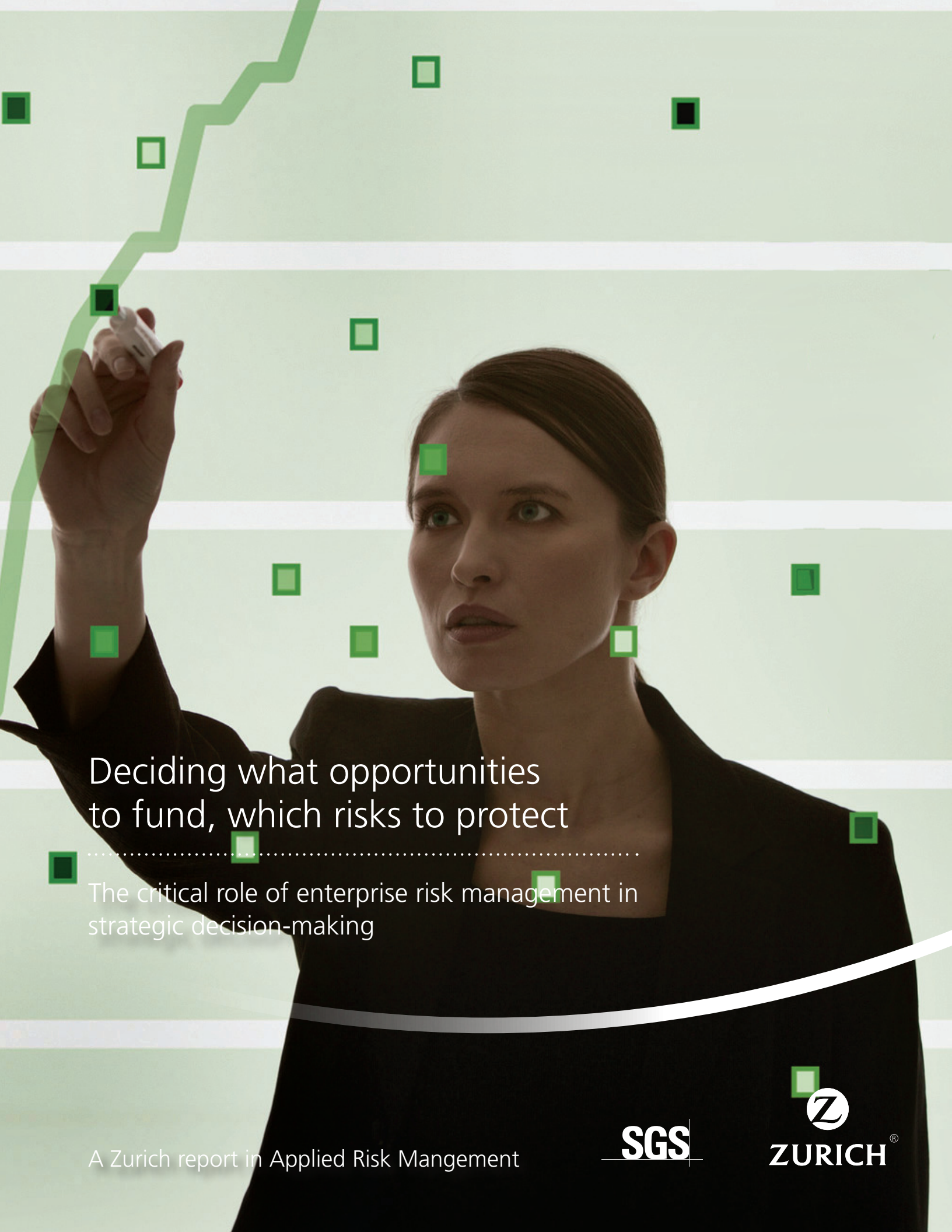


Deciding what opportunities to fund, which risks to protect

The critical role of enterprise risk management in strategic decision-making

A Zurich report in Applied Risk Mangement

SGS

ZURICH®

Table of Contents

Article authors

Linda Conrad
Director of Strategic Business Risk
Zurich Services Corporation

Chris Yau
Senior Manager
Global Products and Services Development, SGS

Enterprise Risk Management as a Strategic Planning Tool

Taking risks is a necessary part of growing a business and adding stakeholder value. An organization that operates too cautiously and misses product or market opportunities can have difficulty attracting the best talent and investor capital. While the upside of risk is the ability to strategically seize business growth opportunities, today's complex world has also revealed the downside of risks. Fragile global supply chains, technology dependence, increased speed of product cycles and complicated financial models and relationships continue to multiply the breadth and depth of risks facing organizations.

> "How can the senior management of an organization be more aware of their potential risks—both the upside and downside?"

Failure to either anticipate growth opportunities or plan for negative events can have serious consequences on business operations, including loss of customers, inadequate asset protection, failure to meet regulatory requirements, lower profitability and share price. How can the senior management of an organization be more aware of their potential risks—both the upside and downside? Recently, there has been an intensifying interest in enterprise risk management, or ERM, as a tool to enable organizations to consider the potential impact of all types of risks on their processes, products, services, activities and stakeholders. In short, an effective ERM approach can help an organization make the most efficient use of its capital. By determining what growth opportunities to fund, and what potential risks need budget support, an organization can better ensure it will meet its business objectives today and into the future.

As early as 2001, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) began efforts to develop a framework that could be used by corporations to evaluate and improve their organizations' enterprise risk management. As defined by COSO, "enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."[1]

The wide array of economic, geopolitical, environmental, technological and other risks of the last decade have heightened the call for a more rigorous risk management approach by organizations. Events like Enron and Worldcom, the Asian tsunami and Chilean earthquakes, the devalued dollar and recent credit crisis have led to the creation of new risk management standards to assist organizations in developing an ERM framework. In 2009, a new international standard was published, ISO 31000, that both expands the framework and clarifies the risk principles set out in the Australia and New Zealand standards developed in 2004 (AS/NZS 4360:2004). The new ISO 31000 defined the application of a risk management framework as a "set of components that provide the foundations and organizational arrangement for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization."[2]

1 "Strengthening Enterprise Risk Management for Strategic Advantage" Committee of Sponsoring Organizations of the Treadway Commission 2009, coso.org

2 ISO 31000 Risk management – Principles and guidelines. International Organization for Standardization, 2009. www.iso.org

External Drivers of ERM for Today's Organizations

Enhancing an organization's growth opportunities, improving financial and operational performance, and reducing losses are some of the internal drivers that spark the development of an ERM framework within organizations today. However, there are significant external drivers–primarily regulatory and legal–that are challenging organizations to formalize their risk management processes. In short, it's just becoming good business practice.

In 2004, the New York Stock Exchange issued corporate governance rules that require audit committees of listed corporations to discuss risk assessment and risk management policies. Executive compensation arrangements are a key area of regulatory attention because there is concern that these arrangements may have encouraged excessive risk-taking in the past, where there has been an undue emphasis on performance without due consideration of risks.

In July 2009, the SEC proposed rules that would require management to increase its disclosures of information that describe the overall impact of compensation policies on risk-taking. The rules would also require disclosure in a proxy statement about the board's role in the company's risk management process, and the effect that this has on the way the company has organized its leadership structure. The SEC believes that disclosure should provide information about how a company perceives the role of its board and the relationship between the board and senior management in managing the risks facing the company. SEC Chairman Mary Schapiro stated, "I want to make sure that shareholders fully understand how compensation structures and practices drive an executive's risk-taking. The Commission will be considering whether greater disclosure is needed about how a company–and the company's board in particular–manages risks, both generally and in the context of setting compensation."

> "greater disclosure is needed about how a company—and the company's board in particular—manages risks"

Last spring, Sen. Charles Schumer, D-N.Y., introduced the Shareholder Bill of Rights Act of 2009 that would require corporations to establish a risk management committee comprised of independent directors. Additionally, the U.S. Treasury Department is considering requiring compensation committees of public financial institutions to disclose strategies for aligning compensation with sound risk management. While this focus is on financial institutions, the link between compensation structures and risk-taking has implications for all organizations.

Ratings agencies and analysts have also taken a keener interest in governance efforts. In 2008, Standard and Poor's (S&P) began assessing ERM processes as part of its corporate credit ratings analysis. S&P reports that of the more than 300 discussions with rated issuers in U.S. and Europe, they have discovered a wide range in the level of adoption, formality and engagement of ERM.[3] In particular, S&P noted that:

3 "Progress Report: Integrating Enterprise Risk Management Analysis Into Corporate Credit Ratings" Standard & Poors Ratings Direct www.standardandpoors.com/ratingsdirect July 2009

- "Silo-based" risk management, focused only at the operational manager's level, continues to be prevalent.
- Companies with a true enterprise-wide approach to ERM appreciate the importance of going beyond only quantifiable risks and increasingly understand the importance of emerging risks.
- Companies often facilitate their ERM execution via separate structures, with associated roles and responsibilities clearly defined.

Corporate boards, facing heightened regulatory and ratings scrutiny, are beginning to insist that management provide sophisticated reports linking risks to their impact on an organization's objectives. Many boards are also more engaged in the oversight of management's risk monitoring processes to determine whether the risks assumed to meet performance objectives are embraced throughout the organization and within established limits. Also of interest to boards is how management's response to existing risks have either helped or hurt the long-term strategies of the organization.

Clearly, the need to create a robust ERM framework is something no senior executive team can ignore today. Risk management has moved beyond just the purview of the CFO and accounting department to become an enterprise-wide responsibility. Today, a limited approach to identifying, assessing and monitoring risks is not enough. In a recent survey of more than 200 risk professionals across a variety of global organizations, more than 62 percent of respondents reported moving beyond a basic, limited ERM, compared with only 38 percent two years earlier.[4]

> "The purpose of this broader assessment is to create a more *resilient business*—one that is better prepared to adapt to changing conditions and leverage emerging opportunities"

ERM: Less Business Continuity, More Business Resilience

Risk management is often used as a synonym with business continuity management. While the two processes share much in common and similar methods, they are different concepts. As defined in this paper, risk management identifies risks that may or may not be threatening to the continued effective operation of an organization, paying equal attention to those identified as "good" risks when associated with growth opportunities.

Business continuity management deals with factors that may cause significant business disruption or may damage the organization's reputation. It emphasizes preparing the organization for and bringing the organization back from a threatening event. In other words, business continuity management is an application of risk management in the context of threatening risks and emphasizing a timely recovery after an incident.

Enterprise risk management, on the other hand, sets down a structured framework for the organization to identify, rank and control *all the* risks concerned. The purpose of this broader assessment is to create a more *resilient business*—one that is better prepared to adapt to changing conditions and leverage emerging opportunities, as well as anticipate surprises and recover from disruptions. Effective enterprise risk management goes hand in hand with a business resilience process by creating a proactive infrastructure for dealing with risks systematically, holistically and successfully.

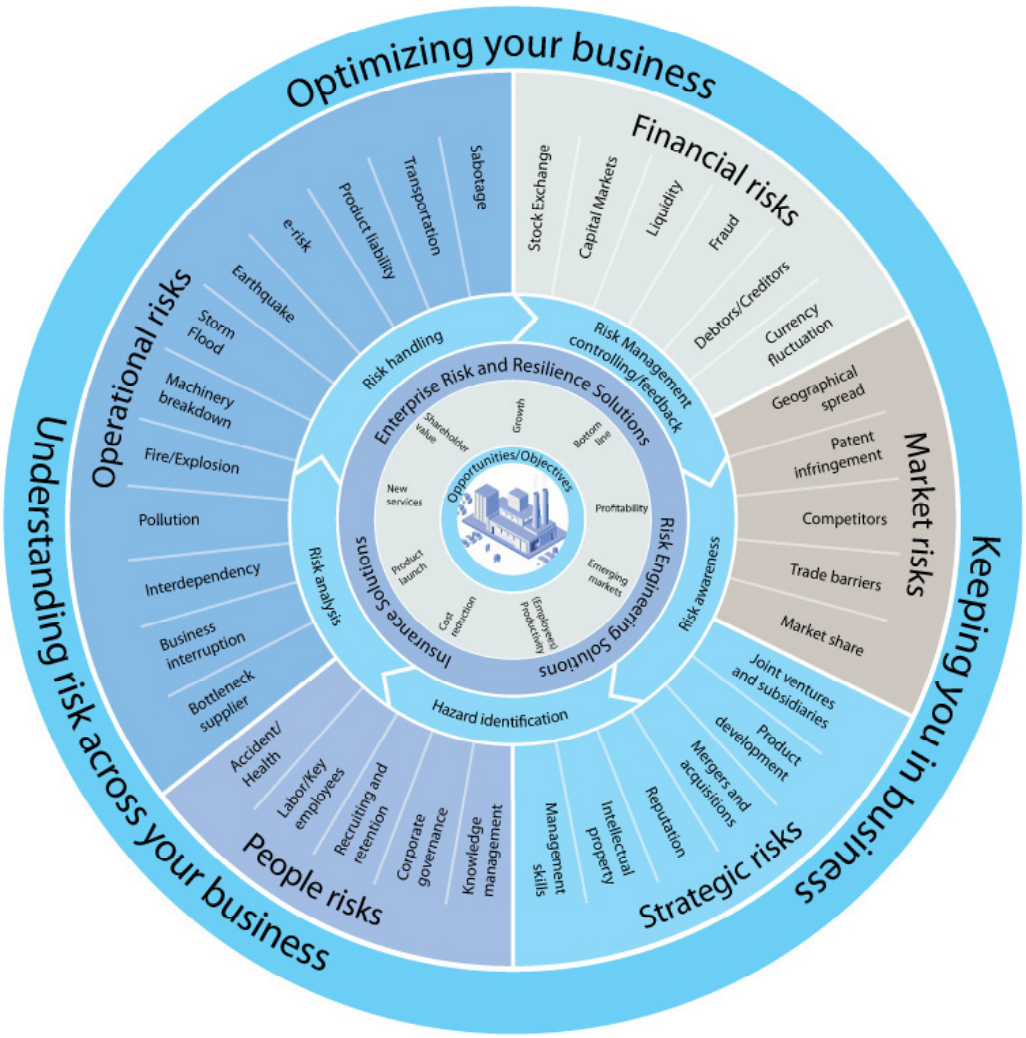
4 "2010 Global Enterprise Risk Management Survey" Aon www.aon.com

Building an ERM Framework

Effective risk management today requires an enterprise approach that views risk from all angles – a strategic, 360-degree view supported by tactical, holistic solutions. Achieving this broad view helps ensure business resilience, reduce total cost of risk and protect profitability by improving a corporation's ERM framework. To help organizations achieve a 360-degree view of their risks, Zurich Strategic Risk Services developed an Enterprise Risk Management Wheel that divides risks into four main categories:

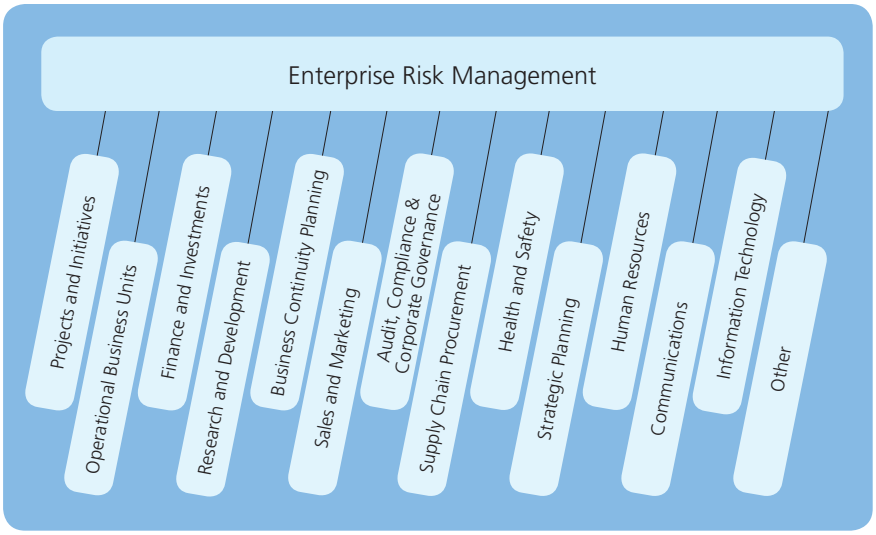
> "an organization with a holistic, 360-degree view of risk can better uncover and manage its business challenges"

Strategic **O**perational/People
Financial **M**arket



Zurich Enterprise Risk Management Wheel

As this wheel demonstrates, an organization with a holistic, 360-degree view of risk can better uncover and manage its business challenges, including operations and procedures, management styles and strategies, industry issues, emerging risks and more. ERM can provide the framework for identifying both threats and opportunities across the enterprise, assessing them in regard to probability and possible impact, developing a response strategy and monitoring the achievement of objectives.



ERM in Action

Over the past five years, Zurich's operational risk capital efficiency has improved through a strengthening of its ERM process, which includes the introduction of an operational risk management framework. This framework provides Zurich with risk management tools to specifically identify, assess, manage and quantify operational risks. Through this framework and the wider ERM process, Zurich increases its ability to achieve efficiency and effectiveness gains. This allows Zurich to better focus on optimizing company resources and in turn decide what opportunities to fund.

For example, one business unit experienced a reduction of 21.7 percent in operational risk-based capital consumption when Zurich moved from an asset-based approach to its current, risk-based approach for operational risk quantification. The business unit management then identified areas of high-risk exposure, performed a deeper assessment and developed measures to mitigate the exposures. As a result, in the following year the unit experienced an additional reduction of 28.9 percent in operational risk capital consumption. The operational risk capital not consumed was then available to fund profitable growth for Zurich.

A 360-degree ERM process can help organizations meet these strategic objectives:

- **Protecting the capital base –** An ERM review can potentially drive meaningful financial benefits including reduced cost of servicing debt, improved access to capital and cost of capital.
- **Enhancing value creation and contribute to optimal risk return profile** ERM can increase probability of the upside, and decrease the probability of a downside.
- **Supporting corporate decision-making process** For senior management, ERM can demonstrate its incorporation of risk information as a decision-making process, especially for rated companies that need to score well on the S&P ERM assessment.
- **Protect reputation and brand by promoting a sound culture of risk awareness** ERM can increase investor confidence through proven management accountability for risk.

In 2008, Zurich's report on applied risk management developed for risk managers[5] after the credit crisis summarized the lessons learned from the failures of those companies that did not perform a strategic, risk management process:

1. **Understanding individual risks are not enough –** Organizations must account for inter-linkages and remote possibilities
2. **Extreme events must be factored in –** The world does not follow a normal, even distribution, and "Black Swans" can appear at any time
3. **Determine the corporate risk appetite –** The strategic function of ERM is to guide corporations in determining their choice of trade-offs between risk and reward
4. **Quantitative models are important, qualitative judgments are imperative –** The arsenal of risk management tools is lengthy, but models cannot replace judgment
5. **A risk culture starts at the top –** To entrench risk management across an organization takes a strong, top-down approach applied across the organization

Creating a Risk Management Policy

What's clear from these lessons is that the important tasks of determining corporate risk appetite and deploying qualitative judgments must be sanctioned by those at the very top—senior management and the board. In order to provide this type of "top-down" guidance, many organizations issue a risk management policy each year. The benefits are many to creating this type of policy, but include keeping the overall risk management approach in line with current best practice, focusing on the intended benefits for the coming year, identifying the risk priorities and ensuring that appropriate attention is paid to emerging risks.

In a report, "A structured approach to ERM and the requirements of ISO 31000," issued by the Public Risk Management Association in the U.K. in early 2010, a risk management policy structure was included that can help corporations ensure their ERM approach is updated and disseminated throughout the organization each year. The following sections were recommended in developing an ERM policy:

- Risk management and internal control objectives (governance)
- Statement of the attitude of the organization to risk (risk strategy)
- Description of the risk aware culture or control environment
- Level and nature of risk that is acceptable (risk appetite)
- Risk management organization and arrangements (risk architecture)
- Details of procedures for risk recognition and ranking (risk assessment)
- List of documentation for analyzing and reporting risk (risk protocols)
- Risk mitigation requirements and control mechanisms (risk response)

5 "Dealing with the Unexpected: Lessons for risk managers from the credit crisis: A Zurich Report in Applied Risk Management, Zurich 2008

- Allocation of risk management roles and responsibilities
- Risk management training topics and priorities
- Criteria for monitoring and benchmarking of risks
- Allocation of appropriate resources to risk management
- Risk activities and risk priorities for the coming year

Technology Support of ERM

For many organizations, the top-down commitment required of an ERM program can be the difficult aspect to embed. Effective utilization of technology can support this objective, and while it cannot replace a good process, it can serve as an invaluable support tool.

Complex organizations often attempt to utilize common spreadsheet applications to bolster their enterprise risk management effort, with the result being a frustrating lack of functionality. Despite significant efforts to manage risk holistically, many companies fail to integrate software that can fully support ERM objectives. Utilizing ERM software can enable a company to amplify its risk management efforts and magnify its insights without creating the need to scale resources accordingly. ERM-specific software is designed to support the user through each distinct stage of the ERM cycle (including establishment of context, risk identification, risk analysis, risk evaluation, risk treatment, monitoring and review).

A software solution can support this growth by providing a solid foundation in the early stages, while including more advanced functionality to be used as appropriate along the journey. Overtime, software will enable a company to more closely align its risk appetite with its corporate strategy. In addition, it enables the company to optimize its capital allocation and reduce its total cost of risk.

> “Utilizing ERM-software can enable a company to amplify its risk management efforts”

Perhaps the biggest advantage ERM software has over traditional tools is the capability to monitor and track risks within its built-in risk register. This risk register is capable of distinguishing between corrective and preventative controls, enabling the user to compare and explore combinations of various options. The tool may also be capable of displaying the residual risk that remains after a control has been implemented, and instantly reporting on the status of a company’s risk profile in a dynamic way. Since a variety of user groups need to access risk reports, ERM software can provide a multitude of ways to make use of data depending on the strategy setting.

When choosing a software program to facilitate an ERM initiative, it is imperative that it can be seamlessly integrated into an organization. Therefore the configuration of the software must be adaptable to the company’s operating structure. The foundational ERM framework should be modeled after the ISO 31000 or similar standard, utilizing the following inputs: contexts, risks, consequences, preventative and corrective controls, triggers and mitigation activities. While it may seem insignificant, using the appropriate terminology may be the first major step towards an effective ERM program. Additional considerations when choosing an ERM software application are:

- Ease of use – can the frontline utilize the interface with minimal training?
- Relevant analysis – will the software produce impactful information?
- Prioritization – can the company's risk identification process be incorporated?
- Notification – will the software actively alert users as appropriate?

In this era, companies face substantial pressure to be transparent about risk. This becomes increasingly difficult as globalization creates a complex environment of interdependency. The trend of risks becoming more difficult to manage will certainly continue, so implementing a software tool capable of growing with the needs of the company at an early stage is critical to a valuable ERM program.

Risk Management and ISO 31000

Many modern management system standards have included risk assessment as part of the essential elements, such as ISO 14001 (environmental management), OHSAS 18001 (occupational health & safety), ISO 27001 (information security), ISO 28000 (supply chain security), ISO 22000 (food safety), ISO 14971 (medical devices), just to name a few.

While risk management is required in many international standards, the principles and guidelines of how risk management is performed are generally not discussed in detail in these standards. On November 15, 2009, the International Organization for Standardization (ISO) published the *ISO 31000:2009, Risk Management – Principles and Guidelines.* ISO 31000 is the first of the ISO 31000 series of risk management standards to be published by ISO. Also in this family of standards is:

1. *ISO Guide 73:2009 Risk Management – Vocabulary.* This standard provides the definitions of generic terms related to risk management and aims to encourage a consistent understanding of, and a coherent approach to, the description of activities related to risk management as well as terminology.
2. *ISO/IEC 31010, Risk Management – Risk Management Techniques.* This is a supporting standard for ISO 31000 offering guidelines on the selection and application of systematic techniques for risk assessment.

ISO 31000 is designed to help organizations:

- Increase the likelihood of achieving objectives
- Encourage proactive management
- Be aware of the need to identify and treat risk throughout the organization
- Improve the identification of opportunities and threats
- Comply with relevant legal and regulatory requirements and international norms
- Improve financial reporting
- Improve governance
- Improve stakeholder confidence and trust

- Establish a reliable basis for decision making and planning
- Improve controls
- Effectively allocate and use resources for risk treatment
- Improve operational effectiveness and efficiency
- Enhance health and safety performance, as well as environmental protection
- Improve loss prevention and incident management
- Minimize losses
- Improve organizational learning
- Improve organizational resilience

Although ISO 31000 provides generic guidelines, it is not the intention of the standard to promote uniformity of risk management techniques across all organizations. Rather, it is to promote the adoption of consistent processes so as to ensure the risk is managed effectively, efficiently and coherently across organizations. It provides a common approach in support of standards (e.g. ISO 27001, ISO 28000, etc.) dealing with specific risks and/or sectors. Because of the guidance nature of this standard, it is not intended for the purpose of certification. Additionally, for organizations and risk practitioners who are interested in pursuing certification, they should know that ISO 31000 by itself does not form a complete management system, i.e. it does not contain some of the management elements such as internal audit, objectives, records control, etc., that typically exist in a management system standard (e.g. ISO 9001).

> "promote the adoption of consistent processes so as to ensure the risk is managed effectively"

The ISO 31000 standard will be useful to:

- Those responsible for implementing risk management within their organizations
- Those who need to ensure that an organization manages risk
- Those needing to evaluate an organization's practices in managing risk
- Developers of standards, procedures and instructions relating to managing risk

Using ISO 31000 Standards to Create a Risk Assessment Process

An organization may consider creating a risk assessment process procedure based on ISO 31000 and assess the organization's adherence to this procedure by the organization's internal audit team or using an external certification body.

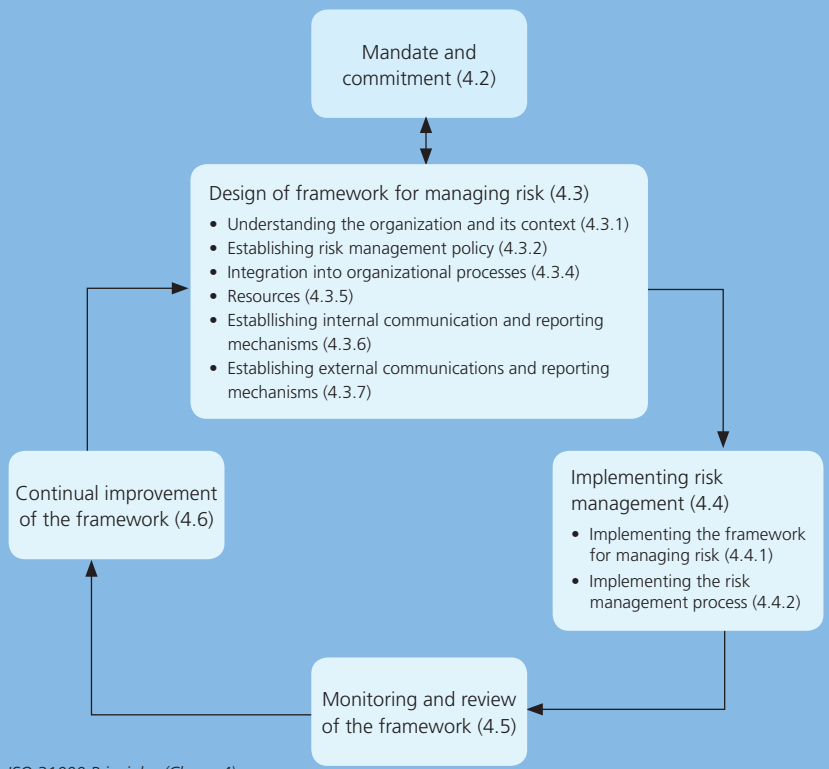
The ISO 31000 Standard consists of three main clauses, each serving a different objective in forming the Standard:

- Clause 3: Principles. The clause lists eleven principles. In order for risk management to be effective, an organization should at all levels comply with these principles:

(a) Risk management creates and protects value
(b) Risk management is an integral part of all organizational processes
(c) Risk management is part of decision making
(d) Risk management explicitly addresses uncertainty
(e) Risk management is systematic, structured and timely
(f) Risk management is based on the best available information
(g) Risk management is tailored
(h) Risk management takes human and cultural factors into account
(i) Risk management is transparent and inclusive
(j) Risk management is dynamic, iterative and responsive to change
(k) Risk management facilitates continual improvement of the organization

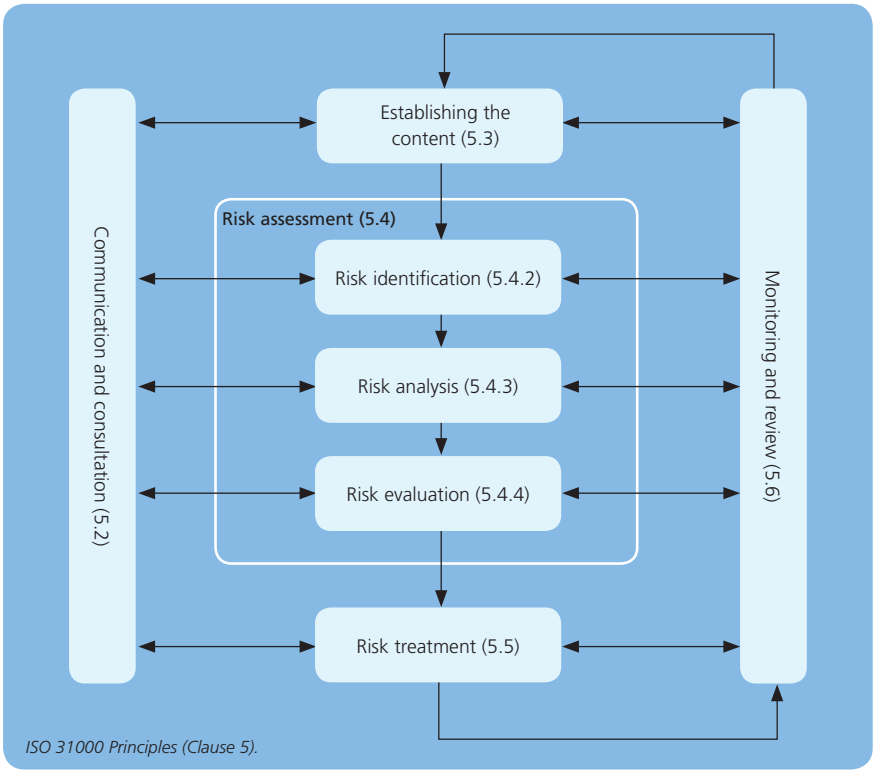
ISO 31000 Principles (Clause 3).

- **Clause 4: Framework.** The framework adds the Plan-Do-Check-Act model to the risk management process. By having the framework structure, the standard allows an organization to integrate risk management into the organization's overall management system. The organization may review its own risk management process and consider adopting this framework if necessary. This framework structure is new to ISO 31000 (compared to AS/NZS 4360:2004). The clauses and interrelation between the framework elements are illustrated below:



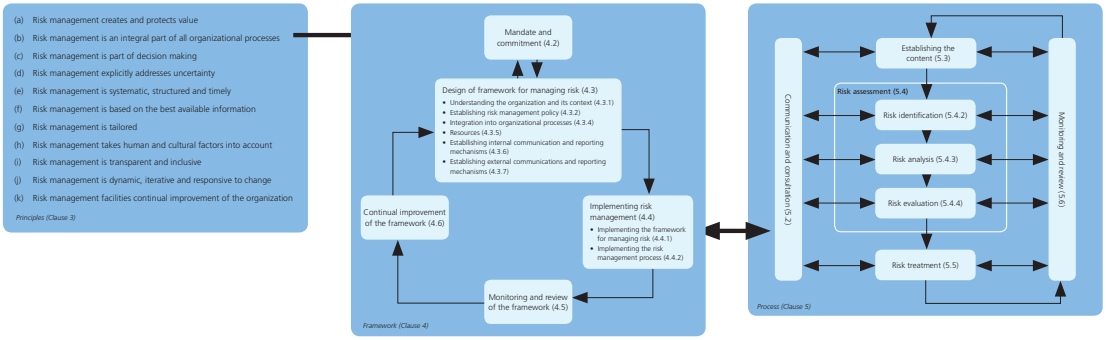
ISO 31000 Principles (Clause 4).

- **Clause 5: Process.** The Process stipulates processes an organization would undertake during implementation. This clause adopts the classic risk identification / risk assessment / risk treatment cycle from AS/NZS 4360:2004 shown here:



ISO 31000 Principles (Clause 5).

- The relationship between the principles for managing risks, the framework in which it occurs and the risk management processes described in these three building blocks above is shown here:



ISO 31000: Relationships between the risk management principles, framework and process.

The Strategic Benefits of ERM

The benefits of developing a new ERM framework or improving upon an existing, more basic, one include:

- Minimizing barriers to achieving objectives and maximizing strategic growth opportunities
- Reducing variability in expected business outcomes to enhance value creation advantage
- Generating superior business intelligence to enable improved strategic decision making
- Decreasing total cost of capital through optimizing the balance of risk and opportunity
- Identifying key exposures, quantifying critical activity and solidifying value chains
- Demonstrating the benefit of increased risk transparency across your organization
- Using additional risk information to improve risk transfer and decrease negative events
- Protecting tangible and intangible assets to minimize impact on bottom-line profitability

> "a leading global not-for-profit management research organization, showed that a strong ERM program is a factor in increasing revenue and shareholder value"

A study of more than 270 organizations by The Conference Board[6], a leading global not-for-profit management research organization, showed that a strong ERM program is a factor in increasing revenue and shareholder value. According to the survey respondents, the incorporation of a sophisticated risk management program yielded increased management accountability, smoother governance practices, increased profitability, reduced earnings volatility and better informed decisions based on risk intelligence.

Clearly, managing risk can no longer be left to one person such as a Chief Risk Officer or siloed into one department, but demands a transparent approach to strategic decisions and daily operations. ERM can encourage resilience and protect profitability in an ever-changing business climate. Applied robustly across all areas of an organization, a strategic ERM process will efficiently manage available capital—budgeting for potential risks, while funding the appropriate growth opportunities.

Sources:

- "Enterprise Risk Management: Complacency Is No Longer an Option, But a Practical Start Is" 2006, KPMG, www.kpmg.com
- "Effective Enterprise Risk Management Starts with a Conversation" American Institute of Certified Public Accountants, September 2009, www.aicpa.org
- ISO 31000 Risk management – Principles and guidelines. International Organization for Standardization, 2009, www.iso.org
- "Strengthening Enterprise Risk Management for Strategic Advantage" Committee of Sponsoring Organizations of the Treadway Commission, 2009, www.coso.org

6 "From Risk Management to Risk Strategy" Report #1363 The Conference Board www.conference-board.org

- "Progress Report: Integrating Enterprise Risk Management Analysis Into Corporate Credit Ratings" Standard & Poors Ratings Direct, www.standardandpoors.com/ratingsdirect, July 2009
- Christina, Diana. "Dissecting the Anatomy of ISO 31000," http://dianechristina.wordpress.com/2010/02/05/dissecting-the-anatomy-of-iso-31000/
- Committee of Sponsoring Organization of the Treadway Commission. "Enterprise Risk Management – Integrated Framework: Executive Summary" Sept. 2004, Good Practice Guidelines 2008, Business Continuity Institute

Strategic Risk Services - Zurich Services Corporation

Zurich's Strategic Risk Services helps organizations improve their business performance through an Enterprise Risk Management approach to strategic, operational and financial exposures. This broad, 360° view helps businesses ensure resilience, reduce total cost of risk, protect profitability and enhance capital efficiency. Applying this risk management approach to its own business, Zurich Financial Services Group was recently upgraded by Standard & Poor's Corporation and its risk-based capital adequacy deemed "strong."*

SGS Worldwide

SGS is the world's leading inspection, verification, testing and certification company. Recognized as the global benchmark for quality and integrity, SGS employs over 55,000 people and operates a network of more than 1,000 offices and laboratories around the world. Headquartered in Geneva, Switzerland, SGS helps customers operate in a more sustainable manner by improving quality and productivity, reducing risk, verifying compliance and increasing speed to market.

Zurich

1400 American Lane, Schaumburg, Illinois 60196-1056
800 382 2150 www.zurichna.com

The information contained in this document represents the current view of the authors on the issues discussed as of the date of publication. Because the authors must respond to changing market conditions, it should not be interpreted to be a commitment on the part of the authoris, and the authors cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. The authors make no warranties, express, implied or statutory, as to the information in this document.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of SGS and Zurich Services Corporation.

SGS and Zurich Services Corporation may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from SGS and Zurich Services Corporation, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Any reproduction, adaptation or translation of this document without prior written permission is prohibited, except as allowed under the copyright laws. ©SGS SA 2010. All rights reserved. ©2010 Zurich Services Corporation. All rights reserved.

* For information about the ratings of Zurich American Insurance Company, access the ratings section on www.zurichna.com. For more complete financial information about the Zurich Financial Services Group and ratings for Zurich Insurance Company Ltd., access www.zurich.com

A1-19022-A (09/10) 10-1455

Zurich HelpPoint

Here to help your world.

ZURICH®

Because change happenz™