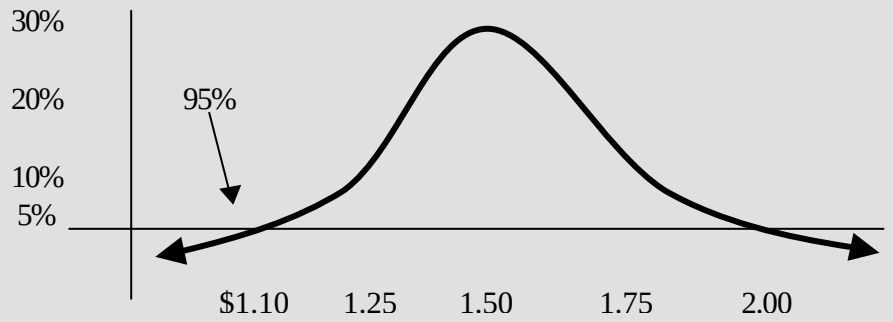
This measure is similar to value at risk, except that it estimates a change in the cash flows of an organization or business unit relative to a targeted cash flow expectation with a given confidence over a defined time horizon. This is based on distributional assumptions about the behavior of changes in cash flows. Cash flow at risk is used for businesses whose results are sensitive to changes in cash flows related to non-market-price factors. For example, a computer manufacturer desiring to measure risk to its net cash flows may use a cash-flow-at-risk technique that includes either one variable such as a foreign currency rate, or multiple variables such as changes in gross domestic product, supply and demand for computer components, and corporate research and development budgets. These measures would allow the company to assess its foreign currency risk in relation to cash flows, or its broader cash flow performance.

Earnings at Risk

Similar to cash flow at risk, earnings at risk estimates a change in the accounting earnings of an organization or business unit, the amount of which is not expected to be exceeded with given confidence over a defined time period, based on distributional assumptions about the behavior of accounting earnings. Exhibit 5.7 provides an example of an earnings-at-risk analysis.

Exhibit 5.7
Earnings-at-Risk Analysis

Management of a pharmaceutical company determines the company's earnings at risk by performing a Monte Carlo simulation on the revenue from sales of prescription drugs, research spending, and other income/expenses. In this example, management is 95% sure that earnings will be at least $1.10 per share.



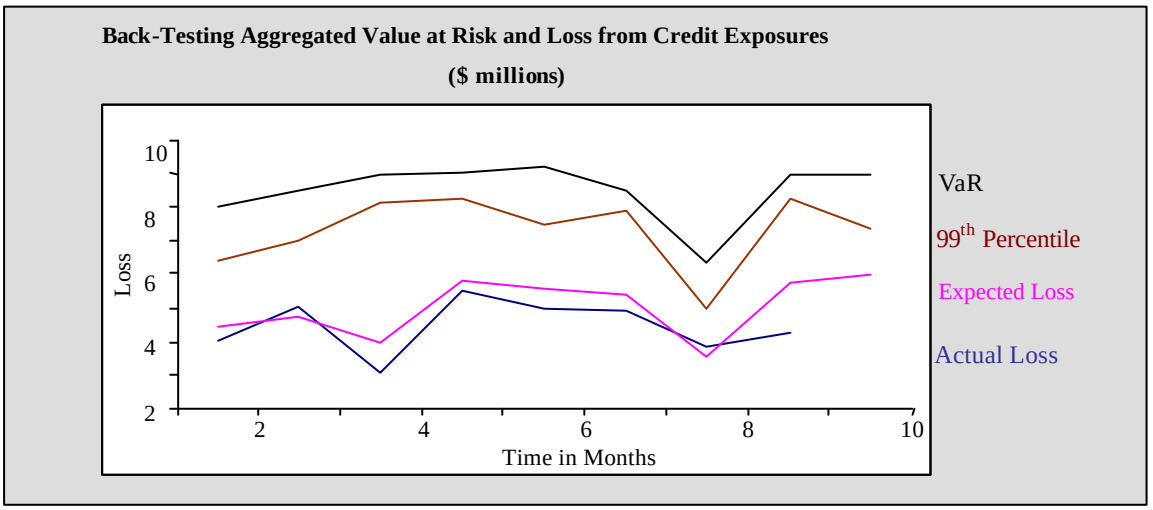
Loss Distributions

Certain operational or credit loss distribution estimations use statistical techniques, generally based on non-normal distributions, to calculate maximum losses resulting from operational risks with a given confidence level. These analyses require collection of operational loss data categorized by root cause of the loss, such as criminal activity, human resources, sales practices, unauthorized activity, management process, and technology. Using these loss data and reflecting data on related insurance costs and proceeds, a preliminary loss distribution is developed and then refined to take into account the organization's risk responses.

Back-Testing

In this context, back-testing typically consists of periodic comparison of an entity's at-risk measures with subsequent profit or loss. Back-testing commonly is used by financial institutions. Some organizations, including many banks, routinely compare daily profits and losses with their risk model-generated outputs to gauge the quality and accuracy of their risk assessment systems, as illustrated in Exhibit 5.8.

Exhibit 5.8
Back-Testing Analysis



Non-Probabilistic Techniques

Non-probabilistic techniques are used to quantify the impact of a potential event, based on distributional assumptions, but without assigning likelihood of event occurrence. Thus, these techniques require that management determine likelihood separately. Commonly used non-probabilistic techniques are sensitivity analysis, scenario analysis, and stress testing.

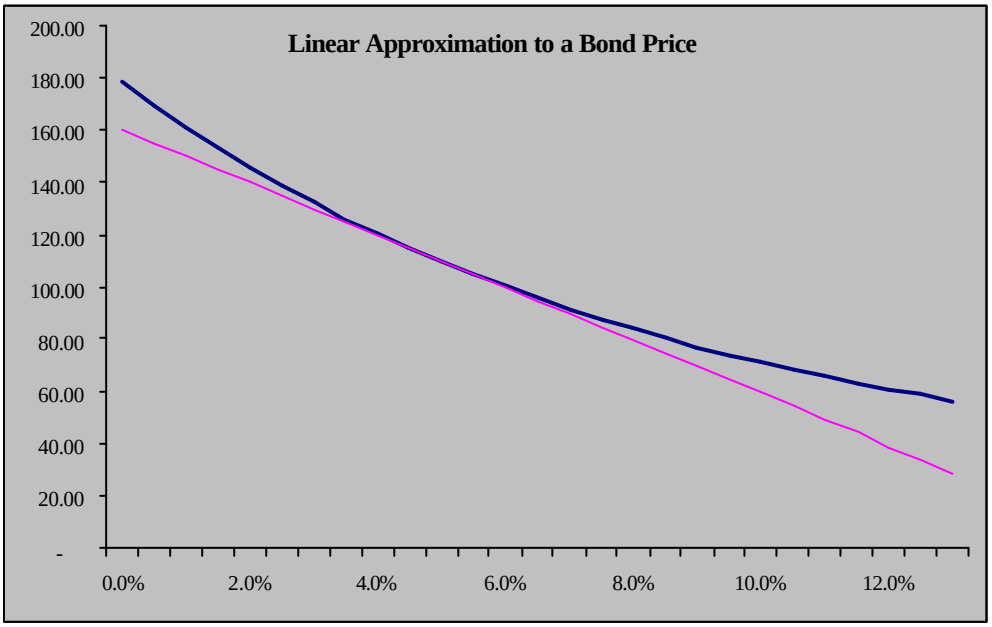
Sensitivity Analysis

Sensitivity analysis is used to assess the impact of normal, or routine, changes in potential events. Due to relative ease of calculation, sensitivity measures sometimes are used to complement a probabilistic approach. Sensitivity analysis is used with:

- Operational measures, such as the effect of changes in sales volume on call center response time or number of manufacturing defects.
- Equity securities, using beta. For equities, beta represents the ratio of the movements of an individual stock relative to the movements of an overall market portfolio or a proxy such as the S&P 500 index.

Exhibit 5.9 illustrates use of a linear approximation to estimate changes in the value of a fixed income security. This approximation (represented by the lighter line in the illustration) is constructed by using a fixed income sensitivity measure, which measures the change in value for a small change in interest rate (between 4½% and 5½% in the illustration), and uses that measure to approximate change in value for large changes (outside the 4½% to 5½% range). The difference between the actual value (represented by the heavier line) and approximated value is due to convexity.

Exhibit 5.9
Sensitivity Analysis of Fixed Income Instruments



Scenario Analysis

Scenario analysis assesses the effect on an objective of one or more events. Scenario analysis may be used in connection with business continuity planning or estimating the impact of a system failure or network failure, and reflects the effects across the business. Scenario analysis may be performed in strategic planning as management seeks to link growth, risk, and return, as shown in Exhibit 5.10, where risks are assessed in terms of shareholder value added.

Exhibit 5.10
Analysis of Various Scenarios Across Multiple Business Units on Total Shareholder Value Added

Impact of Key Potential Business Scenarios on Shareholder Value Added by Business Unit ($ Millions)		
Unit	Potential Business Scenario	Increase (Decrease) in SVA
1	• Risk rating deteriorates by 20%	$ (150)
	• Consumer loans decrease by 10%	(120)
	• Increased competition – one new market entrant	(100)
	• Revenue in the banking group decreases by 15%	(80)
	• Loss of a top-tier customer	(50)
	• …	…
2	• Increased competition – one new market entrant	$ (50)
	• Revenue declines by 10% due to customer service	(30)
	• Loss of a top-tier customer	(20)
	• Unsuccessful new product launch	(20)
	• One new pending "large" (but not "mega") lawsuit	(20)
	• …	…
3	• Increased competition – one new market entrant	$ (40)
	• Loss of a top-tier customer	(30)
	• Reduction of asset base by 10%	(20)
	• …	…

Stress Testing

Stress testing assesses the impact of events having extreme impact. Stress testing differs from scenario analysis in that it focuses on the direct impact of a change in only one event or activity under extreme circumstances, as opposed to focusing on changes on a more normal scale as in scenario analysis. Stress testing generally is used as a complement to probabilistic measures to examine the results of low likelihood, high impact events that might not be captured adequately by distributional assumptions used with probabilistic techniques. Similar to sensitivity analysis, stress testing often is used to assess the impact of changes in operational events or financial market movements in order to avoid big surprises and losses. Stress tests include, for example, estimation of the effect of a rapid and large:

- Increase in product manufacturing defects
- Movement in a foreign exchange rate
- Movement in price of an underlying factor on which a derivative instrument is based
- Increase in interest rates on the value of a fixed income investment portfolio
- Increase in energy prices affecting the cost to run a manufacturing plant

Benchmarking

Some companies use benchmarking techniques to assess a specific risk in terms of likelihood and impact, where management seeks to enhance its risk response decisions to reduce either likelihood or impact. Benchmark data can provide management insight into the likelihood or impact of risks based on experiences of other organizations. Benchmarking also is used with respect to activities in a business process to identify opportunities for process improvement.

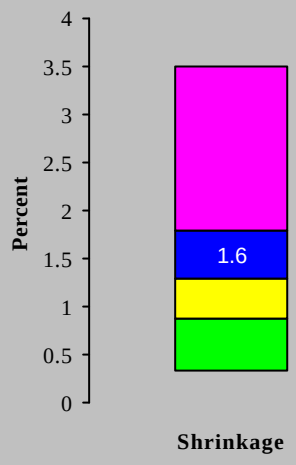
Benchmarks include:

- **Internal** – Compare measures of one department or division with others of the same entity
- **Competitive/industry** – Compare measures among direct competitors or broader groups of companies with similar characteristics
- **Best-in-class –** Look at like measures among companies across industries

An example of a competitive/industry benchmark is presented in Exhibit 5.11, which depicts the effect of events related to shrinkage within a peer group.

Exhibit 5.11
Comparison of Inventory Losses

Benchmarking of Shrink Percentage Among Peer Retail Operations



Definition: Losses in physical inventory from events such as shoplifting or other forms of theft. Shrink percentage is defined as the value of lost physical inventory divided by net sales.

Analyzing performance: Best practice companies reduce shrinkage by selecting risk responses and designing control activities that reduce the likelihood and impact of inventory loss.

Quartile 4:	1.80%–3.50%
Quartile 3:	1.30%–1.80%
Quartile 2:	0.88%–1.30%
Quartile 1:	0.33%–0.88%

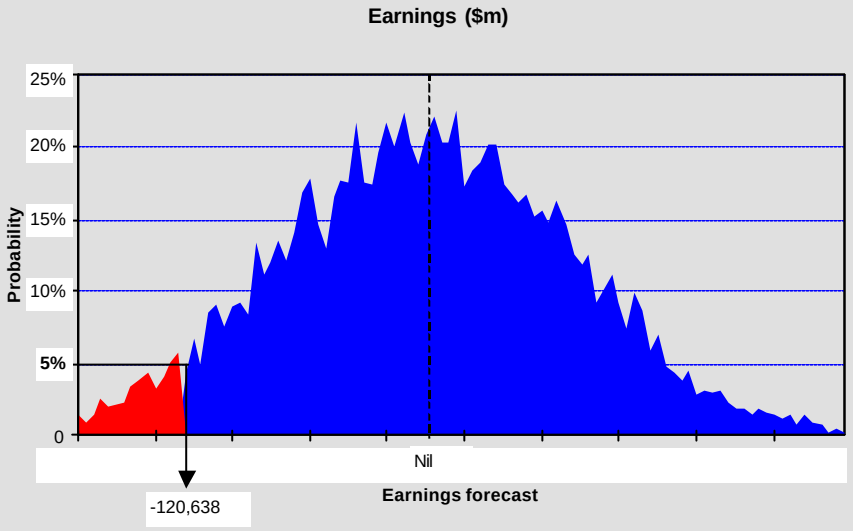
Your Company	Benchmark Group		
	Low	Median	High
1.6%	0.33%	1.30%	3.50%

Risk and Capital Attribution

Some organizations, particularly financial institutions, estimate economic capital. Some companies use this term to refer to the amount of capital required to cover financial exposures. Others use it somewhat differently, as a measure of capital needed to run the business as planned. It is used by management in strategy setting, resource allocation, and performance measurement. An illustration is shown in Exhibit 5.12.

Exhibit 5.12
Using Economic Capital

A bank uses "economic capital" to estimate the amount of equity required. It represents the level of equity capital required within a given time period, at a given confidence level. For example, the bank adopts a 95% confidence level and two-year time period to determine its economic capital requirements. After modeling its expected earnings distribution taking into account market, credit, operational, and fixed asset risk, management identifies its economic capital requirement as $120,638,000, as follows:



Recognizing the lack of precision in operational risk measurement methodology, and recognizing exposure beyond the 95% confidence level, the bank's policy is to create an additional "capital cushion" on top of its economic capital requirement to provide additional confidence that the calculated economic capital balance is sufficient.

The bank also uses the relationship of economic capital to book capital as a guidepost in strategic direction. When book capital minus the capital cushion is less than required economic capital, management looks to whether it should:

- Scale back certain business activities
- Raise additional equity
- Lower its risk positions in its lending, investing, or operational activities

When book capital minus the capital cushion is greater than required economic capital, management considers opportunities to:

- Expand its business into new products or markets
- Take higher-risk positions in its lending, investing, or operational activities
- Return capital to shareholders

Portraying Risk Assessments

Organizations use any of a number of different methods to portray risk assessments. Portraying risks in a clear and concise manner is especially important with qualitative assessment because risks are not summarized in one number or range of numbers as with quantitative techniques. Techniques include risk maps and numerical representations.

Risk Maps

A risk map is a graphic representation of likelihood and impact of one or more risks. Risk maps may take the form of heat maps or process charts that plot quantitative or qualitative estimates of risk likelihood and impact. Risks are depicted in a way that highlights which risks are more significant (higher likelihood and/or impact) and which are less significant (lower likelihood and/or impact). Depending on the level of detail and depth of analysis, risk maps either can present the overall expected likelihood and/or impact or can incorporate an element of variability of likelihood and/or impact. The following examples of risk maps depict assessment of risks relating to the objective of retaining high-performing employees.

Exhibit 5.13 illustrates a heat map, presenting risk levels (likelihood and impact) by color, where red represents high risk, yellow moderate risk, and green low risk.

Exhibit 5.13
Heat Map

A company assesses risks to its objective of maintaining a quality workforce. Likelihood is considered in terms of percentage turnover within a specified period and impact in terms of cost of operational inefficiency and cost to replace, retrain, and develop employees. Color coding highlights those risks that are most likely to occur and most likely to have a significant effect on objectives.

	Topic	Risk Description	Likelihood	Impact
A	Compensation	Employee dissatisfaction with compensation leads to higher staff turnover.	Possible	Moderate
B	Recognition	Employees feel unrecognized, resulting in reduced focus on tasks and higher error rates.	Unlikely	Minor
C	Downsizing	Employees are over-utilized and work considerable overtime. Staff leave to pursue work in other organizations that offer a better work/life balance.	Likely	Moderate
D	Demographics	Changing demographic composition of the employee group causes increased turnover.	Almost Certain	Moderate
E	Employment market	Increased demand for company employees by recruiting firms.	Unlikely	Moderate

	Topic	Risk Description	Likelihood	Impact
F	Performance evaluation	Employee dissatisfaction with performance appraisal measures and processes causes low morale, staff to focus on non-critical objectives, and loss of staff to companies perceived to be employers of choice	Possible	Moderate
G	Communication	Ineffective communication between employees and management results in mixed messages being heard and in the pursuit of alternative employment.	Possible	Moderate
H	Workplace safety	Unsafe workplace causes employee injury and resignations by injured staff and by others concerned over safety issues.	Unlikely	Major
I	Career development	Employees perceive limited control over their career development, causing higher turnover.	Possible	Moderate
J	Work diversity	Employee dissatisfaction with job variety results in rote performance, higher errors in key processes, and pursuit of more interesting job opportunities outside the company.	Possible	Moderate

These same risks can be depicted in a matrix risk map with likelihood on the horizontal axis and impact on the vertical, as illustrated in Exhibit 5.14. Because this provides more information, management can more readily prioritize where attention is needed.

Exhibit 5.14
Risk Map of Mean Values for Likelihood and Impact

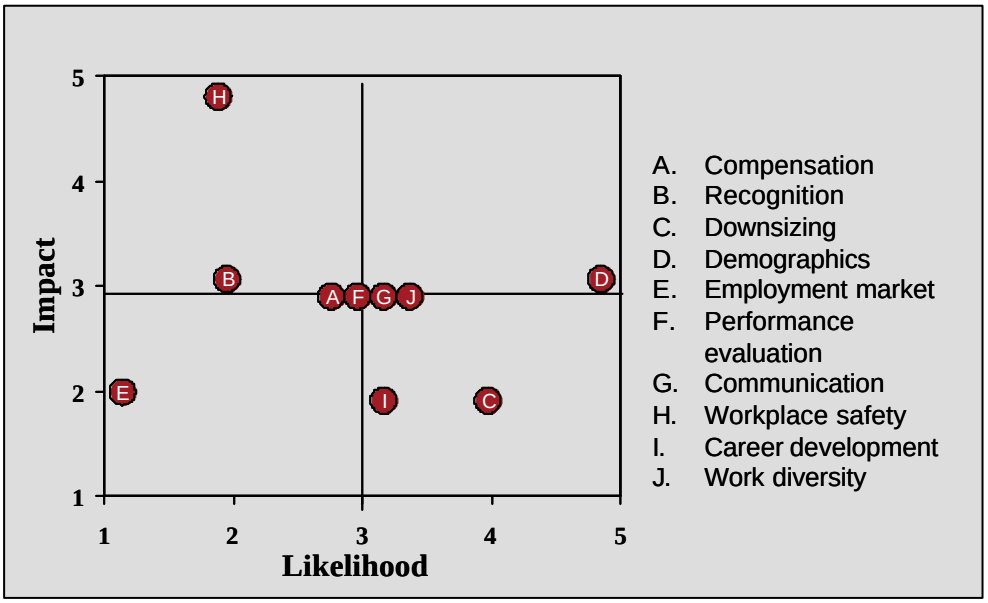
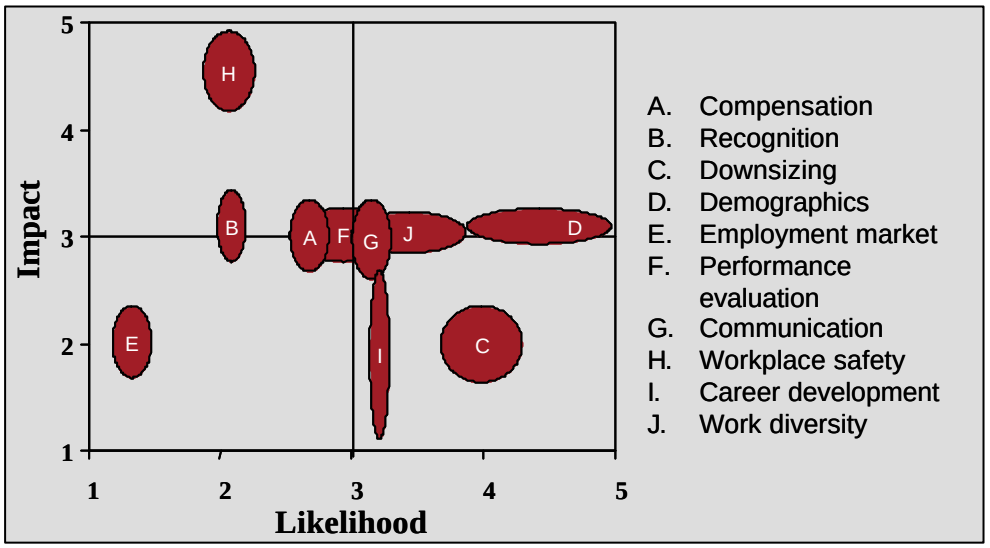


Exhibit 5.15 provides the same basic information, but in still further depth. It presents information on variability around risk likelihood and impact, providing management with an additional perspective on the risks.

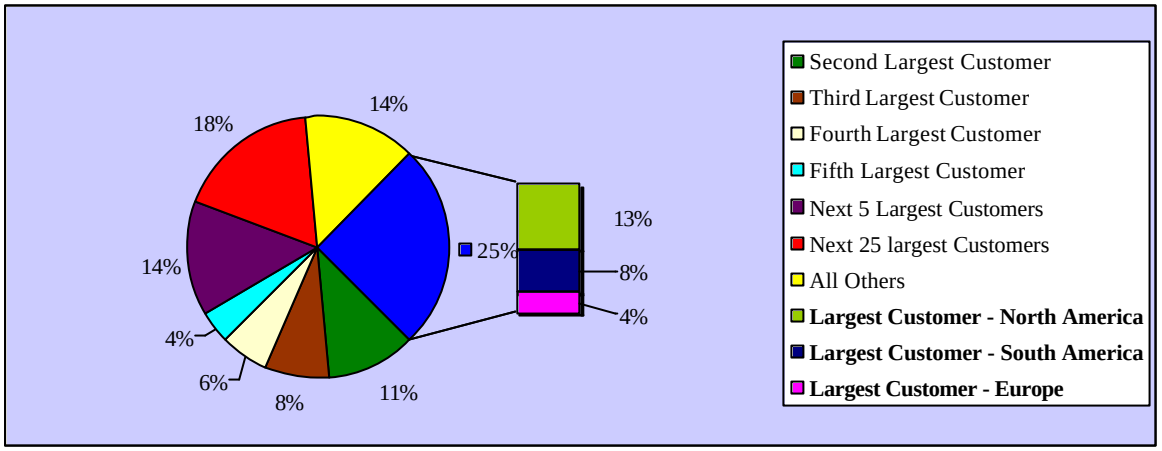
Exhibit 5.15
Risk Map Showing Variability for Likelihood and Impact



Numerical Representations

Depending on the business context, quantitative measures of risk can be presented in monetary or percentage terms, and can be presented with a specified confidence interval, for example, 95% or 99% confidence. One example of a numerical representation is shown in Exhibit 5.6, with a value-at-risk measure. Another is shown in Exhibit 5.10, with a shareholder-value-added measure using scenario analysis. Another example is shown in Exhibit 5.16, illustrating risks related to customer concentrations. In this exhibit, the largest customer is segmented by geographical region, providing information on regional exposure.

Exhibit 5.16
Revenue Analysis by Customer

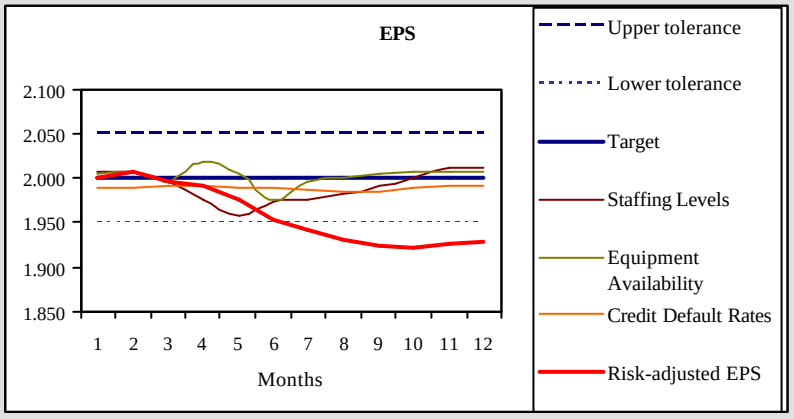


Entity-Level Views

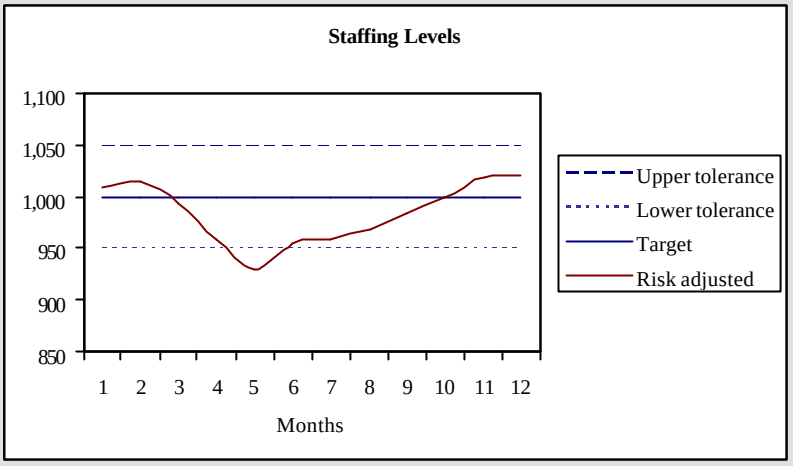
As part of risk assessment, management may leverage business unit risk assessments or conduct a separate assessment using techniques illustrated earlier to form an entity-level risk profile. Overall risk assessments may take the form of an aggregate risk measure where underlying risk measures are of like types and where correlations between risks are considered. Another aggregation approach is to translate related but unlike risk measures to a common unit of measure, as shown in Exhibit 5.17.

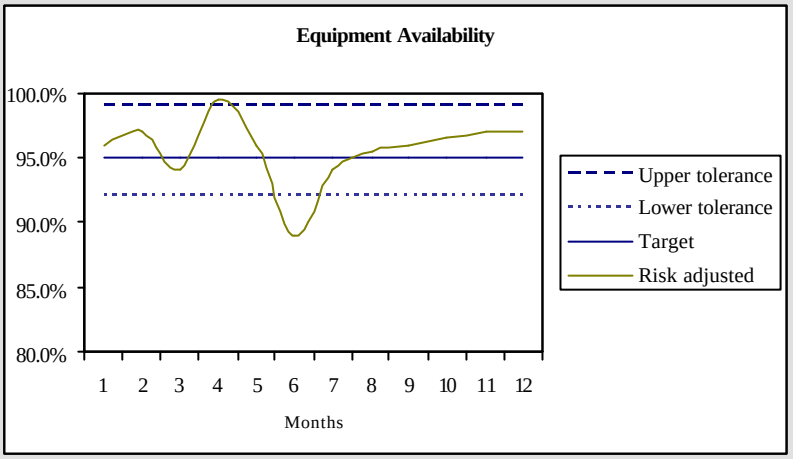
Exhibit 5.17
Analysis of the Effect of Multiple Business Unit Measures on a Single Entity-Level Measure (EPS)

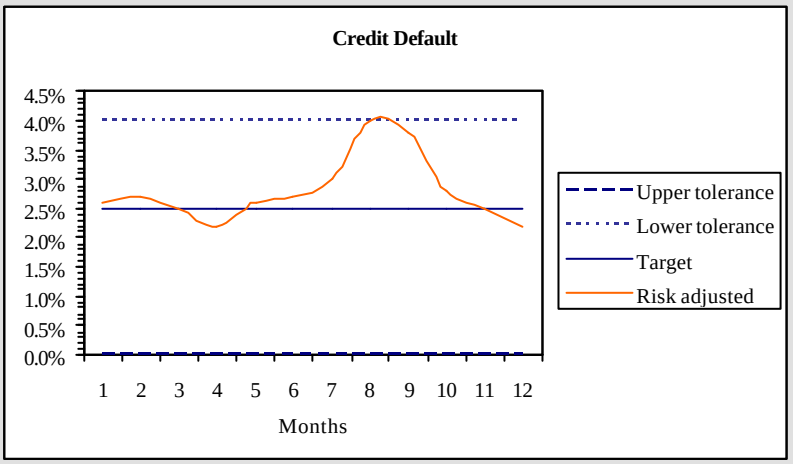
This company assesses the risk impact within its respective departments using the units of measure established for the department: equipment availability, customer payment default, and staffing levels. These are portrayed in the following diagrams. At the entity level, management assesses risk in terms of entity earnings per share (EPS) as shown in the



first diagram, where the effect of each business unit measure is converted to the entity-level measure based on the budgeted contribution or loss from each activity. The dashed lines in the first diagram represent the upper and lower EPS risk tolerances.







When direct aggregation of risk measures is not possible, some managements find it useful to compile measures in a summary report in order to facilitate drawing conclusions and making decisions. In these cases, even though measures are not directly aggregated, management subjectively places the risks on the same qualitative or quantitative scale to assess likelihood and impact of multiple risks to a single objective, or the effect of one risk on multiple objectives.

For example, management of one company estimates the impact on EPS of several different events, as illustrated in Exhibit 5.18. In this exhibit the effects on business units of a 100 basis point decrease in foreign exchange rate naturally offset at the entity level, so that any actions taken by one or more of the business units to manage foreign exchange exposures could adversely affect the entity as a whole. A 100 basis point increase in interest rate would only partially offset on an entity-wide basis, and management might respond to this risk either within one or more of the business units or at the entity level. Similarly, for the risks related to movements in the price of raw material and pending union negotiations, management would decide where and how to respond, to keep within entity-level risk tolerances.

Exhibit 5.18
Analysis of the Effect of Multiple Risks Across Business Units (Dollar Amounts in Thousands Except EPS)

Objective: To achieve consistent earnings growth						
Risk		**Corp**	**Div 1**	**Div 2**	**Div 3**	**Entity**
		Business Unit Contribution	Business Unit Contribution	Business Unit Contribution	Business Unit Contribution	Earnings per Share
Decrease in local currency in relation to U.S. dollar by 100 basis points	Impact	$(1,000)	$600	$300	$100	$ 0.00
	Likelihood	20%				
Increase in interest rate by 100 basis points	Impact	$ (750)	$1,600	$800	$100	$ (0.035)
	Likelihood	20%				
Increase in raw materials price of 10%	Impact	-	$10,000	$5,000	$5,000	$ (0.40)
	Likelihood	-	20%	30%	15%	
Pending union negotiations halt production for > 10 days	Impact	-	$5,000	$0	$1,000	$ (0.12)
	Likelihood	-	10%	0%	25%	

Management of another company assesses the effect of a single event on multiple objectives, illustrated in Exhibit 5.19. Using one of the risks addressed in Exhibit 5.18 – union negotiations halting production for more than 10 days – management assesses its effect on multiple objectives.

Exhibit 5.19
Analysis of the Effect of a Single Risk Across Business Units

Risk: Pending union negotiations halt production for > 10 days					
		Div 1	**Div 2**	**Div 3**	**Entity**
Objective	Likelihood	10%	0%	25%	
Maintain a return on equity of 15%	Unit of Measure	Production Hrs	Production Hrs	Production Hrs	Earnings per Share
	Impact	-50,000	0	-10,000	$ -.80
Increase our market share in Europe	Unit of Measure	-	BU Contribution	-	Earnings per Share
	Impact	-	-500	-	-.45
Increase annual sales per sales representative	Unit of Measure	Units Sold	Units Sold	Units Sold	Earnings per Share
	Impact	-50,000	0	-10,000	-.30
Increase employee productivity	Unit of Measure	Production Units	Production Units	Production Units	Earnings per Share
	Impact	-25,000	0	-5,000	-.05

6. RISK RESPONSE

Framework 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 assesses the effect on risk likelihood and impact, as well as costs and benefits, selecting a response that brings residual risk within desired risk tolerances. Management identifies any opportunities that might be available, and takes an entity-wide, or portfolio, view of risk, determining whether overall residual risk is within the entity's risk appetite.

This chapter illustrates some of the techniques used in risk response. Included are illustrations of techniques used in evaluating risk response alternatives in relation to risk tolerance, evaluating costs and benefits of alternative responses, and considering the portfolio view.

Risk Responses: Avoid, Reduce, Share, Accept

For significant risks, an entity typically considers potential responses from a range of response options.

Examples of risk responses for avoidance, sharing, reduction, and acceptance are presented in Exhibit 6.1.

Exhibit 6.1
Illustrative Risk Responses by Response Type

Avoidance	Sharing
• Disposing of a business unit, product line, geographical segment • Deciding not to engage in new initiatives/activities that would give rise to the risks	• Insuring significant unexpected loss • Entering into joint venture/partnership • Entering into syndication agreements • Hedging risks through capital market instruments • Outsourcing business processes • Sharing risk through contractual agreements with customers, vendors, or other business partners
Reduction	**Acceptance**
• Diversifying product offerings • Establishing operational limits • Establishing effective business processes • Enhancing management involvement in decision making, monitoring • Rebalancing portfolio of assets to reduce exposure to certain types of losses • Reallocating capital among operating units	• "Self-insuring" against loss • Relying on natural offsets within a portfolio • Accepting risk as already conforming to risk tolerances

At the completion of its risk response actions, management may have a view of individual risks and responses and their alignment with associated tolerances, as illustrated in Exhibit 6.2 (which builds on Exhibit 5.1).

Exhibit 6.2
Linking Objectives, Events, Risk Assessment, and Risk Response

Operations objective	• Hire 180 new qualified staff across all manufacturing divisions to meet customer demand without overstaffing • Maintain 22% staff cost per dollar order				
Objective unit of measure	Number of new qualified staff hired				
Tolerance	165–200 new qualified staff, with staff cost between 20% and 23% per dollar order				
Risks	**Inherent risk assessment**		**Risk response**	**Residual risk assessment**	
	Likelihood	**Impact**		**Likelihood**	**Impact**
Decreasing number of qualified candidates available	20%	10% reduction in hiring → 18 unfilled positions	Contract in place with a third party hiring agency to source candidates	10%	10% reduction in hiring → 18 unfilled positions
Unacceptable variability in our hiring process	30%	5% reduction in hiring due to poor candidate screenings → 9 unfilled positions	Review of hiring process conducted every two years	20%	2% reduction in hiring due to poor candidate screenings → 4 unfilled positions
Alignment with risk tolerance	Response expected to bring company within risk tolerance				

Considering Risk Responses

As with assessing inherent risk, residual risk may be assessed qualitatively or quantitatively. Generally, the same measures used in assessing inherent risk are used in assessing residual risk. The approach taken by one company is illustrated in Exhibit 6.3.

Exhibit 6.3
Effect of Risk Response on Residual Risk

Strategic objective	Expand product offerings related to health-based cat foods				
Operations objective	Generate $30 million in "year-one" revenue by introducing one new "healthy-cat" product				
Unit of measure	Revenue from new products				
Risk tolerance	$25–35 million in new revenue				
Risks	Inherent Risk		Risk Response Alternatives	Residual Risk	
	Likelihood	Impact on Revenue from New Product		Likelihood	Impact
Competitor reaches market first	40%	($10,000,000)	**A** – Provide additional funding to the R&D and Production divisions to reach market within the next 90 days	20%	15% less revenue from new products ($4,500,000)
			B – Take no specific action to be first to market	40%	($10,000,000)
Market acceptance of this new product is slower than market research suggests	25%	($15,000,000)	**C** – Co-brand product with an established third party	20%	10% less revenue from new product ($3,000,000)
			D – Pilot in test market; modify marketing approach accordingly	15%	15% less revenue from new product ($4,500,000)
			E– Take no action to ensure market acceptance	25%	($15,000,000)

For some risks, management may rely on multiple techniques to reduce the overall residual risk in order to meet its risk tolerance. Exhibit 6.4 illustrates how a company uses multiple risk response techniques to reduce the risk of non-compliance with local environmental laws and regulations. In this example, management has not evaluated the effect of each risk response selected but has evaluated them together to establish residual risk.

Exhibit 6.4
Multiple Risk Responses

Compliance objective	Pesticides are used at the company premises in accordance with all relevant environmental laws and regulations				
Unit of measure	Rate of compliance				
Target	100% compliance				
Risk tolerance	98%–100%				
Risks	Inherent Risk		Selected Risk Response	Residual Risk	
	Likelihood	Impact		Likelihood	Impact
Pesticides are sprayed in prohibited areas	Moderate	Fines, sanctions, reputational damage	Distribution of all pesticides for use on company grounds is coordinated through the Facilities Department	Low	Fines, sanctions, reputational damage
			A web-based notification form is completed by all grounds persons setting out key details 72 hours before pesticides are applied		
			All prohibited areas are clearly marked		

Costs versus Benefits

Virtually every risk response will incur some direct or indirect cost that is weighed against the benefits it creates. The initial cost to design and implement a response (processes, people, and technology) is considered, as is the cost to maintain the response on an ongoing basis. The costs, and associated benefits, can be measured quantitatively or qualitatively, with the unit of measure typically consistent with that used in establishing the related objective and risk tolerance. A cost–benefit analysis is illustrated in Exhibit 6.5.

Exhibit 6.5
Evaluating the Costs and Benefits of Alternative Risk Responses

A supplier to the automotive industry manufactures aluminum suspension modules. The supplier is in a "tandem" relationship with an original equipment manufacturer (OEM), where the vast majority of revenue is generated with the OEM. This OEM traditionally revises its forecasted demand by an average of 20%, always late in the cycle, creating a high degree of uncertainty for the supplier's production and scheduling activities. If the OEM were not to significantly revise demand late in the cycle, the supplier would be able to increase plant utilization by increasing its manufacturing of products for other customers, thereby increasing profitability. The supplier seeks to optimize scheduling and capacity planning for plant utilization to achieve 95% average monthly utilization. Management assessed the most significant risk to this objective – that is, the high level of uncertainty regarding actual demand from the OEM – and assessed costs and benefits of the following risk responses:

A **Accept** – Absorb the cost of having to respond to late changes in OEM demand, and consider the extent to which it can produce and sell product to other customers within the constraints of the OEM relationship

B **Avoid** – Exit the relationship with the OEM, and establish relationships with new customers offering more stable demand

C **Share** – Negotiate a revision to the current contract, stipulating a "take or pay" clause to ensure a certain rate of return

D **Reduce** – Install a more sophisticated forecasting system, which analyzes external factors (e.g., public information on consumer budgets, OEM and dealership inventories) and internal factors (historical orders from various sources) to better project actual demand from all customers

The following table compares the costs and benefits of these responses. Costs relate predominantly to supply chain management, marketing, information technology, and legal functions. Benefits are expressed using the unit of measure for the objective – plant utilization – and the resulting effect on targeted earnings before interest and taxes (EBIT).

Response		Cost	Description	Benefits
A	Accept	$750,000	Marketing/sales efforts required to generate additional customers, and additional transportation costs, $750,000	Management predicts it can sell an additional 2% to other customers, bringing utilization up to 82% Effect on EBIT: increase of $1,250,000
B	Avoid	$1,500,000	Unit price drops 2% due to smaller customers paying less than premium price	Marketing efforts allow utilization of 97% Effect on EBIT: increase of $1,560,000
			$750,000 in increased salary costs for personnel required to identify, win, and sustain new customers	
			$250,000 in increased outbound logistics costs due to larger number of suppliers	
			$500,000 in legal fees to negotiate and finalize new agreements	

Response		Cost	Description	Benefits
C	Share	$350,000	Unit price drops 5% due to increased pressure from OEM in response to "take or pay" nature of relationship	New contract allows utilization of 99% Effect on EBIT: increase of $100,000
			$250,000 in legal fees to negotiate and revise contract agreement	
			$100,000 to improve data sharing, forecasting, and planning	
D	Reduce	$1,050,000	Average unit price drops 1% due to smaller customers not paying premium price	Improved forecasting provides sufficient time to win alternative customers for a utilization of 98% Effect on EBIT: increase of $3,170,000
			$500,000 for purchasing new software	
			$50,000 for new software training	
			$500,000 for increased forecasting and analysis	
With this analysis, and considering the likelihood of each alternative and sustainability of results, management decided on response D.				

Portfolio View of Residual Risk

With a view of risk for individual units, an enterprise's senior management is well positioned to take a portfolio view, to determine whether the entity's residual risk profile is commensurate with its overall risk appetite relative to its objectives.

A portfolio view of risk can be depicted in any of a number of ways. Exhibit 6.6 illustrates how a company assesses risks from across the organization. The likelihood of events is presented in the context of frequency of occurrence, and the potential impact using a single entity unit of measure – operating earnings.

Exhibit 6.6
Portfolio View of Residual Risk

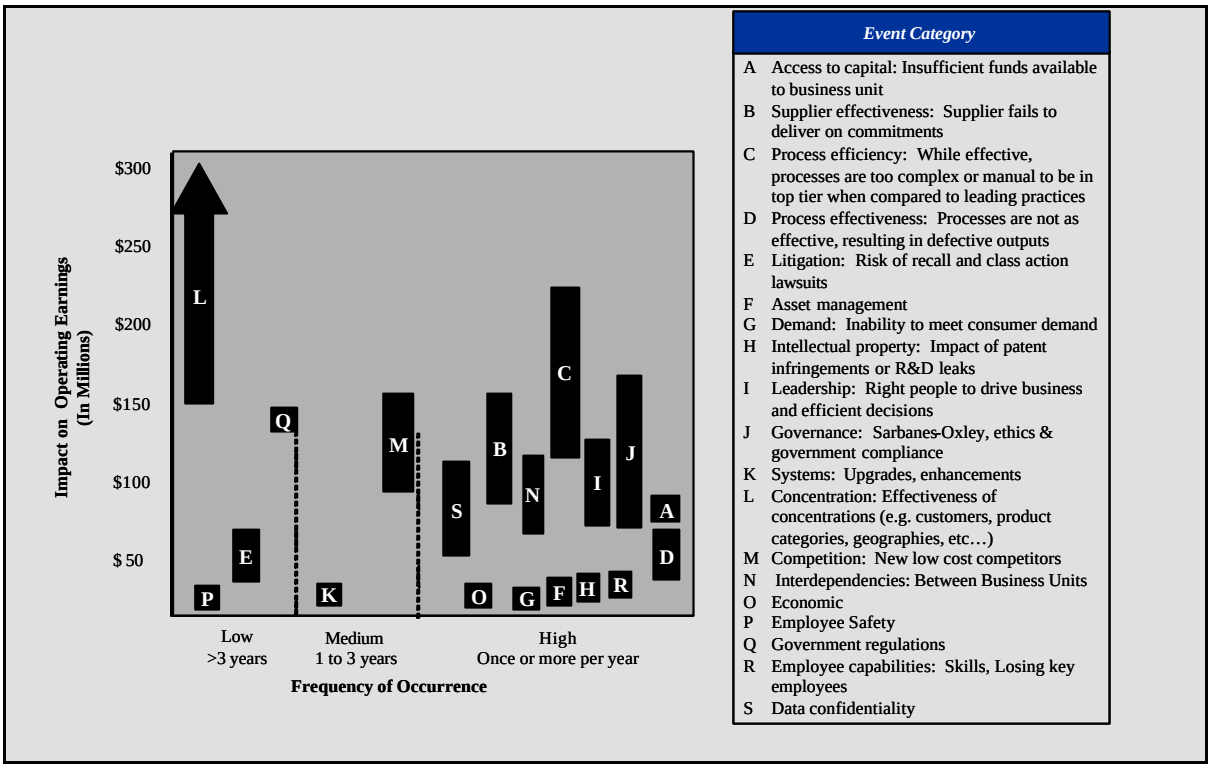


Exhibit 6.7 illustrates how managers of a company's business units establish objectives, risk tolerances, and performance measures relevant to their operations in terms of business unit contribution. The business units' risk assessments then are presented as a portfolio view, enabling entity-level management to consider the units' risks, by objective, in terms of an earnings per share measure relative to the entity as a whole.

Exhibit 6.7
Portfolio View of Residual Risk

A company that manufactures and distributes inflatable rafts for personal recreational use has its corporate headquarters in southern California, and two business units, one in South Carolina and the other in Oregon. The company assessed its key risks, which are changes in interest rates, which correlate directly to customer demand for its product; unexpected increases in the price of raw materials; and the potential of a work stoppage. Management assessed the risks, developed risk responses, and formed a portfolio view in terms of earnings per share. Some risk responses, such as the hedging program to reduce the effect of changing interest rates and the negotiating strategy to reduce the likelihood of a work stoppage, are coordinated and executed at the entity level. Other responses, such as the decision to enter into long-term contracts to reduce the likelihood and impact of unexpected raw materials price increases, and the redistribution of production scheduling to other regions to reduce the impact of a work stoppage, are executed at the regional level.

		Inherent Risk				**Risk Response Actions**				**Residual Risk**
Risk		Corp	Oregon	South Carolina	Entity	Corp	Oregon	South Carolina	Entity	
	Unit of Measure	Business Unit Contribution			Earnings per Share					Earnings per Share
The U.S. interest rate changes by 50, 100, and 200 basis points (BPS) in next 12 months	Impact – 50 BPS	$ 100 ↑	$ 80 ↓	$ 38 ↓	0.10 net ↓	**Reduce** – hedge program at entity level				$0.05↓
	– 100 BPS	$ 200 ↑	$ 160 ↓	$ 75 ↓	0.20 net ↓					$0.10↓
	– 200 BPS	$ 400 ↑	$ 320 ↓	$ 150 ↓	0.40 net ↓					$0.20↓
	Likelihood – 50 BPS	25%								25%
	– 100 BPS	10%								10%
	– 200 BPS	4%								4%
Price of raw materials increases by 10%	Impact	-	$ 100 ↓	$ 50 ↓	0.07 ↓	N/A	**Reduce –** Long-term contracts put in place for raw materials	**Accept –** No actions taken to alter potential price changes for key materials	N/A	$0.05↓
	Likelihood	-	15%	20%		N/A			N/A	10%
	Unit of Measure	Production Hours Lost			Earnings per Share					Earnings per Share
Pending union negotiations halt production for one week	Impact	-	4,000	3,000	0.02	N/A	**Reduce** – Production capacity equal to 50% of output available through alliance partners	**Accept/Reduce** – Production capacity equal to 40% of output transferable to Oregon, if operating	N/A	.01↓
	Likelihood	-	15%	3%		N/A	**Reduce** – Effective negotiating strategy developed by management team to successfully avert work stoppage			5%

7. CONTROL ACTIVITIES

Framework 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.

This chapter illustrates how control activities support risk responses, and how control activities themselves may serve as a risk response.

Integration with Risk Response

Having selected risk responses, management identifies control activities needed to help ensure that the risk responses are carried out properly and in a timely manner.

Exhibit 7.1 provides illustrations of how control activities align with each of the response types of avoidance, reduction, sharing, and acceptance.

Exhibit 7.1
Risk Responses and Control Activities

- **Risk Avoidance** – In looking to improve operating margins, a software company's management considered moving programming activities to a country with lower labor costs. After assessing the associated risks, management decided such a move is outside the company's risk appetite, and that contracting of programming activities will be done only within the company's home country. To help ensure the policy decision is properly implemented, the "New Programmer" form was amended to include the country of vendor operations, which information is reviewed and (electronically) signed by senior management as the basis of programmer selection.
- **Risk Reduction** – A hospital's management recognized that its ability to protect the health and well-being of its patients would be adversely affected by disruption in electrical power supply. Management responded by installing back-up electrical generators. To help ensure that the generators operate when needed, the company's engineering department conducts routine maintenance, with maintenance logs reviewed monthly by the head of the engineering department.
- **Risk Sharing** – A manufacturing company determined that a prolonged disruption to its plant would significantly impact its ability to meet its production targets. Based on assessment of the company's capital position, its risk tolerance, and cost of sharing the risk with an insurer, management approved purchasing insurance coverage for the value of lost production for a period of up to six months. To help ensure that the response is implemented, the Chief Risk Manager periodically reviews the company's coverage, as well as compliance with all negotiated terms and conditions of the agreement with the insurer, and reports to the Chief Operating Officer on compliance.

- **Risk Acceptance** – A company's management identified changes in world commodity prices as a risk. After assessing the risk likelihood and impact and considering the company's risk tolerance, management decided to accept the risk. Management instituted a policy whereby the Treasury Department formally reassesses the exposure every three months and reports to the management committee its recommendation on whether a hedging strategy should be adopted.

Control Activities Serving as Risk Response

While control activities generally are established to ensure risk responses are appropriately carried out, with respect to certain objectives, control activities themselves are the risk response.

In some circumstances control activities themselves serve as the risk response. This frequently is the case with respect to risks related to reporting objectives. Exhibit 7.2 provides an illustration.

Exhibit 7.2
Relationship Between Objectives, Risks, Responses, and Control Activities

Reporting objective	Asset acquisitions and expenses incurred are entered for processing completely (C) and accurately (A), and are valid/occurred (V)				
Unit of measure	Financial reporting errors detected, measured in dollars				
Target	Errors in monthly financial statements are less than $100,000				
Tolerance	Errors less than $110,000				
Risks	**Inherent risk assessment**		**Risk response**	**Residual risk assessment**	
	Likelihood	**Impact**		**Likelihood**	**Impact**
Vendor invoice amounts are captured incorrectly	Possible	Minor $5,000–$15,000	See below for control activities that serve as the responses to these risks	Unlikely	Minor $2,500–$7,500
Vendor invoices are not received prior to the month-end cutoff	Almost Certain	Moderate $10,000–$25,000		Possible	Minor $2,500–$7,500
Vendors are paid from statements as well as invoices, resulting in duplicate payments	Possible	Minor $5,000–$15,000		Unlikely	Minor $5,000–$7,500

Control Activities	• Asset acquisition and expense transactions are subjected to programmed edit/validation checks which include: - Purchasing data (PO number, amount, etc.) are validated against specified files or tables (A) - Key fields are tested for blanks, alphas, values within a specified range (e.g., purchase amounts), missing data elements (e.g., payment due date), and programmed check digits (e.g., vendor number) (A) - Reasonableness tests are performed, comparing data input in two or more different fields based on specified criteria (e.g., sales tax rate is compared with the state tax rate based on the vendor's zip code) (A) - Edit checks compare key amounts with tables to ensure input data are within limits established for each user or class of user (e.g., payment amounts are compared with approval limits for electronic payment) (A) - Edit checks compare vendor name/number and invoice numbers with those on file to ensure valid vendor and to detect duplicate payments (V) • All payment transactions input are matched to the original purchase order details before further processing may occur (A) • Payment amounts, including electronic payment transactions, are verified on screen by someone other than the staff member responsible for the original payment information (A,V) • Staff reconcile each batch or series of on-line transactions with system edit or processing reports (A,C) • Exception reports are produced listing large or unusual items (e.g., amounts exceeding $100,000), which are then individually compared with input documents (A) • Exception reports produce a listing of unmatched purchase orders open for more than 30 days, which are then followed up (C) • Changes to user-defined system parameters (e.g., authorization limits) are automatically reported and checked by an independent official (A,C,V) • Overrides of system warnings by the user are automatically reported for independent approval (A,C,V)

Exhibit 7.3 provides additional illustrations of control activities that also may be the risk response.

Exhibit 7.3
Control Activities as a Risk Response

- To ensure that pension obligations and costs are reported properly in the financial statements, management reviews the company's demographic data and the methods and assumptions used by the actuary, and compares amounts in the actuary's report with those in the financial statements and related footnotes.
- To help ensure that a company's monthly income tax remittances are made in compliance with regulations, an electronic tickler file prompts staff with due dates for tax filings, and a supervisor verifies timely remittance.
- To help ensure that computer interfaces between general ledger systems operate to effect complete and accurate processing, transaction totals from subsidiary systems are compared with the balance in the general ledger control account, with any differences reported and followed up.
- To help minimize inventory losses, transfer documents are reviewed and approved by the warehouse supervisor before goods are released.
- To help ensure that only tested and accepted programs are transferred from test to production libraries, transfers are made only based on completion of testing and related approvals and authorization of the IT and user line/department managers.

8. INFORMATION AND COMMUNICATION

Framework 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 from external sources, providing information for managing 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, such as customers, suppliers, regulators, and shareholders.

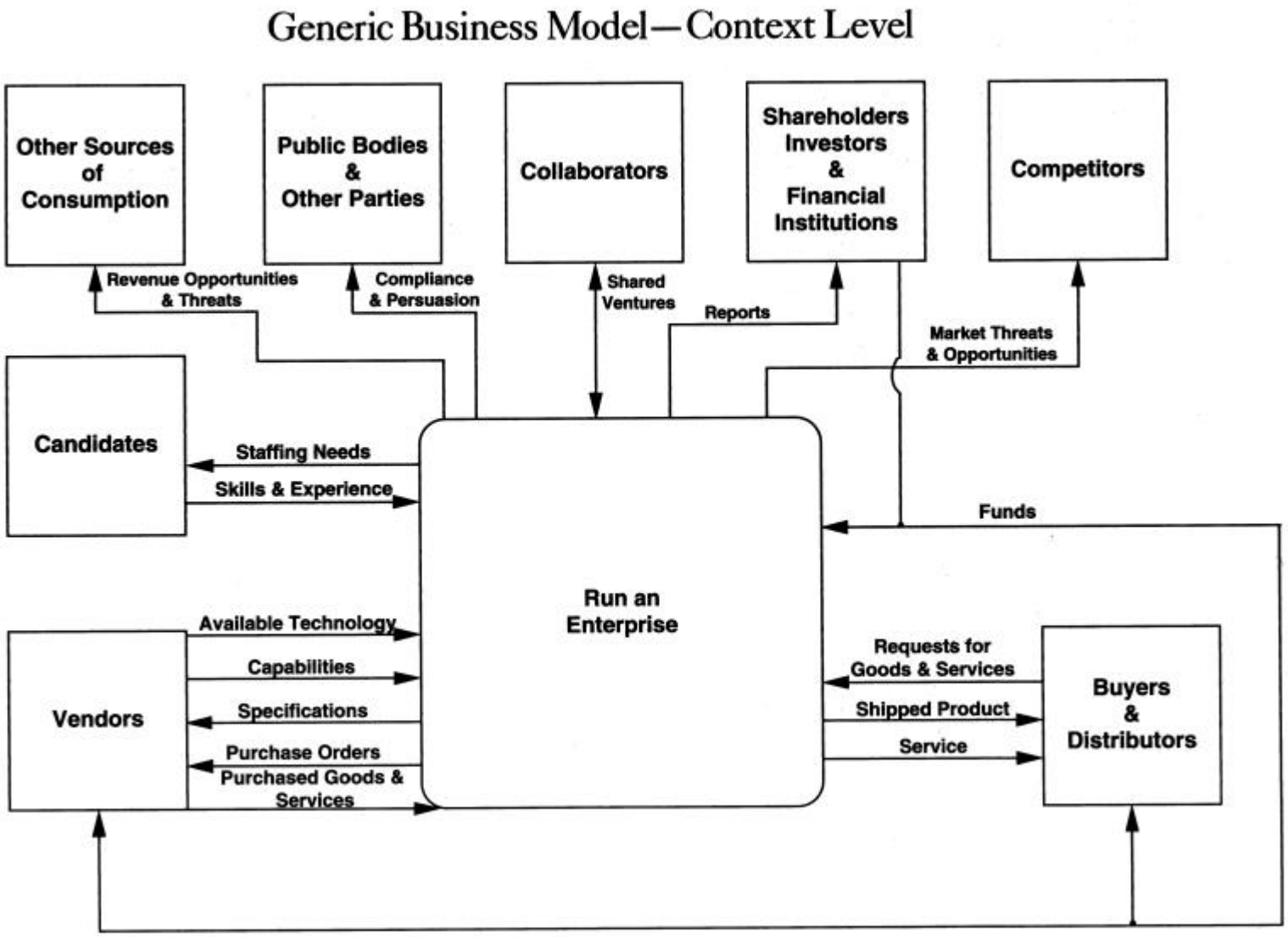
This chapter illustrates how information is obtained and flows in an organization and is used and presented to support enterprise risk management. Also illustrated are techniques that facilitate communication supporting effective enterprise risk management.

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.

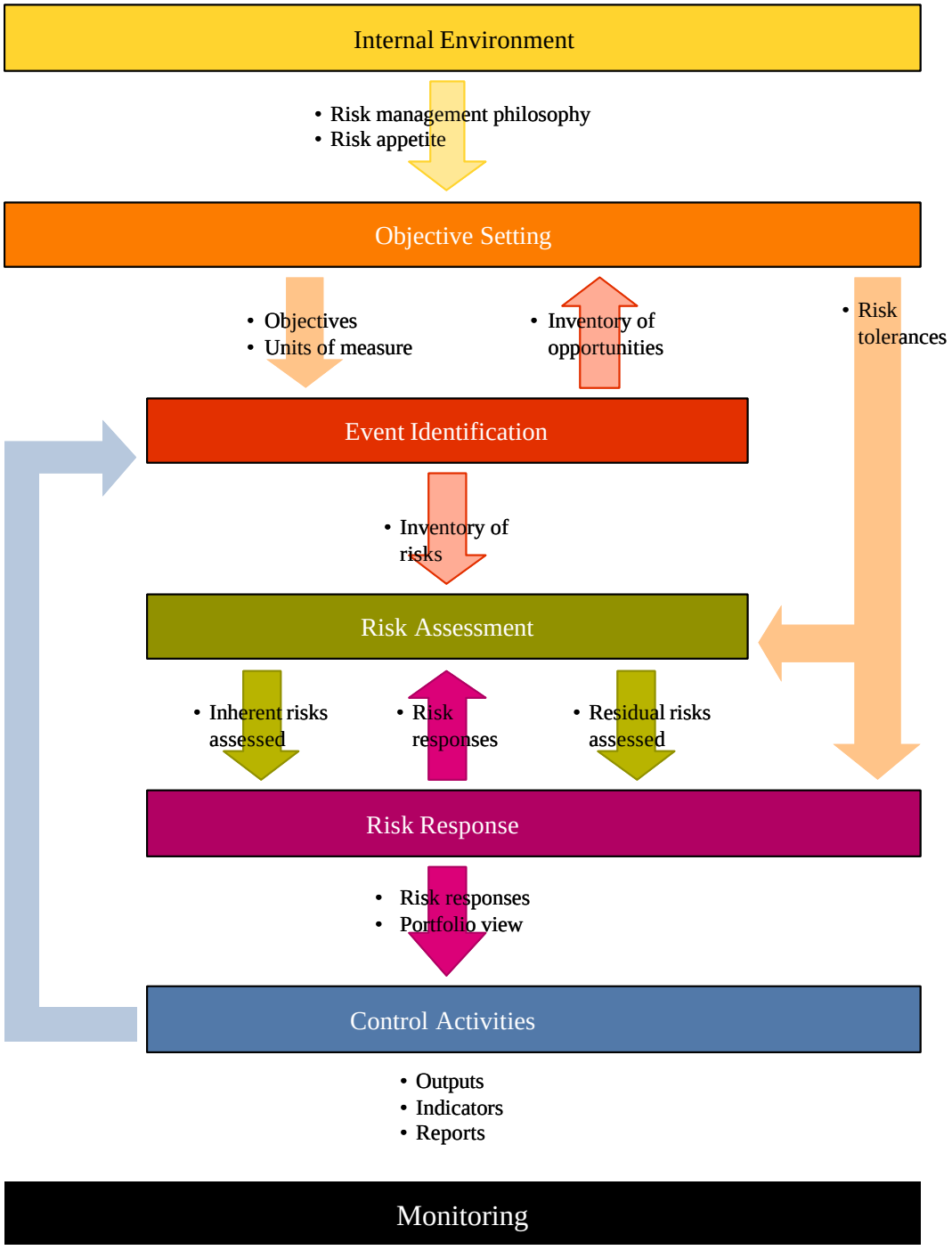
Information both from external sources and internally generated is obtained and analyzed in setting strategy and objectives, identifying events, analyzing risks, determining risk responses, and otherwise effecting enterprise risk management and carrying out other management activities. A broad-based, generic depiction of information flows into, out of, and within an entity to support its ongoing management is shown in Exhibit 8.1 (taken from the *Internal Control – Integrated Framework Evaluation Tools* Reference Manual, and drawn from *Competitive Advantage*, M. E. Porter). Further detail on information flows is shown in the *Internal Control – Integrated Framework Evaluation Tools* Reference Manual.

Exhibit 8.1


Generic Business Model—Context Level
Other Sources of Consumption
Public Bodies & Other Parties
Collaborators
Shareholders Investors & Financial Institutions
Competitors
Revenue Opportunities & Threats
Compliance & Persuasion
Shared Ventures
Reports
Market Threats & Opportunities
Candidates
Staffing Needs
Skills & Experience
Funds
Run an Enterprise
Available Technology
Capabilities
Specifications
Purchase Orders
Purchased Goods & Services
Vendors
Requests for Goods & Services
Shipped Product
Service
Buyers & Distributors

In addition to information flows into and within an organization, there are flows among activities inherent in the enterprise risk management components. Exhibit 8.2 illustrates how these information flows may be conceptualized.

Exhibit 8.2
Information Flows Within Enterprise Risk Management



Technology is applied to improve the effectiveness and efficiency of information processes. Exhibit 8.3 illustrates how a company may utilize information technology to support the timely use of information in an event identification process.

Exhibit 8.3
Use of Information Technology in Event Identification

As part of the event identification process, a chain of automotive dealerships regularly reviews leading newspapers, business publications, and trade journals to keep track of changes in the competitor landscape. Initially done manually, as described in the first bulleted item below, the process was automated, as described in the second.

- A researcher reviewed hard copy of selected publications on a daily, weekly, and monthly basis, provided the information to applicable managers for analysis, and developed related reports. The reports were distributed to unit leaders and others for consideration in the risk assessment process. This process normally took 24–48 hours to complete each week, month, and quarter.
- The company now subscribes to Internet libraries, and the researcher uses web-based search engines to identify relevant information, and attaches "relevance" ratings to the information. The captured information is analyzed, and reports are distributed electronically to the responsible managers. Including the manual analysis, the process now takes only several hours to complete, and garners a broader array of relevant information.

Strategic and Integrated Systems

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.

Technology plays a critical role in enabling the flow of information in an organization, including information directly relevant to enterprise risk management. The selection of specific technologies to support enterprise risk management for an organization typically is a reflection of the:

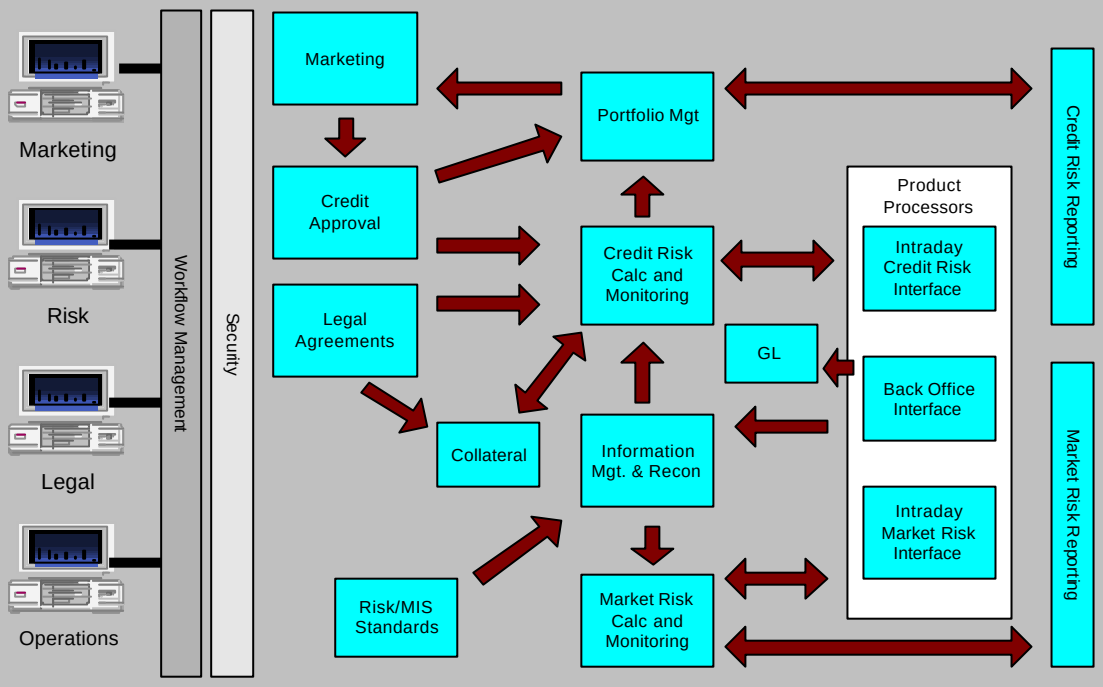
- Entity's approach to enterprise risk management and its degree of sophistication
- Types of events affecting the entity
- Entity's overall information technology architecture
- Degree of centralization of supporting technology

In some organizations, information is managed separately by unit or function, whereas others have integrated systems. Exhibit 8.4 illustrates the loan origination and risk management functions of a corporate bank, where information is developed by functional unit and shared as needed with others in the organization.

.

Exhibit 8.4
Loan Origination Information Flows

Individual functions – marketing, risk management, legal, and operations – are each supported by their own technology, which captures, maintains, and reports relevant information, which then is shared across the organization.



With added focus on information needed for risk management, some organizations have enhanced their technology architectures to allow greater connectivity and usability of data, with some using the Internet and data interchange capabilities. Web services-based information strategies enable real-time information capture, maintenance, and distribution across units and functions, often enhancing information capture, better controlling multiple sources of data, minimizing manual processing of the data, and enabling automated analysis, retrieval, and reporting.

Under an open architecture, technologies such as XBRL, XML, and Web services are used to facilitate data aggregation, transfer, and connectivity between disparate or stand-alone systems. XBRL, the acronym for eXtensible Business Reporting Language, is derived from XML (eXtensible Markup Language). XBRL is an open, royalty-free, Internet-based information standard for business reporting of all kinds. XBRL labels data so that they are provided with context that remains with them and brings conformity to the names by which they are recognized by disparate software.

Web services is an Internet protocol for transporting data between disparate applications, within a company's boundaries or across companies. XBRL, used with Web services, facilitates automated information exchange across diverse platforms and different applications and automates business reporting processes. Exhibit 8.5 illustrates how XBRL and Web services can improve the efficiency of the reporting processes for the loan processing activities identified in Exhibit 8.4.

Exhibit 8.5
Integration of Systems

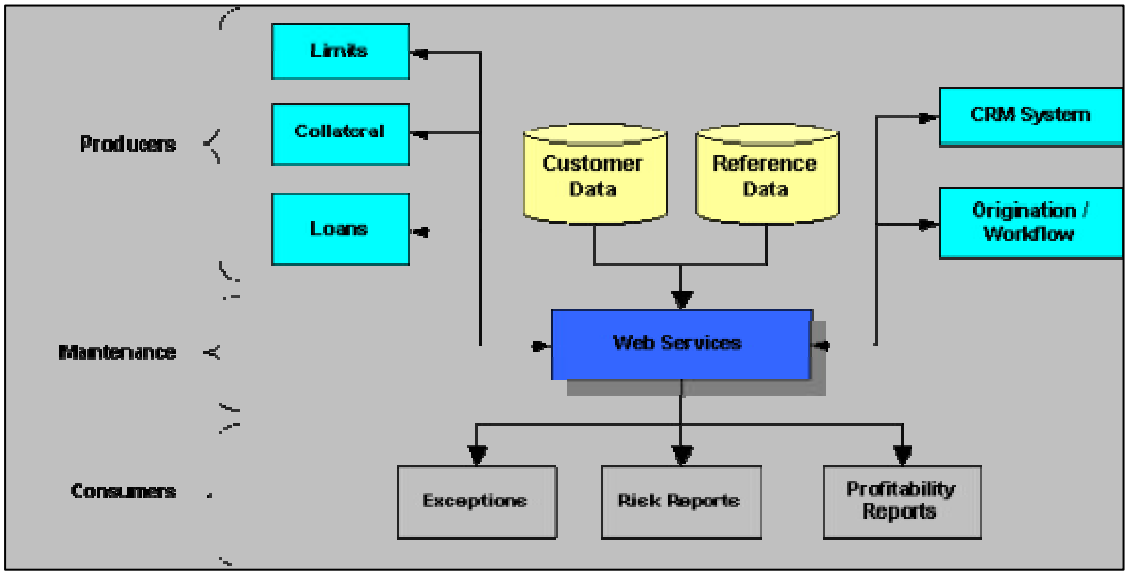


Exhibit 8.6 illustrates how two organizations address the requirements of multiple constituents and leverage information across functions using XBRL and Web services.

Exhibit 8.6
Data, Systems Integration

- A telecommunications company uses XBRL and Web services to automate its billing process. Using an XBRL telecom billing taxonomy, transaction-level data are passed from ordering systems to provisioning and billing systems, and positioned for creating customer invoices. XBRL enables the billing system to feed information directly to company reporting systems via the XBRL general ledger standards-based platform. That platform provides predefined data tags for elements of financial transactions, enabling the company to represent, for example, all parties to a transaction, all resources that are part of the transaction (such as supplies, inventory, and other resources), and all related events (such as when the transaction was created, sent, received, and entered into the system). This audit trail allows managers and auditors to quickly verify information at any consolidation level – in an installation, in an operating unit, or at the entity level. The process reduces the cost of compliance by providing a more efficient platform for communication with regulators, creditors, and other third parties. And, systems changes on either side of the XBRL integration point can proceed with less disruption to the information transfer cycle because the new system can readily understand and use the XBRL-enriched information.
- Another company uses XBRL technology to obtain more complete information on exposures in its accounts receivable. Previously, business units reported receivables from individual customers exceeding a monetary threshold, but the composite reports did not include exposures slightly under the threshold. With XBRL, the company's reports include all exposures to a particular customer, enabling quicker and more relevant management action.

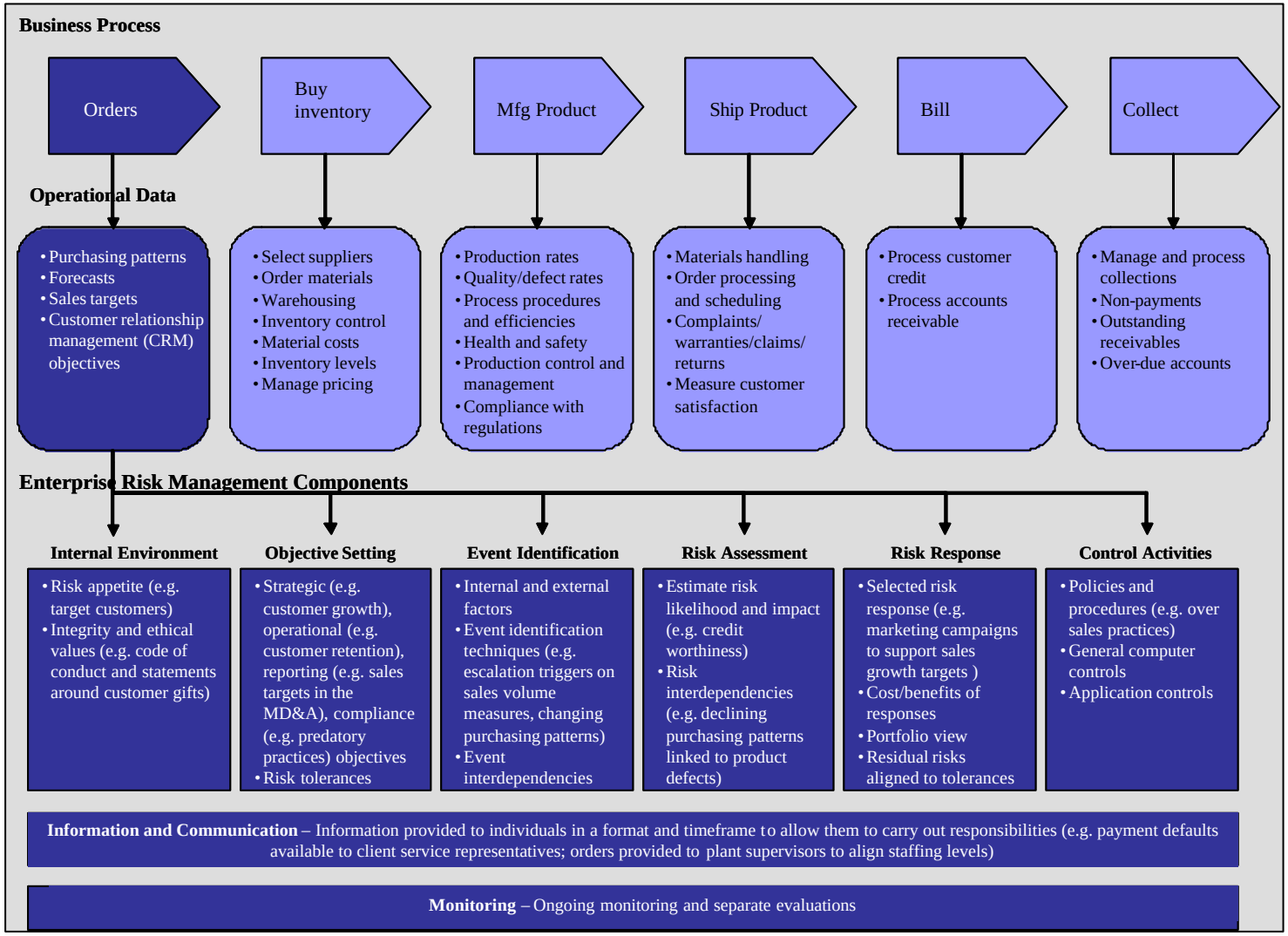
Some organizations, rather than using open architectures, develop customized systems encompassing data warehouses, which generate key metrics and measures to support enterprise risk management.

Integration with Operations

Many organizations have highly complex information technology infrastructures developed over time to support operations, reporting, and compliance objectives. In many instances the information generated by these systems in the regular course of business is integral to the enterprise risk management process.

Exhibit 8.7 illustrates how information used in enterprise risk management is an inherent part of and integrated with business processes – in this instance, the sales process (items listed under the component headings include only examples of relevant information).

Exhibit 8.7
Information Flows Across a Sales Process



Depth and Timeliness of Information

Advances in data collection, processing, and storage have resulted in exponential growth in data volume. With more data available - often in real time - to more people in an organization, the challenge is to avoid "information overload" by ensuring flow of the right information, in the right form, at the right level of detail, to the right people, at the right time.

Exhibit 8.8 illustrates information needs that management may consider when planning and implementing technological infrastructures.

Exhibit 8.8
Considerations in Determining Information Requirements

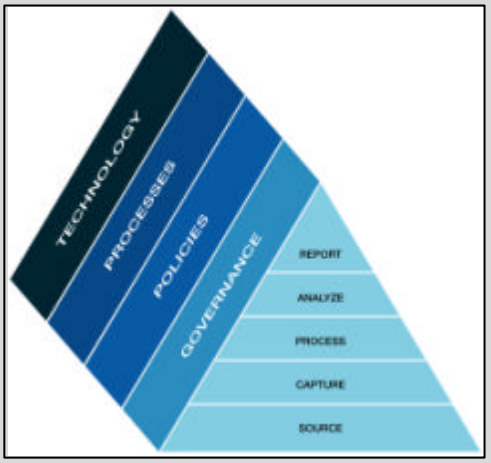
- What are the key performance indicators for the business?
- What key risk indicators provide a top-down perspective of potential risks?
- What performance metrics are required for monitoring?
- What data are required for the performance metrics?
- What level of granularity of information is needed?
- How frequently does the information need to be collected?
- What level of accuracy or rigor is needed?
- What are the criteria for data collection?
- Where and how should data be obtained (e.g., from business units or operating areas, electronically or manually)?
- What data/information are present from existing processes?
- How should data repositories be structured?
- What data recovery mechanisms are needed?

Many organizations have established a structured approach to information management. Such approaches enable management to identify the value and rank the importance of information, and develop effective processes and appropriate tools and methods to reliably collect, store, and distribute data. Exhibit 8.9 illustrates elements of an information management program used by a large retail bank to support management of market risk exposures.

Exhibit 8.9
Managing Market Risk Exposures

The Market Risk Function of a large retail bank tracks the organization's actual and potential exposures to movements in interest rates each day. In identifying the information needed to perform risk assessments, and ensure the bank remains within its risk tolerances, management views information in the context of the following elements:

Primary



- **Source and Capture** – defines how information is to be produced or acquired, from internal or external sources. Rules for modifying or transforming data, methods of extraction, and selection criteria are addressed at this level. For the Market Risk Function, data are sourced from multiple internal systems, including back office trade processing systems and market risk limit systems, and from external sources, including rates from a market data provider. Data are captured by automated interfaces from each of the sources.
- **Process and Analyze –** defines how information is maintained once it is in production. Data integrity, data quality, and data cleansing exercises are performed at this level. Data for the Market Risk Function are processed using market risk models to calculate exposure. Management analyzes resulting information to evaluate the organization's exposure against pre-set tolerances and market risk limits.
- **Report –** defines how information is distributed to end-users. Data aggregation criteria, authorization considerations, and whether information is distributed in raw form or standard or customizable reports, are addressed at this level. In this instance, systems report exceptions in real time to line managers and summarize the daily overall position to senior management.

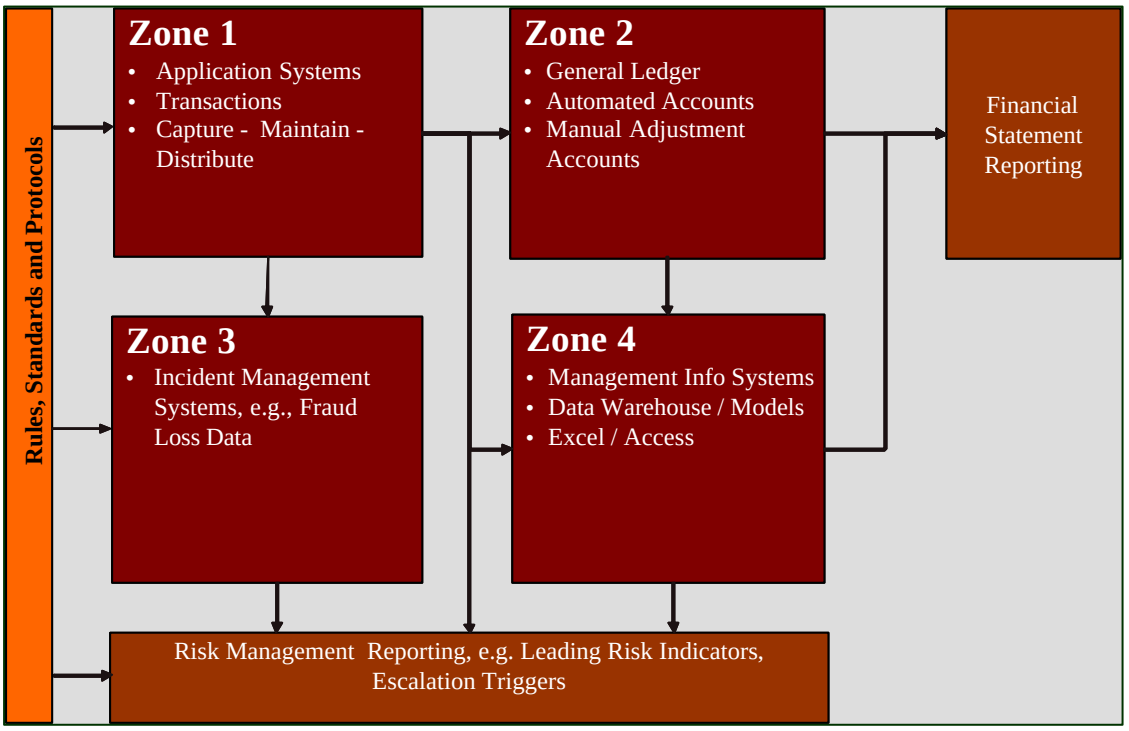
Secondary

- **Governance** – defines the policy, organizational structure, and mandate supporting the primary characteristics.
- **Policies** – define the general principles, standards, and framework.
- **Processes** – define the procedures and standards employed to support the primary characteristics.
- **Technology** – defines the architecture, applications, databases, security, and controls that support the primary characteristics.

Having the right information, on time and at the right place, is essential to effecting enterprise risk management.

Exhibit 8.10 illustrates information sources and flows in a common reporting process. Each of the four zones captures information used in the management process, including risk management. When these disparate systems, such as operational systems (Zone 1), financial reporting systems (Zone 2), performance management systems (Zone 3), and formal and informal data management systems (Zone 4), are integrated, management is able to obtain enhanced risk management reporting on a real-time basis.

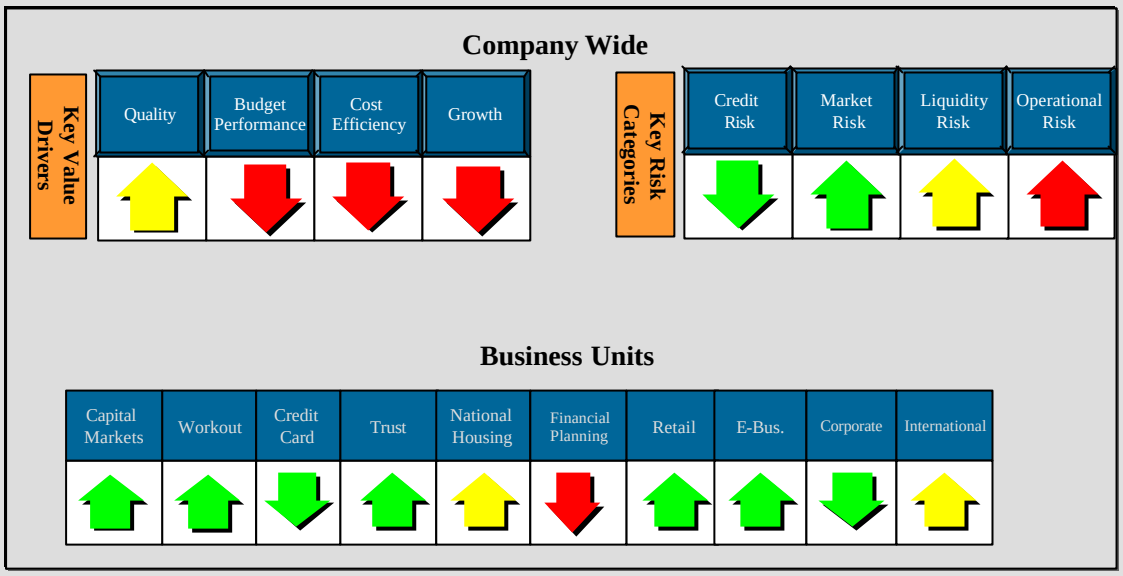
Exhibit 8.10
Overview of Data Flows Within a Reporting Process



"Dashboard"-style reports are used by organizations to present information necessary for enterprise risk management. These dashboard reports enable management to quickly determine the extent to which the entity's risk profile is aligned with risk tolerances. Where misalignment occurs, which suggests existing risk responses or controls are not performing as expected, management can take corrective action. These dashboard reports are generated from information obtained from any or all of the four zones depicted in Exhibit 8.10 and from information external to the company.

A risk profile dashboard used by a large bank is illustrated in Exhibit 8.11, which allows management to view risk relative to both the entity as a whole and individual business units.

Exhibit 8.11
Dashboard Reporting



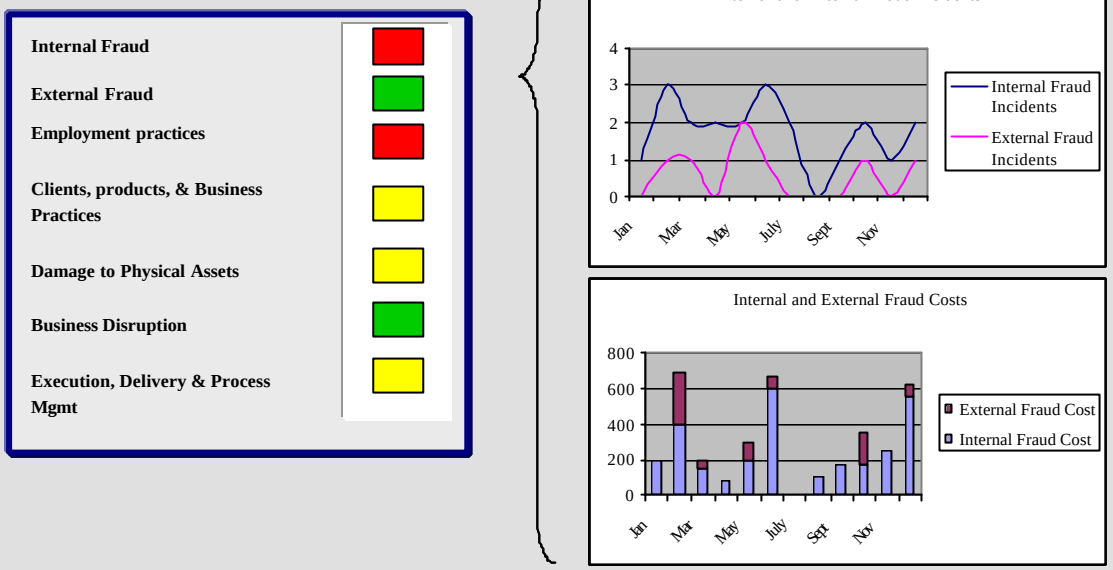
The arrows provide two pieces of information:

- Arrow direction indicates quarter-to-quarter trend in expected loss from the underlying risks, with a down arrow indicating a decline in expected loss trend, and an up arrow an increase.
- Arrow color indicates residual risk in relation to tolerances, where green indicates expected loss safely within risk tolerance, yellow indicates expected loss near or at risk tolerance, and red indicates risk tolerance is exceeded.

Looking at the Capital Markets business unit, for example, the up arrow shows a quarter-to-quarter increase in expected loss, and the color green indicates that the unit's expected loss remains safely within the established risk tolerance.

Many of these dashboard reporting systems allow users to "drill down" to examine the underlying data. For example, Exhibit 8.12 illustrates how the same bank shows the details behind the operational risk arrow in Exhibit 8.11.

Exhibit 8.12
Drilldown to Operational Risk



The data depicted in the charts at the right feed the first two entries in the color-coded graphic at the left, and the data from that graphic in turn feed the entity-level measure in the dashboard in Exhibit 8.11 – in this illustration, supporting the measure for operational risk. The bank established that if none of the business unit measures are coded red (that is, none exceed risk tolerance), then the entity-level measure will be coded green; if one business unit measure is red, the entity-level measure will be coded yellow; and if two or more are red, the entity-level measure will be coded red. While the color scheme at the entity level does not provide precise information, it allows management to quickly focus on those risks not within its tolerances and to drill down for more precise information and to identify areas where action may be required.

Communication

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

Communications are key to creating the "right" internal environment and to supporting the other components of enterprise risk management. For example, embedding the risk management philosophy into an organization's culture is facilitated by top-down communications on what the philosophy is and what is expected of the organization's people, and supported by bottom-up information flows. Similarly, management reinforces or changes an organization's cultures with words and everyday actions. One company adopted an internal communications program, as illustrated in Exhibit 8.13, specifically to support the

integration of its risk management philosophy and to help reinforce an ethical internal environment.

Exhibit 8.13
Communicating Risk Management Philosophy

- Management discusses risks and associated risk responses in regular briefings with employees.
- Management regularly communicates entity-wide risks in employee communications.
- Enterprise risk management policies, standards, and procedures are made readily available to employees along with clear statements requiring compliance.
- Management requires employees to consult with others across the organization as appropriate when new events are identified.
- New hire orientation sessions include information and literature on the company's risk management philosophy and enterprise risk management program.
- Tenured employees are required to take workshops and/or refresher courses on the organization's enterprise risk management initiatives.
- The risk management philosophy is reinforced in regular and ongoing internal communication programs and through specific communication programs to reinforce tenets of the company's culture.

Exhibit 8.14 is an example of a letter from the CEO of one company to employees, emphasizing the importance of enterprise risk management.

Exhibit 8.14
Message from CEO

Our overall objective is to maximize shareholder value.

To achieve this goal we must have superior risk management capabilities, which address the full spectrum of risks facing our businesses. A structured and disciplined approach to risk management will ensure that our strategic efforts are not diminished through avoidable loss, or hampered by change and uncertainty. Additionally, we must harness our ability to cope with emerging risks and opportunities in an increasingly competitive environment.

Everyone has a role to play in our enterprise risk management. This entails understanding the risks and opportunities facing our business, assessing exposure, and taking action to effectively respond to preserve and maximize value.

We have developed a framework document as a tool to guide our efforts to manage the risks, uncertainties, and opportunities of our businesses to support the achievement of organizational objectives and maximize shareholder value.

We look to all our employees to participate in applying this framework on a daily basis to help ensure we fulfill our objectives.

In addition to "top-down" information flows, communications channels should enable personnel to communicate risk-based information across business units, processes, or functional silos. Exhibit 8.15 includes examples of vehicles managements use to communicate such information.

Exhibit 8.15
Communications Vehicles

- Broadcast e-mails
- Broadcast voice mails
- Corporate newsletters
- Databases supporting specific risk issues
- Letters from the CEO
- E-mail discussion groups
- Intranet sites capturing information regarding enterprise risk management for easy access by personnel
- Messages integrated into ongoing corporate communications
- Organization, function, or location-wide webcasts or conference calls
- Posters or signs reinforcing key aspects of enterprise risk management
- Regular face-to-face meetings of "risk champions" or other employees from a range of functions and business units with responsibility for aspects of enterprise risk management
- Regular risk management conference calls among a network of risk champions and other employees
- Regularly issued newsletters from the chief risk officer and associated staff
- "Town-hall" meetings

A desirable goal is, over time, to embed communications on enterprise risk management into an entity's broad-based, ongoing communications programs, consistent with the concept of building enterprise risk management into the fabric of the organization.

Many organizations use technology to facilitate ongoing communication for enterprise risk management. Technology, such as an intranet site, can put enterprise risk management information within easy and constant access of all staff. Exhibit 8.16 illustrates information typically provided and made readily available.

Exhibit 8.16
Intranet Site Information on Enterprise Risk Management

- "Ask anything" links
- CEO's message stating the entity's risk management philosophy, risk appetite, and basic objectives of its enterprise risk management approach
- Discussion forum
- Enterprise risk management policies and procedures
- Frequently asked questions regarding the organization's enterprise risk management program
- Relevant enterprise risk management reports and reporting activities
- Readily accessible information on and links to corporate whistle-blower channels or hotlines
- Links to other organizations' websites providing information on risk management within key functions and processes, such as human resources policies, procurement, travel, vendor relations, etc.
- List of responsibilities and contact information for chief risk officer and key staff supporting the enterprise risk management program

In some circumstances . . . separate lines of communication are needed to serve as a fail-safe mechanism in case normal channels are inoperative.

In the event regular communications channels are not effective or appropriate, many organizations have set up supplemental employee communications channels. These channels, which may be called "whistle-blower" programs or "ethics hotlines," may be voluntary or legally mandated. Their purpose is to provide a ready means whereby employees at any organizational level can confidentially discuss or report perceived or actual illegal, unethical, or otherwise inappropriate behavior.

Exhibit 8.17 provides questions that might be considered when establishing an ethics hotline.

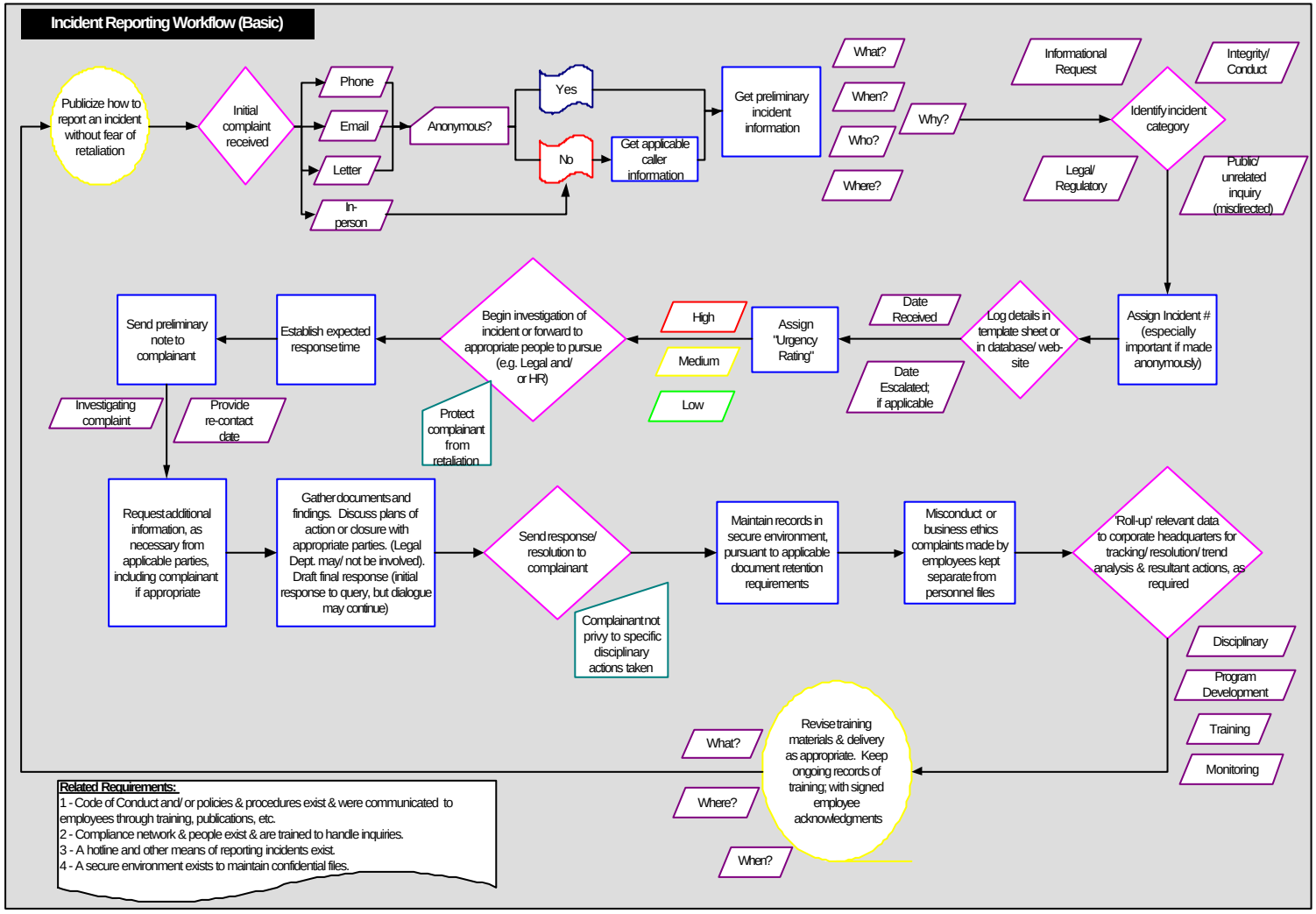
Exhibit 8.17
Considerations for Ethics Hotlines

- Are reporting mechanisms and protocols such that personnel will feel comfortable using the channel?
- What procedures will be used to ensure personnel trust the communications channel, with no concern about potential reprisal?
- Will the system be managed internally or by an external third party?
- How will incidents be prioritized?
- How will appropriate follow-up resources be identified?
- What is target response time?
- What are documentation standards?
- What monitoring processes should be in place?

- Are technology and security resources sufficient to manage the system?
- Who will perform any necessary investigations?
- How will complaints be documented and tracked?
- How will the employee reporting the information be advised of conclusions and actions taken?
- What kinds of summary reports are needed, and with what frequency?
- What mechanisms will be in place to ensure needed broad-based corrective and future preventive actions are taken?

Exhibit 8.18 provides an illustrative work flow diagram for a supplemental reporting process.

Exhibit 8.18
Alternative Reporting Process



9. MONITORING

Framework Chapter Summary: Enterprise risk management is monitored – assessing 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.

This chapter illustrates some the techniques used in ongoing monitoring and separate evaluations, and provides an overview of methodology, tools, documentation, and considerations for reporting deficiencies. In addition to the techniques illustrated here, readers are referred to the evaluation tools provided in *Internal Control – Integrated Framework*, which may serve as a useful reference for separate evaluations of enterprise risk management.

Ongoing Monitoring Activities

Many different activities performed in the ordinary course of running a business serve to monitor the effectiveness of enterprise risk management components. These include day-to-day review of information in carrying out normal business activities, as illustrated in Exhibit 9.1.

Illustration 9.1
Examples of Ongoing Monitoring Activities

- Management reviews reports of key business activity indicators such as flash reports of new sales or cash position, and information on backlog, gross margins, and other key financial and operational statistics.
- Operating management compares production, inventory, quality measures, sales, and other information obtained in the course of daily activities to systems-generated information and to budget or plan.
- Management reviews performance against limits established for risk exposures, such as acceptable error rates, items in suspense, reconciling items, foreign currency exposure balances, or exposure to counterparties.
- Management reviews transactions reported through escalation triggers.
- Management reviews key performance indicators such as trends in direction and magnitude of risks, status of strategic and tactical initiatives, trends or variances in actual results to budget or prior periods, and event triggers, as described in the Event Identification chapter.

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.

Separate evaluations of enterprise risk management typically are conducted periodically. In some cases, they are prompted by change in strategy, key processes, or entity structure. Separate evaluations are conducted by management, the internal audit function, external specialists, or a combination thereof.

Separate evaluations sometimes are broad-based, with scope including the entirety of the entity and all enterprise risk management components. In some cases, the evaluation is limited to a specific business unit, process, or department, with other areas of the business addressed over time. Exhibit 9.2 describes how a manufacturer designed an evaluation of its new inventory control system.

Exhibit 9.2
Separate Monitoring of a New Process

Management of a large manufacturing company installed new modules for its enterprise resource planning system, to enhance its global supply chain processes. Objectives included reducing inventory costs, improving tracking capabilities, and providing better information on inventory availability. Given the critical importance of the system to achieving customer service goals, and the scale of the changes to the processes, it was decided that a separate evaluation of the process would be conducted on a monthly basis for four months following the "go-live" date, and every six months thereafter for two years.

The evaluations were conducted by a team comprising individuals from the information technology function, the internal audit function, and outside consultants. The first evaluation focused on:

- System change controls
- Organizational change readiness
- Security
- Data quality
- Interfaces with legacy systems

Subsequent evaluations addressed accuracy and completeness of processing, including transfers and handoffs, related control activities, changes to and control over access, manual interfaces, and use and usefulness of information outputs.

Internal Audit Reviews

Internal audit functions typically provide an assessment of risks and control activities of a business unit, process, or department. These assessments provide an objective perspective on any or all elements of enterprise risk management, from the company's internal environment through monitoring. In some cases particular attention is given to risk identification, analysis of likelihood and impact, risk response, control activities, and information and communication. Internal audit, based on its knowledge of the business, may be positioned to consider how new company initiatives and circumstances might affect application of enterprise risk management, and to take that into account in its review and testing of relevant information. Further information is available in The Institute of Internal Auditors' Practice Advisories, which set out guidance for evaluating and reporting on risk management effectiveness.

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.

A disciplined process provides a sound basis for an evaluation. Any of a number of approaches and techniques are used, generally depending on the circumstances of the company and nature and scope of the evaluation to be performed. Exhibit 9.3 illustrates one company's basic approach.

Exhibit 9.3
Steps in a Separate Evaluation

Planning

- Define the objectives and scope of the evaluation
- Identify an executive with requisite authority to manage the evaluation
- Identify the evaluation team, support personnel, and key business unit contacts
- Define the evaluation methodology, timeline, and steps to be conducted
- Agree on evaluation plan

Performance

- Gain an understanding of the business unit's/process's activities
- Understand how the unit's/process's risk management process is designed to work
- Apply the agreed-on methods to evaluate the risk management process
- Analyze results by comparison to the Company's internal audit standards and follow up as necessary
- Document deficiencies and proposed remediation, if applicable
- Review and validate findings with appropriate personnel

Reporting and Corrective Actions

- Review results with business unit/process and other management as appropriate
- Obtain comments and remediation plans from unit/business process management
- Incorporate management feedback into final evaluation report

Methodology

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

Evaluators identify methodologies and tools needed to support the evaluation process. A number of structured methodologies and tools exist that are used to document and assess specific aspects of enterprise risk management. Factors in selecting evaluation methodologies and tools include whether they can be readily used by assigned staff, are relevant to the given scope, and are appropriate to the nature and expected frequency of the evaluation. For example, where the scope involves understanding and documenting differences between business process design and actual performance, the evaluation team might review or develop process flowcharts and control matrices, whereas a scope limited to addressing whether specific mandated control activities are present might suggest using a pre-established questionnaire. Exhibit 9.4 lists tools used, either individually or in conjunction with one another.

Exhibit 9.4
Methodologies and Tools

- Process flowcharting
- Risk and control matrices
- Risk and control reference manuals
- Benchmarking using internal, industry, or peer information
- Computer assisted audit techniques
- Risk and control self-assessment workshops
- Questionnaires
- Facilitated sessions

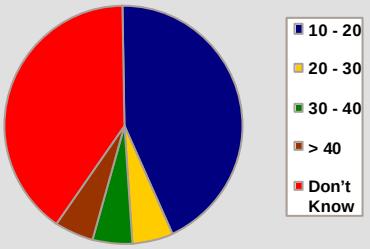
Exhibit 9.5 contains an excerpt of a risk and control self-assessment questionnaire for a payroll process, serving as a diagnostic reference point focusing on the extent to which controls related to payroll processing risks actually are being applied. The results form a basis for needed corrective action.

Exhibit 9.5
Risk and Control Self-Assessment Questionnaire Excerpts

Payroll Questions	Questionnaire Response Options					Policy Reference
1. My department reviews the budget summaries prepared by the Budgeting Department	Yes	No	Don't know	N/A	N/A	Payroll policy #1
2. My department monitors the number of employees paid from your budget	Yes	No	Don't know	N/A	N/A	Payroll policy #2
3. My department reviews the monthly report of salaries and wages posted to our department	Never	Seldom	Usually	Always	N/A	Payroll policy #3
4. When reviewing this payroll report, what would you consider to be an exceedingly high number of overtime payroll hours per person that you would review in detail to determine the underlying cause?	10–20	20–30	30–40	> 40	Don't know	No payroll policy

Summary of Findings

1. 95% of respondents review budget summaries prepared by the Budgeting Department
2. 93% review the number of people paid from their budget
3. 70% always review payroll reports; 18% usually do, and 12% seldom review these reports
4. See graph at right



Documentation

The extent of documentation of an entity's enterprise risk management varies with the entity's size, complexity, and similar factors.

The desired level of enterprise risk management documentation varies by company, often based on size, complexity, and management style. In addition to scale and depth of documentation, considerations include whether it will be paper- or electronic-based, centralized or distributed, and means of access for update and review.

In evaluating enterprise risk management, existing documentation of processes and other activities are reviewed, or may be created, to allow the evaluation team to readily understand the unit, process, or department's risks and responses. Documentation considered in an evaluation may include:

- Organization charts
- Description of key roles, authorities, and responsibilities
- Policy manuals
- Operating procedures
- Process flowcharts
- Relevant controls and associated responsibilities
- Key performance indicators
- Key identified risks
- Key risk measures

Such documentation may form the basis for developing review processes that include tests to determine whether the processes and related policies and procedures represented to have been established are both appropriate to address the entity's risks and being followed.

With regard to what documentation of the evaluation process itself is to be developed, the evaluation team might consider the extent to which documentation is expected to achieve the objectives of:

- Providing an "audit trail" of the evaluation team's assessments and testing
- Communicating the results of the evaluation – findings, conclusions, and recommendations
- Facilitating review by supervisory personnel
- Facilitating evaluations in subsequent periods
- Identifying and reporting broader issues
- Identifying individual roles and responsibilities in the evaluation process
- Supplementing existing enterprise risk management documentation that may be deficient

Reporting Deficiencies

All identified enterprise risk management deficiencies that affect an entity's ability to develop and implement its strategy and to set and achieve its objectives should be reported to those positioned to take necessary action.

Some companies have developed guidelines regarding to whom deficiencies are to be reported, as illustrated in Exhibit 9.6.

Exhibit 9.6
Illustrative Deficiency Reporting Guidelines

- Deficiencies are reported to persons directly responsible for achieving business objectives affected by the deficiency
- Deficiencies are reported to the person directly responsible for the activity and a person at least one level higher
- Alternative reporting channels exist for reporting sensitive information such as illegal or improper acts
- Specified types of deficiencies are reported to more senior management
- Protocols are established for what is reported to the board of directors or a specified board committee
- Information on corrective actions taken or to be taken is communicated back to relevant personnel involved in the reporting process

Another company established criteria for deciding which deficiencies are to be reported to senior management (and depending on significance, to the board of directors), as illustrated in Exhibit 9.7.

Exhibit 9.7
Illustrative Criteria for Reporting to Senior Management

Deficiencies will be reported where the likelihood of an event occurring is not insignificant, and the impact is such that there could be a resulting:

- Adverse impact on safety of staff or others
- Illegal or improper act
- Significant loss of assets
- Failure to achieve key objectives
- Negative effect on the entity's reputation
- Improper external reporting

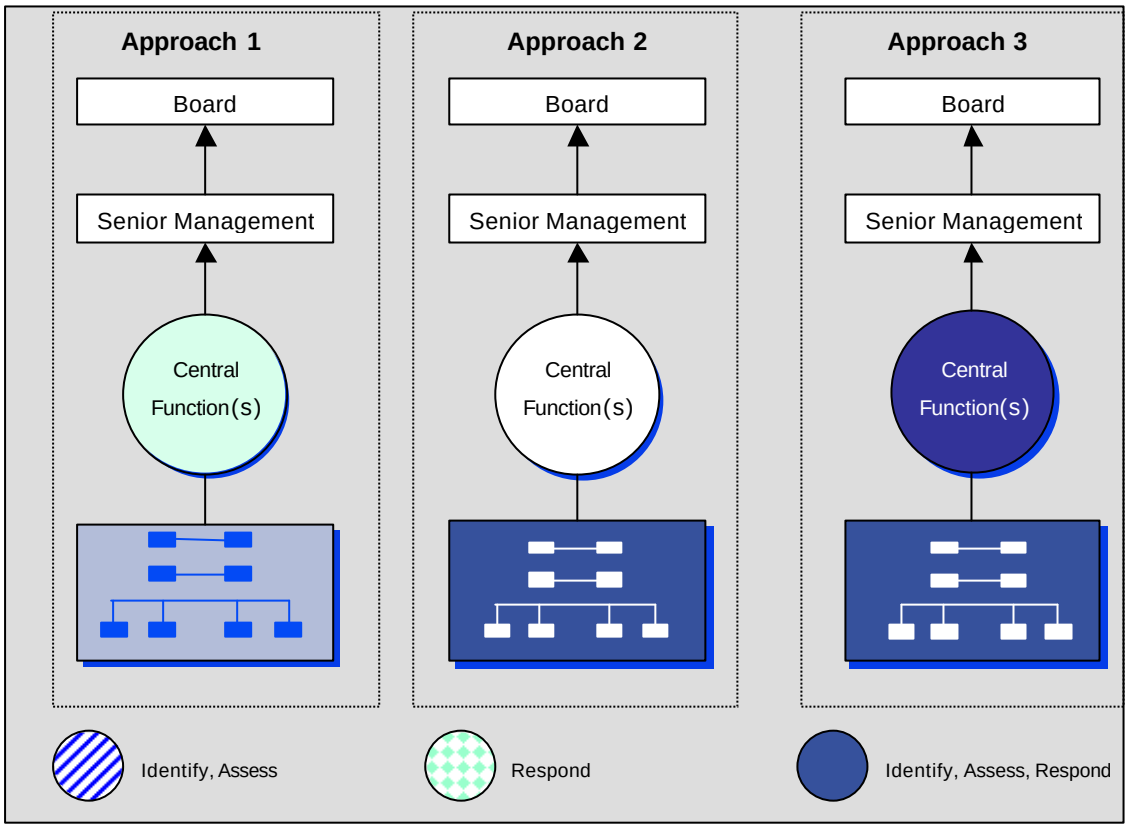
10. ROLES AND RESPONSIBILITIES

Framework 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 support the risk management philosophy, promote compliance with the risk appetite, and manage risks within their spheres of responsibility consistent with risk tolerances. Other personnel are responsible for executing enterprise risk management in accordance with established 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, but they are not responsible for the effectiveness of the entity's enterprise risk management.

This chapter illustrates organizational approaches for assigning roles and responsibilities for enterprise risk management, and provides guidance on the roles and responsibilities of the board of directors, chief executive officer, chief risk officer, business unit management, and internal audit, as well as relevant board and management committees.

A defining characteristic of how enterprise risk management is implemented is the extent to which roles and responsibilities are clearly defined, and whether they are assigned on a centralized or decentralized basis. While how this is done varies widely by entity, commonalities can be observed. Exhibit 10.1 depicts three approaches, each with a different degree to which roles and responsibilities are or are not centralized for identifying, assessing, responding to, and reporting on risks.

Exhibit 10.1
Organizational Approaches



Approach 1 depicts a model where event identification and risk assessment occur in the business lines or departmental management, but authority to determine risk response and related control activities rests with the center, and the center also reports risks upstream. This approach may work for smaller entities where central management has clear sight lines into the business activities, and key decision authorities remain with the center. Approach 2 depicts a model where event identification, risk assessment, risk response, control activities, and reporting are primarily the responsibility of the business lines. The center is involved in monitoring the process and might have a broad-based role in reporting as well. Approach 3 is a variation on Approach 2, illustrating that certain risks may be addressed at the center, such as entity-wide risks of commodity or foreign currency price movements that are tracked and managed at the entity level. Each of these approaches has benefits and challenges, described in Exhibit 10.2.

Exhibit 10.2
Benefits and Challenges of Organizational Approaches

Approach		
1	**2**	**3**
Benefits		
• Effective event identification and risk assessment by those closest to emerging issues • Risk responses determined by higher-level managers	• Ownership of risk response and control activities by managers closest to emerging issues • Ability to generate more complete management information • Enhanced ability to manage risk-based activities	• More significant risks addressed by higher-level managers • Facilitates managing risks on entity-wide basis
Challenges		
• Might be disconnect between risk assessment and response • Lack of ownership by risk takers in risk response	• Potential for less-consistent risk management (but this potentiality is reduced by an effective central support/monitoring function)	• Requires effective communication and coordination with business units

Many companies find that as they expand in size and complexity, they can most effectively apply enterprise risk management principles and disciplines by pushing much, if not all, responsibility to the lines of business and functional support units. At the same time, a small central supporting infrastructure deals with more pervasive, entity-wide risks.

Board of Directors

The board provides oversight with regard to enterprise risk management.

The board has a key role in the oversight of enterprise risk management. The board should be apprised on a timely basis of the most significant risks, management's assessment, and its planned response. Importantly, the board should feel comfortable that appropriate processes are in place and that management is positioned to identify, assess, and respond to risk, and to bring relevant information to the board level.

The types of questions directors ask in performing this oversight role are illustrated in Exhibit 10.3.

Exhibit 10.3
Questions Raised by Boards Regarding Enterprise Risk Management

- What information about the risks facing the organization do we receive to fulfill our fiduciary and advisory governance responsibilities?
- When and how does senior management report risk information to us?
- How do we know that the information we receive on risks and risk management is accurate and complete for our purposes?
- Have we effectively communicated our expectations to senior management concerning the company's risk management process, and is there a clear understanding of those expectations, including what information we expect to receive?
- How do we ensure that the organization is performing according to established risk tolerance limits and overall risk appetite?
- How do we as a board help establish the right "tone at the top" that reinforces the organization's values and promotes a "risk aware culture"?
- Are we effectively carrying out our responsibilities as a board in overseeing risk management?

Boards may choose to delegate responsibilities and accountabilities for specified aspects of enterprise risk management to one or more board committees to help ensure a clear focus on the risk areas.

Audit Committee

It is not uncommon for oversight responsibility for enterprise risk management to be assigned to the audit committee. In many cases it is believed that with its focus on internal control over financial reporting, and possibly a broader focus on internal control, the audit committee already is well positioned to expand its responsibility to overseeing enterprise risk management. Some observers point to certain regulatory standards as providing support for placing responsibility with this committee. See Exhibit 10.4 for an excerpt from the New York Stock Exchange's rules.

Exhibit 10.4
Audit Committee Role

The New York Stock Exchange's Corporate Governance Rules require that a listed company's audit committee have a written charter that addresses the committee's duties and responsibilities, which must include discussing policies with respect to risk assessment and risk management. The rules' commentary notes:

While it is the job of the CEO and senior management to assess and manage the company's exposure to risk, the audit committee must discuss guidelines and policies to govern the process by which this is handled. The audit committee should discuss the company's major financial risk exposures and the steps management has taken to monitor and control such exposures. The audit committee is not required to be the sole body responsible for risk assessment and management, but, as stated above, the committee must discuss guidelines and policies to govern the process by which risk assessment and management is undertaken. Many companies, particularly financial companies, manage and assess their risk through mechanisms other than the audit committee. The processes these companies have in place should be reviewed in a general manner by the audit committee, but they need not be replaced by the audit committee.

Risk Committee

The New York Stock Exchange rule commentary states that some companies assign board-level risk management oversight responsibility to other than the audit committee, and some organizations indeed have determined that tasking the audit committee with oversight of entity-wide risks in non-financial areas (e.g., operational, compliance) exceeds the intended authority of the audit committee and its available resources. Some boards have established a risk committee to focus directly on enterprise risk management. A description of one company's board risk committee is provided in Exhibit 10.5. In this case, senior members of management attend the committee's meetings, and the committee's responsibilities reflect that it works with management in dealing with such matters as developing and refining the enterprise-wide risk appetite and risk tolerances.

Exhibit 10.5
Risk Committee Description

Objectives

The Board of Directors (exercised through the Risk Committee) recognizes its responsibility for ensuring that a comprehensive Risk Management system which includes policies, programs, measures and competencies for identifying, assessing and managing risk needs to be in place to assist senior management in managing growth in a rapidly changing environment.

In this regard, the specific objectives of the Committee include ensuring that:

- Management understands and accepts its responsibility for identifying, assessing and managing risk
- Senior Management and business unit management are strategically focused on the enterprise-wide risk strategy

- Leading tools and processes are provided to the businesses to facilitate achievement of their Risk Management responsibilities
- Business unit risk assessments are performed periodically and completely
- Business unit risk mitigation activities are successful in:
  - safeguarding assets
  - maintaining appropriate standards regarding the environment and health and safety issues
  - meeting legal and regulatory obligations
  - reinforcing the values of the organization by focusing on stakeholder needs
- Proper accounting records are being maintained, appropriate accounting policies have been adopted and financial information is comprehensive and accurate
- Effective risk mitigation/control testing programs are in place and the results evaluated and acted upon

Responsibilities

The Risk Committee's responsibilities include the following:

- Oversee development of and participation in an annual enterprise-wide risk strategy analysis
- Develop and refine the enterprise-wide appetite/tolerance for risk
- Provide direction and oversight to the Chief Risk Officer and the Global Risk Leaders
- Evaluate material risk exposures and report to Board
- Evaluate enterprise-wide risk exposure report
- Evaluate enterprise-wide risk trending report and ensure corporate strategy is responsive to issues raised
- Oversee the role and responsibilities of the Internal Audit Team
- Review semi-annual and annual consolidated accounts

Materiality and Focus

The Committee is charged with ensuring that the competency for identifying, assessing and managing risk continues to evolve in relation to the growing risk appetite of the organization. To that end, it will focus primarily on the effectiveness of enterprise risk management.

The Committee should review those risks which may be deemed material through agreement between the Committee and the Chief Risk Officer. Materiality considerations will be based upon both immediate financial exposure to the organization's shareholders and long term material financial exposure to the organization's shareholders.

The goal of the Committee is to encourage broader thinking by management in relation to risks so that greater focus is applied to continue to evolve the organization's competencies along their risk management vision.

Structure and Membership

- Members of the Committee will be appointed by resolution of the Board
- The Committee will comprise four non-executive Board directors, one of whom will be appointed to chair the Committee

Meetings

- Meetings will be held quarterly prior to Board meetings
- The General Counsel & Secretary will attend all Committee meetings and will act as Committee Secretary. The Chief Risk Officer and the CFO will also attend all Committee meetings
- A report of the meeting will be presented to the next Board meeting following each Committee meeting

Management

Management is directly responsible for all activities of an entity, including enterprise risk management.

Chief Executive Officer

The chief executive's responsibilities include seeing that all components of enterprise risk management are in place.

The chief executive has ultimate ownership responsibility for enterprise risk management. The CEO generally fulfills these responsibilities by providing leadership and direction to senior managers and by setting broad-based policies reflecting the entity's risk management philosophy and risk appetite.

A number of chief executive officers have identified a senior executive to provide direction, under the auspices of the CEO, to the organization on enterprise risk management implementation. Some CEOs have established a committee to provide this direction. Another approach, which is being used by an increasing number of companies, is to establish a chief risk officer to provide direction, guidance, and support to and monitoring of line managers in effecting enterprise risk management.

Enterprise Risk Management Executive Committee

In some large organizations, the CEO has established an enterprise risk management committee of senior executives, consisting of a subset of senior management, including functional managers such as the chief financial officer, chief audit executive, chief information officer, and others.

Functions and responsibilities of the committee include such matters as:

- Overall responsibility for the enterprise risk management process, including the processes used to identify, assess, respond to, and report on risk
- Defining roles, responsibilities, and accountabilities at the executive and senior management level
- Providing policies, frameworks, methodologies, and tools to business units for the identification, assessment, and management of risks
- Reviewing the company's risk profile
- Reviewing performance measures against tolerances and recommending corrective action where appropriate
- Communicating the risk management process to the CEO and the board

The responsibilities of one enterprise risk management committee are outlined in an excerpt from a sample charter, shown in Exhibit 10.6.

Exhibit 10.6
Enterprise Risk Management Committee Charter

The Enterprise Risk Management Committee determines the corporate objectives, risk appetite and aggregate risk tolerance levels. It oversees the process by which business unit management identifies and assesses risks and determines appropriate responses. It addresses enterprise-wide risks, and sets performance measure goals and key risk indicators for those risks. It is responsible for capital allocations, capital planning, and risk capital allocation and overrides. The committee also reviews capital usage and actual risk management performance versus plan.

Chief 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.

Companies that have a chief risk officer (CRO) position tend to be larger and more complex enterprises. An alternative to creating this position is to assign this role to a senior officer, such as chief financial officer, general counsel, or chief compliance officer. Some companies that initially chose this approach found over time that the breadth and scope of dealing effectively with risk require more time and effort than senior officers have available, and have moved to establishing a CRO resource.

A model for the CRO that a number of companies have found successful begins with establishing clarity around the risk officer's responsibilities and accountabilities. While some companies assign direct responsibility for effective risk management to the CRO, many others have found success by maintaining responsibility for risk management with line and functional unit leaders, with the risk officer having important directional, support, and monitoring responsibilities. Experience shows that success also depends on the CRO having

the appropriately high stature within the organization, as well as necessary resources. Some companies provide CRO staff within subsidiaries, business units, and departments, to ensure CRO staff support is close to the entity's operating activities.

One company's CRO job description, which outlines key responsibilities, is illustrated in Exhibit 10.7.

Exhibit 10.7
Chief Risk Officer Job Description

Reports to:
Chairman – Risk Committee of the Board, and CEO

Direct Reports:

- Global Risk Leaders, Group-wide Risk Specialists (pertaining to risk matters)
- Business Unit Risk Coordinators, Internal Audit

Responsibilities:

- Enable the Risk Committee of the Board to fulfill its responsibilities as stated in its Charter
- Communicate and manage the establishment and ongoing maintenance of enterprise risk management pursuant to the Corporation's risk management vision
- Ensure proper risk management ownership by Business Unit CEOs and effective oversight by the Regional/Business Boards
- Validate that enterprise risk management is functioning in each Business Unit and that all significant risks are being recognized and effectively managed in a timely manner
- Communicate with the Risk Committee regarding the status of enterprise risk management
- Promote the enterprise risk management model to the CEO and Business Unit heads and assist in integrating into their business plans and ongoing reporting
- Ensure a risk management capability is developed and maintained in all Business Units and enterprises, including new acquisitions and joint venture investments

Specific Activities:

- Develop integrated procedures to report major risks
- Regularly visit business units and meet with senior executives to promote imbedding risk management into culture and daily activities
- Develop a standardized risk information model and automated process and ensure it is usable across the organization
- Maintain a cost–benefit focus on enterprise risk management
- Ensure employees are educated about risk management. Transfer knowledge and information and generally assist in the efficient management of risk and help maintain an appropriate risk culture
- Work with business unit leaders to ensure business plans and budgets include risk identification and management
- Work with Business Units to ensure monitoring and reporting to ensure compliance with the organization's standards and reporting of the most significant risks

- Report to the Risk Committee regarding the:
  - Progression of enterprise risk management and its implementation
  - Identified significant and material risk exposures and recommendations across the organization
  - Consolidated enterprise risk management plan encompassing analysis and recommendations

Professional Attributes:

- Foundation in enterprise risk management
- Ability to clearly demonstrate grasp of tenets of the organization's enterprise risk management infrastructure
- Creative, "out of the box" thinker
- Experience globally with differing cultures
- Good executive presence
- Exceptional interpersonal communication skills
- Able to demand respect from Board and Business Units
- Senior management experience, i.e., member of executive team responsible for a large group of people, or CFO or COO experience
- Excellent presentation skills, articulate
- Superior facilitation competencies
- Large project management experience
- Strong analytical capabilities
- Exceptional problem-solving skills

The CRO job description for a financial services company, with a somewhat more operational focus, is illustrated in Exhibit 10.8.

Exhibit 10.8
Chief Risk Officer Job Description, Financial Services Company

Responsibilities:

- Establish the corporate-wide risk limits
- Approve risk taking authority, capital allocation and limit setting based on a business unit's:
  - Absolute and risk-adjusted performance
  - Risk profile and strategy
  - Earnings quality/consistency
  - Efficiency of capital usage
  - Diversification benefits or disadvantages
  - Reliability and competence of management
- Establish and maintain corporate-wide risk management standards, such as standards for:
  - Business unit policies and limit frameworks
  - Corporate risk data requirements
  - Reporting to business managers, senior management and the Board
  - Valuation and risk measurement methodology

- Review and approve policy exceptions
- Establish a risk reporting framework including consistent risk-adjusted profitability measurement, analysis and decision-making tools
- Aggregate and analyze common risk factors across business lines (e.g., stress testing/scenario analysis)
- Conduct macro assessments of the risk profile and the drivers of change
- Support management of stakeholder relations

Required Skills:

- Ability to serve as an advisor to and partner of the CEO, CFO and COO
- In-depth industry experience
- Integrity and credibility necessary to communicate with business leaders, regulators and other stakeholders
- Comprehensive risk management experience with an excellent grasp of market risk, credit risk and operational risk issues
- Excellent managerial skills able to motivate and lead a diverse group of professionals with varying backgrounds
- Excellent oral communication skills able to interact with Board members and business leaders
- Quick thinker with polished presentation skills able to communicate with external stakeholders such as regulators, investors and the financial press
- Strong and effective negotiating skills necessary to arbitrate/adjudicate business unit demands for corporate capital (financial and human)
- Strategic thinker able to navigate rapidly changing technology and competitive landscape
- Firsthand experience in lending and/or credit approval extremely desirable
- Ability to effectively formulate policy necessary to meet strategic objectives

Management

Senior managers in charge of organizational units have responsibility for managing risks related to their units' objectives.

Heads of line business units, business processes, and functional departments are responsible for identifying, assessing, and responding to risk relative to meeting the unit's objectives. They ensure that processes utilized are in compliance with the entity's enterprise risk management policies and that their unit's activities are within established risk tolerance levels.

In some companies the job descriptions of these leaders explicitly outline their enterprise risk management responsibilities, as well as associated performance measures. Unit leaders typically report on progress and issues to the CRO and/or another executive.
Unit leaders naturally delegate responsibility for specific business unit enterprise risk management activities to managers in their units, with responsibilities addressing such matters as:

- Complying with enterprise risk management policies and developing techniques tailored to the unit's activities
- Applying enterprise risk management techniques and methodologies to ensure risks are appropriately identified, assessed, responded to, reported on, and monitored
- Ensuring risks are managed on a daily basis
- Providing unit leadership with complete and accurate reports regarding the nature and extent of risks in the business activities

As with unit leaders, some companies' staff job descriptions outline their enterprise risk management responsibilities and associated performance measures.

Internal Auditors

In many companies, internal auditors play a key role in the ongoing functioning of enterprise risk management by providing objective monitoring of its application and effectiveness. Internal auditors may conduct examinations for the purpose of providing an objective assessment of the entire enterprise risk management process or subsets thereof. In this role, internal auditors may support management by providing assurance on the:

- Enterprise risk management processes – both design and function
- Effectiveness and efficiency of risk responses and related control activities
- Completeness and accuracy of enterprise risk management reporting

Internal auditors sometimes act in a consulting role, where they serve to facilitate improvements in the organization's enterprise risk management process. In this capacity, internal auditors may, among other activities, promote development of a common understanding of enterprise risk management, coach management on enterprise risk management concepts, facilitate risk-based workshops, and provide tools and techniques to help managers analyze risks and design control activities.

ACKNOWLEDGMENTS

The COSO Board, Advisory Council, and PricewaterhouseCoopers LLP gratefully acknowledge the many individuals who gave their time and energy to participating in and contributing to various aspects of the application techniques. Also recognized are the considerable efforts of the COSO organizations and their members who responded to surveys, participated in workshops and meetings, and provided comments and feedback throughout the development of these application techniques.

The following PricewaterhouseCoopers partners and staff provided important input to these application techniques: Dick Anderson, Jeffrey Boyle, Glenn Brady, Michael Bridge, John Bromfield, Gary Chamblee, Nicholas Chipman, John Copley, Michael de Crespigny, Stephen Delvecchio, Carlo di Florio, Scott Dillman, P. Gregory Garrison, Bruno Gasser, Suzanne Holifield, Susan Kenney, Brian Kinman, Robert Lamoureux, James LaTorre, Mike Maali, Jorge Manoel, Cathy McKeon, Juan Pujadas, Richard Reynolds, Sonny Sonnenstein, Mark Stephen, Robert Sullivan, Jeffrey Thompson, John Tomac, and Shyam Venkat. Thanks go to Myra Cleary for her editorial guidance.

Also making an important contribution to this document is Kathleen H.J. Leibfried, Senior Global Operational Risk Director, Citigroup Private Bank.