

Excerpt from the Economist Intelligent Unit 2010 research report “Fall guys risk management in the front line”:

Strategic risks—those that pose a threat to a company’s ability to set and execute its overall strategy—dominate the list of concerns for many companies. Asked about the key risks that they will face over the next 12 months, survey respondents point to weak demand as the most worrying threat. Other important issues that keep them awake at night include instability in one of their major markets and financial market volatility. These strategic risks can make the difference between survival and extinction but, in many cases, companies do not have a structured framework for identifying or mitigating them. This is not to say that strategic risks are being ignored—indeed, most board members and executive directors would see this as a fundamental part of their role. But often, these discussions are being held without a formal, structured process for gathering, aggregating and analysing risk information. And without this input, boards may not be making decisions from a position of full knowledge and understanding.

Respondents to our survey recognise the importance of *strategic risk management*, but the complexity of the task appears to prevent them from addressing it in a formal way. When asked about the main objectives of the risk management function, respondents point to the identification of new and emerging risks as the most important goal. And yet, when asked to rate their company’s effectiveness at different aspects of risk management, respondents see the identification of new and emerging risks as one of their biggest weaknesses. Equally, just 46% think that their company is effective at linking risk management with overall corporate strategy.

©2010 EIU  
Reprinted by permission

## Why Strategic Risk Management?

---

A few years ago, the RIMS Board of Directors identified strategic risk management as an emerging practice, viewing it as the next step in the evolution of enterprise risk management. It commissioned an external study in 2009 that came to similar conclusions:

- *Concepts are immature, but developing*
- *Less consideration for the potential upside risks in actual practice*
- *Organizations are seeking direction from a global leading authority that can provide services in these evolving practices*

While a number of organizations already have embraced strategic risk management as an integral part of their respective enterprise risk management practices, others are developing or practicing strategic risk management as a focused discipline outside of a formal enterprise-wide risk management effort. RIMS intends to be the leading global authority on strategic risk management, whether an organization chooses to make it part of its enterprise risk management practices or focus its risk practices on strategy separately.

Recognizing that strategic risk management is an evolving practice, RIMS formed a Strategic Risk Management Development Council to complement the strong work of its ERM Committee in this focused area. This advisory council is comprised of strategic and enterprise risk management practitioners as well as a published academic on the topic. By using common board and staff liaisons, as well as including a member liaison from the ERM Committee, the board sought to secure a solid directional link for RIMS.

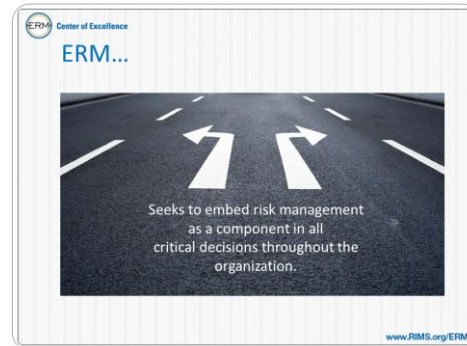
In creating the council, RIMS emphasized that SRM is not meant to supplant ERM, nor is this focus on SRM intended to create a new risk management silo. Indeed, we envision the convergence of ERM and SRM as more organizations formally adopt enterprise risk management. That said, RIMS recognizes that each organization determines what it needs from risk management and that strategy is driven by executive management, primarily through strategic planners. As such, RIMS – in meeting its mission for advancing the risk management discipline – is ready to serve those respective needs.

The following paper is intended to provide the necessary context for two important definitions: **enterprise risk management** and **strategic risk management**.

## What is ERM?

**Enterprise risk management (ERM)** 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.

Along with other principles, ERM encompasses all areas of organizational exposure to risk (including strategic) and seeks to embed risk management as a component in all critical decisions throughout the organization.<sup>1</sup>



As described in RIMS Executive Report, “The 2008 Financial Crisis, A Wake-up Call for Enterprise Risk Management,” all organizations practice risk management in multiple forms, depending on the exposure being addressed. As such, along with financial risk management, we have witnessed the emergence of terms such as IT risk management, operational risk management and supply chain risk management, to name a few. Regardless of focus, risk management is practiced in some form in most organizations.

While some or all of these practices arguably may – and ideally should – be part of a larger enterprise risk management umbrella, not all organizations have embraced the scope of enterprise risk management. Certain organizations do not have an enterprise risk management program nor do they intend to look into one. In such cases, specifically focused risk management practices are important to the organizations in which they are practiced. Other organizations may choose to initiate an enterprise risk management approach from one of the focused areas where risk management practices have matured, or by integrating the more mature focused areas to achieve an interrelated portfolio view. Strategic risk management may make sense as a starting point for an enterprise approach given the visibility risk management has gained at the board level.

<sup>1</sup> The other principles included in the RIMS ERM definition are:

- Prioritizes and manages those exposures as an interrelated risk portfolio rather than as individual “silos”
- Evaluates the risk portfolio in the context of all significant internal and external environments, systems, circumstances, and stakeholders
- Recognizes that individual risks across the organization are interrelated and can create a combined exposure that differs from the sum of the individual risks
- Provides a structured process for the management of all risks, whether those risks are primarily quantitative or qualitative in nature
- Views the effective management of risk as a competitive advantage

## What is SRM?

Specifically focused, **strategic risk management (SRM)** is a business discipline that drives deliberation and action regarding uncertainties and untapped opportunities that affect an organization’s strategy and strategic execution.

Strategic risk management, whether alone or integrated in an ERM program context, can potentially identify situations in which risk can be a competitive advantage instead of only a threat to the strategic plan. SRM encompasses the interdisciplinary intersection of strategic planning, risk management and strategy execution in managing risks and seizing opportunities, not only for protection against losses, but for reducing uncertainties and seizing opportunities, thus enabling better performance in achieving the organization’s objectives and greater resilience in an uncertain environment.



Through the work of the council, RIMS identified ten specific guiding principles important to strategic risk management for strategic decision-making which are more fully described in other RIMS documents:

- Value-driven
- Reflective
- Structured
- Informed
- Dynamic
- Process-based
- Condition-based
- Consequential
- Interdisciplinary
- Scenario-driven

## Frequently Asked Questions

---

### Q1. Isn't SRM part of ERM already?

It depends on whether the *management* of strategic risks is included in the scope and design of ERM. While many organizations do include strategic risks in their respective ERM risk registers, these risks may not be integrated fully into the strategic planning process where decisions on value creation as well as value protection are being made.

Senior management teams may not have embraced strategic risk management as a vital component of enterprise risk management. This limits awareness of ERM's structured discipline and enabling capabilities to help the organization manage the risks most directly related to achievement of the organization's objectives. Furthermore, without a disciplined strategic risk assessment, risks arising from the plans to meet the objectives may be overlooked.

### Q2. We already have a process for developing strategy and risk considerations are part of that process. Isn't that enough?

SRM provides a systematic framework and process to address the uncertainties defined at the outset of strategy-setting. For example, the identification of threats and opportunities in a SWOT analysis may be quite similar to the initial identification approach used in SRM. However the SWOT process does not involve systematic prioritization – or the explicit handling – of the identified threats and opportunities in relation to the organizational strengths and weaknesses. A SWOT analysis generally assumes that this activity is being done in the subsequent operational strategy execution planning process.

There remains a development need for practical risk management applications in reducing uncertainty in strategy-setting as well as strategy execution. Formal risk assessments may be made at different points along the value chain. However, the methods and processes for aggregating and analyzing these strategic risks within an organization's appetite and tolerance for risk against the expected reward outcome are in limited use. The value-driven risk management techniques most useful in a strategic setting are different from those that may be used currently in strategic planning, in ERM or, for that matter, in strategic decision-making outside of the formal strategic planning process.

While many strategy defining processes do embed risk and opportunity identification, few have included systematic or even explicit handling of the identified uncertainties, such as "cut-off" limits based on early warning measures. Furthermore, by applying a consistent SRM framework and process, organizations can gain an advantage by monitoring the consolidated uncertainty exposure of the strategic portfolio – which is not the case if each strategy is defined separately.

Finally, for an organization that has defined its strategic risk appetite, the consolidated measure of exposure can be compared to the risk appetite. This supports deliberations as to whether the proposed strategy portfolio is in fact more ambitious than "allowed" within the appetite, or not ambitious enough – enabling the organization to pursue even higher targets.

### Q3. How are SRM methods and techniques different from those used in ERM?

Overall, they are closely related, particularly in the process used. However, the emphasis is different as the level of insight and certainty differ considerably between current operational and future strategic uncertainties.

ERM risk assessment methodologies used in many organizations focus on certain elements of risk: primarily relative impact (however defined internally) and probability (or frequency/likelihood) of occurrence, frequently focused on the present day or over a relatively short time horizon. Other elements that may be taken into consideration are speed to onset (also referenced as velocity or immediacy), impact to reputation, and impact to various stakeholders outside of the organization. ERM identification and analysis methodologies tend to focus on events, rather than trends, and may rely heavily on historical data, which may or may not be predictive of future conditions. Organizations apply varying levels of qualitative and quantitative techniques in risk evaluation. Monitoring and measuring methods focus on risk and performance indicators related to management of key risks. These risk-based and event-driven techniques may be limiting in strategic planning where the focus tends to be more *trend-driven* while considering potential *future* events.

SRM methods and techniques focus primarily on uncertainty from a relevance and importance perspective in achieving strategic objectives. The assessment elements may also include timing, impact to reputation and impact to various stakeholders, but usually with less emphasis on relative impact and/or likelihood. The methods and techniques are forward looking over the strategic planning time horizon, use scenario planning and stress testing not as predictors but for alternate strategy planning purposes, incorporate emerging and dynamic risks as considerations, integrate change management for effective response to changing conditions, and are strongly linked to planning, allocation and management of capital and funding needs. Metrics and monitoring methods generally are linked to 1) risk/reward outcomes within a defined risk appetite framework and 2) performance, focusing on deviations from expected performance outcomes.

While many of the risk assessment techniques used in an ERM context can be useful in strategic planning and decision-making, different or modified methods and techniques specific to strategy-setting and execution can be applied.

### Q4. Why should an organization that has implemented ERM consider an SRM focus? Aren't the same people involved?

There are multiple reasons why an organization that has an ERM program may want to include a specifically focused SRM approach within its ERM framework and practice.

First, successful achievement of the organization's objectives is not considered fully if the ERM program's primary focus and contribution are on value protection (that is, mitigation, compliance and/or control). Value may be untapped and lost if the organization views risk only as an impediment rather than a potential opportunity.

Second, different people within the organization may be accountable for corporate strategy and execution than those who are responsible for functional day-to-day operations. Decision-makers and influencers at the strategic level may include a board of directors, trustees, executive management and others in strategy setting who have a strong focus on emerging and dynamic risks,

while operational, financial, legal and compliance risks – which may or may not be strategic in nature – generally are managed at various levels throughout the organization with a primary focus on known or foreseen risks.

Third, strategic and emerging risks may not find “natural” owners for identification, assessment, planning, threshold alerts and monitoring in current ERM governance structures, although such risks may affect multiple parts of the organization.

By incorporating a disciplined strategic risk management focus, a more direct connection between the risks related to the strategy itself and its execution is achieved. Furthermore, a strategic risk management focus is more likely to reframe risks as potential opportunities.

Risk practitioners, who support and drive a strong risk management process throughout an organization, provide the common discipline for SRM as well as ERM.

#### Q5. What are the similarities between ERM and SRM?

ERM and SRM are similar in that both evaluate risk in the context of significant internal and external environments and stakeholders. Both provide a structured framework and process, although methods and techniques may differ. Both seek to embed risk management as a critical component in decision-making. In fact, these similarities highlight the benefits of merging SRM into the ERM program and broadening the scope of ERM to include the strategy development process – even when response measures may differ from those applied in traditional ERM.

#### Q6. Can SRM be implemented if ERM has not been implemented or has not met expectations?

Yes, strategic risk management can be implemented as a focused discipline in strategic planning, without having an enterprise risk management program in place. On the other hand, a number of organizations are initially testing or re-evaluating ERM by taking a strategic risk management focus to demonstrate the value of risk management in decision-making for achieving organizational objectives.

#### Q7. What is the purpose of the SRM principles?

The SRM principles are fundamental characteristics offered for guidance and direction. They are by no means prescriptive nor are they sequential, but they all are important for a strategic risk management focus. The degree of relative importance for each of the principles within particular industries, sectors or organizations is left to individual organizations to decide.

#### Q8. Are the SRM principles only useful to organizations that define strategy well?

No. Effective use of the SRM principles actually may help an organization to define its strategy with more clarity, as the discipline drives deeper consideration of the unintended consequences and potential exposures arising from and created by operational plans designed to execute the chosen strategy. Evaluation of significant internal and external conditions, such as organizational capabilities, environments, forces, events, trends and stakeholders – if not already included in the strategy itself – in fact may lead to different and potentially more value-producing strategies.

#### Q9. How would an organization use the SRM principles?

For organizations that formally have integrated risk management into strategic planning and execution already, the principles may serve to validate what is already being practiced, or to identify characteristics that currently are not being embraced by the organization.

For organizations planning to integrate risk management into strategic planning and execution, the principles may serve as guidance as to the characteristics needed for effective implementation and practice.

For organizations that have not considered integrating risk management into strategic planning and execution, the principles may serve as conversation-starters for enhancing the organization's current approach in order to link risk management with its corporate strategy more effectively.

#### Q10. How is SRM related to operational risk management?

Operational risk management generally focuses internally on the risks inherent in or arising from the organization's operations, such as people, processes and technology. It may also consider external events, external resources and regulatory compliance but only to the extent such events might affect operations, and not necessarily the overall strategy.

As noted earlier, SRM specifically focuses on trends, future events and circumstances not only as threats but as untapped opportunities in strategic design, while considering the allocated resources needed to execute the adaptive strategy. While corporate strategies usually are set at an executive level, strategy execution occurs at the operational level. The relationship between strategic and operational risk management is the link between design and implementation. The stronger the link, the more successful the strategy can be. In addition, the link addresses the stakeholder, board and executive management desire for more effective risk management in strategic and operational decision-making.

#### Q11. Who should be involved in SRM and how can it be implemented?

Since this is an emerging practice, the "who" and "how" of SRM are still being defined. As with ERM, collaboration among the various internal stakeholders is required to advance the organizational objectives.

RIMS would like to thank the following individuals for their contributions to this document:

### RIMS Strategic Risk Management Development Council Members

Carol Fox, Council Chair, RIMS

Michael Liebowitz, Council Vice Chair, New York University and Former RIMS President

Judy Aakeberg, Greater Orlando Aviation Authority

Eric Benson

Mark L. Frigo, PhD, DePaul University

Hans Læssøe, LEGO System A/S

Monica Merrifield, YMCA of Greater Toronto

Joe Restoule, Restoule Risk Management and Former RIMS President

Nowell Seaman, University of Saskatchewan

Drew Zavatsky, State of Washington

### RIMS ERM Committee Members

Pete Fahrenthold, Committee Chair, United

Ryan Egerdahl, Committee Vice Chair, Bonneville Power Authority

Grace Crickette, University of California

Radu Demian, University Hospitals Health System Inc.

Carol Fox, RIMS

John Hach, Lincoln Electric Co.

Jayashree Ishwar, Erie Insurance Group

Rupak Mazumdar, eHealth Ontario

Russell McGuire, Milliman Risk Advisory Services

Soubhagya Parija, Sterling Jewelers, Inc.

Nowell Seaman, University of Saskatchewan

Cristina Tate, Hewlett-Packard Company

Walt Williams, Lowe's Companies, Inc.

Drew Zavatsky, State of Washington

RIMS would like to acknowledge the following individuals for their support of this work:

### RIMS Board of Directors

Scott B. Clark, President, Miami-Dade County Public Schools

Deborah M. Luthi, Vice President

San Francisco Public Utilities Commission

Carolyn M. Snow, Treasurer, Humana Inc.

John R. Phelps, Secretary

Blue Cross and Blue Shield of Florida, Inc.

Janet Barnes, Public Utility District No. 1 of Snohomish County

Robert Cartwright, Jr., Bridgestone Retail Operations, LLC

Kim Hunton, City of Ottawa

Daniel H. Kugler, Snap-on Inc.

William J. Montanez, Ace Hardware Corporation

Julie C. Pemberton, Chiquita Brands International

Michael D. Phillipus, ATP Oil & Gas Corporation

Richard J. Roberts, Jr. Ensign-Bickford Industries, Inc.

Frederick J. Savage, Chevron Corporation

Nowell R. Seaman, University of Saskatchewan

Lori Seidenberg, Centerline Capital Group

Terry Fleming, Montgomery County, Maryland

### Executive Director

Mary Roth, RIMS Executive Director