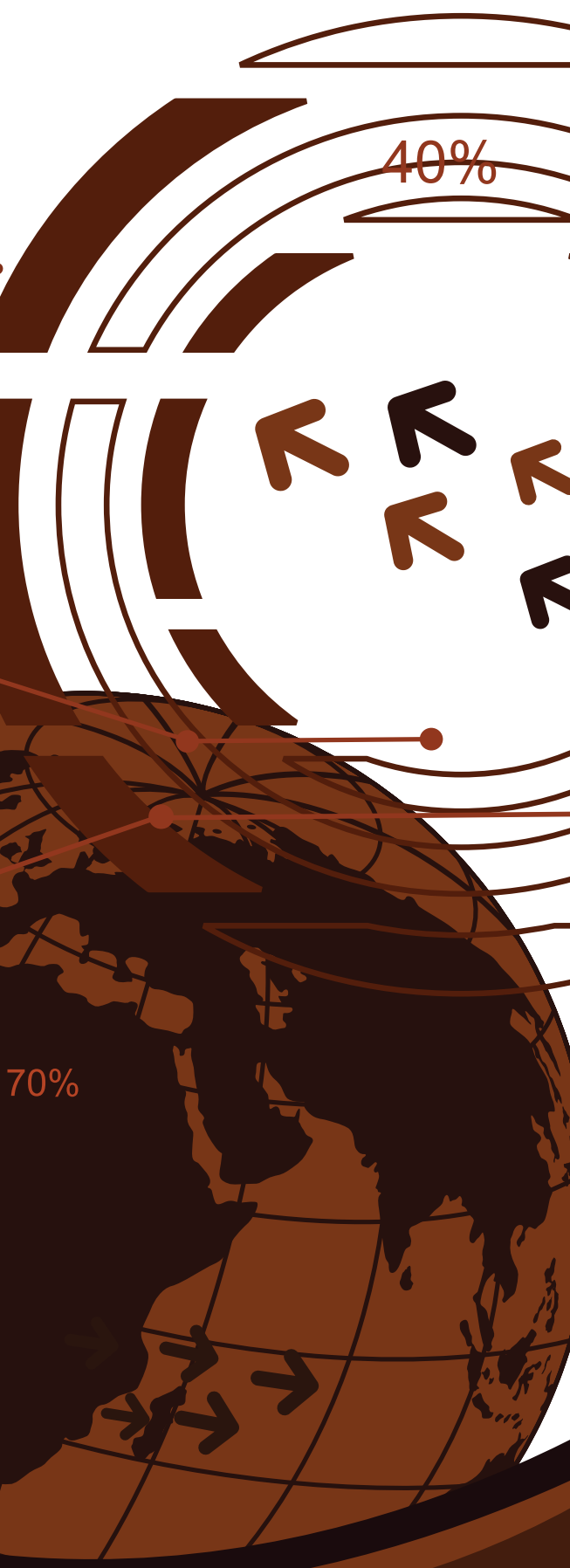




AN OVERVIEW OF WIDELY USED RISK
MANAGEMENT STANDARDS AND GUIDELINES

A Joint Report of RIMS Standards and Practices Committee and RIMS ERM Committee



AN OVERVIEW OF WIDELY USED RISK MANAGEMENT STANDARDS AND GUIDELINES

CONTRIBUTORS

GRACE CRICKETTE

Chief Risk Officer, University of California

KRISTEN DROBNIS

Senior Vice President, Risk Management, Massachusetts Development

RYAN EGERDAHL

Enterprise Risk Manager, Bonneville Power Administration

CAROL FOX

Director of Strategic and Enterprise Risk Practices, RIMS

DOROTHY GJERDRUM

Executive Director, Arthur J. Gallagher Risk Management Services, Inc.

ROBERT GOFOURTH

Vice President of Professional Services, Insite Managed Solutions

YVETTE HO SANG

Risk Management Analyst, Institute of Electrical and Electronic Engineers

RUSSELL MCGUIRE

Senior Consultant, Milliman Risk Advisory Services

MICHAEL MILLER

Director, Risk Assessment & Mitigation, American Broadcasting Companies, Inc.

MARY PETER

Director of Enterprise Risk Management, Eide Bailly LLP

DREW ZAVATSKY

Loss Prevention Coordinator, State of Washington

WITH THANKS

PETE FAHRENTHOLD

Chair, RIMS ERM Committee

MANUS (CHRIS) O'DONNELL

Chair, RIMS Standards and Practices Committee

MARY ROTH

Executive Director, RIMS

INTRODUCTION

Online searches for information on risk management, particularly enterprise risk management, result in more than 20 million references. Wading through the competing standards, frameworks and regulatory guidelines can be a daunting task.

This report is intended to provide the user with a view of six widely used risk management standards, guidelines and self-described “best practices” to help identify common elements in each. We have utilized the attributes from the RIMS Risk Maturity Model for Enterprise Risk Management (RIMS RMM) as the basis for evaluating the common elements and to differentiate among the various documents.

In the context of this report, we define a **primary (or “recognized”) standard** as an established norm or requirement, usually a formal document that establishes criteria, methods, processes and practices under the jurisdiction of an international, regional or national standards body. By contrast, a **de facto standard** is a custom, convention, guidance document, framework, company product or corporate standard that may be developed outside of a recognized standard-setting body but which becomes generally accepted and dominant. In this report, we also use the term **framework** as 1) a structure for supporting the organization’s strategic and operational objectives, and as 2) a system or group of interacting, interrelated, or interdependent elements, such as ideas, principles, methods or procedures, that form a complex whole.

We purposefully limited this review to the following standards and guidelines as we believe that they have been adopted most widely by RIMS member organizations, whether in full or in a modified version:

[ISO 31000: 2009](#)
Risk Management - Practices and Guidelines

[OCEG “Red Book” 2.0: 2009](#)
GRC Capability Model

[BS 31100: 2008](#)
Code of Practice for Risk Management

[COSO: 2004](#)
Enterprise Risk Management - Integrated Framework

[FERMA: 2002](#)
A Risk Management Standard

[SOLVENCY II: 2012](#)
Risk Management for the Insurance Industry

We recognize that there are other standards and guidelines that have been used around the globe, particularly the Australia/New Zealand 4360:2004 standard. With international adoption of the ISO 31000:2009 standard,

RIMS defines enterprise risk management as a strategic business discipline that supports the achievement of an organization’s objectives by addressing the full spectrum of its risks and managing the combined impact of those risks as an interrelated risk portfolio.

however, which is based on AS/NZS 4360, we believe that a review of that and similar national standards is redundant.

Certain regulatory standards were also considered, such as Basel II, but were not included in the scope of this review. With the ongoing developments of the new Basel III standard, coupled with the pending regulatory rules expected from the Dodd-Frank Act for U.S. banking institutions and certain non-bank financial companies, the review would not be complete. Nevertheless, the Basel II standard is included in the groupings noted in Table 1 as it remains a regulatory requirement for financial institutions of a certain size.

Risk management is a constantly evolving discipline. Standards, frameworks and guidelines are modified periodically in light of new research or innovative practices, making it difficult for risk managers to stay current. It is our hope that this review can help simplify this process.

DIFFERENCES BETWEEN STANDARDS, REGULATIONS AND CONTROLS

It is important to know what standards are and what they are not. There is a lot of confusion as to what is a standard (which is typically voluntary) and what is a regulation (mandated through legislation). What is important to note is that standards organizations generally have diverse input and usually develop voluntary standards. For example, standards might become regulated if adopted by a government, or mandatory if agreed upon in a business contract.

In practice, standards often are used by auditors to determine whether a company is complying with these best practices (seen by some as equal to controls). As discussed in the RIMS Executive Report “The 2008 Financial Crisis: A Wake-Up Call for Enterprise Risk Management,” controls typically are founded on standards or regulatory guidance, which are based on a collection of best practices and guidelines. They are developed collaboratively over time through experience. They are expanded or modified periodically to reflect new practices. It is important to note that controls, as such, do not evolve in scope or speed to keep up with new risks that are being taken. They are not designed to be predictive of emerging or future risks. Controls are

vitaly important, but they are inadequate for reasonable assurance that risks are being managed effectively.

In addition, ratings agencies do not produce risk management standards. Rating agency scrutiny of organizations' risk management practices creates intense focus on ERM preparations for the respective credit rating evaluations and, most importantly, the potential bearing that disciplined risk practices may have on credit ratings.

"We do not intend to publish a separate ERM methodology. However, our Corporate Ratings Criteria, a detailed collection of methodologies covering all aspects of our corporate ratings process, will reflect any ERM-related enhancements in management analysis...Any positive credit rating action would stem from sustainably improved cash flows, operating performance, or competitive advantages realized from successfully managing risk. Likewise, a negative rating action would result from unexpected large losses, chronic underperformance, or competitive disadvantages resulting from poor risk management."

– Steven J. Dreyer
Standard and Poor's Credit FAQ
June 24, 2010

COMPARING STANDARDS

Risk management strategies generally focus on one or more of the following elements:

- meeting or exceeding an organization's objectives
- adhering to control-based objectives, rules and/or controls
- complying with regulatory requirements

Even within organizations, the strategy focus may differ by function. Internal audit may focus on controls and assuring that risks are properly mitigated. Compliance functions may focus on the controls needed to manage risk. Strategy development typically sees risk management as a means to improve the success of the organization's longer-term goals and objectives.

Given the sometimes competing objectives of these internal functions, confusion about the purpose and implementation of enterprise risk management can be expected. The use of specific strategies for implementing risk management practices can either help or hinder the ultimately successful adoption of such practices for the intended overarching purpose.

All of the reviewed standards reference the three focuses noted above, that is, alignment with an organization's objectives, adherence to controls as a means of managing risk and the need to meet regulatory requirements. We found that the primary focus of one standard/guideline versus another tended to be weighted more in one area than another. This is important for the risk practitioner because depending on the primary risk management strategy and objective desired, one standard/guideline may be better suited for an organization's purposes. On that basis, the reviewed standards/guidelines were grouped accordingly in Table 1.

Table 1: Comparing Standards

| STRATEGY FOCUS | DESCRIPTION | STANDARD/GUIDELINE | PRIMARY CHALLENGE |
|---------------------------------|---|--|--|
| ORGANIZATIONAL OBJECTIVES | Designed to improve an organization's ability to meet or exceed its objectives through enhanced decision-making and activities that address key uncertainties. | ISO 31000:2009 BS 3100:2008 COSO:2004 FERMA: 2002 | Harmonizing approaches, blending the "siloed" strategies through common elements as found in RIMS Risk Maturity Model (RIMS RMM) |
| COMPLIANCE & CONTROL OBJECTIVES | Seeks to assure the transfer or other mitigation of risks primarily through compliance and control objectives and activities; often based on historic losses, near-miss, etc. | OCEG "Red Book" 2.0:2009 COSO: 2004 | |
| REGULATORY | Used when an organization must apply a designated practice and/or standard and provide evidence in order to meet regulatory requirements. | SOLVENCY II BASEL II | |

RIMS RISK MATURITY MODEL FOR ENTERPRISE RISK MANAGEMENT

The RIMS ERM Risk Maturity Model (RMM) is neither a standard nor a framework. It is not a “how to” guide for implementation nor a prescribed process. It focuses on seven essential attributes with 26 specific success factors (or success behaviors) that organizations may or may not demonstrate along a maturity spectrum from ad hoc (does not exist) to leadership (fully embedded across and throughout the organization). The seven attributes are:

1. *ERM-based approach.* Gaining executive support within the corporate culture
2. *ERM process management.* Integrating ERM into business processes
3. *Risk appetite management.* Establishing accountability within leadership and policies to guide decision-making
4. *Root cause discipline.* Binding events to their process sources
5. *Uncovering risks.* Performing risk assessments to document risks and opportunities
6. *Performance management.* Executing organizational vision, mission and strategy through outcomes-based measurements
7. *Business resiliency and sustainability.* Integrating ERM into operational planning and execution

Each of the six standards, guidelines and frameworks were compared to these seven attributes. See Appendix A Crosswalk for specific references.

SIMILARITIES AMONG THE STANDARDS

Based on the review, all of the standards and frameworks are similar in the following ways. All require:

- Adoption of an enterprise approach, with executive level sponsorship and defined accountabilities
- Structured process steps, oversight and reporting of the identified risks
- Understanding and accountability for defining risk appetite and acceptable tolerance boundaries
- Formal documentation of risks in risk assessment activities
- Establishment and communication of risk management process goals and activities
- Monitored treatment plans

Although there are a number of common elements, certain RIMS RMM success factors were either missing or underdeveloped in the reviewed standards, most notably root cause discipline and risk appetite management. Many of the documents referenced integration into operations, however few linked expected out-

comes with performance management or through an interrelated risk portfolio.

MAJOR DIFFERENCES AMONG THE STANDARDS

ISO 31000: 2009

The primary difference for ISO 31000 is the shift from an event to the effect risk and risk management has on an organization’s objectives. Trying to predict events can be difficult and challenging. Objectives, on the other hand, typically are clearer and more precisely articulated. What ISO 31000 does is put the emphasis squarely on risk management as a strategic discipline for making risk-adjusted decisions, rather than a compliance-based function.

In comparing ISO 31000 to the RIMS RMM attributes, we note that there is little discussion of a portfolio view and interrelated dependencies that risks may have on an organization’s objectives as is contained in RIMS RMM attribute Risk Appetite. Such a portfolio view is alluded to in the following sections: Section 5.3.5, Defining risk criteria: “Decisions should take account of the wider context of the risk and include consideration of the tolerance of the risks borne by parties other than the organization that benefits from the risk.” and Section 5.4.4, Risk evaluation: “... whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered.” Even so, the discussion of an interrelated risk portfolio is somewhat fleeting.

OCEG “Red Book” 2.0: 2009

The major difference for the OCEG approach is the formal integration of the governance, risk and compliance processes, ideally supported by a common technology platform. In this framework, risk is given a limited role focused on identification and measurement. The primary directive for risk, though not exclusively, is to measure the likelihood of an event that has an adverse effect on objectives. The OCEG Capability Model relies heavily on an integrated technology platform as an enabling tool to identify and assess risk for prevention and/or remediation purposes.

In comparing the OCEG framework with others in the crosswalk, two important attributes contained in the RIMS RMM are not explicitly covered in the Red Book: root cause consideration in analysis and risk ownership by business areas. Although the Corrective Controls section within the Respond & Resolve element in the framework does mention that controls must address root causes, this type of analysis is not highlighted within the Assess and Align element nor is it found elsewhere in the document. With respect to the integration for risk management accountability by the business owners themselves, the Roles & Responsibilities element only describes accountabilities for the GRC system. Even though the Red Book specifically mentions roles for oversight, key management, leadership,

operational and assurance roles and accountability, the GRC model itself does not link ownership within the organization business areas explicitly as a key component for risk management.

BS 31100: 2008

The reviewers found the similarities of the British Standard BS 31100 to ISO 31000 to be so significant that no material differences were noted. Organizations located in the UK who have used the HM Treasury's Orange Book, *Management of Risk: Guidance for Practitioners*, published by the Office of Government Commerce, may find its familiarity meaningful. BS 31100 specifically highlights the benefits of using a risk maturity model to improve an organization's risk management capability.

In comparing BS 31100 to the RIMS RMM attributes, there is only a brief discussion of business continuity management in the British Standard. It focuses on this capability to a lesser degree than in the RIMS RMM attribute Business Resiliency and Sustainability. However, the standard states, in section 3.6.5, "... the organization should identify the requirements of specialist functions or individuals managing specific aspects of risk, such as compliance risk, operational risk, health and safety, information security, and business continuity management." Further, BS 31100 directs users to its complementary standard BS 25999, *Business Continuity Management*, which it offers as a standard specifically tailored to business resiliency and sustainability.

COSO: 2004

When comparing COSO 2004 and 2009 to other frameworks and to the RIMS RMM, there are more similarities than differences; however, COSO more than any framework places a greater degree of responsibility on the board, requiring not only that the Board support ERM, but have direct involvement in the ERM process. Another example of COSO specificity is found in the *Application Techniques* document, which provides a variety of "real world" processes, exercises and tools that can be implemented by an organization to fulfill the ERM components. The *Application Techniques* section provides greater depth and detail on how to implement ERM than some of the other frameworks.

The greatest difference between the COSO framework and the RIMS RMM is that the COSO framework's ERM components and associated *Application Techniques* do not speak to root cause analysis or business resiliency and sustainability, although these activities could fall into one of the seven ERM components. An ERM program based solely on the COSO framework without consideration for additional risk management techniques could have some weaknesses; therefore using the RIMS RMM can be very useful in identifying these gaps and enhancing the COSO framework.

FERMA: 2002

The FERMA standard was not designed to create a prescriptive process for enterprise risk management.

Instead, the standard describes necessary component parts of an ERM framework. These components represent "best practice[s] against which organizations can measure themselves." In this process, organizations can leverage an awareness of the "upside and downside" of risk in order to bring value to the organization as well as all stakeholders. The upside and downside of risks are viewed in the context of both the activity and the various stakeholders who can be affected.

In comparing the FERMA standard to the RIMS RMM attributes, other than a passing reference in its Appendix, the document does not discuss root cause as a key component to effective risk management.

SOLVENCY II: 2012

As a regulatory standard to be used by insurance companies in the European Union by November 1, 2012, Solvency II is specific in providing requirements with respect to financial assets/economic capital, governance and risk management, and disclosure and transparency. The major difference is the quantification related to capital requirements. As this standard is designed to address only the risk management practices of European insurers, it differs from the other reviewed standards in its narrow applicability. A number of insurance companies, including those in Bermuda, that are not directly regulated by this regulatory standard are seeking "equivalency" to address their respective business and insureds in the EU. While risk practitioners outside of the EU insurance industry may want to familiarize themselves with the principles being promulgated by the UK Financial Services Authority, the specificity of the standard may be limiting in contexts other than the insurance industry.

However, as the regulations are still evolving readers should keep current with developments. For example, in Q3 2010 draft regulations were published that govern any insurance that applies in the EU. This is likely to have an impact on captive owners and insurers who are not based in the EU but who cover risks there. Guidelines on equivalency rules have also been drafted that may assist non-EU based insurers meet the 2012 deadlines.

COMMENTS ABOUT INDIVIDUAL STANDARDS AND GUIDELINES

ISO 31000:2009

The International Organization for Standardization widely known as ISO, is an international-standard-setting body that "forms a bridge between the public and private sectors." While many of its member institutes are part of the governmental structure of their countries (or are mandated by their government), other members have their roots in the private sector, having been set up by national partnerships of industry associations. ISO promulgates worldwide proprietary industrial and commercial standards. The organization defines itself as a non-governmental organization, comprising a network of the national standards institutes of 163 countries,

one member per country, with a central secretariat in Geneva, Switzerland, that coordinates the system.

ISO 31000 Risk Management Principles and Guidelines has its core in the AS/NZS 4360 with contributions from France, Switzerland and Brazil. The terminology was refreshed in the ISO 73:2009 Risk Management Vocabulary document. These two standards should be considered together for implementation purposes. The AS/NZS HB 436 and Canadian CSA Q850 are guideline documents for implementation. ISO/IEC 31010 Risk Assessment Techniques provides a range of tools for different types of risk assessments.

ISO 31000 is not about a process alone. The standard is structured into principles (11 characteristics of risk management), a five-part framework (mandate, plan, implementation, checks and improvement), and process (communication and consultation, context, risk assessment, treatment and monitoring). (See Figure 2) It is not designed to provide assurance around controls. It focuses on the actions taken on identified risks to cost effectively improve the organization's performance. It gets back to the basics of disciplined decision-making around risks vs. reward and of helping organizations achieve their expected outcomes. It is not specific to any one industry, type or size of organization.

ISO 31000 intentionally aligns risk practices with global standards to drive efficiencies—internationally from an external perspective and specifically within an organization's management systems and contexts. It leads organizations to measure deviations from expected outcomes. In other words, if the organization's objective is to create value, the measurement of risk becomes the deviation (positive or negative) from the expected value created. Specifically,

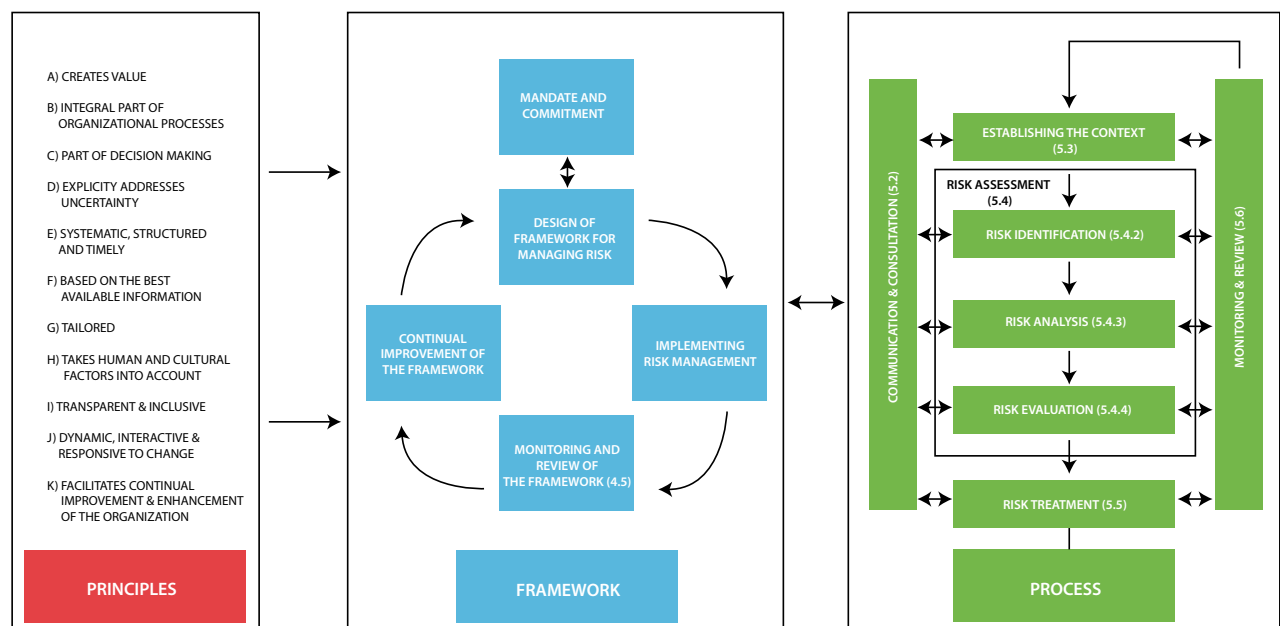
ISO 31000 is a universal standard that can be tailored to the specific needs and structures of an organization and defines risk as "effect of uncertainty on objectives."

So what does all this mean for risk practitioners? The biggest change is shifting an organization's risk focus from a rear-window view to what we can call "a global positioning orientation." In addition to focusing on preventing or mitigating known risks, what is the organization facing on the road up ahead that may get in the way of achieving its objectives? Mitigation and control activities, including preventative measures, are still important. ISO 31000's shift in the view does not replace what risk management already brings to organizations. It expands the value that risk managers can add.

The fundamental organizational need related to this shift is to broaden risk management competencies from reactive to proactive across the enterprise. Thinking about risk in a predictive and strategic way not only protects the value of the organization, it proactively helps to create and capture value - all in alignment with the organization's objectives. Can that be accomplished without a risk management standard? Perhaps, but by utilizing a disciplined and generally accepted approach in strategic as well as operational and day-to-day activities, one begins to establish a pattern of risk-adjusted behavior permanently into the organization's culture.

Accordingly, ISO 31000, while universally applicable in its adaptability and simplicity, may be most helpful to rapidly changing organizations, those with constrained implementation resources, and those looking for greater flexibility in their strategic and operational risk management practices. Also, any organization with a global footprint may find that this international standard is more widely embraced.

Figure 1: ISO 31000 - Risk Management



Reproduced from ISO Standard 31000:2009 with permission from ISO at www.iso.org. Copyright remains with ISO.

OCEG "Red Book" 2.0: 2009

The Open Compliance and Ethics Group (OCEG) describes itself as "a nonprofit think tank that helps organizations drive principled performance by providing standards, tools and resources that enhance corporate culture and integrate governance, risk management, compliance, internal control and ethics processes."

In integrating and aligning governance, risk management and compliance (GRC) efforts, OCEG describes its "framework for principled performance" in two parts: the Red Book, which contains the overview and principles of the GRC capability model, and the Burgundy Book, which contains "procedures and assessment criteria to facilitate management and evaluation of a GRC system." It focuses on the application of GRC methods "by which [the enterprise] establishes and stays within the boundaries it will observe while driving toward its [financial and nonfinancial] objectives."

Access to the model and its technology arenas and modules requires membership in OCEG, which is offered at basic, premier and enterprise levels with varying annual membership fees.

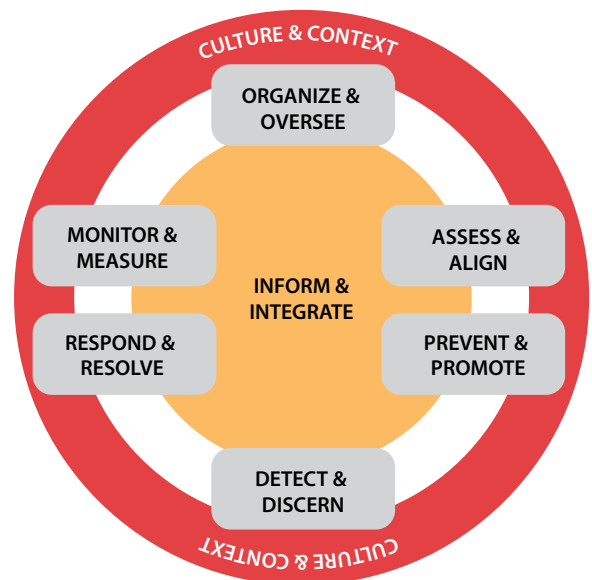
The approach is comprehensive and somewhat prescriptive in identifying accountabilities, as well as the parts of the organization and processes needed to be included in the GRC model. It assumes certain universal outcomes:

- achievement of business objectives
- enhancement of the organizational culture
- increase in stakeholder confidence
- preparation and protection of the organization
- prevention, detection and reduction of adversity
- motivation and inspiration of desired conduct
- improvement in responsiveness and efficiency
- optimization of economic and social value

The document details "GRC Capability Model Elements" for each of its components, which are shown in Figure 2. It defines the role of risk as follows "Risk, in [the GRC] context, is the measure of the likelihood of something happening that will have an effect on achieving objectives; *most importantly, but not exclusively, an adverse effect.* [emphasis added]" In this context, the role of risk management is minimized to the measure-

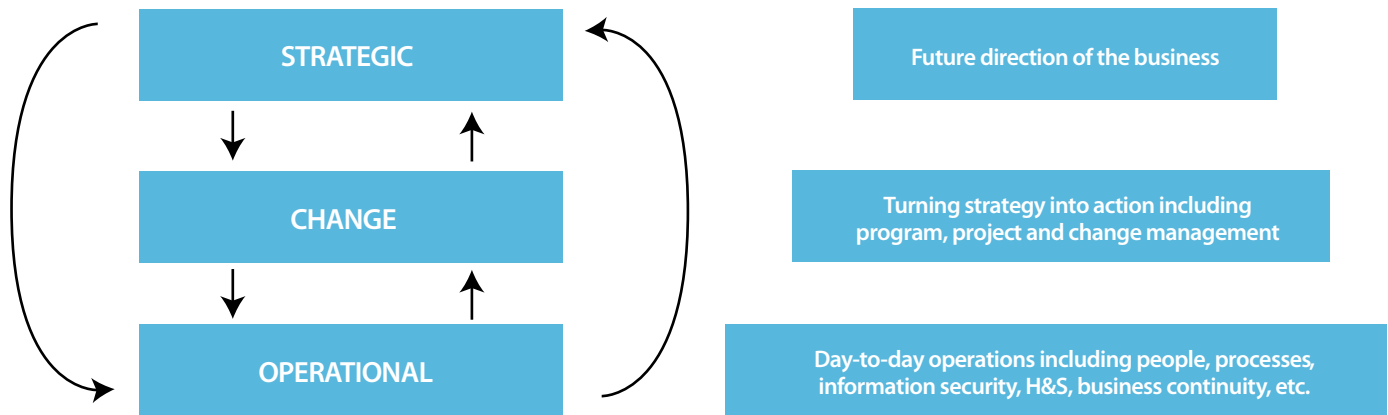
Figure 2: OCEG "Red Book" 2.0: 2009 GRC Capability Model Elements

| | |
|-------------------------------|--|
| CULTURE & CONTEXT | <ul style="list-style-type: none"> • External & internal business context • Culture, values and objectives |
| ORGANIZE & OVERSEE | <ul style="list-style-type: none"> • Outcomes, commitment, role and responsibilities, and accountability |
| ASSESS & ALIGN | <ul style="list-style-type: none"> • Risk identification, analysis and optimization |
| PREVENT & PROMOTE | <ul style="list-style-type: none"> • Codes of conduct, policies, controls, awareness and education, incentives, stakeholders relations, risk financing and insurance |
| DETECT & DISCERN | <ul style="list-style-type: none"> • Hotline, notification, inquiry and survey, detective controls |
| INFORM & INTEGRATE | <ul style="list-style-type: none"> • Information management and documentation, internal and external communications, technology and infrastructure |
| RESPOND & RESOLVE | <ul style="list-style-type: none"> • Internal review and investigation, third party inquiries and investigation, corrective controls, crisis response and recovery, remediation, and discipline |
| MONITOR & MEASURE | <ul style="list-style-type: none"> • Context monitoring performance monitoring and evaluation, systematic improvement, assurance |



Source: Open Compliance and Ethics Group © 2003-2009 OPEN COMPLIANCE AND ETHICS GROUP. Used with permission. www.oceg.org

Figure 3: BS 31100: Risk Management Perspective



Source: BSI (www.bsigroup.com)

ment of events, primarily for purposes of mitigation and control. Its focus on enabling technology leads the practitioner to consider the measurement of risk on historic events as a predictor of future events, which is not conducive to the identification of emerging risks.

In conclusion, this framework provides a unique focus on investigations, technology and remediation. This approach tends to be most closely aligned with security practices (e.g., codes of conduct) and compliance (i.e., controls), while appearing to be most suited for the largest of organizations in which human and technological resources are abundant.

BS 31100: 2008

BSI Group, also known in its home market as the British Standards Institution (or BSI), is the national standards body of the United Kingdom and a multinational business services provider whose principal activity is the production and sales of standards and the supply of standards-related services.

The BS 31100: 2008 is a general risk management standard that provides a basis for understanding, developing, implementing and maintaining proportionate and effective risk management throughout an organization, in order to enhance the organization's likelihood of achieving its objectives. BS 31100 contains a set of basic risk management principles which are applicable to any organization, but the way they are implemented will vary according to an organization's nature, including size and complexity, and context.

It has been drafted to be consistent with the general guidance on risk management that has been given by ISO 31000, but is also developed recognizing the knowledge contained in HM Treasury's Orange Book, *Management of Risk: Guidance for Practitioners* as well as other documents referenced in its introduction.

As seen in other risk management standards, this British Standard describes how risk management embodies a framework and process that enable any organization

to proactively manage uncertainty in a systematic manner at all levels within the organization; from strategic to operational perspectives. These risk management perspectives are found in Figure 3.

BS 31100 is intended for use by anyone with responsibility for any of the following:

- Ensuring an organization achieves its objectives
- Ensuring risks are proactively managed in specific areas or activities
- Overseeing risk management in an organization
- Providing assurance on the effectiveness of an organization's risk management
- Reporting to stakeholders through disclosures in annual financial statements, corporate governance reports and corporate social responsibility reports

This British Standard pays particular attention to the benefits of using a risk maturity model to improve an organization's risk management capability. It describes how this type of planning tool contains the fundamental elements of effective risk management processes and depicts the evolutionary path from ad hoc to mature, repeatable processes.

COSO: 2004

Comprising a variety of professional associations including the American Accounting Association (AAA), American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), the Association for Accountants and Financial Professionals in Business (IMA) and the Institute of Internal Auditors (IIA), the Committee of Sponsoring Organizations (COSO) is a voluntary private-sector organization. COSO describes itself as dedicated to guiding executive management and governance entities toward the establishment of more effective, efficient and ethical business operations on a global basis.

COSO advocates that organizations should implement enterprise risk management (ERM) to better connect

their risk oversight with the creation and protection of stakeholder value. ERM is a process that provides a robust and holistic top-down view of key risks facing an organization. To help boards and management understand the critical elements of an enterprise-wide approach to risk management, in 2004 COSO issued its Enterprise Risk Management - Integrated Framework, which defines ERM as follows:

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

COSO’s Enterprise Risk Management - Integrated Framework highlights four areas that contribute to board oversight with regard to enterprise risk management:

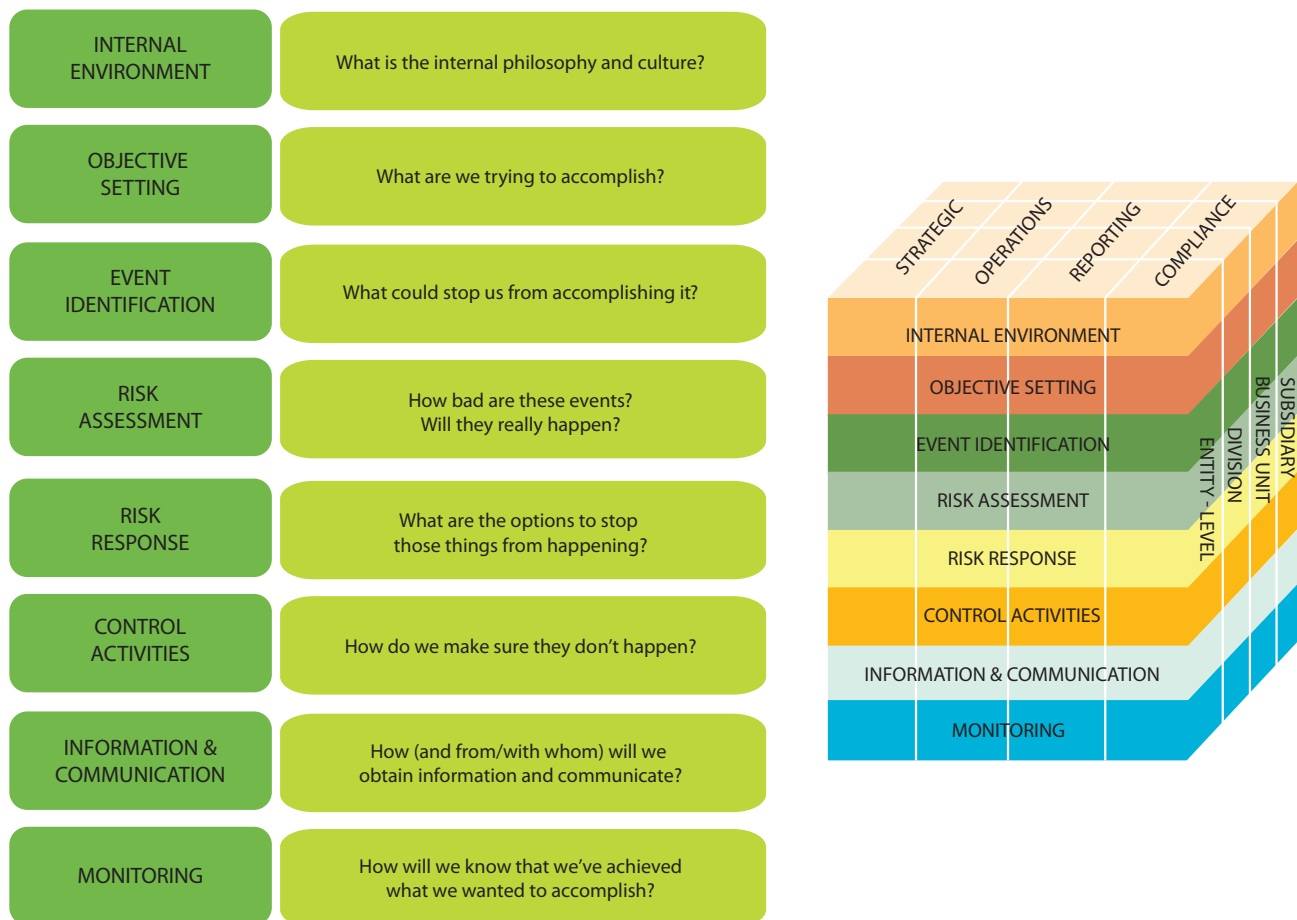
- Understand the entity’s risk philosophy and concur with the entity’s risk appetite.
- Know the extent to which management has established effective enterprise risk management of the organization.
- Review the entity’s portfolio of risk and consider it against the entity’s risk appetite.

- Be apprised of the most significant risks and whether management is responding appropriately.

COSO’s objectives are to improve organizational performance through better integration of strategy, risk, control and governance. The COSO Enterprise Risk Management Framework, as shown in Figure 4, provides a visual picture of how ERM is to be integrated into an organization.

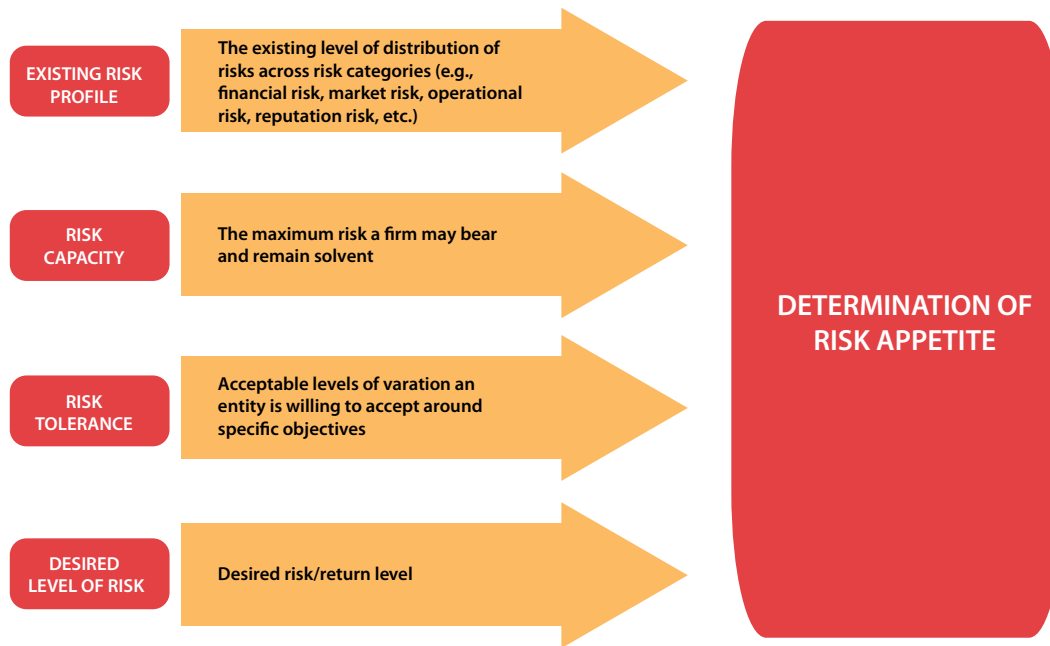
On the right face of the cube are Subsidiary, Business Unit, Division, and Entity Level representing the need for all levels of the organization to be a part of the ERM program. Across the top of the cube are four categories of the organization’s objectives. The organization’s operations and activities can fit into one, multiple or all categories. On the front face of the cube are the ERM interrelated components, which are derived from the way management operates the enterprise and are integrated in the management process. These ERM components need to be present and effective in order to ensure that the organization can operate and have the most optimum outcome. If there are weaknesses in any of the components then the likelihood of an event occurring that might prevent the organization from meeting its objectives increases, if the ERM components are effective and integrated into the organizations processes then the organization can expect successful outcomes and take greater risks.

Figure 4: COSO Enterprise Risk Management Framework



Source: Committee of Sponsoring Organizations of the Treadway Commission www.coso.org. Used with permission.

Figure 5: Elements of Risk Appetite



Source: Committee of Sponsoring Organizations of the Treadway Commission www.coso.org. Used with permission.

Like many of the other available risk management frameworks, COSO's framework too has evolved, moving from a controls approach to a strategic approach:

"In today's environment, the adoption of ERM may be the most effective and attractive way to meet ever increasing demands for effective board risk oversight. If positioned correctly within the organization to support the achievement of organizational objectives, including strategic objectives, effective ERM can be a value-added process that improves long-term organizational performance. Proponents of ERM stress that the goal of effective ERM is not solely to lower risk, but to more effectively manage risks on an enterprise-wide, holistic basis so that stakeholder value is preserved and grows over time. Said differently, ERM can assist management and the board in making better, more risk-informed, strategic decisions."

– *Effective Enterprise Risk Oversight - The Role of the Board of Directors (COSO, 2009)*

Building on the four areas that contribute to board oversight with regard to enterprise risk management, COSO has emphasized the importance of considering risk versus reward and developing risk appetitive strategy (as shown in Figure 5).

While recognizing that one size does not fit all, COSO believes that because its framework is based on identified leading practices and the development of consistent terminology and approaches, it can be successfully used by many organizations in meeting their objectives.

FERMA: 2002

FERMA: 2002 is a risk management standard adopted by the Federation of European Risk Management Associations. It was created by a team comprised of the members of the major United Kingdom-based risk management organizations: the Institute of Risk Management (IRM), the Association of Insurance and Risk Managers (AIRMIC) and ALARM, the National Forum for Risk Management in the Public Sector.

The standard sets out a strategic process, starting with an organization's overall objectives and aspirations, through to the identification, evaluation and mitigation of risk, and finally the transfer of some of that risk to an insurer.

FERMA: 2002 adopts the definition of risk as the combination of "the probability of an event and its consequences." The standard is careful to emphasize the view that in any risk-related circumstance there are "opportunities for benefit (upside) or threats to success (downside)."

Management of these opportunities and threats is described as a key part of any organization's strategic planning. Risk management is described as the methodical process of identifying all risks to achieving objectives and then applying risk treatments that add "maximum sustainable value to the organization." Because the process of risk management addresses the entire organization through the risk identification process, it must be integrated as part of the organization's culture. This includes assigning responsibility for managing risks as a part of the job description of managers and employees to promote operational efficiency at all levels.

The actual risk management process is very similar to the ISO 31000 standard and is shown in Figure 6.

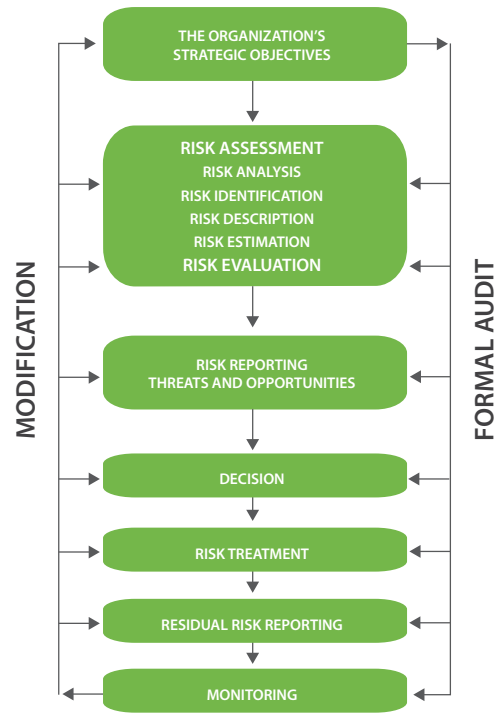
FERMA: 2002 provides a simplified framework for the risk analysis step (for both upside and downside risk), which can be used to organize and categorize risk consequences and their probability of occurrence. This information can then be used as the basis for evaluating the significance of the organization's risks, and to determine how risk treatments should be applied.

The standard states that risk treatment practices, at a minimum, should be consistent with the effective, efficient operation of the organization; should have effective internal controls; and should comply with all applicable laws and regulations. FERMA: 2002 also defines the roles of various groups within the organization, as well as their responsibilities for communicating and monitoring risks.

In addition, FERMA: 2002 identifies specific roles for the board, business units, the risk management unit (if the organization is of sufficient size) and internal audit (Table 2).

Similar to ISO 31000 and COSO: 2004, the FERMA standard highlights the importance of a risk management monitoring process as a tool for continuous improvement. Specific to the FERMA standard are the inclusion of regular audits of compliance with risk management policies and standards, assurance that there are appropriate risk treatments in place and that the treatment procedures are understood and followed, in order to determine whether the intended results were efficiently obtained.

Figure 6: FERMA: 2002 Risk Management Process



Source: FERMA (www.ferma.eu)

Table 2: FERMA: 2002 Roles and Responsibilities

| FUNCTIONAL ROLE | RESPONSIBILITIES |
|-----------------------|---|
| BOARD | Overall direction of the risk management process, including strategic risk management, and for creating the environment and the structures for risk management to operate effectively |
| BUSINESS UNITS | Managing day-to-day risks, for promoting risk awareness within their operations, and for incorporating risk management into the planning, as well as operational aspects, of their work |
| RISK MANAGEMENT UNITS | Building a risk aware culture, setting policy and strategy for risk management, and being the primary champion of risk management at the strategic and operational level |
| INTERNAL AUDIT | Focusing on significant risks identified by management and auditing the risk management processes across the organization; providing assurance on the management of risk and give active support and involvement in the risk management process |

Source: FERMA (www.ferma.eu)

SOLVENCY II: 2012

Solvency II is a regulatory standard to be used by insurance companies located or doing business in the European Union by November 1, 2012. The Financial Services Authority has outlined the economic principles for the measurement of assets and liabilities associated with Solvency II. They are outlined in three pillars as described below.

- Quantitative requirements (for example, the amount of capital an insurer should hold)
- Requirements for the governance and risk management of insurers, as well as for the effective supervision of insurers
- Disclosure and transparency requirements

Solvency II takes a “three lines of defense” approach to protecting the organization against risk through appropriate governance. The three lines are:

1. *Risk management.* The daily activity of board and management in identifying, assessing, managing and reporting risk.
2. *Risk oversight.* The review process starting at the board (or board risk committee), executive committees such as credit, ALM and operational through to the chief risk officer, and on to business unit risk officers.
3. *Risk assurance.* The audit process, starting at the audit committee of the board and may include compliance activity.

Examples of these structures are becoming available on insurer websites and in annual reports, such as Old Mutual PLC, Aviva PLC and Prudential PLC.

As of the date of this report, the only formal guidance is found in consultancy documents. We have compared EMB Business Consultancy, PricewaterhouseCoopers and Deloitte’s views of the pillars and they are in agreement.

The Financial Services Authority has requested that insurance companies voluntarily use Solvency II in the Fifth Quantitative Impact Study (QIS5), which took place between August and October 2010 with the final report to be produced in May 2011.

CONCLUSION

The wealth of available standards describing enterprise risk management demonstrates that it is an emerging—and essential—business discipline. Based on this review, we conclude that:

- Standards and guidelines tend to be conceptual with little guidance on practical implementation
- There are more similarities than differences among the reviewed standards and guidance documents
- The universal applicability of RIMS RMM serves as a harmonizing tool regarding the more practical attributes and behaviors that most of the standards are attempting to address
- Elements in each of the standards and/or guidelines may be useful or adaptable for specific organizations

The fact that all the standards share more characteristic similarities than differences demonstrates that ERM is also an evolving discipline that has meaningful applications to all sectors, whether organizations are structured for profit, not for profit, governmental or non-governmental purposes.



APPENDIX A:

CROSSWALK OF RISK MANAGEMENT STANDARDS, GUIDELINES AND BEST PRACTICES AS COMPARED TO RIMS RMM ATTRIBUTES

RIMS RMM ATTRIBUTE: ADOPTION OF ERM-BASED APPROACH

Denotes the degree of executive support for an ERM-based approach within the corporate culture. Activities cut across all processes, functions, business lines, roles and geographies. Includes integrating, communicating and coordinating with front-line and support areas, including internal audit, information technology (IT), compliance, corporate security, business continuity and risk management.

| Common Elements and Issues Addressed | ISO 31000: 2009 Risk Management - Principles and Guidelines | OCEG "Red Book" 2.0: 2009 GRC Capability Model | BS 31100: 2008 Code of Practice for Risk Management | COSO:2004 Enterprise Risk Management — Integrated Framework | FERMA: 2002 A Risk Management Standard | SOLVENCY II: 2012 |
|--|--|--|--|--|--|---|
| Executive support for ERM | 4.2 Mandate and commitment | C3 Culture 02.2 Management Roles & Accountabilities 02.3 Leadership Roles & Accountabilities | 3.1 Governance | Effective Risk Oversight: The Role of the Board of Directors | 8.1 Risk Management Policy | Pillar 3 Market Discipline: Transparency (Disclosure) |
| Business process definition | 4.3.4 Integration into organizational processes Annex A.3.3 [integration] Annex A.3.5 [governance / goal achievement] | 03.2 Define GRC processes and align with business processes | Figure 1 Risk management perspectives | Executive Summary, page 2 Strengthening ERM for Strategic Advantage, page 1 | 4.5 Risk Profile | Pillar 2 Supervisor Review: Regulations on financial services supervision (Control) |
| Risk ownership | 4.3.3 Accountability Annex A.3.2 [accountability] | 02 Roles and Accountabilities | 3.6 Roles, responsibilities and authorities (the entire section) | Effective Risk Oversight: The Role of the Board of Directors, Integrated Framework, page 83 Strengthening ERM for Strategic Advantage, page 1 | 4.5 Risk Profile | Pillar 3 Market Discipline: Disclosure requirements (Disclosure) |
| Far-sighted risk management vision | 3. Principles 4.4.1 Implementing the framework for managing risk Annex A.1-A.3 [performance goals, accountability, integration] | 01 Outcomes and Commitment | 2 Risk management principles 3.2 Risk management strategy | Executive Summary, page 3 Strengthening ERM for Strategic Advantage. pages 1, 12 | 4.1 Risk Identification | Pillar 2 Supervisor Review: Quantitative requirements (Control) |
| Front line and support process owner participation | 4.1 Framework - General 4.4.1 Implementing the framework for managing risk 4.4.2 Implementing the risk management process 5.1.1 Process - General 5.2 Communication and consultation | 03 Approach & Accountability | 3.5 Building capability and competence 3.6.3 The role of individuals 3.6.4 The roles of the risk owners and risk response owners | Executive Summary, page 6 Integrated Framework, page 18 Strengthening ERM for Strategic Advantage. pages 12 | 8.1 Risk Management Policy | Pillar 3 Market Discipline: Competition related elements (Disclosure) |

RIMS RMM ATTRIBUTES: ERM PROCESS MANAGEMENT

Denotes the degree of incorporation of repeatable and scalable risk management process into all business and resource/support units, bolstered by qualitative and quantitative measurements, analyses, tools and models; robust reporting on risk management activities; and clarity of oversight, including roles and responsibilities. The ERM process is defined as a sequential series of steps that support the reduction of uncertainty and promote the exploitation of opportunities.

| Common Elements and Issues Addressed | ISO 31000: 2009 Risk Management - Principles and Guidelines | OCEG "Red Book" 2.0: 2009 GRC Capability Model | BS 31100: 2008 Code of Practice for Risk Management | COSO: 2004 Enterprise Risk Management — Integrated Framework | FERMA: 2002 A Risk Management Standard | SOLVENCY II: 2012 |
|---|--|---|--|--|--|---|
| Repeatability and scalability | 1. Scope | C Culture and Context C2.2 Determine Changes Needed to Align the Internal Context and GRC System O1.1 Define GRC System Scope | 1. Scope | Application Techniques, page 1 Integrated Framework, page 17 | N/A | Pillar 3 Market Discipline: Competition related elements (Disclosure) |
| ERM process oversight | 4.3.3 Accountability 5.3.4 Establishing the context of the risk management process | O2.1 Define and Enable GRC System Oversight Roles and Accountability | 3.1 Governance 3.6.2 Senior management responsibilities 3.6.5.a Risk management oversight body | Effective Risk Oversight: The Role of the Board of Directors, Strengthening ERM for Strategic Advantage, page 12 | 9. Monitoring and Review | Pillar 3 Market Discipline: Transparency (Disclosure) |
| ERM process steps (includes risk assessment) | 5. Process (inclusive of 5.1-5.7) | Process Embedded in GRC Capability Model A Assess & Align P Prevent and Promote D Detect and Discern I Inform & Integrate R Respond & Resolve M Monitor & Measure | 4 Risk management process | Application Techniques, page 1 Integrated Framework, page 17 | 2.2 The Risk Management Process | Pillar 2 Supervisor Review: Quantitative requirements (Control) |
| Risk culture, accountability and communication (includes building a risk awareness culture) | 4.3.3 Accountability 5.2 Communication and consultation 5.3 Establishing the [internal and external] context Annex A.3.2 [accountability] Annex A.3.4 [communications] | C3 Culture O3 Approach & Accountability I2 Internal & External Communication | 3.4 Risk management culture 3.6 Roles, responsibilities and authorities 3.11 Risk communication 3.5.4 Risk management monitoring, review, and continual improvement | Integrated Framework, pages 27, 67, 75 | 8.1 Risk Management Policy | Pillar 3 Market Discipline: Disclosure requirements (Disclosure) |
| Risk management reporting | 5.6 Monitoring and review 5.7 Recording the risk management process | I1 Information Mgt. & Documentation | 3.12 Risk reporting 4.6 Risk management process reporting | Integrated Framework, page 67 | 9. Monitoring and Review | Pillar 3 Market Discipline: Transparency (Disclosure) |

RIMS RMM ATTRIBUTES: RISK APPETITE MANAGEMENT

Denotes the degree of understanding and accountability throughout organizations for 1) defining acceptable boundaries for risk types; 2) calculating and articulating approved variations for risks outside of boundaries (risk tolerance) 3) developing views of risk impact, likelihood and assurance from different perspectives such as operations and financial reporting (risk portfolio views); 4) considering the benefits of risk and reward tradeoff scenarios in daily management of business and resource/support units; and 5) attacking gaps between perceived and actual risks.

| Common Elements and Issues Addressed | ISO 31000: 2009 Risk Management - Principles and Guidelines | OCEG "Red Book" 2.0: 2009 GRC Capability Model | BS 31100: 2008 Code of Practice for Risk Management | COSO: 2004 Enterprise Risk Management — Integrated Framework | FERMA: 2002 A Risk Management Standard | SOLVENCY II: 2012 |
|--|---|--|--|--|--|---|
| Risk portfolio view | 5.3.5 Defining risk criteria 5.4.3 Risk analysis Annex A.2.1 Key outcomes: risks are [fully] understood | C4.4 Define Indicators, Targets and Tolerances A1.8 Identify Risk Trends and Interrelatedness | 3.8 Risk appetite and risk profile | Effective Risk Oversight: The Role of the Board of Directors, Application Techniques, page 16 Integrated Framework, page 59 Strengthening ERM for Strategic Advantage, page 14 | 8.1 Risk Management Policy | Pillar 2 Supervisor Review: Quantitative requirements (Control) |
| Risk-reward tradeoffs (includes developing risk responses) | 5.3.5 Defining risk criteria 5.4.4 Risk evaluation 5.5.2 Selection of risk treatment options Annex A.2.2 Key outcomes are within [established] risk criteria | A2 Risk Analysis A3 Risk Optimization | 3.8 Risk appetite and risk profile 3.10 Risk criteria | Application Techniques, page 18 Strengthening ERM for Strategic Advantage, page 9 | 2. Risk Management 5. Risk Evaluation | Pillar 1 Quantitative Requirements: Investment (Implementation) |

RIMS RMM ATTRIBUTES: ROOT CAUSE DISCIPLINE

Denotes the degree of discipline to measuring a problem's root cause by: 1) determining the sources or causes of identified risks and opportunities; 2) understanding the sources and impacts of risks on other areas within an organization; 3) identifying the trends in root cause categories; and 4) collecting information and measurements related to the effectiveness of controls with consideration given to sources of identified risks.

| Common Elements and Issues Addressed | ISO 31000: 2009 Risk Management - Principles and Guidelines | OCEG "Red Book" 2.0: 2009 GRC Capability Model | BS 31100: 2008 Code of Practice for Risk Management | COSO: 2004 Enterprise Risk Management — Integrated Framework | FERMA: 2002 A Risk Management Standard | SOLVENCY II: 2012 |
|---|---|--|--|---|---|--|
| Dependencies and consequences | 5.4.2 Risk identification 5.4.3 Risk analysis | A1.8 Identify Risk Trends and Interrelatedness | 4.3 Risk identification 4.4 Risk assessment | Effective Risk Oversight: The Role of the Board of Directors, Executive Summary, page 6 Strengthening ERM for Strategic Advantage, page 17 | N/A | Pillar 2 Supervisor Review: Regulations on financial services supervision (Control) |
| Indicator classifications (includes internal and external risk factors) | 4.5 Monitoring and review of the framework 5.6 Monitoring and review | A1.9 Categorize Risk C1 External Business Context C2 Internal Business Context C4.4 Define Indicators, Targets and Tolerances | 3.9 Risk and consequence categorization and measurement Annex A - Risk categories | Integrated Framework, page 75 Strengthening ERM for Strategic Advantage, page 10 | N/A | Pillar 2 Supervisor Review: Quantitative requirements (Control) |
| Risk and opportunity information collection | 5.4.2 Risk identification | A1 Risk identification A1.7 Identify Risks That May Afford Opportunities | 4.3 Risk identification 4.4 Risk assessment Annex B Risk management tools | Integrated Framework, pages 41, 67 Strengthening ERM for Strategic Advantage, page 10 | N/A | Pillar 1 Quantitative Requirements: Regulations on minimum capital requirements (Implementation) |
| Root cause consideration | 5.4.3 Risk analysis | N/A (although R3 Corrective Controls mentions that controls must address root causes, the GRC model itself does not link root cause analysis (RCA) as a risk management technique or necessary step). | 4.3.1 Risk identification - General | Application Techniques, page 47 Integrated Framework, page 45 Strengthening ERM for Strategic Advantage, page 17 | N/A (although the Appendix (Risk ID Techniques and Risk Analysis Methods) mentions various types of root cause analysis, the standard as a whole does not link RCA explicitly as a risk management technique or necessary step.) | Pillar 3 Market Discipline: Competition related elements (Disclosure) |

RIMS RMM ATTRIBUTES: UNCOVERING RISKS

Denotes the degree of quality and coverage (penetration) throughout organizations for 1) documenting risks and opportunities in risk assessment activities; 2) collecting knowledge from employee expertise, databases and other electronic files to uncover dependencies and correlation across the enterprise; 3) using adverse events to create opportunities; 4) establishing risk ownership by business and resource/supports units; 5) formalizing risk indicators and measurements; and 6) follow-up reporting on risk management activities from varying perspectives.

| Common Elements and Issues Addressed | ISO 31000: 2009 Risk Management - Principles and Guidelines | OCEG "Red Book" 2.0: 2009 GRC Capability Model | BS 31100: 2008 Code of Practice for Risk Management | COSO: 2004 Enterprise Risk Management — Integrated Framework | FERMA: 2002 A Risk Management Standard | SOLVENCY II: 2012 |
|---|--|---|---|---|---|---|
| Formalized risk indicators and measures | 4.5 Monitoring and review of the framework 5.6 Monitoring and review | A3.4 Develop Key Risk Indicators | 4.4 Risk assessment 4.5 Responding to risks 5.4.3 Learning from risk events | Application Techniques, page 27 Strengthening ERM for Strategic Advantage, page 17 | 4.3 Risk Estimation Monitoring (+ all 3 tables) | Pillar 3 Market Discipline: Transparency (Disclosure) |
| Adverse events as opportunities | 1 Scope 5.3 Establishing the context 5.3.5 Establishing risk criteria | A1.7 Identify Risks That May Afford Opportunities | 5.4.3 Learning from risk events Annex E Incorporating potentially positive consequences of risk | Application Techniques, page 30 Integrated Framework, page 15 | 1. Risk [definition] 2.2 The Risk Management Process | Pillar 3 Market Discipline: Competition related elements (Disclosure) |
| Follow-up reporting | 4.3.6 Establishing internal communication and reporting mechanisms 5.6 Monitoring and review 5.7 Recording the risk management process | M2.2 Review and Reconsider Risks M2.5 Identify Monitoring Information M2.6 Perform Monitoring Activities M2.7 Analyze and Report Monitoring Results | 3.12 Risk reporting 4.6 Risk management process reporting 5.5 Risk management development reporting | Application Techniques, page 55 Integrated Framework, page 67 | 9. Monitoring and Review | Pillar 2 Supervisor Review: Quantitative requirements (Control) |
| Risk ownership by business areas | 3 Principles 4.1 Framework - General 4.3.3 Accountability Annex A.3.2 [accountability] | N/A (although O2. Roles & Responsibilities mentions oversight, key management, leadership, operational and assurance roles and accountability, the GRC model itself does not link ownership within the organization business areas explicitly as a key component for risk management). | 3.6.4 The roles of risk owners and risk response owners 3.6.5 c) Additional roles, responsibilities and authorities - organization units | Executive Summary, page 6 Integrated Framework, pages 18, 83 Strengthening ERM for Strategic Advantage, page 12 | 4.5 Risk Profile | Pillar 3 Market Discipline: Transparency (Disclosure) |

RIMS RMM ATTRIBUTES: PERFORMANCE MANAGEMENT

Denotes the degree to which organizations are able to execute on vision and strategy in tandem with risk management activities by 1) clearly articulating and communicating organizational goals to all business and resource/support units; 2) ensuring that goals and objectives are specific, measurable, attainable, realistic and trackable (SMART); 3) mandating that deviations from plans or expectations are measured and reported against goals and objectives; and 4) aligning ERM process goals and activities with organizational goals and objectives.

| Common Elements and Issues Addressed | ISO 31000: 2009 Risk Management - Principles and Guidelines | OCEG "Red Book" 2.0: 2009 GRC Capability Model | BS 31100: 2008 Code of Practice for Risk Management | COSO: 2004 Enterprise Risk Management — Integrated Framework | FERMA: 2002 A Risk Management Standard | SOLVENCY II: 2012 |
|--------------------------------------|--|--|--|---|---|---|
| ERM information and planning | 4.2 Mandate and commitment 4.3 Design of framework for managing risk 4.3.2 Establishing risk management policy 4.3.5 Resources Annex A.3.1 [establishing performance goals] | C4 Values & Objectives O1.1 Define GRC System Scope O1.2 Define GRC System Style and Goals O1.3 Obtain Commitment to the GRC System | Introduction 3.1 Governance | Effective Risk Oversight: The Role of the Board of Directors, Integrated Framework, page 35 | 7.1 Internal Reporting | Pillar 1 Quantitative Requirements: Regulations on minimum capital (Implementation) |
| Communicating goals | 4.3.6 Establishing internal communication and reporting mechanisms 4.3.7 Establishing external communication and reporting mechanisms Annex A.3.1 [communicating performance goals] | C4.6 Communicate Mission, Vision and Values P4 Awareness & Education | 3.2 Risk management strategy 3.3 Risk management policy | Application Techniques, page 67 Integrated Framework, pages 35, 67, 75 | 8.2 Role of the Board 8.3 Role of the Business Units 8.4 Role of the Risk Management Function | Pillar 3 Market Discipline: Transparency (Disclosure) |
| ERM process goals and activities | 3 Principles (b) Risk management is an integral part of all organizational processes 4.2 Mandate and commitment 4.3.4 Integration into organizational processes 4.6 Continual improvement of the framework 5.1 Process - General | P5 Human Capital Incentives M2 Performance Monitoring & Evaluation | 3.2 Risk management strategy 3.6 Roles, responsibilities and authorities 5.2.4 Developing objectives and plans | Effective Risk Oversight: The Role of the Board of Directors, Application Techniques, page 1 Integrated Framework, page 17 | 8.1 Risk Management Policy | Pillar 1 Quantitative Requirements: Regulations on minimum capital (Implementation) |

RIMS RMM ATTRIBUTES: BUSINESS RESILIENCY AND SUSTAINABILITY

Denotes the extent to which an organization integrates business resiliency and sustainability aspects for its operational planning into its ERM process by 1) evaluating how planning by business and resource/support units support resiliency and value; 2) ensuring that units acknowledge their responsibility for resiliency in their planning activities; 3) balancing short-term deliverables with longer-term value; 4) documenting logistics, security, resources and organization of response procedures; and 5) relying on analysis-based planning (for example, stress-testing investment portfolios).

| Common Elements and Issues Addressed | ISO 31000: 2009 Risk Management - Principles and Guidelines | OCEG "Red Book" 2.0: 2009 GRC Capability Model | BS 31100: 2008 Code of Practice for Risk Management | COSO: 2004 Enterprise Risk Management — Integrated Framework | FERMA: 2002 A Risk Management Standard | SOLVENCY II: 2012 |
|---|---|---|---|---|--|---|
| Analysis-based planning | 1 Scope 5.4.3 Risk analysis 5.4.4 Risk evaluation | A2.2 Analyze Current Approaches to Risk Optimization A3.1 Evaluate Risk Optimization Tactics and Activities A3.2 Determine Planned Residual Risk A3.3 Determine Optimizing Activities A3.5 Develop Risk Optimization Plan | 3.8 Risk appetite and risk profile 4.4 Risk assessment | Executive Summary, page 3 Integrated Framework, page 35 | 9. Monitoring and Review | Pillar 3 Market Discipline: Disclosure requirements (Disclosure) |
| Resiliency and operational planning (includes external communication) | 5.5 Risk treatment | P3 Preventive Controls P6 Risk Financing/ Insurance P7 Stakeholder Relations & Requirements R4 Crisis Response, Continuity and Recovery R5.3 Disclose Issue Resolution | 4.5 Responding to risks | Effective Risk Oversight: The Role of the Board of Directors, Application Techniques, pages 16, 18 Integrated Framework, page 59 | 9. Monitoring and Review | Pillar 3 Market Discipline: Competition related elements (Disclosure) |
| Understanding consequences | 5.4.3 Risk analysis | A1 Risk Identification A2.1 Analyze Inherent Risk | 4.4 Risk assessment | Application Techniques, page 55 Integrated Framework, pages 59, 61 | 6. Risk Treatment | Pillar 1 Quantitative Requirements: Investment (Implementation) |

| Demographics | ISO 31000: 2009 Risk Management - Principles and Guidelines | OCEG "Red Book" 2.0: 2009 GRC Capability Model | BS 31100: 2008 Code of Practice for Risk Management | COSO: 2004 Enterprise Risk Management — Integrated Framework | FERMA: 2002 A Risk Management Standard | SOLVENCY II: 2012 |
|--|--|--|---|--|---|--|
| Sponsoring Organization | International Organization for Standardization (ISO) | Open Compliance and Ethics Group (OCEG) | British Standards Institution (BSI) | Committee of Sponsoring Organizations (COSO) | Federation of European Risk Management Associations (FERMA) | European Commission on Insurance |
| Number of Pages | 30 pages | 239 pages | 40 pages | 125 pages | 16 pages | N/A |
| Described Scope and Intended Audience from the Documents | This international Standard provides principles and generic guidelines on risk management. This standard can be used by any public, private or community enterprise, association, group or individual. Therefore, this International Standard is not specific to any industry or sector. | GRC is ... relevant in all industries and sectors, all over the world, and ... affects all functions in a modern enterprise. | BS 31100 is intended for use by anyone with responsibility for any of the following: <ul style="list-style-type: none"> • Ensuring an organization achieves its objectives; • Ensuring risks are proactively managed in specific areas or activities; • Overseeing risk management in an organization; • Providing assurance on the effectiveness of an organization's risk management; and/or • Reporting to stakeholders, e.g. through disclosures in annual financial statements, corporate governance reports and corporate social responsibility reports. | While it is not intended to and does not replace the internal control framework, but rather incorporates the internal control framework within it, companies may decide to look to this enterprise risk management framework to satisfy their internal control needs and to move toward a fuller risk management process. Use of this report is intended for board(s) of directors, senior management, other entity personnel, regulators, professional organizations and educators. | The standard represents best practice against which [any and all] organizations can measure themselves. | Insurance companies in the European Union (EU) or underwriting risks in the EU |
| Ancillary document references | ISO 31010:2009 Risk Assessment ISO Guide 73:2009 Vocabulary | The Burgundy Book Content Domains GRC Requirements Database GRC-IT Blueprint™ | | Application Techniques Strengthening Enterprise Risk Management for Strategic Advantage | | |
| Website | www.iso.org | www.oceg.org | www.bsigroup.com | www.coso.org | www.ferma.eu | www.ec.europa.eu www.fsa.gov.uk |

APPENDIX B. OVERVIEW OF WIDELY USED RISK MANAGEMENT STANDARDS AND GUIDELINES

| | ISO 31000: 2009 Risk Management Practices and Guidelines | OCEG "Red Book" 2.0: 2009 GRC Capability Model | BS 31100: 2008 Code of Practice for Risk Management | COSO: 2004 Enterprise Risk Management Integrated Framework | FERMA: 2002 A Risk Management Standard | SOLVENCY II: 2012 A Regulatory Standard |
|--------------------------------|--|--|---|---|--|--|
| Applicable to | All industries and sectors | All industries and sectors | All industries and sectors | Companies interested in satisfying internal control needs and in moving to a fuller risk management process | All organizations | Insurance companies located in or doing business in the European Union |
| Primary Objective ¹ | Organizational | Compliance and Control | Organizational | Organizational, Compliance and Control | Organizational | Regulatory |
| Type of Document ² | Primary standard | Guidance document | Primary standard | Guidance document | Guidance document | Primary standard |

1. ORGANIZATIONAL

Designed to improve an organization's ability to meet or exceed its objectives through enhanced decision-making and activities that address key uncertainties.

COMPLIANCE AND CONTROL

Seeks to assure the transfer or mitigation of risks primarily through compliance and control objectives and activities; often based on historic losses, near-misses, etc.

REGULATORY

Used when an organization must apply a designated practice and/or standard in order to meet regulatory requirements.

2. **PRIMARY STANDARD** (or "recognized" standard) as an established norm or requirement, usually a formal document that establishes criteria, methods, processes and practices under the jurisdiction of an international, regional or national standards body. It may be used for regulatory compliance; public validation, verification and/or possibly certification; generally accepted knowledge about risk topic; may provide formal implementation guidance.

GUIDANCE DOCUMENT or framework, custom, convention, company product, corporate standard, etc. that may be developed outside of a recognized standard setting body. When the document becomes generally accepted and dominant, it is often called a de facto standard. It is generally used for internal operational or process implementation guidance.

APPENDIX C: OVERVIEW OF COMMON ELEMENTS OF WIDELY USED RISK MANAGEMENT STANDARDS AND GUIDELINES

| RIMS RMM ATTRIBUTE | ISO 31000 | OCEG | BS 31100 | COSO | FERMA | SOLVENCY II |
|--------------------------------------|-----------|------|----------|------|-------|-------------|
| ERM-Based Approach | X | X | X | X | X | X |
| Process Management | X | X | X | X | X | X |
| Risk Appetite Management | X | X | X | X | X | X |
| Root Cause Discipline | X | | X | | | X |
| Uncovering Risks | X | X | X | X | X | X |
| Performance Management | X | | X | X | X | X |
| Business Resiliency & Sustainability | X | X | | | | X |

APPENDIX D: COMMENTARY ON STANDARDS

BENEFITS OF USING RECOGNIZED STANDARDS

Recognized standards provide a number of benefits. They generally have been vetted and benchmarked as best practices for decision-making. They rely on a management system rather than a program to allow adoption within all levels of an organization. They are inclusive in development, which provides a broad perspective on successful controls and procedures. Most importantly, they help establish reasonable and measurable goals that can be tied to articulated organizational objectives. Organizations can choose to be certified against certain standards such as ISO 9001:2008 Quality Management Requirements or ISO 14001:2004 Environmental Management Requirements, for example.

That said, there is value to understanding and using whatever portions of the standards that can help an organization meet its objectives. One of the benefits is that standards can provide ideas about how to launch and organize a program. And since the process of standards making is inclusive, it gives some assurance for consensus and provides impetus for specialized training. They can also be used for outside organizations to benchmark against a particular standard. In fact, in some cases, certification to certain standards can reduce the number of outside audits as company is asked to undertake. For example, being ISO 14000 certified can put a company on a list of potential vendors for chemical manufacturers. Without it, the company might not be invited to bid. (It is important to note that ISO 31000, unlike ISO 9000 and 14000, is not intended for certification.)

Using standards may be a proactive way to protect your brand and reputation, in addition to providing a defensible position. The bottom line benefit for using standards is that, whatever else you take from them, their use can make your organization more resilient in the face of emerging risks and adverse events.

BACKGROUND ON PRIMARY STANDARDS

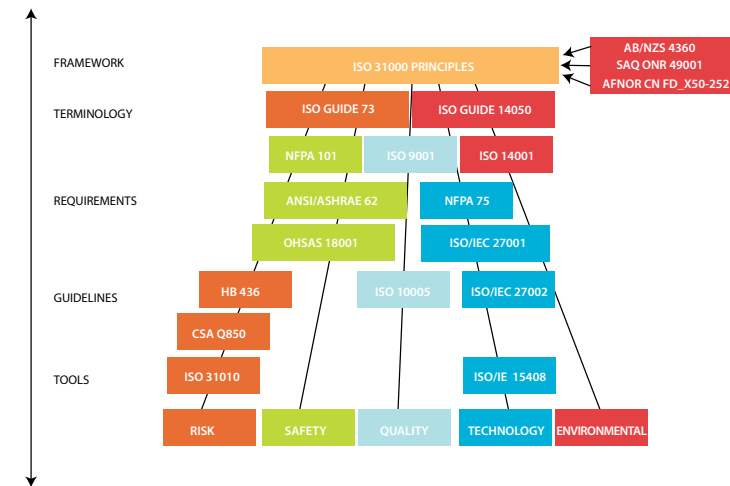
Consider how standards are made. Generally, primary or recognized standards are made at international, national and regional levels.

ISO (International Organization for Standardization) is the recognized international standards-setting body. It is the world's largest developer and publisher of international standards and forms a bridge between public and private sectors. Think of it as a network of the national standards institutes of 162 countries. As a non-governmental organization, ISO does not regulate, legislate or enforce.

Many standards start out as national standards and through consensus-building among member countries, become adopted and published as an ISO standard. This is exactly how ISO 31000 was developed. Generally, once ISO or a regional standards body such as CEN (the European Committee for Standardization) adopts a standard, the individual national standards are dissolved. Countries may choose an international standard such as ISO 31000 as its national standard through the recognized national standards organizations. The American National Standards Institute (ANSI), the Canadian Standards Association (CSA) and the Australian Standards (AS) and New Zealand Standards (NZS) organizations have all recently adopted ISO 31000: 2009 as their respective national risk management standards.

It is important to recognize that there is no single standard that covers an entire field. Rather, there are "families of standards" that appear in a hierarchy from framework, to terminology to requirements, and may include guidelines and tools. A few of the standards that risk managers typically face are listed in the figure to the right. By adding national, regional and "de facto" standards, and one can begin to appreciate just how ubiquitous standards really are.

A Selection of Standards



Benefits of Using Recognized Standards

- Set of benchmark tools and processes
- Systematically identify risks and obstacles
- Problem-solving and decision-making tools
- Inclusive process
- Specialized training
- Establishes operational controls/procedures
- Measurable/verifiable goals and methods for accomplishing identified objectives
- Protect reputation and brand
- Model for continual improvement
- Proactively improve organizational resiliency and sustainability