RIMS Executive Report

The Risk Perspective

ABOUT THE

RIMS RISK MATURITY MODEL

Logic Manager™
Manage Tomorrow's Surprises Today®

RIMS™
the risk management society

ABOUT THE RIMS RISK MATURITY MODEL

TABLE OF CONTENTS

PREFACE 3
EXECUTIVE SUMMARY 4
A Few Words about Maturity Models 5
The Benefits of Using a Maturity Model for ERM 6
How to Use the RIMS Risk Maturity Model 6
The RMM Structure and Assessment 7
The Seven Attributes 7
- Attribute 1: ERM-Based Approach 8
- Attribute 2: ERM Process Management 8
- Attribute 3: Risk Appetite Management 8
- Attribute 4: Root Cause Discipline 9
- Attribute 5: Uncovering Risks 9
- Attribute 6: Performance Management 9
- Attribute 7: Business Resiliency and Sustainability 9

The 25 Competency Drivers 10
RECOMMENDATIONS 11

Logic Manager™

Manage Tomorrow's Surprises Today®

LogicManager provides configurable ERM software solutions and mentoring services to accelerate risk management effectiveness and help organizations prevent surprises. LogicManager solves the problem of how to best allocate resources and integrate all risk, governance and compliance activities by using an risk-based approach to improve business performance and reduce costs. LogicManager makes it easy for managers across the enterprise to assess their risks and opportunities, create action plans based on strategic goals, and provide evidence of their successes to internal and external stakeholders. More information is available at www.logicmanager.com.

RIMS™ the risk management society

RIMS is a not-for-profit membership association dedicated to advancing the practice of risk management. Founded in 1950, RIMS represents more than 3,500 industrial, service, nonprofit, charitable and government entities. The Society serves more than 11,000 risk management professionals who are located in more than 60 countries. More information on RIMS programs and services, membership and access to the RIMS Strategic and Enterprise Risk Center can be found online at www.RIMS.org/resources and www.RIMS.org/ERM.

The *RIMS Risk Maturity Model for ERM*© is published by RIMS, produced by LogicManager and authored by Steven Minsky, with contributions by members of the RIMS ERM Committee and several of LogicManager's data analysts.

About the Authors

Steven Minsky

Steven Minsky is the Chief Executive Officer and Founder of LogicManager. He is a RIMS Fellow (RF) and has helped hundreds of 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.

Carol Fox

Carol Fox is the Director of Strategic and Enterprise Risk Practice for RIMS. She has held progressively responsible risk management positions in the customer care, telecommunications, manufacturing, defense, and insurance industries. Known for her risk management experience and writings, she received RIMS' 2009 Harry & Dorothy Goodell Award. In 2011, *Treasury & Risk* named her as one of the 100 Most Influential People in Finance. Carol is the chair of the U.S. Technical Advisory Group to ANSI for the ISO 31000 risk management standards, a participant in the COSO ERM Advisory Council, and serves on Miami University's Center of Business Excellence Advisory Board.

Copyright © 2015 Risk and Insurance Management Society, Inc. (RIMS) and Logic Manager. All rights reserved.

PREFACE

RIMS defines enterprise risk management (ERM) as follows: Enterprise risk management is a strategic business discipline that supports the achievement of an organization's objectives by addressing the full spectrum of its risks and managing the combined impact of those risks as an interrelated risk portfolio.

Taking an enterprise risk management approach transitions beyond the traditional realms of risk management in that it:

1. Encompasses all areas of organizational exposure to risk (financial, operational, reporting, compliance, governance, strategic, reputational, etc.);
2. Prioritizes and manages those exposures as an interrelated risk portfolio rather than as individual 'silos';
3. Evaluates the risk portfolio in the context of all significant internal and external environments, systems, circumstances, and stakeholders;
4. Recognizes that individual risks across the organization are interrelated and can create a combined exposure that differs from the sum of the individual risks;
5. Provides a structured process for the management of all risks, whether those risks are primarily quantitative or qualitative in nature;
6. Views the effective management of risk as a competitive advantage; and
7. Seeks to embed risk management as a component in all critical decisions throughout the organization.

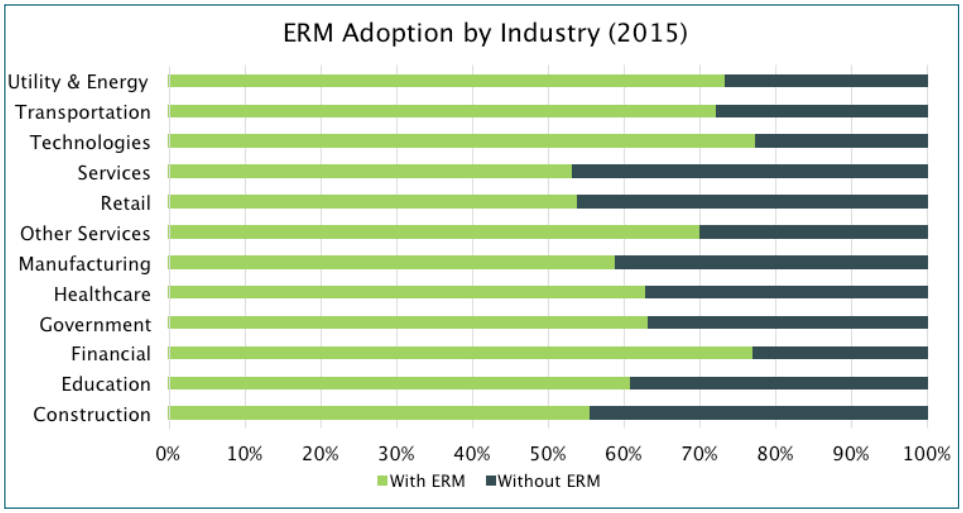
THE HISTORY OF THE RIMS RISK MATURITY MODEL (RMM)

RIMS recognized early on that ERM is a core organizational competency. In 2004, The RIMS ERM Committee was established 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 the committee's 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. RIMS selected LogicManager, a leader in ERM expertise and innovative software solutions, to develop a risk maturity model for ERM. With contributions from members of RIMS initial ERM Development Committee, the *RIMS Risk Maturity Model for ERM© (RMM)* was launched in 2006.

Maturity models are a recognized measurement concept for demonstrating development progress and for highlighting consistent outcomes across organizations. Since its creation, the *RIMS Risk Maturity Model for ERM© (RMM)* has been a best practice requirements model used by executives in risk management and others charged with risk management responsibilities. The model helps to design sustainable ERM programs and infrastructure by reflecting an organization's strategy and short-, mid- and long-term business objectives. The RMM also evaluates the effectiveness and efficiency of existing ERM programs and serves as an important educational, planning and measurement and benchmarking resource for boards of directors, chief executive officers, chief financial officers, chief audit executives, risk professionals, and consultants. This report provides information about the model itself.

Since its inception, the RMM has been used by both publically traded and private companies across various geographical regions of the world to collaborate with their board of directors, senior management, operations management and managers from support functions of strategy planning, IT, internal audit, compliance, etc. to advance risk management performance competencies within their respective organizations. The ERM discipline has been adopted in nearly every industry, although maturity levels tend to vary.

Copyright © 2015 Risk and Insurance Management Society, Inc. (RIMS) and Logic Manager. All rights reserved.



Based on more than 2,400 organizations assessing ERM programs with the RIMS RMM online assessment

EXECUTIVE SUMMARY

Enterprise Risk Management (ERM) reduces uncertainty and, over time, improves the prospect 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 an organization's competency levels improve, so do the odds of successfully managing all kinds of risks.

In today's complex and interconnected world, companies are in need of a formal evaluation of the effectiveness and maturity of their enterprise risk management programs in order to achieve corporate goals, effectively respond to changing regulations, protect themselves from negative events or trends, and maintain (or improve) credit ratings for efficient borrowing.

INFLUENCES ON ERM

Certain forces have influenced wider adoption of ERM in the last decade. These include:

- Board accountability and disclosure requirements regarding risk management have been enacted.
- ERM has become a component for evaluating and publishing corporate credit ratings by credit agencies.
- ERM value has been shown to provide bottom-line and longer-term benefits through academic research.

These influences have spotlighted the value that organizations are expected to deliver from their risk management activities, as well as the value that those organizations with more mature programs have been shown to deliver.

Understanding existing and emerging risks at every level and being able to report on such risks for greater understanding of multi-dimensional implications regarding the objectives of an organization is extremely difficult to do without a plan. Given the evidential connection between the effectiveness found in more mature ERM programs maturity and firm value, board members and senior-level officers responsible for their respective organizations' risk management oversight would benefit their organizations by committing to use the RIMS RMM to develop risk management competency irrespective of the other standards they currently use for internal guidance.

A key part of the model is the Risk Maturity Assessment. The free and publicly available assessment (www.RIMS.org/RMM) allows organizations to score their programs in each competency area, and receive an immediate gap analysis report that can serve as the foundation for an organization to set its priorities for future improvements.

Copyright © 2015 Risk and Insurance Management Society, Inc. (RIMS) and Logic Manager. All rights reserved.

A FEW WORDS ABOUT MATURITY MODELS

DEMONSTRATING RISK MANAGEMENT DEVELOPMENT PROGRESS TO MEET STAKEHOLDER NEEDS

Individuals who are accountable for risk management implementation, sustainability and oversight are charged with understanding and articulating the value and performance of the organization's risk management capabilities to stakeholders. Stakeholder expectations require organizations to demonstrate that risk management practices not only exist, but have developed sufficiently to deliver results effectively. How do organizations evaluate how well risk management practices and outcomes are developing? A number of organizations use maturity levels for this purpose.

Maturity is a recognized measurement concept for demonstrating progress in development and for highlighting consistent outcomes across organizations. Maturity refers to an evolution toward full development of the risk management attributes and competency drivers. Linked closely with continuous improvement, risk management maturity represents the degree of formality and effectiveness of risk management activities and processes in an organization at different levels, from ad hoc practices, to formally defined steps, to managed result metrics, to actively making the most effective use of the processes and capabilities.

DEMONSTRATING MANAGEMENT'S COMMITMENT TO RISK MANAGEMENT MATURITY

An organization may choose a specific level of the development evolution as its goal within a specific time frame. For incremental improvement until it reaches its desired maturity level, an organization may re-evaluate whether the "level" goal was accomplished and set a new level for future achievement. At times, various parts of an organization may exhibit different maturity level characteristics.

Although an organization may plateau at a certain level, improvement generally is made as an organization, or its divisions, incrementally move up as noted in the example provided in Table 1.

Table 1

Maturity (level)	Maturity Level Characteristics
Ad hoc (1)	The organization may be compliant with legal and regulatory requirements, but without consistent, formalized or documented risk management arrangements or processes. Implies an extremely primitive level of ERM maturity where risk management typically depends on the actions of specific individuals, with improvised procedures and poorly understood processes.
Initial (2)	The organization is aware of the need for a more formal risk management approach. Risk management arrangements and processes are structured, but incompletely put into practice. Formalization is on-going but not fully accepted in the organization. Risk is managed independently, with little integration or risk gathering from all parts of the organization. Processes typically lack discipline and rigor. Risk definitions often vary across the organization. Risk is managed in silos, with little integration or risk aggregation. Processes typically lack discipline and rigor. Risk definitions often vary across the silos.
Repeatable (3)	Risk management arrangements and processes are standardized with defined and documented procedures. Risk management awareness may be included in organizational training. A standardized procedure is generally in place with the senior levels of the organization being provided with risk overviews/reports. Risk management is aligned with the organization's external and internal environment, as well as the organization's risk profile. The risk management arrangements and processes are established and repeatable as a standard organizational approach. Risk assessments are conducted throughout departments with the goal of gathering input from the frontline. Information is aggregated to the board of directors, senior management, committees and regulators for risk overviews. Approaches to risk management are established and repeatable.
Managed (4)	Enterprise-wide risk management activities, such as monitoring, measurement and reporting are integrated and harmonized with measures and controls established. Risk arrangements, assessments, and treatments are organized, monitored, and managed at many levels of the organization. Risk information is structured in a manner that it can easily be cascaded throughout the organization for information collection and aggregated for senior level reporting. Measurement metrics are standardized and incorporated into the organization's performance metrics. Risk procedures are communicated and fully understood throughout the organization with the risk management principles integrated fully within the management process. Mechanisms are in place for alerting management about changes in the organization's risk profile that may affect the organization's objectives.
Leadership (5)	Risk procedures are communicated and fully understood throughout the organization with the risk management principles integrated fully within the management process. Risk-based discussions are embedded to a strategic level, such as long-term planning, capital allocation and decision-making. Risk appetite (risk/reward) and tolerances are clearly understood with alerts in place to ensure the board of directors and executive management is made aware when set thresholds are exceeded. Planned critical review of the risk management program provides guidance for adjusting/improving application of the risk management principles, arrangements and processes across the organization to advance objectives.

Copyright © 2015 Risk and Insurance Management Society, Inc. (RIMS) and Logic Manager. All rights reserved.

THE BENEFITS OF USING A MATURITY MODEL FOR ERM

The maturity model approach is a method that applies across a variety of industries. Based on studies in which this maturity model approach was used over more than 10 years, evidence demonstrates that with each step up in maturity level, organizations can gain positive results. The RIMS RMM is a structured way of highlighting aspects of effective ERM.

BENEFITS FOR RISK PROFESSIONALS AND PRACTITIONERS

- Establish a baseline of maturity levels.
- Build consensus about areas for improvement and establish milestones.
- Communicate clearly to the board, regulators, rating agencies, executive management, process owners, and support functions that enable the rest of the organization, such as human resources, IT, internal audit, and compliance, etc.

BENEFITS FOR ERM STAKEHOLDERS

- Streamline ERM processes.
- 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 uncertainties 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 less expensive than simply treating the symptom. ERM uncovers and attacks the root cause.

INCREASE EFFICIENCIES

In assimilating risk assessments into business processes, operational planning and execution in a universally understood way as decisions are made (rather than after), more efficient use is made of scarce resources, such as finances, staff and time.

FRAMEWORK COMPATIBILITY

The RIMS RMM is designed to be compatible with various specialized standards and guidance, such as the International Organization for Standardization (ISO) 31000 series of standards on risk management, the Committee of Sponsoring Organization (COSO) guidance on ERM, ISACA's integration of risk management into its COBIT standard for information technology, rating agency guidance on the implications of the strength of risk management practices on credit ratings, as well as regulatory requirements.

Regardless of which risk management standard or framework an organization uses, risk professionals and their internal auditors can use the RIMS Risk Maturity Model assessment for assurance purposes to determine whether the organization's risk management program is meeting expectations, and for considering potential recommendations to mature the program.

INCREASE TOP LINE REVENUE

ERM unlocks interdependencies that can lead to new revenue generation. One issue can lead to rethinking business strategy and finding an opportunity to create additional value. ERM helps managers think and act more strategically.

Using the data gathered from RMM assessments over five years, Mark Farrell, actuarial science and risk management program director at Queens University Management School of Belfast (QUMS), and Dr. Ronan Gallagher, of the University of Edinburgh Business School, provided empirical evidence that firms—regardless of industry—that have reached mature levels of ERM, as defined by the RIMS Risk Maturity Model, exhibit a **25% higher firm value**. The broad data set encompassed publically traded organizations from a variety of industries. The highest marginal valuation impacts are associated with two specific attributes: Performance Management and ERM Process Management contributing to 23% and 20% respectively to the firms' value.[1]

HOW TO USE THE RIMS RISK MATURITY MODEL

There are three steps to using the RIMS Risk Maturity Model to gain the benefits outlined above for any type of organization.

1. **Understand the model:** The RMM is based on seven attributes, 25 competency drivers and 68 supporting key readiness indicators that ERM programs are benchmarked against, identifying strong and weak areas of each program. See page 7.
2. **Take self-assessment:** To enable organizations to understand where they lie on the maturity scale, the RIMS Risk Maturity Model is a free assessment tool for executives in risk management—and others charged with risk management responsibilities—to develop and improve sustainable enterprise risk management programs. This online resource for ERM allows an organization to score its risk management program and receive an immediately available report.
3. **Review with internal stakeholders to determine adequacy of results:** After understanding the principles of the RMM attributes and taking the RMM Assessment, compare the personalized report against the "well-managed" guidelines below, and develop an action plan to take the risk management program to the next level.

In addition to your Risk Maturity Assessment, you will receive a complimentary copy of the RIMS State of ERM Report. The report provides insight and perspectives on risk management programs based on data collected from thousands of risk practitioners for comparison against the organization's results.

[1] Farrell and Gallagher, "The Valuation Implications of Enterprise Risk Management Maturity," *The Journal of Risk and Insurance*, March 2014.

Copyright © 2015 Risk and Insurance Management Society, Inc. (RIMS) and Logic Manager. All rights reserved.

THE RMM STRUCTURE AND ASSESSMENT

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 contain supporting 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 (see Figure 1). Possible scores for each factor range from high success to low success.

Each competency driver scored on a scale of 1-10 for each of three the following assessment dimensions:

- **Capability for ERM activities:** Measures how well your organization understands how to implement key risk management activities. (i.e., is there internal organizational understanding of how to implement best practices? Are these practices well documented?)
- **Degree of proactivity:** Measures the nature of risk management, whether it is proactive or reactive. (i.e., are these activities a reaction to negative events, or part of a repeatable process?)
- **Coverage:** Measures the breadth and depth of risk management within the organization (i.e., does responsibility span across all departments and all vertical levels of the organization? How engaged are your stakeholders?

Based on the results of the competency driver assessments on the above dimensions, the organization is placed on the maturity scale from an informal "Ad hoc" level to a fully realized "Leadership" capability level (see Figure 2).

Figure 1 | RIMS Risk Maturity Components



Figure 2 | RIMS Risk Maturity Levels



THE SEVEN ATTRIBUTES

The RIMS RMM model is based on seven attributes that encompass ERM's value and utility within an organization (Figure 3).

Figure 3 | The 7 Attributes Considered in the RIMS Risk Maturity Model

ERM-based approach	Executive support within the corporate culture.
ERM process management	Integration into business processes.
Risk appetite management	Accountability within leadership and policy to guide decision-making.
Root cause discipline	Linking outcomes with their sources.
Uncovering risks	Analyzing and documenting risks and associated uncertainties in considering threats and opportunities.
Performance management	Executing vision, mission and strategy utilizing risk management methods.
Business resiliency and sustainability	Integration into operational planning and execution.

Copyright © 2015 Risk and Insurance Management Society, Inc. (RIMS) and Logic Manager. All rights reserved.

THE SEVEN ATTRIBUTES

ATTRIBUTE 1: ERM-BASED APPROACH

Attribute 1 denotes the degree of executive support for an ERM-based approach within the corporate culture. Risk management activities within organizations committed to an ERM-based approach go beyond regulatory compliance.

What "Well-Managed" Looks Like:
An organization with a mature risk culture analyzes and reports on risk management activities using a systematic approach. Executive sponsorship is strong, and the tone from the top has embedded an ERM-based approach into the corporate culture. Activities cut across all processes, functions, business lines, roles and geographies and include integrating, communicating and coordinating with front-line and support areas; including strategy planning, internal audit, information technology (IT), compliance, corporate security, business continuity and risk management. Boards of directors, senior management and senior risk officers communicate the importance of risk management in daily decision-making to each business function. All areas and all levels in the organization use risk-based best practices. Risk management competency is a prerequisite for promotion to all leadership positions, and risk-based goals are required for pay-for-performance bonuses.

ATTRIBUTE 2: ERM PROCESS MANAGEMENT

Attribute 2 denotes the degree of incorporation of repeatable and scalable risk management processes into business and resource/support units, bolstered by qualitative and quantitative measurements, analyses, tools and models; robust reporting on risk management activities; and clarity of oversight, including roles and responsibilities. The ERM process is defined as a sequential series of steps that support the reduction of uncertainty and promote the exploitation of opportunities. The process is structured so that risk information can regularly be cascaded throughout the organization for input collection and aggregated for senior management level for reporting, analysis and decision making.

What "Well-Managed" Looks Like:
In all units, roles and responsibilities are process-driven. Teams collaborate across support and operating functions. Risk and performance assumptions made for quantitative and qualitative measurements are routinely revisited and updated. Organizations use the ERM process for sequential steps to improve decision-making and performance. Accountability for risk management is woven into all business units, processes, support functions, business lines and geographies as the preferred way to achieve goals. Committed organizations create ERM plans to define the context in which the rest of the process will take place.

The ERM process within an ERM plan generally follows a number of steps. This process is structured so that risk information can regularly be cascaded throughout the organization for input collection and aggregated for senior management level for reporting, analysis and decision making:

1. Identify where, when, why and how business model, market, events, operations, third parties and other elements associated with business changes, issues and others—whether known or underreported—might prevent, degrade or support goals;
2. Analyze perceived uncertainties and opportunity through consistent, objective and pervasive assessment evaluation criteria, such as impacts, likelihood, assurance (effectiveness of controls) and other variables, such as speed to onset and time horizon, to determine potential consequences and the estimated risk level relevant to business objectives;
3. Evaluate risk tolerance to determine acceptable risk levels, considering the balance between risk and reward, such as potential benefits (including unexpected opportunities) and drawbacks (see Attribute 3: Risk Appetite Management);
4. Create strategies and action plans and create potential additive value by modifying and optimizing risk, leveraging opportunity activities to reduce uncertainty, increase potential benefits and possibly decrease unnecessary costs; and
5. Monitor the timeliness and effectiveness of activities by risk owners and gauge the program to ensure that changing circumstances are recognized and that appropriate alterations to priorities are made. Rather than allowing problems to escalate, the focus on shifting priorities encourages value creation and reductions in overspending on controls that may not be needed.

ATTRIBUTE 3: RISK APPETITE MANAGEMENT

Attribute 3 denotes the degree of understanding and accountability throughout organizations for:

- defining acceptable boundaries for risk types (risk appetites);
- calculating and articulating approved variations for risks related to set boundaries (risk tolerances);
- developing views of risk impact, likelihood and assurance (effectiveness of controls) from different perspectives such as operations, regulatory categories, strategic goals and financial reporting (risk portfolio views);
- considering the benefits of risk and reward tradeoff scenarios in daily management of business and resource/support units; and
- attacking gaps between perceived and actual risks.

What "Well-Managed" Looks Like:
Organizations achieving a managed maturity level for Risk Appetite Management generally employ enterprise risk committees or councils. Such councils should suit the entity's structure and culture. They may have different levels of authority in various organizations, but should be aligned with the top governing body. Ultimately, such councils should have direct reporting into C-level management. Considering the organizations' short- and mid-term objectives, as well as their longer-term strategic plans and goals, these councils may be authorized to define or recommend acceptable boundaries for risk types to senior management and/or the board. Typical risk appetite decisions may include, but are not limited to, taking more risk to gain market share or establishing a conservative hold position to protect the brand. Risk tolerances are expressed for each risk factor assessed by front-line risk owners in any process throughout the organization.

Established risk tolerances are revisited during planning and execution activities at various levels, and evidence can be provided of challenges and re-evaluation of risk tolerance that take place during the ERM process. Boards and senior leadership, supported by enterprise risk councils, define organizational risk tolerances that business and resource/support units recognize in their daily risk management activities. A

Copyright © 2015 Risk and Insurance Management Society, Inc. (RIMS) and Logic Manager. All rights reserved.

transparent mechanism compares and reports units' actual assessed risk to the organization's defined risk tolerances. Units have risk plans that either defend variations or incorporate plans to reduce variations. Senior leadership (perhaps through its designated risk councils) and units determine priorities and allocate resources in the best interest of the organization, which aligns units' tactical plans with organizational goals.

ATTRIBUTE 4: ROOT CAUSE DISCIPLINE

Attribute 4 denotes the degree of discipline applied to measuring a problem's root cause by:

- determining the sources or causes of identified threats and opportunities;
- understanding the sources and impact of risks on other areas within an organization;
- identifying trends in root cause categories; and
- collecting information and measurements related to the effectiveness of controls with consideration given to sources of identified risks.

What "Well-Managed" Looks Like:
Organizations achieving a managed maturity level for this attribute explore risks caused by sources and as a result:

1. Are better able to identify causes, rather than symptoms
2. Understand the how, what and why of past and future outcomes
3. Allocate resources more efficiently to modify controls for greatest effect

One example of source categories is external, people, processes, relationships and systems. Organizations focus on sources and causes in all risk management activities. "Post mortems" are performed to deconstruct past outcomes (either their own or others') into root cause categories to better prepare for future events. The frequency, impact and likelihood of identified risks and their sources are analyzed and evaluated as a routine part of risk management activities. The discipline of reviewing multiple risk sources and causes is promoted to provide a comprehensive view of threat and opportunity. This represents preemptive risk management, rather than simple problem management.

ATTRIBUTE 5: UNCOVERING RISKS

Attribute 5 denotes the degree of quality and pervasiveness throughout organizations for:

- documenting uncertainties, perceived as both threats and opportunities, in risk assessment activities;
- collecting knowledge from employee expertise, databases and other electronic files to uncover dependencies and correlation across the enterprise;
- using potentially adverse uncertainties to create opportunities;
- establishing risk ownership by business and resource/support units;
- formalizing risk indicators and measurements; and
- follow-up reporting on risk management activities from varying perspectives.

What "Well-Managed" Looks Like:
Organizations that achieve a managed maturity level for Attribute 5 have routine, often real-time reporting mechanisms that bring uncertainties, identified at all levels of the organization, to senior management's attention for timely consideration and deployment of resources. Organizations' ERM infrastructures actively engage frontline employees in identifying emerging threats and opportunities, and then assess the risks to determine the appropriate treatment approaches and activities to address the risks in the context of risk and reward tradeoffs.

Organizations' enterprise risk councils regularly review critical risk indicators with units. Councils add and review risk indicators that can be assessed and modified by the units in order to achieve organizational goals and objectives. Councils also review and approve standardized criteria used by units to score risk or performance, such as impact, likelihood and control effectiveness. Standardized scoring criteria are applied consistently throughout an organization so that units' assessments may be evaluated comparatively. Comparisons of units' assessments are used to prioritize resource allocations and follow-up reporting. Process owners regularly review and recommend risk indicators that best measure their areas' risks.

ATTRIBUTE 6: PERFORMANCE MANAGEMENT

Attribute 6 denotes the degree to which organizations are able to execute on vision and strategy in tandem with risk management activities by:

- clearly articulating and communicating organizational goals to all business and resource/support units;
- ensuring that goals and objectives are specific, measureable, attainable, realistic and trackable;
- mandating that deviations from plans or expectations are measured and reported against goals and objectives; and
- aligning ERM process goals and activities with organizational goals and objectives.

What "Well-Managed" Looks Like:
Organizations that achieve a managed maturity level for Attribute 6 stress that the ERM process is an important element in strategy and planning activities at all levels within their organizations.

Organizations incorporate ERM information—and link ERM activities—to specific business objectives and performance measurements within the organization's chosen planning and execution timeframes, which may include short-, mid- and long-term timespans.

Clear communication of organizational goals to units is critical for overall alignment and effective tactical execution of activity-level plans and use of resources. Reports cover deviations from plans or expectations. Leading organizations structure pay-for-performance goals to include how well individuals manage risks that threaten or contribute to the achievement of their objectives.

ATTRIBUTE 7: BUSINESS RESILIENCY AND SUSTAINABILITY

Attribute 7 denotes the extent to which an organization integrates business resiliency and sustainability aspects for its operational planning into its ERM process by:

- evaluating how planning by business and resource/support units support resiliency and value;

Copyright © 2015 Risk and Insurance Management Society, Inc. (RIMS) and Logic Manager. All rights reserved.

- ensuring that units acknowledge their responsibility for resiliency in their planning activities;
- balancing short-term deliverables with longer-term value;
- documenting logistics, security, resources and organization of response procedures; and
- relying on analysis-based planning (for example, stress-testing investment portfolios).

"Resiliency" is defined as an organization's ability to recover quickly from setbacks.

"Sustainability" is defined as an organization's ability to maintain something of value over time (for example, demand of services and products by customers—the ongoing ability to create and capture value).

What "Well-Managed" Looks Like:
Organizations achieving a managed maturity level for Attribute 7 frame issues within the context of continuity of services to their respective stakeholders. The particulars of Business Resiliency and Sustainability are defined differently by each organization and at different levels within the organization, based on their respective priorities. Business activities are linked to resources, such as critical vendors, in order to understand dependencies. Activities and resources are prioritized based on business-driven impact analysis.

Companies operate in a dynamic and evolving environment. Therefore, long-term sustainability requires continuous adaptation in order to respond to changing business conditions and competitive priorities. Areas for which leading organizations commonly address resiliency and sustainability include IT recovery, third-party vendor and distribution channel dependencies, supply-chain disruptions, unexpected market changes, cash-flow volatility, business liquidity and so on. Well-managed organizations instill "Resiliency" and "Sustainability" in existing business analysis and planning processes.

THE 25 COMPETENCY DRIVERS

Underpinning the seven attributes are 25 competency drivers, as shown in Figure 4. The competency drivers reflect certain organizational capabilities within each of the seven attributes that have been shown to produce higher firm value.[2]

Within each competency driver, there are numerous supporting key readiness indicators (68 in all), that evidence the degree of organizational capability for each of the competencies. As an example, there are three key readiness indicators associated with the 'ERM program insight' competency driver:

- Operational managers actively participate in the ERM program.
- Process and risk ownership are clearly defined.
- Risk management accountability is woven into all processes, support functions, business lines and geographies to achieve goals.

Figure 4 | RIMS RMM Competency Drivers within the Seven Attributes

7 Attributes	5 Maturity Levels →				
	Level 1 Ad hoc	Level 2 Initial	Level 3 Repeatable	Level 4 Managed	Level 5 Leadership
1 Adoption of ERM-based approach	Competency Drivers: Degree of: 1. Executive support of ERM 2. Business process definition and risk ownership 3. Far-sighted risk management vision 4. Front line and support process owner participation				
2 ERM process management	Competency Drivers: Degree of: 5. Repeatability and scalability 6. ERM program oversight 7. ERM process steps 8. Risk culture, accountability and communication 9. Risk management reporting				
3 Risk appetite management	Competency Drivers: Degree of: 10. Risk portfolio view 11. Risk-reward tradeoffs				
4 Root cause discipline	Competency Drivers: Degree of: 12. Dependencies and consequences 13. Indicator classifications 14. Risk (uncertainties) and opportunity information collection 15. Root cause consideration				
5 Uncovering risks	Competency Drivers: Degree of: 16. Formalized risk indicators and measures 17. Adverse (potential) outcomes as opportunities 18. Follow-up reporting 19. Risk ownership by business areas				
6 Performance management	Competency Drivers: Degree of: 20. ERM information and planning 21. Communicating goals 22. ERM process goals and activities				
7 Business resilience and sustainability	Competency Drivers: Degree of: 23. Analysis-based planning 24. Resilience and operational planning 25. Understanding consequences				

[2] "The Valuation Implications of Enterprise Risk Management Maturity," *The Journal of Risk and Insurance*, March 2014.

Copyright © 2015 Risk and Insurance Management Society, Inc. (RIMS) and Logic Manager. All rights reserved.

RECOMMENDATIONS

By using the RIMS Risk Maturity Model for ERM©, executives can gauge the degree to which their organization's ERM program is achieving real results. This does not just give a sense of how far along an organization is in the process of adopting ERM, but it also provides a view as to how well the organization is capitalizing on the value that ERM can bring, adjust its approach as needed, and document that the benefits expected from its ERM program are on track.

Adopting ERM is a commitment that requires an enterprise to examine how it can manage its risk in a comprehensive manner to achieve its business objectives in an increasingly complex and fast-paced environment. For those organizations that gauge the maturity of their ERM program, the path will be that much easier to navigate, and that much more likely to deliver the kinds of results that have made ERM such a value-adding strategic business discipline.

RIMS and LogicManager encourage you to make full use of the Risk Maturity Model for ERM©. Each organization's approach to ERM may vary depending on their particular risks, risk appetites and priorities. This makes adapting ERM within an organization a very dynamic and challenging journey, one that benefits from using the RIMS Risk Maturity Model.

Copyright © 2015 Risk and Insurance Management Society, Inc. (RIMS) and Logic Manager. All rights reserved.