Securities and Exchange Commission
Chairman Mary Shapiro
100 F Street, N.E., room 10700
Washington, D.C. 20549
RE: SEC Release NOS. 33-9052 Proxy Disclosure and Solicitation Enhancements, File Number S7-13-09

Dear Madame Chair:

The Securities and Exchange Commission has proposed an expansion of the disclosure requirements for public companies to include information regarding the role of the board of directors in the management of risk (SEC Release NOS. 33-9052 34-60280 IC-28817 File S7-13).

The goals outlined to enhance transparency on activities that materially contribute to risk profile are well articulated. Please find below three enhancements that would make the SEC ruling even more effective in achieving the desired results.

1) Requirements are needed for businesses to disclosure their enterprise risk management processes. The process of determining which risks materially contribute to a company's risk profile is as important as the disclosures themselves. A robust objective and repeatable process is required to extend down to the level of risk where activity occurs. Corporations need to disclose how they directly engage front line management in their analysis to uncover and address risks with material impact.

In the RIMS State of ERM Report that I authored (see attached or download from www.rims.org/rmm) it was determined that 96% of public sector organizations do not have an adequate enterprise risk management process in place. However, those organizations achieving a managed level of maturity in their enterprise risk management processes will already have the complete and accurate information to satisfy this new SEC disclosure ruling with minimal additional time. Requiring transparency on how a corporation achieves risk management competency is critical to the completeness and accuracy of the corporation's disclosures.

2) A standard set of industry independent enterprise risk management guidelines should be referenced in the SEC ruling so that boards, management, regulators, auditors and rating agencies can objectively evaluate and measure risk management competency.

To objectively measure risk management competency across different organizations and across different industry segments these critical process aspects must be in place.
1. Formalized industry independent indicators to measure risk competency
2. Infrastructure to gather information and perform analysis in a timely fashion and
3. Robust and consistent scoring methodology relevant to all risk cultures, processes and industries.

The Risk and Insurance Management Society's Risk Maturity Model for ERM (RMM)(see attached or download from www.rims.org/rmm) meets all three of these criteria. In 2007, risk practitioners from

564 organizations of all types participated in an in-depth assessment of their ERM practices. Using the RMM, participants assessed their organizations ERM program against 68 key readiness indicators identified as risk management competency drivers across all industries. The result of the study concluded at the 95% confidence level the positive correlation—the direct relationship—between higher RMM scores and higher business performance. Providing transparency on the standards used to measure competency provides for true accountability.

3) Compensation needs to be tied to risk management competency at the front-line management level. According to the RIMS State of ERM Report direct, extensive involvement in ERM by front-line management at all levels is the competency driver that is most strongly positively correlated with higher business performance. Three other competency drivers that also have strong correlation are:
1. the degree to which risk assessments are effectively conducted by all business areas and aggregated
2. the extent to which corporate goals and risk management issues are clearly understood at all levels and
3. the depth to which ERM is woven into strategy and planning.

There remains a significant disconnect between the knowledge of risk management processes at the executive team level versus what actually takes place on the front-line. Formally tying a portion of compensation to risk management competency, the type of imbalance between risk and reward will be effectively addressed. Using the existing performance review process as a mechanism to assess this risk management competency will incent both front-line management and senior management with minimal impact to operations. ERM should not be conducted in a silo as a separate activity, but rather it is a standardized and common framework approach to operational management to surface and prioritize the most material issues for remediation or disclosure. Requiring compensation to be meaningfully tied to achievement of risk management competency at all levels produces the behavior that is paid for.

In closing, the new disclosures proposed by the SEC with these clarifications will benefit all stakeholders of all industries by increasing the transparency of the registrant's enterprise risk management competency which has been proven to be correlated positively and directly with increased business performance.

Warm regards,

Steven Minsky
Chief Executive Officer
LogicManager, Inc.

November 27, 2006

RIMS Risk Maturity Model (RMM) for Enterprise Risk Management

To benchmark your ERM program and receive a personalized assessment, go to http://www.RIMS.org/RMM

Risk and Insurance Management Society, Inc.®

Preface and History

The Risk and Insurance Management Society, Inc. (RIMS) is a nonprofit organization dedicated to advancing risk management, a profession that protects physical, financial and human resources. Founded in 1950, RIMS represents nearly 3,900 industrial, service, nonprofit, charitable and government entities. The society serves about 9,600 risk management professionals around the world.

RIMS has adopted Enterprise Risk Management (ERM) as a core competency and will dedicate significant resources to it. To build an Enterprise Risk Management community, RIMS has launched the Enterprise Risk Management Center for Excellence. This provides educational and networking opportunities for members and coordinates important ERM resources. John Phelps, a RIMS board member, is chairman of the RIMS ERM Development Committee. The ERM Committee recognized the need for ERM education and a mechanism for measuring ERM maturity, so it created a Risk Maturity Model to let organizations reach risk management's next level.

The ERM Committee recognized the value of partnering with an expert ERM solutions provider to tap RIMS' practitioners' expertise and create the RIMS Risk Maturity Model. RIMS selected LogicManager, a leading developer of Enterprise Risk Management solutions and creator of its own innovative risk maturity model. LogicManager, based in Boston, donated its intellectual property, expertise and services and the RIMS Risk Maturity Model was born.

This RIMS Risk Maturity Model is primarily an educational and benchmarking resource for Chief Risk Officers and other risk professionals to collaborate with their Board of Directors, senior management, operations management and managers from support functions of IT, internal audit, compliance, etc.

Acknowledgements

Risk and Insurance Management Society, Inc. (RIMS) wishes to recognize:

ERM Development Committee

ERM Development Committee Chair
John Phelps, *Director of Risk Management, Blue Cross and Blue Shield of Florida, Inc.*

ERM Development Committee Vice Chair
Carol Fox, *Senior Director, Risk Management, Convergys Corporation*

ERM Development Committee Liaison
Mary Roth, *Executive Director, Risk and Insurance Management Society, Inc. (RIMS)*
1065 Avenue of the Americas, 13th Floor, New York, NY 10018 Phone: 212.286.9292

ERM Development Committee Members

Eric Benson, *Principal Risk Analyst, Corporate Risk Management, Allianz Life Insurance Co. of NA*
Roy Fox, *Enterprise Risk Management Manager, Bonneville Power Administration*
Dan Kugler, *Assistant Treasurer, Risk Management, Snap-on Inc.*
Michael Maida, *Corporate Risk Manager, Agricore United*
Joanna Makomaski, *P. Eng., Manager, Risk Management, Enbridge Gas Distribution Inc.*
Julie Pemberton, *ARM, Manager, Enterprise Risk Management, Chiquita Brands International Inc.*
Beaumont Vance, *Senior Enterprise Risk Manager, Sun Microsystems Inc.*

ERM Risk Maturity Model Developer

Steven Minsky, *Chief Executive Officer, LogicManager, Inc. (www.logicmanager.com)*
30-31 Union Wharf, Boston, MA 02109
Phone: 617.649.1320

We welcome your feedback. Please provide us your comments and questions on the RIMS Risk Maturity Model to: steven.minsky@logicmanager.com.

Board of Directors Members

President
Michael Liebowitz, *Director of Insurance and Risk Management, New York University*

Vice President
Janice Ochenkowski, *Managing Director, Jones Lang LaSalle*

Treasurer
Deborah Luthi, *Director, Risk Management Services, University of California, Davis*

Secretary
Joseph Restoule, *Senior Risk Consultant, NOVA Chemicals Corporation*

Directors
Janet Barnes, *Snohomish County PUD No. 1*
Karen Beier, *Vice President, Risk Management, Shaklee Corporation*
Scott Clark, *Risk & Benefits Officer, Miami-Dade County Public Schools*
Terry Fleming, *Director, Division of Risk Management, Montgomery County, Maryland*
Michael Gaona
Jackie Hair, *Corporate Director, Worldwide Risk Management, Ingram Micro Inc.*
John Hughes, *Director, Risk Management, Alex Lee, Inc.*
Kim Hunton, *Risk Manager, City of Ottawa*
Daniel Kugler, *Assistant Treasurer, Risk Management, Snap-on Inc.*
Janice McGraw, *Manager, Risk Management & Insurance, McGill University*
John Phelps, *Director of Risk Management, Blue Cross and Blue Shield of Florida, Inc.*
Ellen Vinck, *Vice President, Risk Management & Benefits, BAE Systems Ship Repair*

RIMS Risk Maturity Model (RMM) for Enterprise Risk Management

Overview

Smart, dedicated workers aren't enough. The Software Engineering Institute (SEI) at Carnegie-Mellon University, which pioneered the Maturity Model concept in the mid-1980s, said, "Everyone realizes the importance of having a motivated, quality work force and the latest technology, but even the finest people can't perform at their best when the process is not understood or operating at its best." Enterprise Risk Management (ERM) is a process. What is lacking, is a tool for objective and consistent measurement of its effectiveness. The RIMS ERM Development Committee and LogicManager stepped in to develop this missing link -- the RIMS Risk Maturity Model. A benchmarking framework designed to create clear, precise criteria, RIMS Risk Maturity Model (RMM) facilitates thorough planning and communication and guides monitoring and control.

The role of the RIMS Risk Maturity Model for Enterprise Risk Management

If Enterprise Risk Management is the weapon, the RIMS Risk Maturity Model (RMM) is the plan of attack. The RIMS RMM provides ERM practitioners with a way to combine all the best elements from the most important models and standards. This applies to all industries and across the risk spectrum. This RIMS RMM is a ladder of progressively organized and mature performance levels, a way to evaluate and set goals.

Focus the risk picture

While the risk officer ranks fill up rapidly, most learn on the job. They come to risk management with a variety of backgrounds -- legal, finance, internal audit, risk management, compliance or IT. Their views tend to align with their backgrounds and responsibilities. Rigorous controls might take precedence for the internal auditor, for instance, while regulations might be a priority for the compliance team. Security might be key for the information technology group and brand and company reputation could be a top goal for marketing.

The smart risk officer recognizes the importance of all of those, but doesn't stop there. The team must also be led to balanced, big-picture decisions. The RIMS RMM crystallizes the risk picture by analyzing best practices and setting goals. This lets the risk officer and stakeholders build consensus about priorities and tactics. A common approach ensures results – efficiencies in the short term, reduced uncertainty in routine decisions in the mid-term and, in the long term, a competitive advantage gained by making big bets on emerging trends. For both veteran risk managers and novices, RIMS RMM is an indispensable tool that provides a game plan for program development and enhances risk management. And it also speeds the delivery of a rock-solid ERM Process, building a foundation for improving programs, strengthening objectivity and prioritizing resources for allocation.

Benefits of using a Maturity Model

The Maturity Model approach is a method that's proven across a variety of industries. Based on extensive case studies in which a Maturity Model approach was used over the past 25 years, the evidence shows that with each step up in maturity level, organizations get concrete results. A Maturity Model is a structured way of highlighting aspects of effective ERM Processes.

Benefits for Practitioners

- Build consensus and establish milestones.
- Benchmarking from best practices.
- Communicate clearly to the board, regulators, rating agencies, executive management, process owners, support functions (back office groups such as internal audit, IT and compliance), etc.

Benefits for ERM stakeholders

- Streamline the ERM Process.
- Eliminate duplication of efforts and connect support functions with process owners.
- Measure ERM value, based on priorities.
- Create a shared language and vision.

Benefits for Organizations

- Tackle inadequately addressed risks and opportunities.
- Resolve business process inefficiencies.
- Build a repeatable and scalable process for better decision making

Reduce costs

Understanding a risk's root cause is much cheaper than simply treating the symptom. ERM uncovers and attacks the root cause. Example: a global energy company tried to save 10 percent on maintenance costs, but

pipeline leaks cost them billions of dollars in clean-up costs and damage to their reputation. ERM connects the root cause to the ultimate cost and improves decision making at a fraction of the cost.

Increase top line revenue
A compliance issue can lead to rethinking business strategy and finding an opportunity to generate revenue. Example: a bank responds to a government regulation requiring it to switch from paper checks to digital images. It uses ERM to uncover a strategy to acquire customers nationally, rather than regionally, by expanding where it once had no infrastructure to transport paper checks. ERM helps managers think strategically.

Reduce variance on plan achievement reporting. Planning is essential to success and allocating resources. Uncertainty in planning leads to bad decisions. Volatility of earnings effects stock prices because it undermines confidence in the planning cycle. ERM uncovers the uncertainty and helps managers plan better, creating more reliable results. Example: Bad weather doesn't make workers late, but ignoring the weather forecast and not leaving extra time for inevitable delays does. ERM is about using the weather report that lets workers understand the likelihood that a storm will occur. The impact is the size of the storm and the controls' effectiveness are the alternate routes to work.

> "ERM – considering risk in a new way."

To determine how these benefits apply to your organization, conduct a baseline assessment and use real observations and details to create an effective ERM process that produces results.

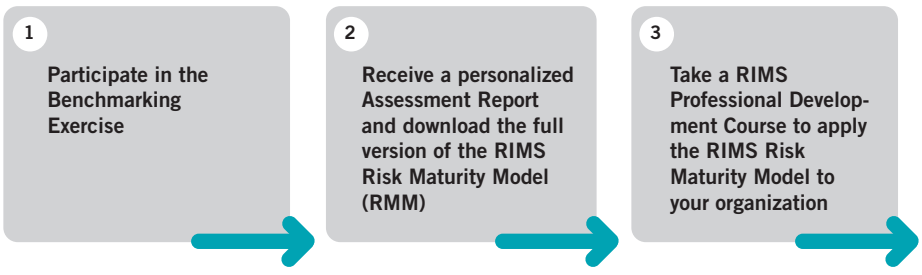
How to use the RIMS RMM

Culture is the way we think, believe and behave. A risk management competency is made up of a set of common values about how we manage risk and uncertainty. The culture within an organization greatly affects the drives the effectiveness of an ERM program including how we value skepticism and doubt, and how clearly we understand influences that impact our judgment. The RIMS Risk Maturity Model (RMM) defines the elements and characteristics, called attributes, that make up a strong risk management competency within the organization's culture. The RIMS RMM defines these seven attributes on a scale of five maturity levels. Each level ranks an organization according to its achievement of Enterprise Risk Management best practices in its processes. A chain is only as strong as its weakest link. A strong risk management cultural competency is demonstrated by the highest level on each of the RIMS Risk Maturity Model Attributes.

RIMS RMM Professional Development Courses

RIMS offers professional development courses that provide the methodology of how to maximize the RIMS RMM to build stronger ERM programs and achieve success by evolving a stronger risk management competency within an organization's existing culture. Measuring where you are in the development process is the first step to set goals and measure progress this organizational competency. The RIMS courses help risk managers perform a gap analysis between capabilities and best practices outlined in the RIMS RMM to achieve higher capability. Objective evaluation criteria and a scoring methodology provide the basis to evaluate use of risk management best practices. The concept of a cost-benefit analysis helps managers prioritize goals within their ERM programs to increase their capabilities and maturity level.

In utilizing the RIMS RMM, everyone assesses their own business areas, contributes to ERM goals and plans how to achieve them. Often, it's the way information is collected and used that influences choices, not the information itself. With the RIMS RMM, all stakeholders are involved in the process, meaning everyone rallies around the final results.



Stronger risk management cultural competency

RIMS Risk Maturity Model (RMM) Definition of Terms

Enterprise Risk Management (ERM) Framework

The culture, processes and tools to identify strategic opportunities and reduce uncertainty. The framework establishes communication and consultation methods with respect to critical risks in order to achieve an organization's business objectives. It formalizes process and content accountability. The ERM Process is the time-tested foundation of risk management methodology, pioneered by the risk management discipline and detailed in the Associate in Risk Management (ARM) designation program. It was later adopted and enhanced by other standards organizations[1]

The ERM Process

A sequential process that supports the reduction of uncertainty and promotes the exploitation of opportunities. The ERM Process steps are detailed below.

Plan Focus - Establish external, internal and risk management criteria for evaluating risk.

1. **Identify where, when, why and how business model, market, events, and operations, etc. associated with business changes, issues, and others – whether known or under-reported – might prevent, degrade or support goals.**

2. **Assess perceived risk through consistent, objective and pervasive evaluation criteria of impact, likelihood and effectiveness of controls to quantify the risk level. Potential opportunity is measured by impact, timeliness and assurance to examine the performance level. This creates a way to calculate an internal index. This analysis considers the range of potential consequences, and how to prioritize risks and opportunities. The residual risk or potential gain is determined.**

3. **Evaluate risk tolerance to determine acceptable risk and opportunity levels and consider the balance between potential benefits and drawbacks. Decide on scope, priorities and timelines.**

4. **Mitigate risk and exploit opportunities. Develop risk or opportunity activities for reducing uncertainty, increasing potential benefits and reducing potential costs. Collaborate with stakeholders and leverage expertise (Six Sigma[2], compliance, internal audit and others) to design improvement, transfer, control and other action activities. Weigh the cost of activities against the expected value of future uncertain events[3]**

5. **Monitor timeliness and effectiveness of mitigation activities by risk owners. Gauge program to ensure changing circumstances do not alter priorities and escalate issues. Unacceptable tolerance and mitigation should be reported to the appropriate manager.**

Business Process Owner

the individual (s) responsible for process design and performance. The process owner is accountable for sustaining the gain and identifying risk and future improvement opportunities on the process

Risk Owner

the individual who is accountable for the validation, assessment and action plan to care for a particular risk[4]

Risk Plan

the basic communication for each specified Plan Focus that is used throughout the ERM Process to gather, organize and report information. Its items might also include contacts, activities, journal entries, notes and documents.

Attributes

Similar to individual employee performance evaluations, the RIMS RMM provides a set of attributes that drive business value. The RIMS RMM Attributes are designed to be compatible with various specialized frameworks, such as the Australian/New Zealand Risk Standard, COSO ERM, COBIT 4.0, Standard & Poor's ERM, Sarbanes-Oxley, etc.[5]

Maturity Levels

Detailed descriptions for each Attribute provide five maturity levels ranging from Non-existent to Leadership. Organizations measure their ERM Process against these maturity levels and set improvement targets.

Benchmarking

Using the RIMS Risk Maturity Model, RIMS sponsors cross-industry benchmarking to identify emerging trends. RIMS and non-RIMS members are invited to participate in this global exercise. Comparing maturity levels of other organizations highlights ERM priorities and evolving industry requirements. For more information on participating in the benchmarking survey, go to the Enterprise Risk Management (ERM) Center of Excellence page on the RIMS website. (http://www.RIMS.org/ERM)

[1]Standards Australia International Ltd and Standards New Zealand (The AS/NZL 4360), 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, ISO/IEC Guide 73, JIS Q 2001 Japanese Industrial Standards Committee "International Risk Management Standard", COSO Enterprise Risk Management Integrated Framework 2004 "Treadway commission", Canadian BIP 2012, CAN/CSA Q850-07, etc.

[2]Six Sigma definition, Trademark of Motorola corporation

[3]Taking into consideration whatever is appropriate for the organization to approve an action plan including capital at risk, Risk Adjusted Return on Capital (RAROC), cost benefit analysis, time value of money discounted in net present value, etc.

[4]For the context of this document Process Owners are assumed to be Risk Owners. However, in some organizations the risk owner may or may not be the same as the process owner. For example in the case where a process is outsourced, the risk owner remains within the corporation.

[5]Examples of specialized approaches: **COSO ERM Framework**: Internal Environment, Objective Setting, Event Identification, Risk Assessment, Risk Response, Control Activities, Information & Communication, Monitoring; **Standard & Poor's ERM**: Risk Management Culture, Risk Controls, Extreme-event Management, Risk and Capital Models, Strategic Risk Management; **COBIT Report Framework**: Awareness and Communication, Policies, Standards and Procedures, Tools and Automation, Skills and Expertise, Responsibility and Accountability, Goal Setting and Measurement.

The RIMS Risk Maturity Model:

Attributes

These core competencies measure how well risk management is embraced by management and ingrained within the organization. A maturity level is determined for each attribute and ERM maturity is determined by the weakest link.

1. **ERM-based approach** - Degree of executive support for an ERM-based approach within the corporate culture. This goes beyond regulatory compliance across all processes, functions, business lines, roles and geographies. Degree of integration, communication and coordination of internal audit, information technology, compliance, control and risk management.
2. **ERM process management** - Degree of weaving the ERM Process into business processes and using ERM Process steps to identify, assess, evaluate, mitigate and monitor. Degree of incorporating qualitative methods supported by quantitative methods, analysis, tools and models. See ERM Process definitions.
3. **Risk appetite management** – Degree of understanding the risk-reward tradeoffs within the business. Accountability within leadership and policy to guide decision-making and attack gaps between perceived and actual risk. Risk appetite defines the boundary of acceptable risk and risk tolerance defines the variation of measuring risk appetite that management deems acceptable.
4. **Root cause discipline** - Degree of discipline applied to measuring a problem's root cause and binding events with their process sources to drive the reduction of uncertainty, collection of information and measurement of the controls' effectiveness. The degree of risk from people, external environment, systems, processes and relationships is explored.
5. **Uncovering risks** - Degree of quality and penetration coverage of risk assessment activities in documenting risks and opportunities. Degree of collecting knowledge from employee expertise, databases and other electronic files (such as Microsoft® Word, Excel®, etc) to uncover dependencies and correlation across the enterprise.
6. **Performance management** - Degree of executing vision and strategy, working from financial, customer, business process and learning and growth perspectives, such as Kaplan's balanced scorecard, or similar approach. Degree of exposure to uncertainty, or potential deviations from plans or expectations.
7. **Business resiliency and sustainability** – Extent to which the ERM Process's sustainability aspects are integrated into operational planning. This includes evaluating how planning supports resiliency and value. The degree of ownership and planning beyond recovering technology platforms. Examples include vendor and distribution dependencies, supply chain disruptions, dramatic market pricing changes, cash flow volatility, business liquidity, etc.

Maturity Levels

Five maturity levels for each RIMS RMM Attribute with diminishing maturity from level 5 to level 1. ERM is a process and the Attributes below evaluate its quality and determine a maturity level.

Key Drivers

Profiling issues that best differentiate maturity levels within an attribute. Key drivers for each attribute summarize the Maturity Model. The full Maturity Model attributes measure an ERM Process and help set goals for improvement.

Attributes	Maturity Levels					
	Level 5: **Leadership**	Level 4: **Managed**	Level 3: **Repeatable**	Level 2: **Initial**	Level 1: **Ad hoc**	**Nonexistent**
1 Adoption of ERM-based approach	**Key Drivers: Degree of ...** • support from senior management, Chief Risk Officer • business process definition determining risk ownership • assimilation into support area and front-office activities • far-sighted orientation toward risk management • risk culture's accountability, communication and pervasiveness					
2 ERM process management	**Key Drivers: Degree of ...** • each ERM Process step (see definition) • ERM Process's repeatability and scalability • ERM Process oversight including roles and responsibilities • risk management reporting • qualitative and quantitative measurement					
3 Risk appetite management	**Key Drivers: Degree of ...** • risk-reward tradeoffs • risk-reward-based resource allocation • analysis as risk portfolio collections to balance risk positions					
4 Root cause discipline	**Key Drivers: Degree of ...** • classification to manage risk and performance indicators • flexibility to collect risk and opportunity information • understanding dependencies and consequences • consideration of people, relationships, external, process and systems views					
5 Uncovering risks	**Key Drivers: Degree of ...** • risk ownership by business areas • formalization of risk indicators and measures • reporting on follow-up activities • transforming potentially adverse events into opportunities					
6 Performance management	**Key Drivers: Degree of ...** • ERM information integrated within planning • communication of goals and measures • examination of financial, customer, business process and learning • ERM process goals and activities					
7 Business resiliency and sustainability	**Key Drivers: Degree of ...** • integration of ERM within operational planning • understanding of consequences of action or inaction • planning based on scenario analysis					

Attribute 1 ERM-based approach

Degree of executive support for an ERM-based approach within the corporate culture. This goes beyond regulatory compliance across all processes, functions, business lines, roles and geographies. Degree of integration, communication and coordination of internal audit, information technology, compliance, control and risk management.

Nonexistent

No recognized need for an ERM Process and no formal responsibility for ERM. Internal audit, risk management, compliance and financial activities might exist but aren't integrated. Business processes and risk ownership aren't well defined.

Level 1: Ad hoc

Corporate culture has little risk management accountability. Risk management is not interpreted consistently. Policies and activities are improvised. Programs for compliance, internal audit, process improvement and IT operate independently and have no common framework, causing overlapping risk assessment activities and inconsistencies. Controls are based on departments and finances. Business processes and process owners aren't well defined or communicated. Risk management focuses on past events. Qualitative risk assessments are unused or informal. Risk management is considered a quantitative analysis exercise.

Level 2: Initial

Risk culture is enforced by policy interpreted as compliance. An executive champions ERM management to develop an ERM Process. One area has used the ERM Process, as shown by the department head and team activities. Business processes are identified and ownership is defined. Risk management is used to consider risks in a far-sighted manner.

Level 3: Repeatable

ERM risk plans are understood by management and the organization. Senior management expects that a risk management plan includes a qualitative risk assessment for significant projects, new products, business practice changes, acquisitions, etc. Most areas use the ERM Process and report on risk issues. Process owners take responsibility for managing their risks and opportunities. Risk management creates and evaluates far-sighted scenarios.

Level 4: Managed

Risk culture is associated with career advancement. The organization is self-governed with shared ethics and trust; promise-makers are held accountable. Risk management issues are understood at all levels and risk plans are conducted in all business process areas. The Board of Directors, CEO and Chief Risk Officer expect a risk management plan to include a qualitative risk assessment for significant projects, new products, business practice changes, acquisitions, etc. with reporting to the Board on priorities. All areas use the ERM Process to enhance their functions via the ERM framework, with frequent and effective communication on risk issues. Process owners incorporate managing their risks and opportunities within regular planning cycles. All areas create and evaluate far-sighted scenarios and follow-up activities.

Level 5: Leadership

Risk culture is analyzed and reported as a systematic view of evaluating risk. Executive sponsorship is strong and the tone from the top has sewn an ERM Process into the corporate culture. Board of Directors, senior management and the Chief Risk Officer communicate risk management's importance in daily decisions. Risk management is embedded in each business function. Internal audit, information technology, compliance, control and risk management are highly integrated and coordinate and report risk issues. All areas use risk-based best practices. The risk management lifecycle for each business process area is routinely improved.

Attribute 2 ERM process management

Degree of weaving the ERM Process into business processes and using ERM Process steps to identify, assess, evaluate, mitigate and monitor. Degree of incorporating qualitative methods supported by quantitative methods, analysis, tools and models. See ERM Process definitions.

Nonexistent
There's little recognition of the ERM Process's importance.

Level 1: Ad hoc
Management is reactive and ERM might not yet be seen as a process. Few processes are standardized and are improvised instead. There are no standard risk assessment criteria. Risk management is involved in business initiatives only in later stages or centrally. Risk roles and responsibilities are informal. Risk assessment is improvised. Standard collection and assessment processes aren't identified.

Level 2: Initial
Management recognizes a need for an Enterprise Risk Management Process. Agreement exists on a framework, which describes roles and responsibilities. Evaluation criteria are accepted. Risk mitigation activities are sometimes identified but not often executed. Qualitative assessment methods are used first in all areas and determine what needs deeper quantitative methods, analysis, tools and models.

Level 3: Repeatable
The ERM Process accommodates all business and support areas' needs. ERM is a process of steps to identify, assess, evaluate, mitigate and monitor. ERM Process includes the management of opportunities. An Enterprise Risk Council exists and senior management actively reviews risk plans. The ERM Process is collaborative and directs important issues to senior management.

Level 4: Managed
Management is clearly defined and enforced at every level. A risk policy articulates management's responsibility for risk management, according to established risk management processes. An Enterprise Risk Council exists and management develops and reviews risk plans. The ERM Process is coordinated with managers' active participation. Opportunities associated with risk are part of risk plans' expected outcome. Authentication, audit trail, integrity and accessibility promote roll-up information and information sharing. Periodic reports measure ERM progress for stakeholders, including the Board of Directors.

Level 5: Leadership
ERM, as a management aspect, is embedded in all business processes and strategies. Roles and responsibilities are process driven with teams collaborating across central and field positions. Risk and performance assumptions within qualitative assessments are routinely revisited and updated. The organization uses an ERM process of sequential steps that improves decision-making and performance. A collaborative, enterprise-wide approach includes all supporters. Accountability for risk management is woven into all processes, support functions, business lines and geographies as a way to achieve goals.

Attribute 3 Risk appetite management

Degree of understanding the risk-reward tradeoffs within the business. Accountability within leadership and policy to guide decision-making to attack gaps between perceived and actual risk. Risk appetite defines the boundary of acceptable risk and risk tolerance defines the variation of measuring risk appetite that management deems acceptable.

Nonexistent
The need for formalizing risk tolerance and appetite isn't understood.

Level 1: Ad hoc
Risk management might lack a portfolio view of risk. Risk management might be viewed as risk avoidance and meeting compliance requirements or transferring risk through insurance. Risk management might be a quantitative approach focused on the analysis of high-volume and mission-critical areas.

Level 2: Initial
Risk assumptions are only implied within management decisions and aren't understood outside senior leadership with direct responsibility. There's no ERM framework for resource allocation. Defining different views of business areas from a risk perspective can't be easily created and compared.

Level 3: Repeatable
Risk assumptions within management decisions are clearly communicated. There's a structure for evaluating risk on an enterprise-wide basis and for gauging risk tolerance. Risks and opportunities are routinely identified, evaluated and executed in alignment with risk tolerances. The ERM framework quantifies gaps between actual and target tolerances as part of the ERM Process. Portfolio views to balance risk positions are created and risk tolerance is evaluated based on portfolio analysis.

Level 4: Managed
Risk appetite is considered in each ERM Process step. Resource allocation decisions consider the evaluation criteria of business areas. The organization forecasts planned mitigation's potential effects versus risk tolerance as part of the ERM Process. Portfolio views are dynamic and risk tolerance is evaluated based on different views. Risk is managed by process owners. Risk tolerance is evaluated as a decision to increase performance and measure results. Risk-reward tradeoffs within the business are understood and guide actions.

Level 5: Leadership
A process for delegating authority to accept risk levels is communicated throughout the organization. Risk management uncovers risk, reduces uncertainty and costs and increases return on equity by risk awareness. The management team and Enterprise Risk Council define tolerance levels for all departments. A mechanism compares and reports actual assessed risk versus risk tolerance. The organization manages business areas and has portfolio collection to balance risk positions. Management prioritizes resource allocation based on the gap between risk appetite and assessed risk and opportunity. The established risk appetite is examined periodically as part of planning. Example: Take more risk and gain more market share versus a conservative hold position and protect the brand.

Attribute 4 Root cause discipline

Degree of discipline applied to measuring a problem's root cause and binding events with their process sources to drive the reduction of uncertainty, collection of information and measurement of the controls' effectiveness. The degree of risk from people, external environment, systems, processes and relationships is explored.

Nonexistent

The effects of risky events might be identified but not linked to goals. Events aren't associated with their process sources.

Level 1: Ad hoc

Cost savings aren't evaluated based on risk-based consequences. Risks aren't consistently evaluated. Perceived risk's frequency isn't tracked or connected to a process. Risk indicators and goals aren't organized within a framework and aren't central to the ERM Process. Many root causes have a wide array of implications. Does not formally track root causes throughout the ERM Process.

Level 2: Initial

The cause and effect chain from the top-down and the bottom-up isn't defined. Only past risk events are considered, leaving most possible risk areas not covered. A terminology and classification for collecting risk information exists. Awareness of a root cause approach's importance exists, but no robust scheme organizes risk indicators or performance indicators as the core of a risk management framework and ERM Process.

Level 3: Repeatable

The cause and effect chain from the top-down and the bottom-up is understood. A terminology and classification for collecting risk information is used. The ERM framework is organized around root cause risk categories such as internal people, external environment, relationships, systems and processes. The root cause approach is important in each ERM Process step, from the Identify step, to ensure all risk sources' are reviewed, to the Monitor step, to verify that the problem -- not the symptom --is attacked. Scenarios are developed and the root cause that makes the difference in scenario outcomes between worse case and best case are uncovered.

Level 4: Managed

A terminology and classification for collecting risk information is fully implemented. Causes, rather than only results, are identified, measured and managed. Risk and performance information is collected from all areas to identify dependencies and root cause indicators' frequency. Residual risk's financial implications are managed without distortive double counting within risk assessments. Operational, financial and strategic risks' root cause drivers are investigated, defined, quantified and routinely monitored. Scenario analysis is used throughout planning. Events are associated with their process sources to drive progress and measure the controls' effectiveness.

Level 5: Leadership

Mitigation measures are determined and a method to quantify effectiveness is understood. There's an obvious focus on root cause to achieve goals and maximize risk's upside. The organization uses "post mortems" to deconstruct past events (either its own or others') into root cause categories to prepare for future events. Scenarios are developed to evaluate potential benefits and drawbacks on a risk-adjusted basis. The organization tracks events and traces root cause in evaluating cost benefits of improvements. Risk elements' frequencies are identified and monitored. The discipline of reviewing all risky avenues is promoted to provide a comprehensive view of risk and opportunity. This is proactive risk management, rather than problem management.

Attribute 5 Uncovering risks

Degree of quality and penetration coverage of risk assessment activities in documenting risks and opportunities. Degree of collecting knowledge from employee expertise, databases and other electronic files (such as Microsoft® Word, Excel®, etc) to uncover dependencies and correlation across the enterprise.

Nonexistent

There might be a belief that the most important risks are known, although there is probably little documentation.

Level 1: Ad hoc

Risk is owned by specialists, centrally or within a department. Risk information provided to risk managers is probably incomplete, dated or circumstantial, so there's high risk of misinformed decisions, with potentially severe consequences. Further mitigation, supposedly completed, is probably inadequate or invalid.

Level 2: Initial

Formal lists of risks for each department and discussions of risk are part of the ERM Process. Corporate risk indicators are collected centrally, based on past events. Departments might maintain their own informal risk checklists that affect their areas, leading to potential inconsistency, inapplicability, lack of sharing or under-reporting.

Level 3: Repeatable

An ERM team manages a growing list of business area specific risks, creating context for risk assessment as a foundation of the ERM Process. Risk indicator lists are collected by most process owners. Upside and downside outcomes of risk are understood and managed. Standardized evaluation criteria of impact, likelihood and controls' effectiveness are used, prioritizing risk for follow-ups. Enterprise level information on risks and opportunities are shared. Risk mitigation is integrated with assessments to monitor effective use.

Level 4: Managed

Process owners aggressively manage a growing list of business area specific risks locally to create context for risk assessment activities as a foundation of the ERM Process. Risk indicators that are deemed critical to their areas are regularly reviewed in collaboration with the ERM team. Measures ensure downside and upside outcomes of risks and opportunities are aggressively managed. Standardized evaluation criteria of impact, likelihood and controls' effectiveness are used to prioritize risk for follow-up activity. Risk mitigation is integrated with assessments to monitor effective use.

Level 5: Leadership

Internal and external best practices, support functions, business lines and regions are systematically gathered and maintained. A routine, timely reporting structure directs risks and opportunities to senior management. The ERM Process promotes frontline employees' participation and documents risk issues' or opportunities' significance. Process owners regularly review and recommend risk indicators that best measure their areas' risks. The results of internal adverse event planning are considered a strategic opportunity.

Attribute 6 Performance Management

Degree of executing vision and strategy, working from the financial, customer, business process and learning and growth perspectives, such as Kaplan's balanced scorecard, or similar approach. Degree of exposure to uncertainty, or potential deviations from plans or expectations.

Nonexistent
No formal framework of indicators and measures for goals and management exists.

Level 1: Ad hoc
Not all goals have measures and not all measures are linked with goals. Strategic goals aren't articulated in terms that the frontline management understands. Compliance focuses on policy and is geared toward satisfying external oversight bodies. Process improvements are separate from compliance activities. Decisions to act on risks might not be systematically tracked and monitored. Monitoring is done and metrics are chosen individually. Monitoring is reactive.

Level 2: Initial
The ERM Process is separate from strategy and planning. A need for an effective process to collect information on opportunities and provide strategic direction is recognized. Motivation for management or support areas to adopt a risk-based approach is lacking.

Level 3: Repeatable
The ERM Process contributes to strategy and planning. All goals have measures and all performance measures are linked with goals. While compliance might trigger reviews, other factors are integrated, including process improvement and efficiency. The organization indexes opportunities qualitatively and quantitatively, with consistent criteria. Risk management criteria are part of management's performance evaluations. Employees understand how a risk-based approach helps them achieve goals. Accountability toward goals and risk's implications are understood, and are articulated in ways that frontline personnel understand.

Level 4: Managed
The ERM Process is an integrated part of strategy and planning. Risks are aggressively considered as part of strategic planning. Risk management is a formal part of goal setting and achievement. Incentive for effective risk management is part of compensation and career development. Investment decisions for resource allocation examine the criteria for evaluating opportunity impact, timing and assurance. The organization forecasts planned mitigation's potential effect on performance impact, timing and assurance prior to use. Employees at all levels use a risk-based approach to achieve goals.

Level 5: Leadership
The ERM Process is an important element in strategy and planning. Evaluation and measurement of performance improvement is part of the risk culture. Measures for risk management include process and efficiency improvement. The organization measures the effectiveness of managing uncertainties and seizing risky opportunities. Deviations from plans or expectations are also measured against goals. A clear, concise and effective approach to monitor progress toward risk management goals is communicated regularly with business areas. Individual, management, departmental, divisional and corporate goals are linked with standard measurements.

Attribute 7 Business resiliency and sustainability

Extent to which the ERM Process's sustainability aspects are integrated into operational planning. This includes evaluating how planning supports resiliency and value. The degree of business ownership and planning beyond recovering technology platforms. Examples include vendor and distribution dependencies, supply chain disruptions, dramatic market pricing changes, cash flow volatility, business liquidity, etc.

Nonexistent
Resiliency and sustainability is limited to an IT infrastructure orientation of continuity and disaster recovery.

Level 1: Ad hoc
Management is aware of resiliency-related risks and focused on infrastructure rather than the business. Users respond to disruptions with workarounds. The response to major disruptions is reactive. Departmental requirements to avoid risk often don't consider business needs. Impact of external and internal events on the business model isn't systematically reviewed.

Level 2: Initial
The organization recognizes broader planning's importance. This highlights the business aspects in addition to traditional disaster recovery. There's recognition that resiliency is an issue that needs consideration in each ERM Process step, and not just in mitigation, as is common with traditional business impact analysis. Achieving balance between quarterly deliverables versus mid-term and long-term value is considered.

Level 3: Repeatable
Resiliency uses far-sighted scenario analysis to document key drivers. The organization indexes priorities qualitatively and quantitatively, with consistent and objective criteria. Resiliency and sustainability are part of every risk plan and considered in each ERM Process step. Business model issues include geography, disruptive technology, competitors, leadership and environmental changes, with reporting and control by senior management.

Level 4: Managed
A comprehensive approach to resiliency considers the people, external, relationship, systems and process aspects. Logistics, security, resources and organization of response procedures are well documented. Resiliency and sustainability are part of the ERM Process and business continuity as mitigation. As a result of the risk process's evaluation, business-driven impact analysis is initiated. Reporting on how external and internal events might impact the business model is raised to the Board of Directors. Balance is achieved between quarterly deliverables and mid-term and long-term value.

Level 5: Leadership
All issues are framed within the context of continuity of services to all stakeholders. Resiliency or sustainability might be defined differently by each organization, with business-driven impact analysis initiated at all levels, based on priorities. Sustainability isn't a reachable end state; rather, it is characteristic of a dynamic and evolving system. Long-term sustainability results from continuous adaptation.

Conclusion

Enterprise Risk Management has evolved over the last two decades from a compelling new concept to a risk management requirement. Now a roadmap for implementing and benchmarking Enterprise Risk Management programs is crucial. No company can confidently say that it has embraced Enterprise Risk Management if there's no way to measure the program. And a set of solid empirical guidelines for measuring Enterprise Risk Management competency is fundamental. These guidelines, designed to deliver business value and compatible with existing frameworks, also provides a way to benchmark ERM progress.

By using the RIMS Risk Maturity Model, risk managers can finally gauge their ERM program's results. This does not just measure how well an organization has adopted ERM. It also provides an unprecedented way to evaluate the ERM process, adjust it as needed and ensure that the intended benefits are delivered.

Adopting ERM is a major undertaking. It requires an enterprise to examine how to manage risk comprehensively. That's how you can achieve competitive advantage even as business risk keeps increasing. For organizations that gauge their ERM program's maturity, the ERM journey is much easier to navigate, and much more likely to deliver business value.

RIMS encourages you to maximize the Risk Maturity Model. Each organization's ERM approach varies depending on its particular risks, risk appetites and priorities. This makes adapting ERM a very dynamic and challenging journey, and one that benefits most from powerful tools like the RIMS Risk Maturity Model.

To benchmark your ERM program and receive a personalized assessment, go to http://www.RIMS.org/RMM

We welcome your feedback. Please provide us your comments and questions on the RIMS Risk Maturity Model to: steven.minsky@rims.logicmanager.com

RIMS STATE OF ERM REPORT 2008

Risk and Insurance Management Society, Inc.®

ROOT CAUSE ASSESSMENT • MATURITY MODEL READINESS
FINANCIAL ELEMENTS • BUSINESS PROCESSES
ERM PLANS • RESOURCES

Authored and Produced by:

Logic Manager™

Table of Contents

Preface

About this Report

The Risk and Insurance Management Society, Inc. (RIMS) has adopted enterprise risk management (ERM) as a core competency and dedicates significant resources to developing tools that will support risk practitioners in establishing effective ERM programs. The RIMS ERM Development Committee was mandated by the RIMS board of directors to identify or develop training, resources and tools to help members establish, lead and sustain ERM processes within their respective organizations. One of its early initiatives was to institute a mechanism for measuring ERM maturity so that organizations can better understand their risk management requirements and strategize how to reach their targeted level of risk maturity. The RIMS ERM Development Committee selected LogicManager, a leader in ERM expertise and innovative software solutions, to develop a risk maturity model for ERM. LogicManager donated its intellectual property, expertise and services; and with acknowledged contributions from ERM Development Committee members, the *RIMS Risk Maturity Model for ERM* © (RMM) was born in 2006.

RIMS Risk Maturity Model for ERM is a requirements model used by executives in risk management and others charged with risk management responsibilities to design sustainable ERM programs and infrastructure reflecting their organizations' strategy and short-, mid- and long-term business objectives. The RMM is also an educational, planning and measurement resource for boards of directors, chief executive officers, chief financial officers, chief audit executives and consultants to evaluate the effectiveness and efficiency of an organization's ERM program. The RMM model consists of 68 key readiness indicators that describe 25 competency drivers for 7 attributes that create ERM's value and utility in an organization. The RMM maturity ladder is organized progressively from "ad hoc" to "leadership" and depicts corresponding levels of risk management competency. A key part of the model is the Risk Maturity Assessment that allows risk managers to score their risk programs online and receive a real-time report. This generates their ERM requirements customized for their organizations' unique industries, structures, geographies, cultures and resources. This gap analysis, based on best practices, then serves as a foundation for the organization to set its priorities for future ERM improvements (***http://www.RIMS.org/RMM***).

RIMS State of ERM Report 2008 is based on Risk Maturity Assessments collected over a 14-month period for 564 organizations, commencing December 2006. *RIMS State of ERM Report 2008* and *RIMS Risk Maturity Model for ERM* are published by RIMS, produced by LogicManager and authored by Steve Minsky, with contributions by members of the RIMS ERM Development Committee.

About the Author, Steven Minsky

Steven Minsky is the chief executive officer and founder of LogicManager. He is the instructor of the RIMS Fellow (RF) workshop titled "Move Your Program to the Next Level: RIMS Risk Maturity Model for ERM" and has helped more than 150 organizations design their ERM charters and action plans. He is a patented author of risk and process management technologies and holds MBA and MA degrees from the University of Pennsylvania's Wharton School of Business and The Joseph H. Lauder Institute of International Management. ***More about the author***.

About the Producer, LogicManager

LogicManager provides configurable ERM software solutions and mentoring services to accelerate risk management effectiveness. LogicManager solves the problem of how to best allocate resources by using an ERM approach to improve business performance and reduce the cost of capital. LogicERM makes it easy for managers across the enterprise to assess their risks and opportunities, create action plans and provide evidence of their successes to stakeholders. More information is available at ***http://www.logicmanager.com***.

About the Publisher, Risk and Insurance Management Society, Inc. (RIMS)

The Risk and Insurance Management Society, Inc. is a not-for-profit membership association dedicated to advancing the practice of risk management. Founded in 1950, RIMS represents nearly 4,000 industrial, service, nonprofit, charitable and government entities. The Society serves more than 10,700 risk management professionals around the world. More information on RIMS programs and services, membership and access to the ERM Center of Excellence can be found online at ***http://www.RIMS.org*** and ***http://www.RIMS.org/ERM***.

About the Contributors

The author would like to acknowledge the contributions made by the following members of RIMS in making this report valuable to ERM practitioners:

John Phelps, ARM, CPCU
Member, RIMS Board of Directors
Blue Cross and Blue Shield of Florida

Carol Fox, ARM
Chair, RIMS ERM Development Committee
Convergys Corporation

Jeff Vernor, ARM
Vice-Chair, RIMS ERM Development Committee
Russell Investments

Laurie Champion, CPCU
Member, RIMS ERM Development Committee
Formerly Coca-Cola Enterprises

Special thanks to Mary Roth, ARM, RIMS Executive Director

Executive Summary

Enterprise risk management (ERM) reduces uncertainty and, over time, improves the prospects of success for organizations that have risk management competency. More than just traditional financial and insurable hazards, ERM encompasses the entire spectrum of risk, including strategy, operations, reputation, finance, compliance and information. As organizations' competency levels improve, so do the odds of successfully managing all kinds of risks.

Marquee companies collapse, high-profile executives step down in disgrace, and thousands of corporations are forced to restate financial reports.[1] The impact of these risks is preventable if resources are allocated while there is still time to change the outcome. Are organizations managing their risks effectively? On the surface, they seem to be trying. Boards create risk management committees, CEOs hire senior risk officers and organizations in North America alone spend nearly $30 billion annually on compliance—$6 billion just on Sarbanes-Oxley (SOX) compliance.[2] Yet something is obviously wrong. Total losses for the global financial crisis have been estimated to reach $945 billion.[3] How can so many smart people overestimate their risk management competency? Did they not have the right infrastructure in place? Did they not aggregate and measure risk effectively? Would these catastrophic events have been prevented if this same spending had been invested in an ERM approach?

The current crisis is now largely seen as a failure of risk management. New government regulation formally enforcing enterprise risk management can be expected. This will have fundamental and far-reaching ramifications for the governance of organizations as well as regulators. Key members of publicly-traded organizations' management are already required to discuss major risk factors, opportunities and related mitigation activities in filings. External auditors already are required to perform risk-based audits, which include evaluating organizations' risk management competency. The expectation is that organizations now will be required to go into depth on how they identify risk, set risk tolerances and provide evidence of effectiveness. Since 2006, boards of directors in the United Kingdom have been held accountable by The Combined Code on Corporate Governance to review and express opinions on their ERM processes and systems, based on the renowned Turnbull Report.[4] Organizations should prudently expect that similar comprehensive requirements are imminent in the United States.

From a personal perspective, our individual risk management competency predicts our credit ratings. Decision makers use our personal credit ratings for purposes far beyond traditional lending decisions, from extending insurance coverage to job offers.[5] For example, personal credit ratings are positively correlated to the frequency and severity of insurance claims.[6] More than 90 percent of insurance companies use personal credit ratings as a key indicator of future claims performance based on individual risk management competency.[7] If individual risk management competency is measured by personal credit ratings, can the same be true of corporate credit ratings? How can boards, management, regulators, auditors and rating agencies better evaluate and measure corporate risk management competency? How can organizations use an ERM approach to allocate resources to better balance risk and reward?

1. ***Treasury & Risk Magazine, Glass Lewis & Co. report***, February 2008.
2. ***AMR Research***. Total compliance spending in 2007 was estimated to be $29.9 billion.
3. ***International Monetary Fund (IMF) annual Global Financial Stability Report***, April 8, 2008.
4. ***The Combined Code on Corporate Governance***, June 2006.
5. ***"How credit scores affect insurance rates,"*** September 2003.
6. ***"How Credit Scores Affect Insurance Rates,"*** May 2007.
7. ***"Credit Impact,"*** Credit.com.

Although intuition frequently suggests to us as individuals that certain concepts have merit, we need evidence with analytical support for them to gain general acceptance and practical application in business. The relationship between risk management competency and corporate credit ratings has not been widely accepted for three reasons:

1. absence of formalized indicators to measure risk competency;
2. absence of infrastructure to gather information and perform analysis in a timely fashion; and
3. absence of a robust and consistent scoring methodology relevant to all risk cultures.

These significant challenges have been surmounted by the development of the Risk and Insurance Management Society's *Risk Maturity Model for ERM © (RMM)*. The RMM codifies 68 key readiness indicators and standardizes a three-dimensional scoring methodology achieved in an online assessment tool.[8] This tool enabled large numbers of organizations to score their organizations' practices against standardized criteria that could then be aggregated, analyzed and compared to each other and to published credit ratings.

As the credit crunch and other market uncertainties in the economy came to light in 2007, risk practitioners from 564 organizations of all types participated in an in-depth assessment of ERM. The study, based on guidelines modeled in the RMM, attempted to improve competency for managing risks, avoiding surprises and leveraging opportunities. Using the RMM, participants compared their organizations' ERM activities against 68 key readiness indicators identified as risk management competency drivers. They scored their organizations in three dimensions:

- effectiveness of ERM activities;
- degree of proactivity; and
- coverage – pervasiveness throughout the organization.

The RMM represents best-practice requirements for developing and maintaining effective ERM programs. The RMM assessment tool allows risk practitioners to score their risk programs against the same 68 key readiness indicators on which the *RIMS State of ERM Report 2008* is based and receive a personalized report on their ERM program maturity level. The RMM, summarized in Table 2 (page 9), models the indicators as the key competency drivers of seven major attributes found in formalized ERM programs.

8. The 68 key readiness indicators are derived from the RIMS RMM and reflect the Australian/New Zealand and COSO ERM risk standards.

Better-managed companies tend to have higher credit ratings—and higher ERM competency. Thus, over time, the likelihood of success is better for organizations that have appropriate ERM discipline, methodology and infrastructure.

Although this hypothesis has been difficult to test, this study demonstrates its validity to a 95 percent or greater confidence level with the following positive correlations.[9]

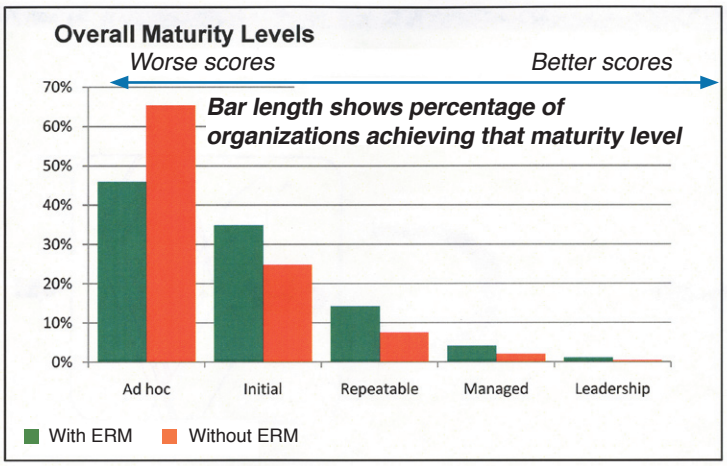
- Organizations with formalized ERM have higher RMM scores.
- Organizations with higher RMM scores have higher credit ratings.
- Organizations without formalized ERM have lower RMM scores.
- Organizations without formalized ERM have lower credit ratings.

While a statistically positive correlation does not prove cause and effect, such correlations—such direct relationships—are accepted as powerful and persuasive evidence for decision-making. For example, Moody's Investors Service and others have proven that there is a direct relationship between **better-managed companies** *as measured by higher credit ratings* and **better performance** *as measured by fewer defaults on financial obligations.*[10] It is impractical—or even impossible—to prove cause and effect, as studies of management examine real organizations as they are in the real world, not in laboratories with control groups. But the relationship between management and performance is undisputed.

This study proves the positive correlation—the direct relationship—between higher RMM scores and higher credit ratings. This powerful correlation argues, but does not need to prove, that there is a cause-and-effect relationship. And this relationship is further validated by the changes that rating agencies now make to organizations' ratings based on evaluation of ERM competency levels. Over time, most organizations that follow the requirements outlined in the RMM will demonstrate better business performance and higher credit ratings than those that do not.

Direct, extensive involvement in ERM by front-line management at all levels is the competency driver that is most strongly correlated with higher credit ratings. Three other competency drivers that also have strong correlation are:

- the degree to which risk assessments are effectively conducted by all business areas and aggregated;
- the extent to which corporate goals and risk management issues are clearly understood at all levels; and
- the depth to which ERM is woven into strategy and planning.



Indicators Validated as Competency Drivers

Participants' assessments statistically validated that organizations with formalized ERM infrastructures embody the 68 key readiness indicators.[11] ERM infrastructures allow organizations to objectively and repeatedly plan, measure and achieve improvements in risk management competency. Of the

9. Credit ratings for participating companies were compared using statistical analysis to measure the relationship between credit rating scores and RIMS RMM scores. The correlation coefficient was calculated for each RMM factor and was found, on average, to be 0.145 and positive. Due to the high population size, this correlation coefficient has a greater than 95 percent confidence level. In probability theory and statistics, correlation, often measured as a correlation coefficient, indicates the existence and direction of a linear relationship between two random variables.
10. ***Understanding Moody's Corporate Bond Ratings And Rating Process***, Moody's Investors Service.
11. A statistical analysis was done comparing the RIMS RMM scores of two groups: *With ERM* and *Without ERM*. The result was *statistically significant*: With greater than 95 percent confidence, the difference in scores between the two groups is unlikely to have occurred by chance.

responding organizations, 39 percent had formalized ERM infrastructure (*With ERM*). Organizations *With ERM* scored 90 percent better in raw RMM index scores for all risk management competency drivers than did organizations without formalized ERM infrastructure (*Without ERM*).

Study results also point to significant differences in maturity levels of risk management competency between organizations *With ERM* and organizations *Without ERM*. Ninety-three percent more organizations *With ERM* had an overall advantage in repeatable or better maturity levels for all seven RMM attributes than organizations *Without ERM*. Increased competency suggests that organizations *With ERM* make better risk-informed decisions, which, arguably, lead to competitive advantage.

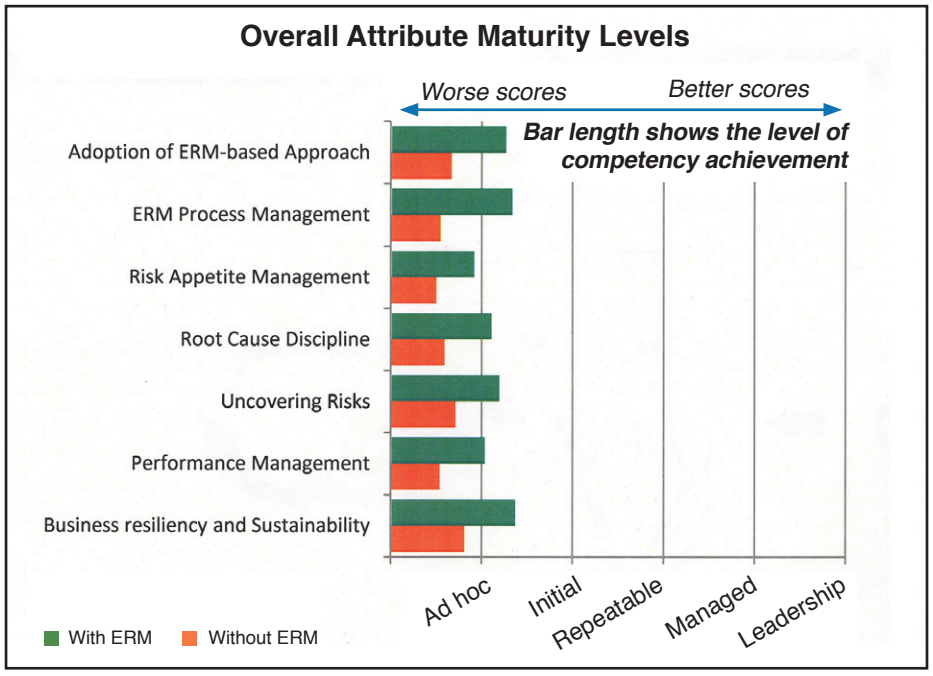
Significant Shortfall for Organizations *With ERM*

Study results further show that organizations *With ERM* may have a false sense of security. They struggle to achieve a managed or better maturity level in most of the critical risk management competencies. Within the "Root Cause Discipline" attribute, for example, only 6 percent achieved that level for "dependencies and consequences" and 7 percent for "classification of risk and performance indicators."[12] Within the "Performance Management" attribute, only 6 percent achieve that level for "ERM process goals and activities" and "communicating goals."[13]

The data show a severe lack of capabilities by organizations *With ERM* to:

- collect risk information from all processes (especially front-line management);
- detect cross-departmental effects and dependencies;
- link risks to their respective organizations' performance goals and objectives; and/or
- effectively compare actual risk against assessed risk.

All of these issues are symptoms of an organization's failure to implement strong risk management governance and infrastructure.



12. The RIMS RMM defines "Root Cause Discipline" as the degree to which risk from people, external environment, systems, processes and relationships is explored.
13. The RIMS RMM defines "Performance Management" as the degree of executing vision and strategy, working from financial, customer, business process and learning and growth perspectives, such as Kaplan's balanced scorecard or similar approach. The "Balanced Scorecard" is a "performance planning and measurement framework" publicized by Robert S. Kaplan and David P. Norton in the early 1990s.

Conclusions

In addition to the important strategic benefits associated *With ERM*, there are now proven direct relationships among higher ERM competency, effective ERM governance and infrastructure, better business performance and reduced short-term bottom-line costs. With the tightening of credit and better credit ratings as important as ever to an organization's cost of capital, brand equity and business viability, the following recommendations are outlined as a result of this study:

Organizations *Without ERM*: This study provides empirical evidence demonstrating why boards and CEOs should use the 68 key readiness indicators within the RMM as the basis to **formalize their ERM infrastructures** and set goals and a timeline to formalize them.

Organizations *With ERM*: Boards, CEOs and committees should use the RMM competency drivers as the basis to:

- assess their own maturity level against these drivers and
- build ERM governance and infrastructure to achieve their targeted maturity level.

It is particularly important to:

- properly evaluate the degree of their organizations' adoption and effectiveness of all RMM competency drivers across the organization;
- implement direct front-line management accountability in ERM;
- consider appropriate organizational structure and reporting relationships for a senior risk management position;
- apply a risk-based approach to prioritize existing activities to reduce internal and external costs; and
- consolidate multiple assessments into one assessment that covers the needs of all functional areas.

All Organizations: Rating agencies, regulators, capital markets and the courts now have reliable guidance on how to evaluate organizations' risk management competency. Boards, CEOs and senior risk officers responsible for their organizations' oversight should be committed to using the RMM to develop risk management competency that is defensible when compared to the five layers of ERM infrastructure listed below. Each layer is assessed with enterprise-wide criteria. Together, they provide one consolidated approach—not silos—to reduce duplication and prioritize existing and new activities.

1. **RIMS Risk Maturity Model for ERM**—Risk managers should engage all organizational functions to build an ERM framework for their organizations. The RIMS RMM is a statistically validated tool that (1) helps organizations identify gaps and (2) provides a roadmap to improve risk management competency, governance and infrastructure. They should go online and to assess their organizations' risk management competencies at ***http://www.RIMS.org/RMM***. They should then prioritize goals and create action plans to achieve them.
2. **Financial Elements**[14]—Risk managers should engage chief financial officers (CFOs) to integrate financial reporting with risk management. Operational risks must be examined, given scores and linked to financial elements if tomorrow's surprises are to be managed in time to change the outcome.
3. **Business Processes**—Risk managers should engage department heads in collecting and prioritizing risks that threaten the capabilities of major processes to deliver services and products to customers and provide accurate data for managing and reporting.
4. **ERM Plans**—Risk managers should engage managers of processes with their teams to uncover risks and root cause dependencies among business areas. They should study the consequential impact on linked corporate objectives after considering risk priorities established by high assessment scores for financial elements and business processes.
5. **Resources**—Risk managers should link prioritized business activities within ERM plans directly to important related physical and informational assets to determine the impact on management's short-, mid- and long-term goals. Prioritizing risks to these assets enhances traditional impact analysis with the likelihood of occurrence and controls assurance dimensions.

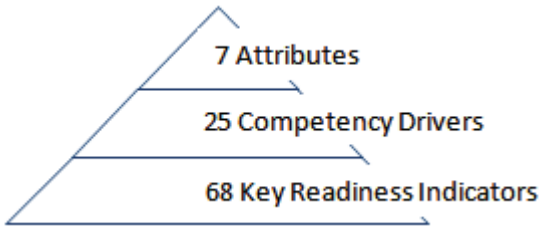
14. "Financial Elements," also called "accounts" or "line items," are components of the financial statements, such as revenue, tax and cost of goods sold.

ERM Proven to Provide Bottom-Line Benefits

One large insurance company has been among only 15 property and casualty insurance companies recognized by A.M. Best Co. for maintaining an A+ or higher financial ranking for 50 straight years. This company recognized the potential effects of an increasingly competitive business environment and moved away from following a traditional compliance approach of simply documenting controls and managing activities. It chose, instead, to apply the five layers of ERM infrastructure and directly involve its front-line risk owners. The result was a dramatic reduction of internal staff hours across the board spent on existing compliance activities and a 60 percent reduction of external audit hours.[15]

Risk Competency Within Attributes

RIMS RMM for ERM has seven core attributes that describe the fundamental characteristics of an effective ERM process. Each attribute contains subgroups referred to as "competency drivers." Each competency driver contains key readiness indicators that drive risk management competency in ERM programs. There are 25 competency drivers and 68 key readiness indicators within the seven core attributes. Possible scores for each factor range from high competency to low competency. Scores for each factor are aggregated to produce scores for related attributes.



Correlation of Risk Competency to Credit Ratings in Organizations *With ERM*

One goal of an enterprise and, thus, of ERM is to improve its sustainability and longevity. One critical measure of that goal is the enterprise's credit rating. Credit ratings are not only a short-term direct cost of capital, but also, more importantly, a concrete measure of business performance. Study results have statistically validated the correlation of an organization's formalized ERM program, embodying all 68 key readiness indicators and all 25 competency drivers, and its credit rating. Further, the correlation to higher credit ratings was strongest for the competency drivers related to front-line risk participation, linkage and governance oversight—three foundational capabilities:

1. **Front-line risk participation**—Front-line employees can identify risks to their processes, including the impact on specific financial elements, and then link risks with the corresponding mitigating process controls regardless of which areas throughout their organization perform the controls.
2. **Linkage**—Management can evaluate each financial element, process and resource and determine whether underlying risks and controls are sufficiently balanced to achieve corporate goals and objectives.
3. **Governance oversight**—ERM governance oversight can reallocate organizational resources to improve the balance between risk and control to address risk when it exceeds the organization's risk tolerance. In the long term, this high level of competency in reducing uncertainties in business is the catalyst for obtaining competitive advantage through improved decision-making (for example, sales targets, cost reductions, acquisitions or even elimination of entire business lines).

When organizations lack competency in any one of the 25 competency drivers—and particularly in the 15 related to these foundational capabilities—the scenario is quite different. Management may not:

- realize that the organization's risks are outside of its tolerance level;
- fully understand the balance of interdependencies between risks, controls, processes and financial elements; or
- recognize the organization's inability to achieve, in a repeatable fashion, corporate goals and objectives.

Consequently, there may be no insight for timely intervention (business decision-making) to alter an undesirable outcome, including a negative impact on credit ratings. Organizations seeking better performance need to broaden and deepen their programs to mature in the competency drivers that support front-line risk ownership, linkage and governance oversight.

15. "Audit Busters," *Treasury and Risk Magazine*, February 2008.

Table 1 depicts median scores for the 25 competency drivers as assessed by organizations with formalized ERM programs (*With ERM*). All of them fall within the bottom 30th percentile of the scoring range. On average, organizations *With ERM* had the least competency in the 15 competency drivers most strongly connected to front-line risk ownership, linkage and governance oversight:

- Eight of the 15 underperforming competency drivers (53 percent) affect front-line risk ownership.
- Three (20 percent) affect linkage.
- Four (27 percent) affect governance oversight.

For organizations *With ERM* to achieve expected benefits from ERM investments, competency in front-line risk ownership and linkage must be achieved so that governance oversight has the necessary insight to better interpret and manage risks within chosen tolerance levels and properly consider complex interdependent issues. Organizations' failure to attain meaningful involvement of front-line process owners in the ERM process have significantly more risk exposure than management and stakeholders realize and than boards knowingly accepted.

Risk management competency reduces:

- **compliance burden and cost in the short term**
- **uncertainties for better business decisions in the long term**

Long-Term Benefits of Improving Risk Competency in Organizations *With ERM*

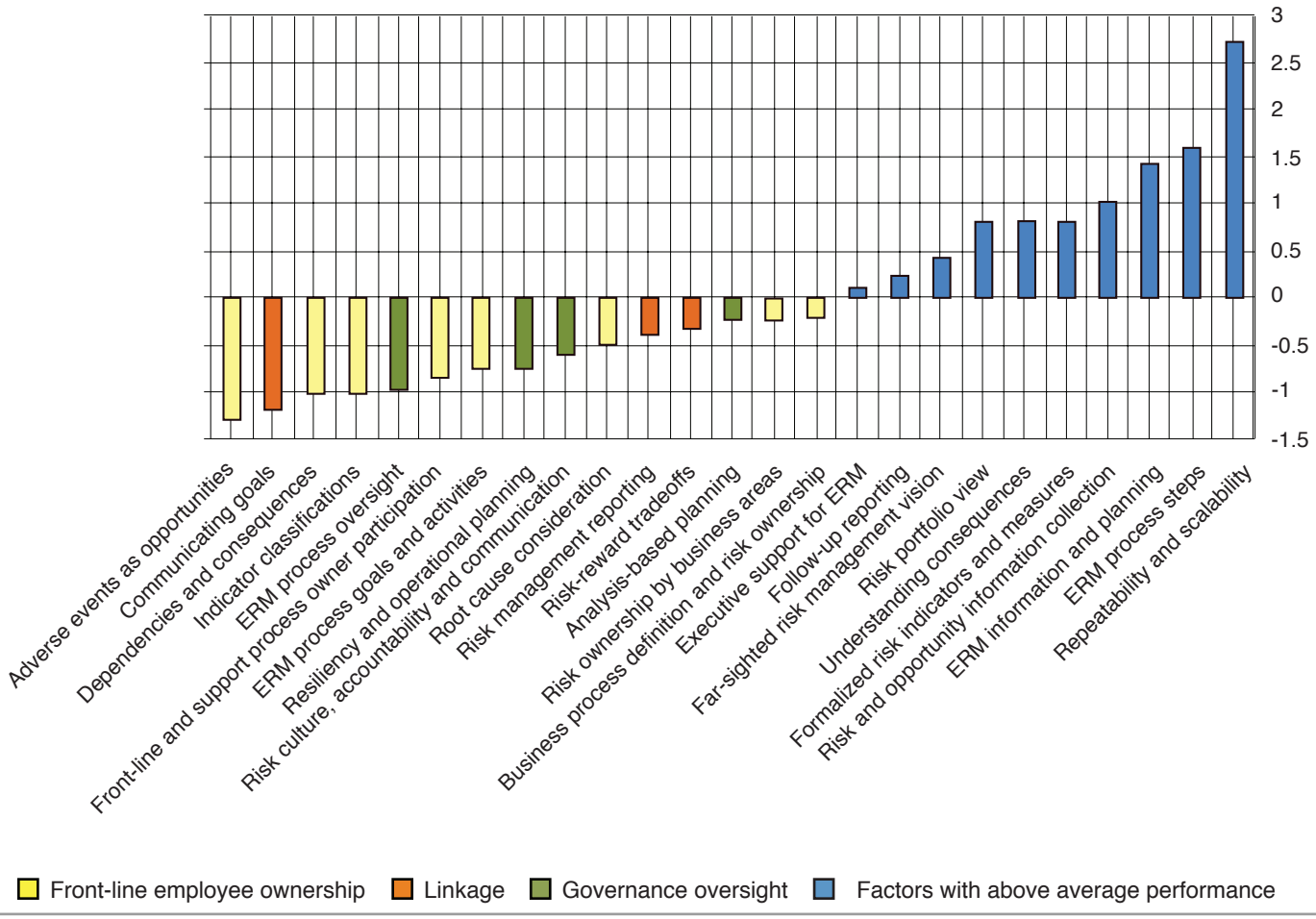
ERM enables organizations to gain efficiencies and effectiveness through a consistent and more comprehensive approach. Investigations to determine and verify organizations' risk management competency will continue to increase.

Boards, CEOs and senior risk officers must be able to defend and demonstrate their organizations' ERM effectiveness in order to achieve the following objectives:

- Companies can avoid potential future rating agency downgrades and increased cost of capital. Standard & Poor's and other rating agencies have incorporated ERM into their methodologies. As their expertise in evaluating ERM grows, the requirements for stronger ERM competency will most likely become an expectation.
- Companies can minimize the personal liability of board members and the risk of criminal charges against CEOs and CFOs for failure to act reasonably in making SOX quarterly certifications about the adequacy of internal controls over financial reporting (ICFR), including changes to ICFR and fraud occurrences.[16]
- Companies can protect the organizations' Securities and Exchange Commission (SEC) safe harbor offered for performing risk-based management assessments of ICFR.
- Board members and senior executives can receive protection against large fines and penalties under Federal Sentencing Guidelines for Organizations. Penalties will be reduced by as much as 95 percent if organizations demonstrate that they periodically assess the risk of criminal conduct, have procedures to detect and prevent violations of law and have implemented procedures to establish an ethical culture.[17]
- Companies can meet regulators' expectations of effective ERM. Regulators expect organizations to have effective ERM for the broad spectrum of risks, representative of their principles-based approach in examinations versus a rules-based approach. Public, nonprofit and government entities are required by state and federal laws to perform risk-based management assessments.
- Board members and senior executives can develop scoping for control and fraud assessment activities to maximize benefits (for example, reduce fees and internal efforts) from the top-down, risk-based mandate of Public Company Accounting Oversight Board (PCAOB) Auditing Standard 5.

16. Public Company Accounting Oversight Board (PCAOB) Auditing Standard 5, July 2007.
17. ***An Overview of the Organizational Guidelines***, United States Sentencing Commission.

Table 1: Competency Driver Performance Organizations With ERM



This chart depicts the competency drivers covered in this study. Drivers with below the line scores indicate areas where participants, on average, have made the least progress. Each competency driver below the line has been colored coded to associate it with a foundational capability as described above.

Table 2: RIMS Risk Maturity Model for ERM Summary[18]

Attributes	Maturity Levels				
	Level 5 Leadership	Level 4 Managed	Level 3 Repeatable	Level 2 Initial	Level 1 Ad hoc
1 Adoption of ERM-based approach	**Competency Drivers: Degree of** • Executive support for ERM • Business process definition and risk ownership • Far-sighted risk management vision • Front line and support process owner participation				
2 ERM process management	**Competency Drivers: Degree of** • Repeatability and scalability • ERM process oversight • ERM process steps • Risk culture, accountability and communication • Risk management reporting				
3 Risk appetite management	**Competency Drivers: Degree of** • Risk portfolio view • Risk-reward tradeoffs				
4 Root cause discipline	**Competency Drivers: Degree of** • Dependencies and consequences • Indicator classifications • Risk and opportunity information collection • Root cause consideration				
5 Uncovering risks	**Competency Drivers: Degree of** • Formalized risk indicators and measures • Adverse events as opportunities • Follow-up reporting • Risk ownership by business areas				
6 Performance management	**Competency Drivers: Degree of** • ERM information and planning • Communicating goals • ERM process goals and activities				
7 Business resiliency and sustainability	**Competency Drivers: Degree of** • Analysis-based planning • Resiliency and operational planning • Understanding consequences				

18. See ***RIMS Risk Maturity Model for ERM***.

