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]

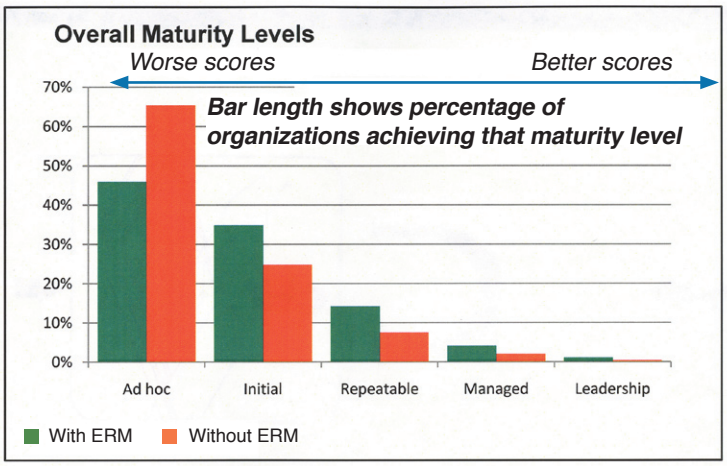
- Organizations with formalized ERM have higher RMM scores.
- Organizations with higher RMM scores have higher credit ratings.
- Organizations without formalized ERM have lower RMM scores.
- Organizations without formalized ERM have lower credit ratings.

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.

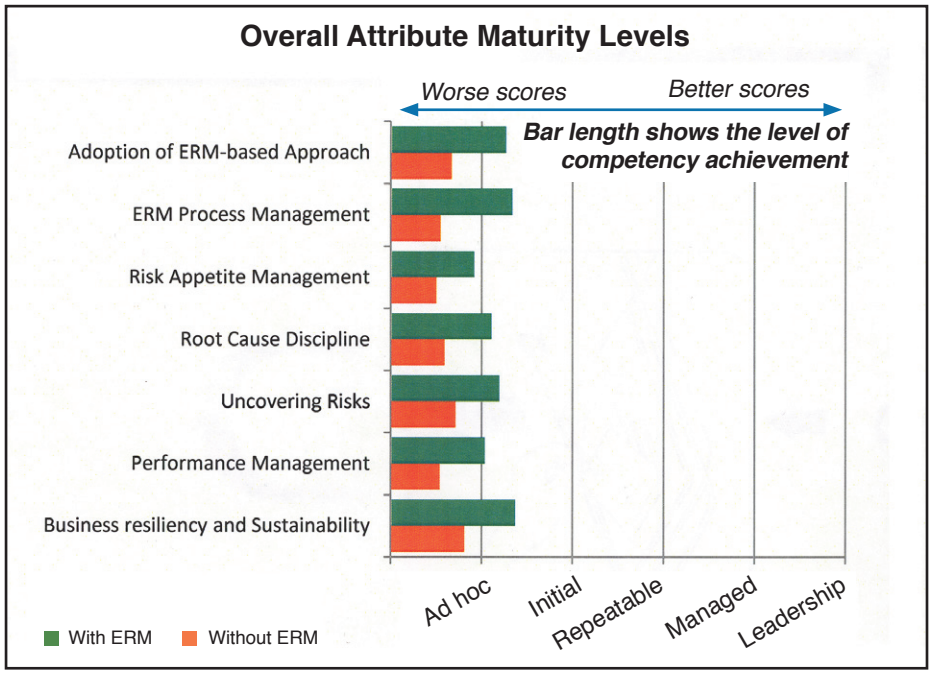
Significant Shortfall for Organizations *With ERM*

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.

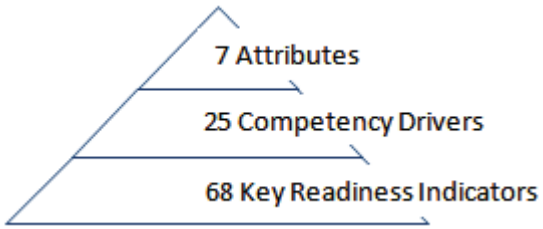
14. "Financial Elements," also called "accounts" or "line items," are components of the financial statements, such as revenue, tax and cost of goods sold.

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*

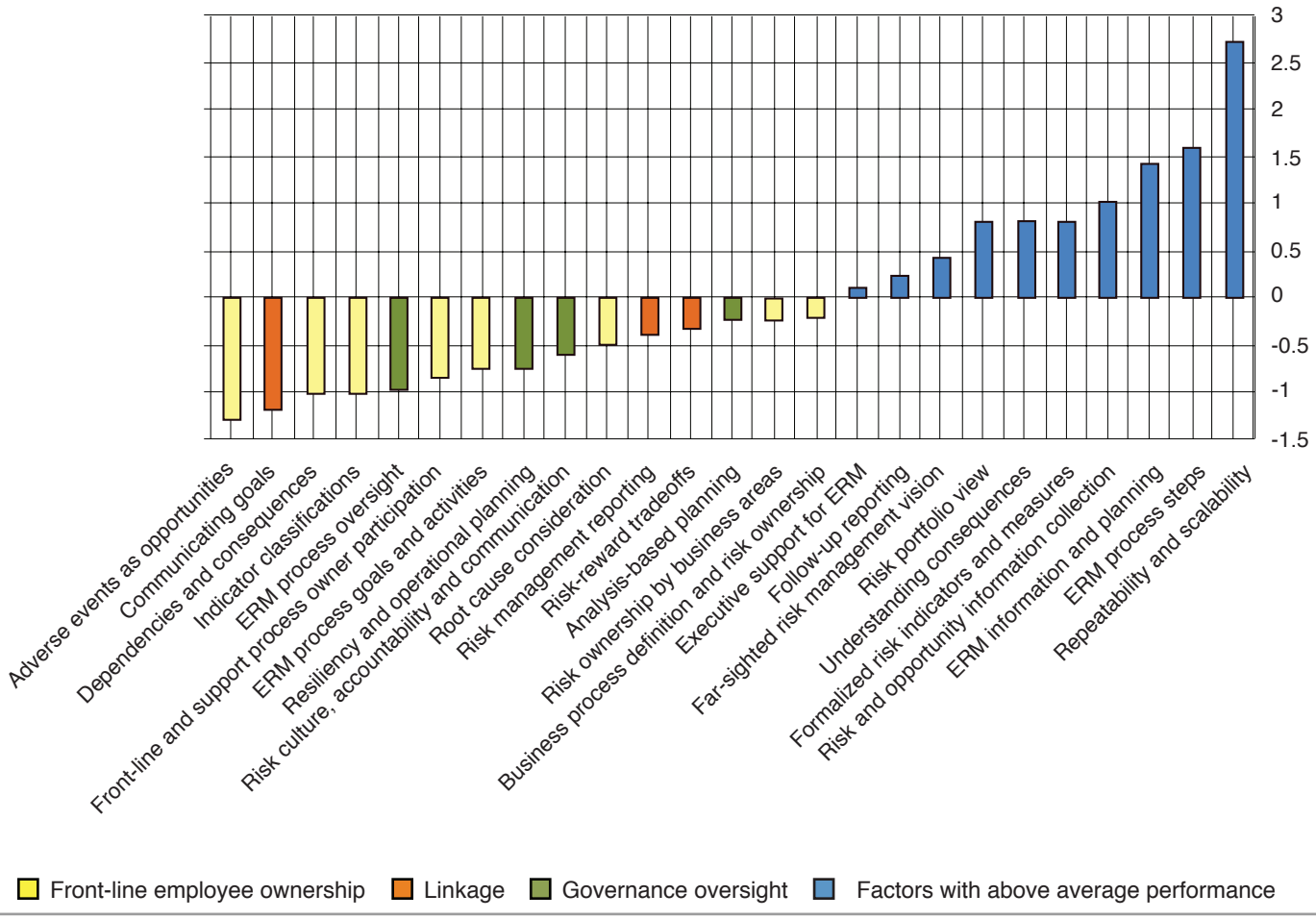
ERM enables organizations to gain efficiencies and effectiveness through a consistent and more comprehensive approach. Investigations to determine and verify organizations' risk management competency will continue to increase.

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***.

