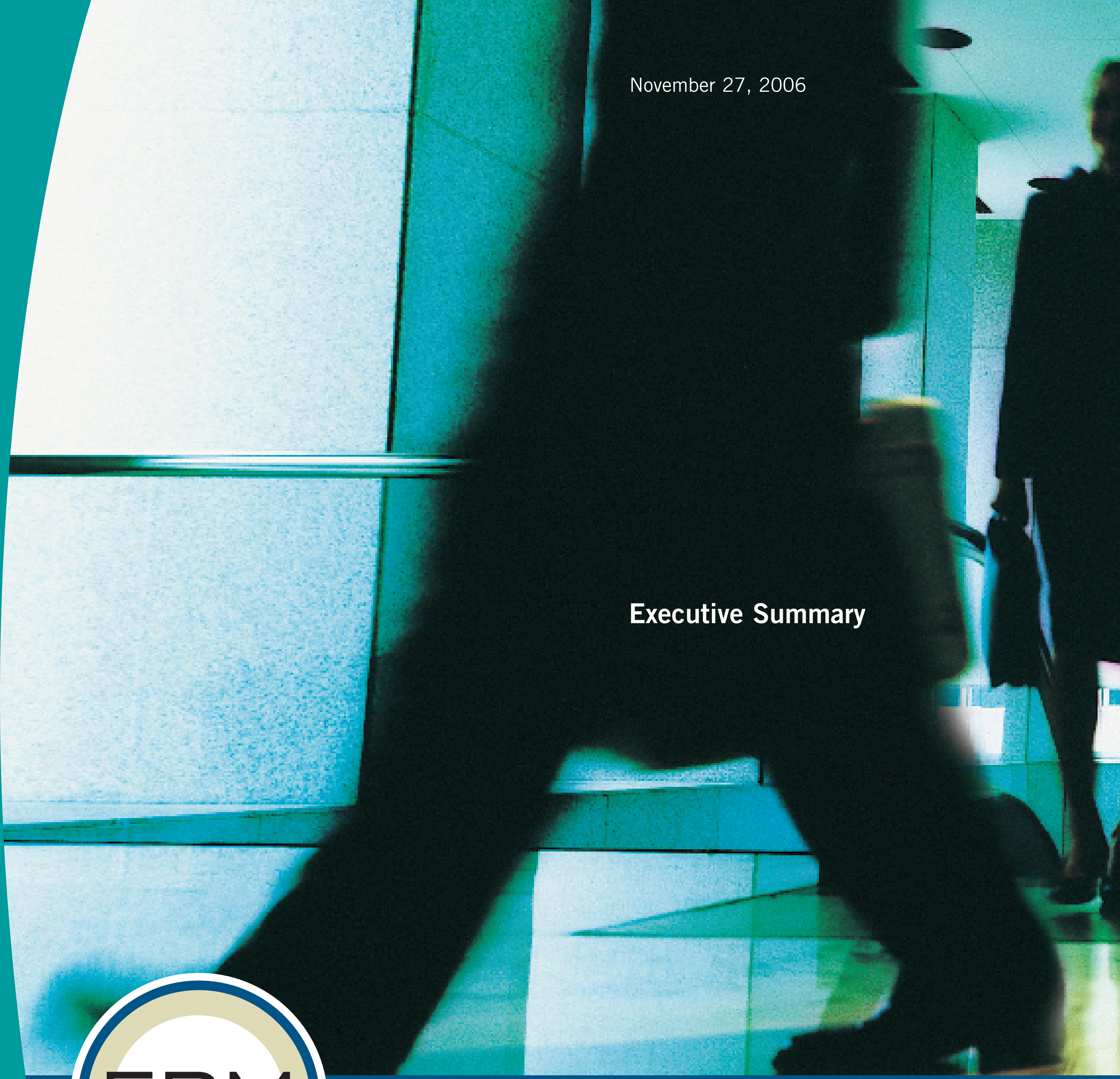


November 27, 2006

Executive Summary

ERM

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*

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.

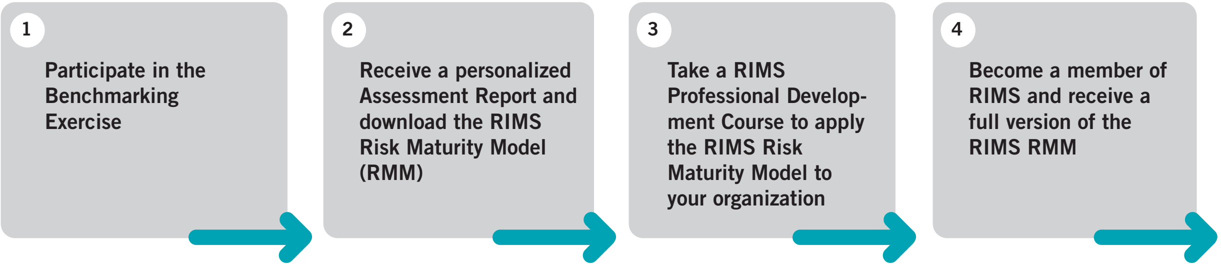
How to use the RIMS RMM

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.



1 Participate in the Benchmarking Exercise

2 Receive a personalized Assessment Report and download the RIMS Risk Maturity Model (RMM)

3 Take a RIMS Professional Development Course to apply the RIMS Risk Maturity Model to your organization

4 Become a member of RIMS and receive a full version of the RIMS RMM

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.

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.

<table>
<tr><th>Attributes</th><th colspan="6">Maturity Levels</th></tr>
<tr><td></td><td>Level 5:
Leadership</td><td>Level 4:
Managed</td><td>Level 3:
Repeatable</td><td>Level 2:
Initial</td><td>Level 1:
Ad hoc</td><td>Nonexistent</td></tr>
<tr><td>1
Adoption of ERM-based approach</td><td colspan="6">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</td></tr>
<tr><td>2
ERM process management</td><td colspan="6">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</td></tr>
<tr><td>3
Risk appetite management</td><td colspan="6">Key Drivers: Degree of …
• risk-reward tradeoffs
• risk-reward-based resource allocation
• analysis as risk portfolio collections to balance risk positions</td></tr>
<tr><td>4
Root cause discipline</td><td colspan="6">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</td></tr>
<tr><td>5
Uncovering risks</td><td colspan="6">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</td></tr>
<tr><td>6
Performance management</td><td colspan="6">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</td></tr>
<tr><td>7
Business resiliency and sustainability</td><td colspan="6">Key Drivers: Degree of …
• integration of ERM within operational planning
• understanding of consequences of action or inaction
• planning based on scenario analysis</td></tr>
</table>

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@logicmanager.com