The RIMS State of ERM Report 2015 is based on data from RIMS Risk Maturity Model for ERM® assessments collected over a seven year period from more than 2,400 organizations. The RIMS State of ERM Report 2015 and RIMS Risk Maturity Model for ERM® are published by RIMS, produced by LogicManager, and authored by Steven Minsky, with contributions from members of the RIMS ERM Development Committee and several of LogicManager’s data analysts.

THE HISTORY OF THE RIMS RISK MATURITY MODEL (RMM)

RIMS recognizes that enterprise risk management (ERM) is a core organizational competency. 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 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. The RIMS ERM Development Committee selected LogicManager, a leader in ERM expertise and innovative software solutions, to develop a risk maturity model for ERM. With contributions from ERM Development Committee members, the RIMS Risk Maturity Model for ERM® (RMM) was launched in 2006.

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.

CONTRIBUTORS

Sarah Beals, Client Solutions Manager, LogicManager
Morgan Keane, Manager of ERM Division, The Port Authority of New York and New Jersey and Member of RIMS ERM Committee
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.

ABOUT THE RIMS RISK MATURITY MODEL

Maturity models are a recognized measurement concept for demonstrating development progress and for highlighting consistent outcomes across organizations. Since its creation in 2006, the RIMS Risk Maturity Model for ERM (RMM) has been a best practice requirements model used by executives and others charged with risk-related 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 resource for boards of directors, chief executive officers, chief financial officers, chief audit executives and consultants.

Within the RMM, organizations are placed on the maturity scale from an informal “ad hoc” level to a fully realized “leadership” capability level. To enable organizations to understand where they fall within the maturity scale, the RIMS Risk Maturity Model Assessment is a key part of the model. The free and publicly available assessment (www.RIMS.org/RMM) allows organizations to score their programs in the RMM competency areas, and receive an immediate gap analysis report that can serve as the foundation for the organization to set its priorities for future improvements.

RIMS RMM for ERM has seven core attributes that describe the fundamental characteristics of an effective ERM process (Figure 1). 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 (Figure 2). The full list of the competency drivers can be found in the Appendix on page 12.

Each driver is scored on a scale of 1-10 ranging from high success to low success, for each of 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?)

• Degree of proactiveness: Measures the nature of risk management, and specifically whether it is proactive or reactive. (i.e., does the organization wait until an adverse event occurs to mitigate risk or are future scenarios planned for?)

• 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?)

Based on the results of the assessments on the above dimensions, the organization is placed on the maturity scale (Figure 3).

To learn more about the RIMS RMM, read About the RIMS Risk Maturity Model 2015.

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 SINCE 2008

• Board accountability and disclosure requirements

• A component of corporate credit ratings and a predictor of future success

• Demonstrated value in providing long-term, bottom-line benefits through academic research

TRENDS

• The number of organizations using the RMM to benchmark the state of their ERM programs has grown 250%.

• More organizations are reaching proficient ERM maturity levels, defined as those who achieve a score at the “repeatable” level or above on the RIMS RMM maturity scale.

• Though there has been improvement in the engagement levels of companies adopting formalized ERM programs, and an improvement in overall maturity scores, an opportunity exists for these organizations to improve their ERM maturity to a more proficient level. Only at a repeatable level and above do organizations begin to see the benefits of investing in ERM.
ERM INFLUENCES SINCE 2008

BOARD ACCOUNTABILITY AND DISCLOSURE REQUIREMENTS

Since the first RIMS State of ERM Report was released in early 2009, government regulations formally enforcing enterprise risk management have been enacted.

The SEC Proxy Disclosure Enhancements rule of 2010 requires boards of directors and senior-level executives to be accountable for all material risks and related mitigation activities at all levels of their organizations. In 2014, the SEC reiterated that enforcing this mandate was one of their highest examination priorities. This mandate extends risk management accountability of organizations in three important ways:

1. Holding boards of directors liable for risk down to the front-line management of organizations and throughout their supply chains
2. Linking risk and reward tradeoff activities
3. Requiring attestation and disclosure of the effectiveness of their organization’s risk management program oversight

The SEC mandate has also influenced regulators and auditors to step up their risk management oversight roles. For example, The Institute of Internal Auditors has made it a practice requirement for internal auditors to evaluate their organizations’ risk management competencies and report their findings to the board of directors1.

The SEC announced enforcement actions in 2013 that resulted in a record $3.4 billion in monetary sanctions, which was 10% higher than fiscal year 2012 and 22% higher than fiscal year 2011 (when the SEC filed the most actions in agency history)2. In its 2013 announcement, the SEC highlighted the following with respect to financial crisis enforcement actions: With several more enforcement cases in fiscal year 2013 against individuals and entities whose actions contributed to the financial crisis, the SEC has now filed enforcement actions against 169 individuals and entities arising from the financial crisis resulting in more than $3 billion in disgorgement, penalties, and other monetary relief for the benefit of harmed investors. The individuals charged include 70 CEOs, CFOs or other senior executives.

The financial crisis signaled a wakeup call for enterprise risk management. Ultimately, when we look for a cause of the 2008 financial crisis, it is critical to remember that organizations failed to do a number of things:

1. Truly adopt an enterprise risk management culture
2. Embrace and demonstrate appropriate enterprise risk management behaviors or attributes
3. Develop and reward internal risk management competencies
4. Use enterprise risk management to inform management decision-making in both taking and avoiding risks3.

A COMPONENT OF CORPORATE CREDIT RATINGS AND A PREDICTOR OF FUTURE SUCCESS

As discussed in the RIMS State of ERM Report 2008, the existence of a mature enterprise risk management program has been a factor commonly used to determine an organization’s credit rating. Companies with mature ERM programs tend to be those that are more successful in setting, keeping and tracking long-term performance goals and objectives. This high degree of forward-looking planning and reporting also leads to these organizations being more prepared for adverse events; they are able to anticipate changes in their operating environment easier and faster than companies without ERM programs. Thus, it comes as no surprise that these companies also tend to receive high credit ratings, an indicator of corporate stability and personal accountability within the organization. In turn, high credit ratings are correlated with higher employee performance, lower accident rates, better borrowing rates, and overall long-term growth and success.

According to Standard & Poor’s Management and Governance Criteria for Nonfinancial Corporate Entities:

“The evaluation of management and governance encompasses the broad range of oversight and direction conducted by an enterprise’s owners, board representatives, executives, and functional managers. Their strategic competence, operational effectiveness, and ability to manage risks shape an enterprise’s competitiveness in the

1 The Institute of Internal Auditors “Revisions to Internal Audit Standards Approval, Changes to Take Effect January 2013,” October, 2012.
marketplace and credit profile. If an enterprise has the ability to manage important strategic and operating risks, then its management plays a positive role in determining its operational success. Alternatively, weak management with a flawed operating strategy or an inability to execute its business plan effectively is likely to substantially weaken an enterprise’s credit profile. The analysis of management and governance is one of the most qualitative aspects of our rating methodology. However, the analysis of management and governance is evidence-based. The impact of management and governance analysis ranges from plus one notch to minus two or more notches.” [emphasis added.]

DEMONSTRATED VALUE IN PROVIDING BOTTOM-LINE AND LONGER-TERM BENEFITS

Valuations of firms are not only short-term estimates of current net worth, but they also reflect an estimate of the future earnings of the company based on its current vision and strategy within a given market.

Academics from the University of Georgia and the University of Mississippi published a 2011 study, based on 117 publicly traded U.S. insurance companies, examining the effect of ERM. The Farrell and Gallagher study examined the value additivity of maturation of specific aspects of the ERM practices. The attributes with the highest valuation impact were performance management (23%) and ERM process management (20%). Both attributes are process-focused and communication-centered.

Upon breaking down the maturity score into its core characteristics, the researchers found that the most important aspects of ERM from a valuation perspective relate to embedding discipline throughout the organization. For ERM to be effectual and add value, the study highlights the need for a strong risk management culture—through senior management and employee deployment and utilization of ERM—to aid in meeting the strategic objectives set by the executives of the firm.

Organizations reaching proficient levels have some opportunity for additional value growth by focusing on improving RMM maturity in the “performance management” and “root cause discipline” attributes, both of which are not among top-performing attributes for those organizations at “repeatable” or above.

THE TRENDS

Given the connection between the effectiveness found in more mature ERM programs (those that achieve maturity scores at the “repeatable” level or above) and firm value, how can today’s organizations achieve better performance? What does a mature ERM program require? What does ERM need to measure and improve?

ORGANIZATIONS ARE IMPROVING, BUT MORE CAN BE DONE

It is safe to say that enterprise risk management is still an evolving discipline, and that organizations are at different maturity levels. In a recent article, Drs. Annette Mikes of HEC Lausanne and Robert S. Kaplan of Harvard Business School believe that “risk management approaches are largely unproven and still emerging.” They go on to state that “all Wall Street financial firms had risk management functions and CROs during the expansionary period of 2002-2006… some of these firms failed in the subsequent crisis while others survived quite well.”6 Our findings support the idea that organizations are at different levels of ERM maturity, and that a large percentage are still at an “ad hoc” or “initial” level (see Figure 5).

6 Evidence of the Value of Enterprise Risk Management Robert E. Hoyt, University of Georgia, and Andre P. Liebenberg, University of Mississippi Journal of Applied Corporate Finance, Winter 2015


---

**Figure 4**

<table>
<thead>
<tr>
<th>RIMS RMM Attribute</th>
<th>Individual Value Contribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance Management</td>
<td>23%</td>
</tr>
<tr>
<td>ERM Process Management</td>
<td>20%</td>
</tr>
<tr>
<td>Adoption of ERM Based Approach</td>
<td>17%</td>
</tr>
<tr>
<td>Root Cause Discipline</td>
<td>16%</td>
</tr>
<tr>
<td>Uncovering Risks</td>
<td>15%</td>
</tr>
<tr>
<td>Risk Appetite Management</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>Business Resilience and Sustainability</td>
<td>&lt;1%</td>
</tr>
</tbody>
</table>

**Figure 5** | Percentage of Companies by Maturity Level

<table>
<thead>
<tr>
<th>Less than 10% of Companies Are Achieving ‘Proficient’ Maturity Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.6%</td>
</tr>
<tr>
<td>90.4%</td>
</tr>
</tbody>
</table>

---

Copyright © 2015 Risk and Insurance Management Society, Inc. (RIMS) and Logic Manager. All rights reserved.
The good news is that more organizations are reaching a proficient maturity level, meaning they achieve a “repeatable” or above score on the RIMS RMM maturity scale. The opportunity is for the large percentage of organizations that still are at the “initial” or “ad hoc” levels to move to a more proficient level.

More than 2,000 organizations are using the RIMS RMM to assess their maturity levels and plan improvement actions, a 250% increase over the 564 organizations studied in 2008. The percentages representing the respective maturity levels of total organizations remain similar to those noted in the 2008 report, with approximately 20% of those with ERM achieving a “proficient” score of repeatable and above, compared to approximately less than 10% of all organizations achieving that level. (Figure 6)

Another positive trend since 2008 is the percentage of competency drivers that, on average, score above the “ad hoc” maturity level. RMM users report average scores within the bottom “ad hoc” maturity level for only 4% (or one) of the 25 competency drivers covered in the assessment, whereas in 2008 fully one-fifth (or five) of the average competency driver scores fell into the “ad hoc” level. This means that organizations are incorporating more of these competency drivers as they move into the “initial” maturity level. (Figure 7)

THE DATA SHOW THAT ORGANIZATIONS WITH ERM PERFORM BETTER THAN ORGANIZATIONS WITHOUT ERM

Our study results point to significant differences in maturity levels of risk management competency drivers between organizations in the with ERM group and organizations in the without ERM group. Eighty-seven percent more organizations with ERM had an overall advantage over organizations without ERM in proficient maturity levels for all seven RMM attributes. Increased competency suggests that organizations with ERM make better risk-informed decisions, which leads to competitive advantage. (Figure 8)

ERM CONTINUES TO BE ADOPTED ACROSS A WIDE RANGE OF INDUSTRIES

While financial institutions continue to lead other industries in the rate of ERM adoption, technology companies hold a similar adoption rate of nearly 80%, followed closely by utility and energy entities and transportation organizations. Regulations enacted and enforced since 2008 may explain, in part, these higher adoption rates in three out of four of these industries. Even though adoption rates in other industries lag behind these four, every industry shows adoption rates greater than 50%. (Figure 9)
STATE OF ERM 2015

As concluded in the Farrell and Gallagher peer-reviewed academic study, greater maturity in the seven RMM attributes correlates positively to a 25% firm valuation premium in organizations the reach mature levels of enterprise risk management. In the State of ERM 2015 study, there were three particular attributes in which organizations reaching proficient levels stand out.

MATURETY BY ATTRIBUTE

Organizations that have reached proficient levels of ERM program maturity (“repeatable” or above) excel in the following top attributes, risk management competency drivers and associated readiness indicators:

**ATTRIBUTE:** ADOPTION OF ERM-BASED APPROACH
**COMPETENCY DRIVER:** BUSINESS PROCESS DEFINITION AND RISK OWNERSHIP
Key readiness indicators:
- Process owners are accountable for managing risks and use the ERM process to enhance their functions.
- Processes are defined and process-specific risks are identified.
- Risk issues are communicated and acted upon effectively and in a timely manner.
- Process owners consistently balance risk and reward when considering and making decisions about potential opportunities within regular planning cycles.

**ATTRIBUTE:** ERM PROCESS MANAGEMENT
**COMPETENCY DRIVER:** REPEATABILITY AND SCALABILITY
Key readiness indicators:
- Risk and performance assumptions are included in qualitative assessments, which are routinely revisited and updated.

**ATTRIBUTE:** ERM PROGRAM OVERSIGHT
**COMPETENCY DRIVER:** RISK OWNERSHIP
Key readiness indicators:
- 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.

**ATTRIBUTE:** RISK CULTURE, ACCOUNTABILITY AND COMMUNICATION
**COMPETENCY DRIVER:** RISK OWNERSHIP BY BUSINESS AREA
Key readiness indicators:
- Front-line risk owners identify risks that are specific to their business areas and processes to create meaningful context for their risk management activities, such as mitigation strategies and action plans.

**ATTRIBUTE:** UNCOVERING RISKS
**COMPETENCY DRIVER:** RISK OWNERSHIP BY BUSINESS AREA
Key readiness indicators:
- Front-line risk owners identify risks that are specific to their business areas and processes to create meaningful context for their risk management activities, such as mitigation strategies and action plans.
COMPETENCY DRIVER THEMES

RIMS STATE OF ERM REPORT 2015
COMPETENCY DRIVER PERFORMANCE

Figure 10 depicts median scores for the 25 competency drivers as assessed by organizations with formalized ERM programs (with ERM). On average, organizations with ERM had the least competency in 10 of the 13 competency drivers most strongly connected to front-line employee engagement, cross-functional connections and ERM program oversight:

- Four of the 11 underperforming competency drivers affect front-line employee engagement.
- Five affect cross-functional connections.
- One affects ERM program oversight.

Organizations with ERM that scored at a proficient level of maturity excel in engaging all levels of the organization, and have successfully crossed business silos to reach all departments. They have overcome the tendency to limit ERM program involvement to senior leadership teams. Instead, organizations at these higher maturity levels enact policies and processes that make a formal connection between risk identification, modification decisions and controls at the operational level.

Competency drivers that are most closely aligned with higher RMM scores show that ERM maturity depends on more than one or two of the attributes. Establishing and executing a far-sighted risk management vision—a competency driver within the ERM-based approach attribute—is most strongly correlated with better RMM scores and overall success. However, three other competency drivers also have strong correlation with better RMM assessment scores: risk-reward tradeoffs, ERM information and planning, and risk dependencies and consequences. (Figure 11)

Competency drivers that have the strongest correlation with proficient RMM scores are also those where organizations with ERM are underperforming. Organizations that are proficient can realize even greater firm value. Unfortunately, few organizations are achieving the maturity required to see such results. Within the “Adoption of an ERM-Based Approach” attribute, for example, only 12% of organizations with ERM achieve a proficient level for the “Far-Sighted Risk Management Vision” competency driver. Obviously, there is significant room for improvement. Even though companies with ERM are still better off from a valuation standpoint than those organizations without ERM, it is possible to be missing opportunities where ERM programs can contribute more. As a result, they may not be experiencing all of the possible benefits of such programs.

Competency drivers associated with basic ERM frameworks (or how risk management is adapted within the organization’s existing organizational arrangements), have grown stronger over time. This suggests that organizations are investing in these fundamental capabilities. For organizations with ERM to achieve additional benefits from their ERM investments, organizations may choose to invest more heavily in the organizational competencies (factors comprising basic ERM frameworks noted in Figure 10).

---

**Figure 10 | Competency Driver Performance for Organizations with ERM in 2015**

<table>
<thead>
<tr>
<th>Competency Driver</th>
<th>Associated Attribute</th>
<th>Degree of Understanding, Accountability and Execution with Respect To:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Far-sighted risk management vision</td>
<td>ERM-based approach⁶</td>
<td>Clear purpose and longer-term expectations that an organization has of its risk management practices at all levels</td>
</tr>
<tr>
<td>Risk-reward tradeoffs</td>
<td>Risk appetite management</td>
<td>Risk exposure that the organization is willing to undertake and the optimal maximization of value or opportunity from the selected risk amount</td>
</tr>
<tr>
<td>ERM information and planning</td>
<td>Performance management</td>
<td>ERM process as an integral element in strategy and planning activities</td>
</tr>
<tr>
<td>Risk dependencies and consequences</td>
<td>Root cause discipline</td>
<td>Examining the implications of risks to objectives throughout all areas of the organization, establishing the true source of relevant threats and opportunities, and measuring the effectiveness of controls</td>
</tr>
</tbody>
</table>

⁶ The RIMS RMM defines “Adoption of an ERM-Based Approach” as the degree of executive support within the corporate culture for an ERM-based approach to manage risks within the organization.
RECOMMENDATIONS

Recent studies have revealed a direct relationship between greater maturity in risk management and better business performance. However, the same studies also show that the majority of organizations with ERM are not yet achieving the necessary program maturity to realize as much value as they could. In light of these findings, we recommend the following:

Organizations without ERM:
This and other studies provide empirical evidence that initiating a formal ERM program can improve business performance. Board members and CEOs can use the seven attributes, 25 competency drivers, and 68 key readiness indicators within the RIMS RMM as a basis for formalizing an ERM program within existing organizational structures. These organizations can use the free online assessment to establish a baseline, and then set goals and timelines to develop the needed competencies and achieve the desired levels of maturity.

Organizations with ERM:
Boards, CEOs, risk professionals, and other risk-related committees can use the RIMS RMM competency drivers as the basis to periodically assess their organization’s maturity level against these drivers.

Based on the results of the RIMM assessment, these groups can evaluate, and possibly re-evaluate, actions designed to:

• Reinforce the adoption and effective performance of RMM competency drivers across their organizations
• Communicate operational accountability for using ERM processes in decision-making and execution
• Apply a risk-based approach to prioritize existing activities, reduce internal and external costs, and achieve goals
• Consider appropriate organizational structure and reporting relationships for a senior risk management position to be responsible for driving the 25 competencies throughout the organization
• Ensure ERM is woven into strategy and planning, so that risk-reward tradeoffs are understood in strategic decision-making and execution
• Take a root-cause approach and use standardized criteria so that risk and performance information can be compared cross-functionally and aggregated at a strategic level

All Organizations:
Understanding existing and emerging risks and being able to report on such risks at every level is crucial for gaining a greater understanding of multi-dimensional implications on the objectives of an organization. While crucial, this is extremely difficult to do without a plan. The RMM is an actionable model that complements the practices from all major standards on ERM, including COSO and ISO. The RMM provides an actionable roadmap to establish and mature an ERM program. The RMM allows organizations to understand where their respective ERM programs are sufficient, what is lacking, and what specific actions are needed to improve. Boards and senior-level risk officers responsible for their organizations’ 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.

USING RISK COMPETENCY DRIVERS

The following two foundational areas related to the associated risk competency drivers are particularly important to achieve greater value as the average scores for a number of these competency drivers were found to be weak but have been shown to be highly correlated with increases in firm value:

1. Front-Line Employee Engagement: Business process owners, particularly those responsible for delivering an organization’s products and services, have a primary “risk ownership” role for “ERM process goals and activities,” particularly in identifying, assessing by considering ‘root causes’, and modifying risks on a day-to-day basis. Operational managers and employees, including those responsible for support processes, can identify and assess the appropriate subset of the organization’s overall risk portfolio. These “front-line” employees have the capacity to suggest additional and emerging risks that may not be evident elsewhere in the organization. Such assessment may include the “dependencies and consequences” on specific strategic, operational and financial objectives, as well as opportunities for creating additional value. Depending on whether such risks fall outside the boundaries set by the organization in managing its risk appetite and tolerance, risks can then be linked with corresponding modifying and control activities, regardless of which areas throughout their organization perform the controls.

2. Cross-Functional Connections: Forming connections between risk and strategic objectives (and their execution) requires a “risk portfolio view”, one that does not focus on a specific risk in isolation but understands the connections and “risk-reward tradeoffs” across the organization’s entire value chain, regulatory environment, and geographic reach. This starts with “risk and reward information collection,” or said another way, a thorough understanding of the organization’s business model, specific strategic opportunity initiatives and how risk (that is, uncertainty) may affect achievement of the associated goals and objectives. However, it is not enough to understand. The competency driver “communicating goals” relates to both the goals of the organization and the goals for risk management in supporting strategic and operational decision-making and execution. The fifth competency driver “follow-up reporting” completes the cross-functional connection area, reporting whether the expected results affected the risk portfolio in the way the organization planned.

When organizations lack competency in any one of the 25 competency drivers—and particularly in the ones related to these two foundational areas and respective competency drivers—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, resources and financial consequences.
• Recognize the organization’s inability to achieve, in a repeatable fashion, corporate goals and objectives.

Consequently, there may be no insight for timely intervention and avoidance of an undesirable outcome. Organizations seeking better performance need to broaden and deepen their programs to mature in the areas that support front-line employee engagement and cross-functional connections.
CLOSING COMMENTS

The findings in this report suggest that the competency drivers comprising basic ERM process management frameworks have improved markedly since the 2008 report. This indeed is good news. While continuing to improve these core competency drivers of performance by providing necessary resources and visible executive sponsorship, organizations may benefit by investing in competency drivers associated with front-line employee engagement and maintaining cross-functional connections. These competency drivers are highly correlated with higher proficiency scores and enable organizations to better interpret and manage risks within chosen tolerance levels and properly consider complex interdependent issues within the organization’s risk portfolio. Organizations that fail to focus investments in these two important foundational ERM areas and associated competency drivers potentially have significantly more risk exposure than management and stakeholders may realize and perhaps more than board members knowingly accepted.

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.

ABOUT THIS REPORT

A statistical analysis was done comparing the RIMS RMM scores of more than 1,000 organizations into two groups: with ERM and without ERM. The result was statistically significant: With greater than 95% confidence, the difference in scores between the two groups is unlikely to have occurred by chance. Our data demonstrates the following positive correlations:

- The presence of a formalized ERM program and better RMM scores.
- The lack of a formalized ERM program and worse RMM scores.

While a positive correlation does not prove cause and effect, our data show that the relationship between exceptional risk leadership and firm performance is undisputed. The link between ERM maturity and firm valuation has also been validated by independent statistical studies.

Participants’ assessments statistically validated that organizations with formalized ERM infrastructures embody the 68 key readiness indicators.

Users of the RIMS RMM reflect a diverse group of organizations from across multiple industries, representing both privately and publicly held organizations. Therefore, the data is not specific to any industry or to type of organization.

Figure 12 | Industry Affiliation of all Respondants

Figure 13 | Ownership Structure of Respondants

---

7 Attributes for participating companies were compared using statistical analysis to measure the relationship between existing risk management processes and RIMS RMM scores, a proven component of financially successful companies. The correlation coefficient was calculated for each RMM factor and was found, on average, to be 0.157 and positive. Due to the high population size, this correlation coefficient has a greater than 95% 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.

### RIMS Risk Maturity Model for ERM

<table>
<thead>
<tr>
<th>7 Attributes</th>
<th>5 Maturity Levels</th>
<th>Maturity (level)</th>
<th>Maturity Level Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ad hoc (1)</strong></td>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Initial (2)</strong></td>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Repeatable (3)</strong></td>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Managed (4)</strong></td>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Leadership (5)</strong></td>
<td></td>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

#### RIMS Risk Maturity Model for ERM

<table>
<thead>
<tr>
<th>Level 1 Ad hoc</th>
<th>Level 2 Initial</th>
<th>Level 3 Repeatable</th>
<th>Level 4 Managed</th>
<th>Level 5 Leadership</th>
</tr>
</thead>
</table>
| **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 | | |