SECURITIES AND EXCHANGE COMMISSION

17 CFR 229, 239, and 240

[Release Nos. 33-10668; 34-86614; File No. S7-11-19]

RIN 3235-AL78

Modernization of Regulation S-K Items 101, 103, and 105

AGENCY: Securities and Exchange Commission

ACTION: Proposed rule

To: Vanessa Countryman, Secretary

RE: Comments for File No. S7-11-19

I respectfully submit these comments for consideration under Section 3 General Request for Comments. I would like to take this opportunity to submit my thoughts and recommendations regarding the proposed changes. Unfortunately, given the length of the proposed rule, I apologize in advance for the brevity of the comments. The comments are divided into both general comments and observations on some of the individual section change proposals.

I have had the opportunity to study Sections 101, 103 and 105 in dozens of public company 10K's over the course of the last 7 years while teaching Enterprise Risk Management in the Business School at the University of Colorado Denver. After reading nearly identical disclosures across multiple companies in different industries, it is easy to understand why the average investor understands these potential risks and their impacts as well as college students studying them for the first time. This proposed rule can upgrade a decades old and outdated requirement and bring much greater clarity to an opaque process.

Focusing on the proposed rules principles-based approach, comments will be focused around two important concepts: context and communication. Incorporating these two important principles will provide greater insight into the enterprise risks an organization faces and how it organizes itself to mitigate those risks.

General Comments

I believe the proposed rules have identified the most important concept that should be embodied in any changes made to the existing rules. The concept is materiality. Ever since “Significant Risks” were established as the disclosure criteria decades ago, significant risks to the organization has devolved into a laundry list of boilerplate disclosures that provide little to no communicated value to the average investor. The recommendation of migrating to “Material” risks will significantly enhance informative disclosure.

However, materiality as currently taught, consists of 2 primary components and neither one is suggested in any of the proposed changes. Those two components are risk appetite and risk tolerance. Risk appetite is typically a statement of desired risk as articulated by the organization's management. Understanding how much risk an organization wants to take on to achieve desired goals is highly relevant to the average investor and should be memorialized in an organizational statement.

Risk tolerance is the actual internally financially calculated amount that the organization can bear without significantly negative operational impact. That dollar figure defines which risks are material to an organization that require the focus of management to mitigate.

By requiring disclosure of their risk tolerance number, it will facilitate a more detailed risk discussion within the organization and outside parties will no longer be able to prepare risk factors meaningfully. This item will be addressed separately in the discussion on Item 103 and Item 105.

Another relevant comment involves the evolution of risk oversight and responsibilities for public companies. In the recent update of the COSO ERM Framework (The Executive Summary of this update is attached for citation and review as Exhibit 1), COSO (Committee of Sponsoring Organizations of the Treadway Commission) identified governance and risk oversight as the first principle of enterprise risk management. In their document, COSO stresses that enterprise risk management is not a function or a department, instead it is a practice that allows for the more effective governance of the organization to include communicating with internal and external stakeholders. How actual risks are defined and communicated in Section 105 will be commented on further.

Finally, while also not identified for consideration in the proposed rules, how an organization structures itself around enterprise risk management is also very relevant. For while identifying significant risks of a particular organization is important, it is also critically important to understand how the organization has created an accountability system to mitigate its key risks and for the most part, those risks are ones that are not insurable. It is one thing to identify broad generic risks but also identifying key risk owners and their mitigation plans and responsibilities would be far more reassuring to investors and other key stakeholders. While such detail is most likely beyond the scope of the 10k, I have no longer become surprised at the number of multi-billion-dollar revenue companies that have one person appointed to risk management. Obviously, no one person can have enterprise risk oversight over a large organization, therefore disclosing the process for enterprise risk oversight becomes very meaningful.

Section 101 (C)

The comment on the Narrative Description of Business is that another item should be added to the principle disclosures of this section. Considering today's rapidly involving business environment, an item on emerging risk, to include emerging trends and emerging technologies, should be incorporated into 101 C. While a discussion on the Narrative Description of the Business as it exists today is very relevant, what should also be disclosed is management's strategy around the potential disruption of the current business model by emerging risk. While I can imagine significant pushback around this type of requirement by business, disruption has caused several name brand companies to disappear fairly abruptly. In addition, any prognostication by management around potential upside risk or downside risk should be protected by the Safe Harbor Act. This type of information is certainly material to an understanding of the registrant’s business taken as a whole.

Legal Proceedings (Item 103)

Under Item 103, Legal Proceedings, it has been proposed that the limits for disclosure of environmental liability legal proceedings be raised from the current decades old $100,000 to an inflation adjusted amount of $300,000. While I agree that full disclosure of material legal proceedings is important, the issue with this approach is context. To apply an arbitrary number of $300,000 to corporations that can easily range in size from $300 Million to $30 Billion, it becomes easy for the larger organization as well as outside parties to look at that number as immaterial to them.

To my earlier comment, potentially the best requirement for this section is for the organization to disclose any legal proceedings that meets both the organization's individual definition for risk tolerance and $300,000, as every organization of size will have a risk tolerance greater than $300,000. However, once again, the registrant would again have to demonstrate a higher level of risk oversight.

Risk Factors (Item 105)

The Proposed Rules have suggested that when risk factors exceed 15 pages, a summary table of those risks should precede the actual listing of risks. While I believe such a requirement would make the risk factors easier to review, I do not believe the summary table goes far enough. Again, the issue here is context. As stated earlier, there are numerous boilerplate risk disclosures that exist in nearly every public filing. I am a proponent of organizing those mostly general, hard to define risks into a general risk category. However, there are numerous material risks that organizations deal with daily that do not make it into that risk disclosure section.

The proposed solution to elevating and better communicating material risks issues would be to require the summary table of risks to be organized by potential "material" impact to the organization. At a minimum, this will require the organization to conduct some form of risk ranking exercise to comply with the requirement. But this is not an exercise for the sake of exercise. This provides informed disclosures of the material risks that are specific to that organization for both internal and external stakeholders.

This solution solves two issues. The first is that many risk factors disclosed are so ambiguous in nature as to be unquantifiable. The second is that it highlights management's perception of these risks in comparison to the organization's calculated risk tolerance level. In turn It facilitates better communication both internally and externally regarding material risks and actions that are being taken to mitigate those risks.

The second concept this comment is focused on is communication. If the SEC were to enact a rule that required to incorporating a simple impact rating system in the summary of risks, such a rule would facilitate much greater communication within organizations regarding material risks. This would come at a time when such communication is being urgently requested at the Board level of many companies. Personally, as a longtime member of both the Risk and Insurance Management Society and the National Association of Corporate Directors, I can definitively report that the risk function within an organization, senior management and the Board of Directors are all clamoring for improved risk information. While the focus of this effort is on providing adequate public disclosure, within the organizations themselves, they are looking for a higher level of risk insight.

Today many Board audit committees will work with their outside auditors to craft today's significant risk factors while both management and board members are trying to ensure that risk information is properly communicated throughout the organization. This subject was addressed in a RIMS publication last year titled “Communication Risk to the C-Suite and the Board. (That RIMS Professional Report is attached for citation and review as Exhibit 2)

This is also another opportunity to demonstrate the level of appetite an organization may have. If Cyber Liability does not appear near the top of the list because management, who takes a conservative stance on this issue and buys high limits of insurance protection, feels they have sufficient mitigation plans in place. This is potentially an opportunity to demonstrate a positive competitive differentiator.

Obviously, changes to the risk factors disclosure requirements present the greatest opportunity sure positive change in public disclosures. This could not come add a more relevant time as the velocity of change in risk continues to accelerate. Incorporation of any of the proposed rule changes will have a positive effect. The need for more informed risk disclosures is clear and not limited to public filings such as 10K’s. I recently received investment profiles on several various funds. In the disclosure section of each of the funds was a section on Principal Risks and Investment Risk. Those two sections were nearly identical for every single fund. To the average investor, they are literally of no use at all. Corporations should thoroughly and honestly disclose those risks that keep management and the board awake at night. They are unconcerned with space debris, nuclear wars, climate change and global economic meltdowns but the average investor does deserve to know what causes them to lose sleep.

Potential Costs and Benefits

Under Section 4 Potential Costs and Benefits, an economic analysis was provided to demonstrate the potential costs of enacting these rules. The suggestions in this comment are intended to be simple to implement as the organization should already be doing some form of enterprise risk management already. Whether required by regulation or implemented for greater operational efficiency, many organizations have been slowly developing enterprise risk management oversight to better ensure the stability of operational results.

While I won't specifically opine on the projected costs, I would like to raise the question “What is the cost of not informing shareholders of material risks and the potential impact?” The obvious ensuing Directors & Officers litigation provides its own substantial costs. While reputational damage and economic loss exist at the organizational level, the individual investor usually fares worse. As seen recently, the suddenly realized risks in a company about to go public can result in tens of billions of dollars being shaved off the company’s valuation. How does that cost compare?

Conclusion

This brief comment obviously does not address all the questions as put forth in the Proposed Rule. I applaud the work the SEC is doing in modernizing the 10K. In today’s world, there is no rationale for generalized, non-quantifiable risk factors to be disclosed in a public filing. The reason it is called a public filing is so that the public will know as much as possible regarding the organization they will entrust their assets with.

There is no desire to shortchange the rule questioning process as shown. While not in a position to comment on every question, I would affirmatively answer each question with a yes. The rationale is that every question promoted a better, more transparent practice to be instituted. The risk management community in general supports that effort at every step.

Please do not hesitate to reach out for any clarifications or questions. I appreciate the opportunity to provide comments on this important and look forward to the positive change you can create.

Respectfully,

David J Young

Lecturer

Risk Management and Insurance (RMI) Program

University of Colorado Denver | Business School

1475 Lawrence St., Denver, CO 80202

☎[redacted] | ✉[redacted]

business.ucdenver.edu/rmi

Committee of Sponsoring Organizations of the Treadway Commission

Enterprise Risk Management

Integrating with Strategy and Performance

Executive Summary

June 2017

This project was commissioned by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which is dedicated to providing thought leadership through the development of comprehensive frameworks and guidance on internal control, enterprise risk management, and fraud deterrence designed to improve organizational performance and oversight and to reduce the extent of fraud in organizations. COSO is a private sector initiative, jointly sponsored and funded by:

- American Accounting Association
- American Institute of Certified Public Accountants
- Financial Executives International
- Institute of Management Accountants
- The Institute of Internal Auditors

Foreword

In keeping with its overall mission, the COSO Board commissioned and published in 2004 *Enterprise Risk Management—Integrated Framework*. Over the past decade, that publication has gained broad acceptance by organizations in their efforts to manage risk. However, also through that period, the complexity of risk has changed, new risks have emerged, and both boards and executives have enhanced their awareness and oversight of enterprise risk management while asking for improved risk reporting. This update to the 2004 publication addresses the evolution of enterprise risk management and the need for organizations to improve their approach to managing risk to meet the demands of an evolving business environment.

The updated document, now titled *Enterprise Risk Management—Integrating with Strategy and Performance*, highlights the importance of considering risk in both the strategy-setting process and in driving performance. The first part of the updated publication offers a perspective on current and evolving concepts and applications of enterprise risk management. The second part, the Framework, is organized into five easy-to-understand components that accommodate different viewpoints and operating structures, and enhance strategies and decision-making. In short, this update:

- Provides greater insight into the value of enterprise risk management when setting and carrying out strategy.
- Enhances alignment between performance and enterprise risk management to improve the setting of performance targets and understanding the impact of risk on performance.
- Accommodates expectations for governance and oversight.
- Recognizes the globalization of markets and operations and the need to apply a common, albeit tailored, approach across geographies.
- Presents new ways to view risk to setting and achieving objectives in the context of greater business complexity.
- Expands reporting to address expectations for greater stakeholder transparency.
- Accommodates evolving technologies and the proliferation of data and analytics in supporting decision-making.
- Sets out core definitions, components, and principles for all levels of management involved in designing, implementing, and conducting enterprise risk management practices.

Readers may also wish to consult a complementary publication, COSO's *Internal Control—Integrated Framework*. The two publications are distinct and have different focuses; neither supersedes the other. However, they do connect. *Internal Control—Integrated Framework* encompasses internal control, which is referenced in part in this updated publication, and therefore the earlier document remains viable and suitable for designing, implementing, conducting, and assessing internal control, and for consequent reporting.

The COSO Board would like to thank PwC for its significant contributions in developing *Enterprise Risk Management—Integrating with Strategy and Performance*. Their full consideration of input provided by many stakeholders and their insight were instrumental in ensuring that the strengths of the original publication have been preserved, and that text has been clarified or expanded where it was deemed helpful to do so. The COSO Board and PwC together would also like to thank the Advisory Council and Observers for their contributions in reviewing and providing feedback.

Robert B. Hirth Jr.
COSO Chair

Dennis L. Chesley
PwC Project Lead Partner and Global and APA Risk and Regulatory Leader

Committee of Sponsoring Organizations of the Treadway Commission

Board Members

Robert B. Hirth Jr.
COSO Chair

Richard F. Chambers
The Institute of Internal Auditors

Mitchell A. Danaher
Financial Executives International

Charles E. Landes
American Institute of Certified Public Accountants

Douglas F. Prawitt
American Accounting Association

Sandra Richtermeyer
Institute of Management Accountants

PwC—Author

Principal Contributors

Miles E.A. Everson
Engagement Leader and Global and Asia, Pacific, and Americas (APA) Advisory Leader
New York, USA

Dennis L. Chesley
Project Lead Partner and Global and APA Risk and Regulatory Leader
Washington DC, USA

Frank J. Martens
Project Lead Director and Global Risk Framework and Methodology Leader
British Columbia, Canada

Matthew Bagin
Director
Washington DC, USA

Hélène Katz
Director
New York, USA

Katie T. Sylvis
Director
Washington DC, USA

Sallie Jo Perraglia
Manager
New York, USA

Kathleen Crader Zelnik
Manager
Washington DC, USA

Maria Grimshaw
Senior Associate
New York, USA

The Changing Risk Landscape

Our understanding of the nature of risk, the art and science of choice, lies at the core of our modern economy. Every choice we make in the pursuit of objectives has its risks. From day-to-day operational decisions to the fundamental trade-offs in the boardroom, dealing with risk in these choices is a part of decision-making.

As we seek to optimize a range of possible outcomes, decisions are rarely binary, with a right and wrong answer. That's why enterprise risk management may be called both an art and a science. And when risk is considered in the formulation of an organization's strategy and business objectives, enterprise risk management helps to optimize outcomes.

Our understanding of risk and our practice of enterprise risk management have improved greatly over the past few decades. But the margin for error is shrinking. The World Economic Forum has commented on the "increasing volatility, complexity and ambiguity of the world."[1] That's a phenomenon we all recognize. Organizations encounter challenges that impact reliability, relevancy, and trust. Stakeholders are more engaged today, seeking greater transparency and accountability for managing the impact of risk while also critically evaluating leadership's ability to crystalize opportunities. Even success can bring with it additional downside risk—the risk of not being able to fulfill unexpectedly high demand, or maintain expected business momentum, for example.

Organizations need to be more adaptive to change. They need to think strategically about how to manage the increasing volatility, complexity, and ambiguity of the world, particularly at the senior levels in the organization and in the boardroom where the stakes are highest.

Enterprise Risk Management—Integrating with Strategy and Performance provides a Framework for boards and management in entities of all sizes. It builds on the current level of risk management that exists in the normal course of business. Further, it demonstrates how integrating enterprise risk management practices throughout an entity helps to accelerate growth and enhance performance. It also contains principles that can be applied—from strategic decision-making through to performance.

Below, we describe why it makes sense for management and boards to use the enterprise risk management framework,[2] what organizations have achieved by applying enterprise risk management, and what further benefits they can realize through its continued use. We conclude with a look into the future.

Management's Guide to Enterprise Risk Management

Management holds overall responsibility for managing risk to the entity, but it is important for management to go further: to enhance the conversation with the board and stakeholders about using enterprise risk management to gain a competitive advantage. That starts by deploying enterprise risk management capabilities as part of selecting and refining a strategy.

Most notably, through this process, management will gain a better understanding of how the explicit consideration of risk may impact the choice of strategy. Enterprise risk management enriches management dialogue by adding perspective to the strengths and weaknesses of a strategy as conditions change, and to how well a strategy fits with the organization's mission and vision. It allows management to feel more confident that they've examined alternative strategies and considered the input of those in their organization who will implement the strategy selected.

1 The Global Risks Report 2016, 11th edition, World Economic Forum (2016).

2 The Framework uses the term "board of directors" or "board," which encompasses the governing body, including board, supervisory board, board of trustees, general partners, or owner.

Once strategy is set, enterprise risk management provides an effective way for management to fulfill its role, knowing that the organization is attuned to risks that can impact strategy and is managing them well. Applying enterprise risk management helps to create trust and instill confidence in stakeholders in the current environment, which demands greater scrutiny than ever before about how risk is actively addressing and managing these risks.

The Board's Guide to Enterprise Risk Management

Every board has an oversight role, helping to support the creation of value in an entity and prevent its decline. Traditionally, enterprise risk management has played a strong supporting role at the board level. Now, boards are increasingly expected to provide oversight of enterprise risk management.

The Framework supplies important considerations for boards in defining and addressing their risk oversight responsibilities. These considerations include governance and culture; strategy and objective-setting; performance; information, communications and reporting; and the review and revision of practices to enhance entity performance.

The board's risk oversight role may include, but is not limited to:

- Reviewing, challenging, and concurring with management on:
  - Proposed strategy and risk appetite.
  - Alignment of strategy and business objectives with the entity's stated mission, vision, and core values
  - Significant business decisions including mergers acquisitions, capital allocations, funding, and dividend-related decisions
  - Response to significant fluctuations in entity performance or the portfolio view of risk.
  - Responses to instances of deviation from core values.
- Approving management incentives and remuneration.
- Participating in investor and stakeholder relations.

Over the longer term, enterprise risk management can also enhance enterprise resilience—the ability to anticipate and respond to change. It helps organizations identify factors that represent not just risk, but change, and how that change could impact performance and necessitate a shift in strategy. By seeing change more clearly, an organization can fashion its own plan; for example, should it defensively pull back or invest in a new business? Enterprise risk management provides the right framework for boards to assess risk and embrace a mindset of resilience.

Questions for management

Can all of management—not just the chief risk officer—articulate how risk is considered in the selection of strategy or business decisions? Can they clearly articulate the entity's risk appetite and how it might influence a specific decision? The resulting conversation may shed light on what the mindset for risk taking is really like in the organization.

Boards can also ask senior management to talk not only about risk processes but also about culture. How does the culture enable or inhibit responsible risk taking? What lens does management use to monitor the risk culture, and how has that changed? As things change—and things will change whether or not they're on the entity's radar—how can the board be confident of an appropriate and timely response from management?

What Enterprise Risk Management Has Achieved

COSO published *Enterprise Risk Management—Integrated Framework* in 2004. The purpose of that publication was to help entities better protect and enhance stakeholder value. Its underlying philosophy was that "value is maximized when management sets strategy and objectives to strike an optimal balance between growth and return goals and related risks, and efficiently and effectively deploys resources in pursuit of the entity's objectives."[3]

[3] *Enterprise Risk Management—Integrated Framework*, Executive Summary, COSO (2004).

Since its publication, the *Framework* has been used successfully around the world, across industries, and in organizations of all types and sizes to identify risks, manage those risks within a defined risk appetite, and support the achievement of objectives. Yet, while many have applied the *Framework* in practice, it has the potential to be used more extensively. It would benefit from examining certain aspects with more depth and clarity, and by providing greater insight into the links between strategy, risk, and performance. In response, therefore, the updated Framework in this publication:

- More clearly connects enterprise risk management with a multitude of stakeholder expectations.
- Positions risk in the context of an organization's performance, rather than as the subject of an isolated exercise.
- Enables organizations to better anticipate risk so they can get ahead of it, with an understanding that change creates opportunities, not simply the potential for crises.

This update also answers the call for a stronger emphasis on how enterprise risk management informs strategy and its performance.

Benefits of Effective Enterprise Risk Management

All organizations need to set strategy and periodically adjust it, always staying aware of both ever-changing opportunities for creating value and the challenges that will occur in pursuit of that value. To do that, they need the best possible framework for optimizing strategy and performance.

That's where enterprise risk management comes into play. Organizations that integrate enterprise risk management throughout the entity can realize many benefits, including, though not limited to:

- *Increasing the range of opportunities:* By considering all possibilities—both positive and negative aspects of risk—management can identify new opportunities and unique challenges associated with current opportunities.
- *Identifying and managing risk entity-wide:* Every entity faces myriad risks that can affect many parts of the organization. Sometimes a risk can originate in one part of the entity but impact a different part. Consequently, management identifies and manages these entity-wide risks to sustain and improve performance.
- *Increasing positive outcomes and advantage while reducing negative surprises:* Enterprise risk management allows entities to improve their ability to identify risks and establish appropriate responses, reducing surprises and related costs or losses, while profiting from advantageous developments.

Clearing up a few misconceptions

We've heard a few misconceptions about the original *Framework* since it was introduced in 2004. To set the record straight:

Enterprise risk management is not a function or department. It is the culture, capabilities, and practices that organizations integrate with strategy-setting and apply when they carry out that strategy, with a purpose of managing risk in creating, preserving, and realizing value.

Enterprise risk management is more than a risk listing. It requires more than taking an inventory of all the risks within the organization. It is broader and includes practices that management puts in place to actively manage risk.

Enterprise risk management addresses more than internal control. It also addresses other topics such as strategy-setting, governance, communicating with stakeholders, and measuring performance. Its principles apply at all levels of the organization and across all functions.

Enterprise risk management is not a checklist. It is a set of principles on which processes can be built or integrated for a particular organization, and it is a system of monitoring, learning, and improving performance.

Enterprise risk management can be used by organizations of any size. If an organization has a mission, a strategy, and objectives—and the need to make decisions that fully consider risk—then enterprise risk management can be applied. It can and should be used by all kinds of organizations, from small businesses to community-based social enterprises to government agencies to Fortune 500 companies.

- *Reducing performance variability:* For some, the challenge is less with surprises and losses and more with variability in performance. Performing ahead of schedule or beyond expectations may cause as much concern as performing short of scheduling and expectations. Enterprise risk management allows organizations to anticipate the risks that would affect performance and enable them to put in place the actions needed to minimize disruption and maximize opportunity.
- *Improving resource deployment:* Every risk could be considered a request for resources. Obtaining robust information on risk allows management, in the face of finite resources, to assess overall resource needs, prioritize resource deployment and enhance resource allocation.
- *Enhancing enterprise resilience:* An entity's medium- and long-term viability depends on its ability to anticipate and respond to change, not only to survive but also to evolve and thrive. This is, in part, enabled by effective enterprise risk management. It becomes increasingly important as the pace of change accelerates and business complexity increases.

These benefits highlight the fact that risk should not be viewed solely as a potential constraint or challenge to setting and carrying out a strategy. Rather, the change that underlies risk and the organizational responses to risk give rise to strategic opportunities and key differentiating capabilities.

The Role of Risk in Strategy Selection

Strategy selection is about making choices and accepting trade-offs. So it makes sense to apply enterprise risk management to strategy as that is the best approach for untangling the art and science of making well-informed choices.

Risk is a consideration in many strategy-setting processes. But risk is often evaluated primarily in relation to its potential effect on an already-determined strategy. In other words, the discussions focus on risks to the existing strategy: We have a strategy in place, what could affect the relevance and viability of our strategy?

But there are other questions to ask about strategy, which organizations are getting better at asking: Have we modeled customer demand accurately? Will our supply chain deliver on time and on budget? Will new competitors emerge? Is our technology infrastructure up to the task? These are the kinds of questions that executives grapple with every day, and responding to them is fundamental to carrying out a strategy.

However, the risk to the chosen strategy is only one aspect to consider. As this Framework emphasizes, there are two additional aspects to enterprise risk management that can have far greater effect on an entity's value: the possibility of the strategy not aligning, and the implications from the strategy chosen.

The first of these, **the possibility of the strategy not aligning with an organization's mission, vision, and core values**, is central to decisions that underlie strategy selection. Every entity has a mission, vision, and core values that define what it is trying to achieve and how it wants to conduct business. Some organizations are skeptical about truly embracing their corporate credos. But mission, vision, and core values have been demonstrated to matter—and they matter most when it comes to managing risk and remaining resilient during periods of change.

A chosen strategy must support the organization's mission and vision. A misaligned strategy increases the possibility that the organization may not realize its mission and vision, or may compromise its values, even if a strategy is successfully carried out. Therefore, enterprise risk management considers the possibility of strategy not aligning with the mission and vision of the organization.

The other additional aspect is **the implications from the strategy chosen**. When management develops a strategy and works through alternatives with the board, they make decisions on the trade-offs inherent in the strategy. Each alternative strategy has its own risk profile—these are the implications arising from the strategy. The board of directors and management need to determine if the strategy works in tandem with the organization's risk appetite, and how it will help drive the organization to set objectives and ultimately allocate resources efficiently.

Here's what's important: Enterprise risk management is as much about understanding the *implications from the strategy and the possibility of strategy not aligning* as it is about managing risks to set objectives. The figure below illustrates these considerations in the context of mission, vision, core values, and as a driver of an entity's overall direction and performance.

Enterprise risk management, as it has typically been practiced, has helped many organizations identify, assess, and manage risks to the strategy. But the most significant causes of value destruction are embedded in the possibility of the strategy not supporting the entity's mission and vision, and the implications from the strategy.

Enterprise risk management enhances strategy selection. Choosing a strategy calls for structured decision-making that analyzes risk and aligns resources with the mission and vision of the organization.

A Focused Framework

Enterprise Risk Management—Integrating with Strategy and Performance clarifies the importance of enterprise risk management in strategic planning and embedding it throughout an organization—because risk influences and aligns strategy and performance across all departments and functions.

The Framework itself is a set of principles organized into five interrelated components:

1. **Governance and Culture**: Governance sets the organization's tone, reinforcing the importance of, and establishing oversight responsibilities for, enterprise risk management. Culture pertains to ethical values, desired behaviors, and understanding of risk in the entity.
2. **Strategy and Objective-Setting**: Enterprise risk management, strategy, and objective-setting work together in the strategic-planning process. A risk appetite is established and aligned with strategy; business objectives put strategy into practice while serving as a basis for identifying, assessing, and responding to risk.
3. **Performance**: Risks that may impact the achievement of strategy and business objectives need to be identified and assessed. Risks are prioritized by severity in the context of risk appetite. The organization then selects risk responses and takes a portfolio view of the amount of risk it has assumed. The results of this process are reported to key risk stakeholders.
4. **Review and Revision**: By reviewing entity performance, an organization can consider how well the enterprise risk management components are functioning over time and in light of substantial changes, and what revisions are needed.
5. **Information, Communication, and Reporting**: Enterprise risk management requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organization.

The five components in the updated Framework are supported by a set of principles.[4] These principles cover everything from governance to monitoring. They're manageable in size, and they describe practices that can be applied in different ways for different organizations regardless of size, type, or sector. Adhering to these principles can provide management and the board with a reasonable expectation that the organization understands and strives to manage the risks associated with its strategy and business objectives.

Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues Improvement in Enterprise Risk Management

Information, Communication, & Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

Looking into the Future

There is no doubt that organizations will continue to face a future full of volatility, complexity, and ambiguity. Enterprise risk management will be an important part of how an organization manages and prospers through these times. Regardless of the type and size of an entity, strategies need to stay true to their mission. And all entities need to exhibit traits that drive an effective response to change, including agile decision-making, the ability to respond in a cohesive manner, and the adaptive capacity to pivot and reposition while maintaining high levels of trust among stakeholders.

As we look into the future, there are several trends that will have an effect on enterprise risk management. Just four of these are:

- *Dealing with the proliferation of data:* As more and more data becomes available and the speed at which new data can be analyzed increases, enterprise risk management will need to adapt. The data will come from both inside and outside the entity, and it will be structured in new ways. Advanced analytics and data visualization tools will evolve and be very helpful in understanding risk and its impact—both positive and negative.
- *Leveraging artificial intelligence and automation:* Many people feel that we have entered the era of automated processes and artificial intelligence. Regardless of individual beliefs, it is important for enterprise risk management practices to consider the impact of these and future technologies, and leverage their capabilities. Previously unrecognizable relationships, trends and patterns can be uncovered, providing a rich source of information critical to managing risk.
- *Managing the cost of risk management:* A frequent concern expressed by many business executives is the cost of risk management, compliance processes, and control activities in comparison to the value gained. As enterprise risk management practices evolve, it will become important that activities spanning risk, compliance, control, and even governance be efficiently coordinated to provide maximum benefit to the organization. This may represent one of the best opportunities for enterprise risk management to redefine its importance to the organization.

[4] A fuller description of these twenty principles is provided at the end of this document.

- *Building stronger organizations:* As organizations become better at integrating enterprise risk management with strategy and performance, an opportunity to strengthen resilience will present itself. By knowing the risks that will have the greatest impact on the entity, organizations can use enterprise risk management to help put in place capabilities that allow them to act early. This will open up new opportunities.

In summary, enterprise risk management will need to change and adapt to the future to consistently provide the benefits outlined in the Framework. With the right focus, the benefits derived from enterprise risk management will far outweigh the investments and provide organizations with confidence in their ability to handle the future.

Acknowledgments

A special thank you to the following companies and organizations for allowing the participation of Advisory Council Members and Observers.

Advisory Council Members

Companies and Organizations

- Athene USA (Jane Karli)
- Edison International (David J. Heller)
- First Data Corporation (Lee Marks)
- Georgia-Pacific LLC (Paul Sobel)
- Invesco Ltd. (Suzanne Christensen)
- Microsoft (Jeff Pratt)
- US Department of Commerce (Karen Hardy)
- United Technologies Corporation (Margaret Boissoneau)
- Zurich Insurance Company (James Davenport)

Higher Education and Associations

- North Carolina State University (Mark Beasley)
- St. John's University (Paul Walker)
- The Institute of Internal Auditors (Douglas J. Anderson)

Professional Service Firms

- Crowe Horwath LLP (William Watts)
- Deloitte & Touche LLP (Henry Ristuccia)
- Ernst & Young (Anthony J. Carmello)
- James Lam & Associates (James Lam)
- Grant Thornton LLP (Bailey Jordan)
- KPMG LLP Americas (Deon Minnaar)
- Mercury Business Advisors Inc. (Patrick Stroh)
- Protiviti Inc. (James DeLoach)

Former COSO Board Member

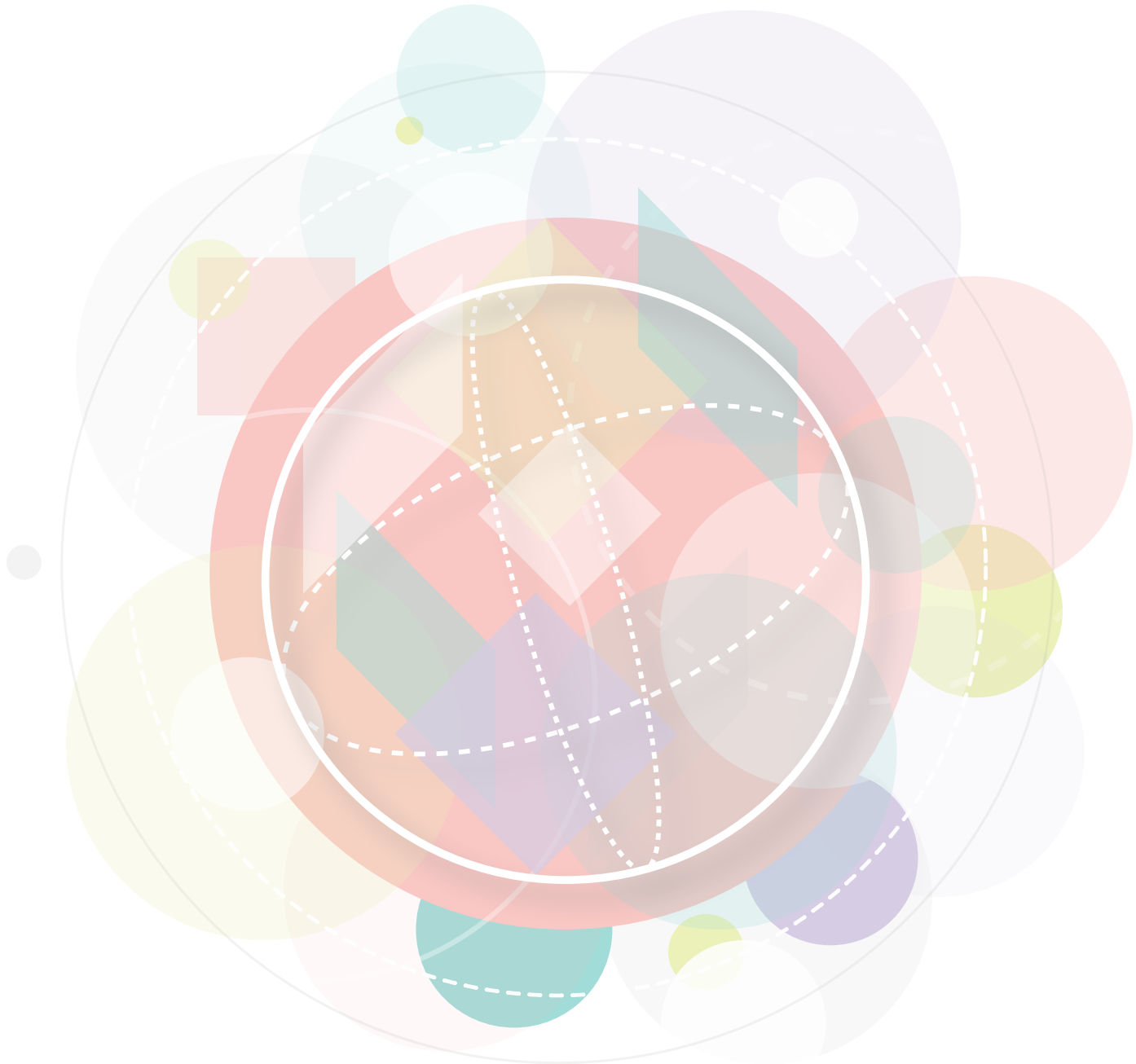
- COSO Chair, 2009–2013 (David Landsittel)

Observers

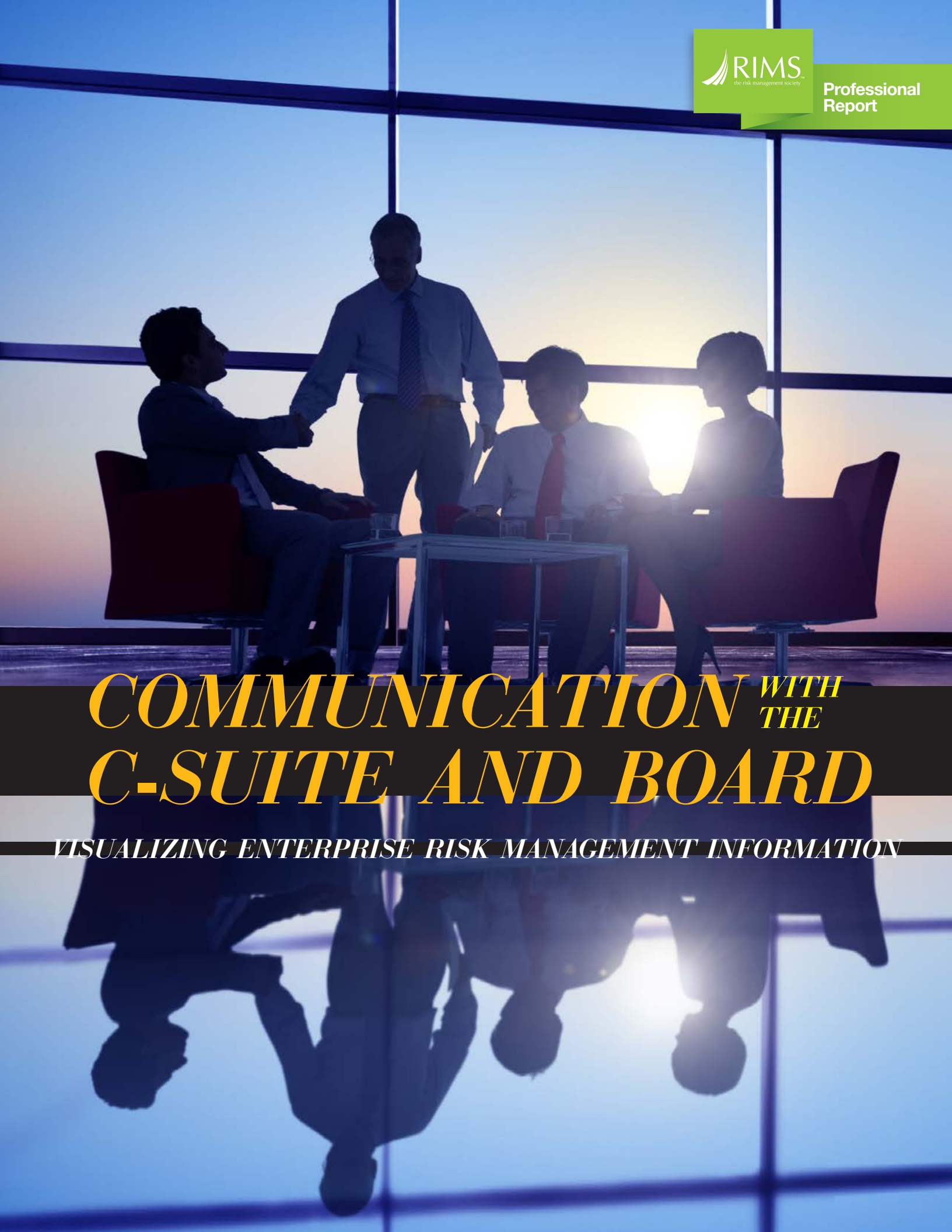
- Federal Deposit Insurance Corporation (Harrison Greene)
- Government Accountability Office (James Dalkin)
- Institute of Management Accountants (Jeff Thompson)
- Institut der Wirtschaftsprüfer (Horst Kreisel)
- International Federation of Accountants (Vincent Tophoff)
- ISACA (Jennifer Bayuk)
- Risk Management Society (Carol Fox)

Components and Principles

1. **Exercises Board Risk Oversight**—The board of directors provides oversight of the strategy and carries out governance responsibilities to support management in achieving strategy and business objectives.
2. **Establishes Operating Structures**—The organization establishes operating structures in the pursuit of strategy and business objectives.
3. **Defines Desired Culture**—The organization defines the desired behaviors that characterize the entity's desired culture.
4. **Demonstrates Commitment to Core Values**—The organization demonstrates a commitment to the entity's core values.
5. **Attracts, Develops, and Retains Capable Individuals**—The organization is committed to building human capital in alignment with the strategy and business objectives.
6. **Analyzes Business Context**—The organization considers potential effects of business context on risk profile.
7. **Defines Risk Appetite**—The organization defines risk appetite in the context of creating, preserving, and realizing value.
8. **Evaluates Alternative Strategies**—The organization evaluates alternative strategies and potential impact on risk profile.
9. **Formulates Business Objectives**—The organization considers risk while establishing the business objectives at various levels that align and support strategy.
10. **Identifies Risk**—The organization identifies risk that impacts the performance of strategy and business objectives.
11. **Assesses Severity of Risk**—The organization assesses the severity of risk.
12. **Prioritizes Risks**—The organization prioritizes risks as a basis for selecting responses to risks.
13. **Implements Risk Responses**—The organization identifies and selects risk responses.
14. **Develops Portfolio View**—The organization develops and evaluates a portfolio view of risk.
15. **Assesses Substantial Change**—The organization identifies and assesses changes that may substantially affect strategy and business objectives.
16. **Reviews Risk and Performance**—The organization reviews entity performance and considers risk.
17. **Pursues Improvement in Enterprise Risk Management**—The organization pursues improvement of enterprise risk management.
18. **Leverages Information Systems**—The organization leverages the entity's information and technology systems to support enterprise risk management.
19. **Communicates Risk Information**—The organization uses communication channels to support enterprise risk management.
20. **Reports on Risk, Culture, and Performance**—The organization reports on risk, culture, and performance at multiple levels and across the entity.



A full version of *Enterprise Risk Management—Integrating with Strategy and Performance* can be purchased by visiting the www.coso.org website.



RIMS the risk management society

Professional Report

COMMUNICATION WITH THE C-SUITE AND BOARD

VISUALIZING ENTERPRISE RISK MANAGEMENT INFORMATION

COMMUNICATION WITH THE C-SUITE AND BOARD

VISUALIZING ENTERPRISE RISK MANAGEMENT INFORMATION

AUTHORS

David J. Young
Lecturer, Risk Management and Insurance (RMI) Program,
University of Colorado Denver, Business School

Christine Novotny, ARM, RIMS-CRMP
Manager, Risk and Insurance, PeaceHealth

Julie Cain
Senior Strategic Advisor, Information and Technology
Risk Management, Educational Testing Service

EDITOR

Justin Smulison
RIMS

ART DIRECTOR

Joe Zwielich
RIMS

RIMS
the risk management society™

As the preeminent organization dedicated to educating, engaging and advocating for the global risk community, RIMS, *the* risk management society™, is a not-for-profit organization representing more than 3,500 corporate, industrial, service, nonprofit, charitable and government entities throughout the world. RIMS has a membership of approximately 10,000 risk practitioners who are located in more than 60 countries. For more information about the Society's world-leading risk management content, networking, professional development and certification opportunities, visit www.RIMS.org.

INTRODUCTION

In 2014, the National Association of Corporate Directors (NACD) and Oliver Wyman produced *Risk Communication – Aligning the Board and C-Suite*, a seminal document which noted: "Without robust information about risk, directors cannot offer effective oversight. Therefore, management should carefully evaluate the format and purpose of board risk communication with consideration to risk governance responsibilities, risk appetite, and the intersection between risk and strategy. This process also ensures that the risk information is of value to the management team as well and not simply 'paperwork.'"

Indeed, with increasing global uncertainty and accelerating pace of change impacting business on many levels, expectations for improved risk management and information reporting have significantly increased since that paper was published. Stakeholder pressures, regulatory requirements, credit rating agency calculations, massive increases in cyberrisk and disclosure requirements, and the threat of reputation damage has moved enterprise risk management (ERM) to the front of the conversation regarding risk and its impact on organizational performance.

Accordingly, board reporting needs to focus on the key risk portfolio—the aggregate view of all the key enterprise risks. The key risk portfolio allows the board to consider the overall view of risk the company is facing relative to the its strategy, operational goals and objectives. That is where ERM comes into play.

Since the 2014 Oliver Wyman paper, many influential reports have emphasized the growing importance of ERM, the value an ERM program brings to an organization and the growing regulatory and business pressures requiring the adoption of such a program. This paper will build on those concepts by identifying one of the biggest challenges in the ERM space—determining what information risk managers should present to decision-makers and how that information should best be communicated.

EXAMINING THE NEED FOR INFORMATION

Boards have expressed the need for specific information in order for them to be proactive, underscoring the need for an effective ERM program. According to the National Association of Corporate Directors' *2017–2018 NACD Public Company Governance Survey*, "Directors themselves admit that they need to do a better job in contributing to strategy. Seventy-one percent of directors indicate that their boards must better understand the risks and opportunities that affect performance and drive strategic choices over the next 12 months." It also noted that "fewer boards also hear directly from specialist functions, such as internal audit (39%), compliance and ethics (30%), and enterprise risk management (20%), which possess a much deeper and perhaps more independent perspective on the strength of the corporate culture than the CEO does."

COSO's newly updated 2017 framework, *Enterprise Risk Management–Integrating with Strategy and Performance*, also recognizes leadership's role in ERM. The framework recognizes "tone from the top" as the single most important cultural aspect of a successful program. Organizational leaders are seeking to be more engaged and informed. They want improved transparency and better accountability of enhanced risk reporting for managing key material risks, whether to minimize downside risk or exploit upside risk. As COSO noted, ERM will continue to change and adapt to today's rapidly evolving risk environment. The benefits derived from the right focus will produce a strong return on investment and ability to capitalize on risk.

In addition to the new COSO framework, the International Organization for Standardization recently released ISO 31000:2018, *Risk Management–Guidelines*, another widely used standard for ERM, which provides a more simplified framework focused on the principles and processes for managing risk. Used by organizations regardless of its size, activity or sector, it also stresses the importance of leadership by top management and the integration of risk management to include the streamlining of information content with greater focus on sustaining an open systems model to fit the multiple needs and contexts of different organizations.

ERM'S EVOLUTIONARY STAGES

Based on the volume of suggested reportable ERM information to the C-suite and board of directors as compared to an organization's current information reporting practices, an evolutionary path has emerged with respect to the state of ERM within an organization. This evolution can often serve as a guide to how ERM information can best be communicated throughout the organization. The path can be broken down into three categories:

- Emerging: Emerging organizations may only be armed with a risk register and a desire to implement an ERM program with adequate executive reporting. While it can be difficult for them to demonstrate the return on investment (ROI) of implementing a working program, they recognize that there are many downsides to not acting on this initiative, from financial to operational.
- Evolving: In these organizations, an ERM program has been implemented and is in the process of continuous improvement.
- Exploiting: An organization with a fully implemented and monitored ERM program is delivering significant value to the organization and allowing it to exploit risk to the benefit of all stakeholders. Executive leadership is keenly aware of both upside and downside risks facing the organization and adjusts strategy to mitigate key risks and avoid the negative ramifications.

WHO SHOULD RECEIVE RISK INFORMATION?

Before developing a risk report, it is helpful to identify and prioritize who should receive the information and how it should be presented. Models and methods will vary from company to company, but examples include:

- Board Risk Committee: As an emerging best practice, boards of directors are now forming board risk committees at an increased rate. As with other board committees, the risk committee should have its own charter that allows it to operate as a strategic asset and defines its responsibilities and authority. In lieu of a board risk committee, at a minimum, an organization should have an internal risk executive committee that regularly reports to the board.
- Internal ERM Engagement Model by Risk Category: Using an organizationally specific risk categorization system, an ERM Engagement Model specifically outlines senior leadership responsibility for enterprise risk and better defines accountability for these risk categories.

Sample ERM Engagement Model

	Board of Directors							
	Senior Leadership Team							
Risk Pillar Owners	*Strategic*		*Operations*		*Financial*		*Hazard*	
	CEO		COO		CFO		General Counsel	Chief Risk Officer
Leadership Community	Chief Marketing Officer	Corporate Strategy & Planning	Operations Group	CIO	Chief Accounting Officer	Treasurer	Deputy General Counsel	Director, Risk Management
	Technology & Research	Chief Economist	Sales & Marketing	CISO	Tax	FP&A	Contracts & Litigation	Risk Management Department
External Partners	Marketing Firms	Consulting Firms	Marketing & Communications Firms	Cybersecurity	Accounting Firm	Financial Advisors	Outsider Counsel	Insurance Brokers
	Other Vendors	Other Vendors	Regulatory Advisors	Other IT Vendors	Audit Firm	Banking Partners	Legal Vendors	Other Vendors

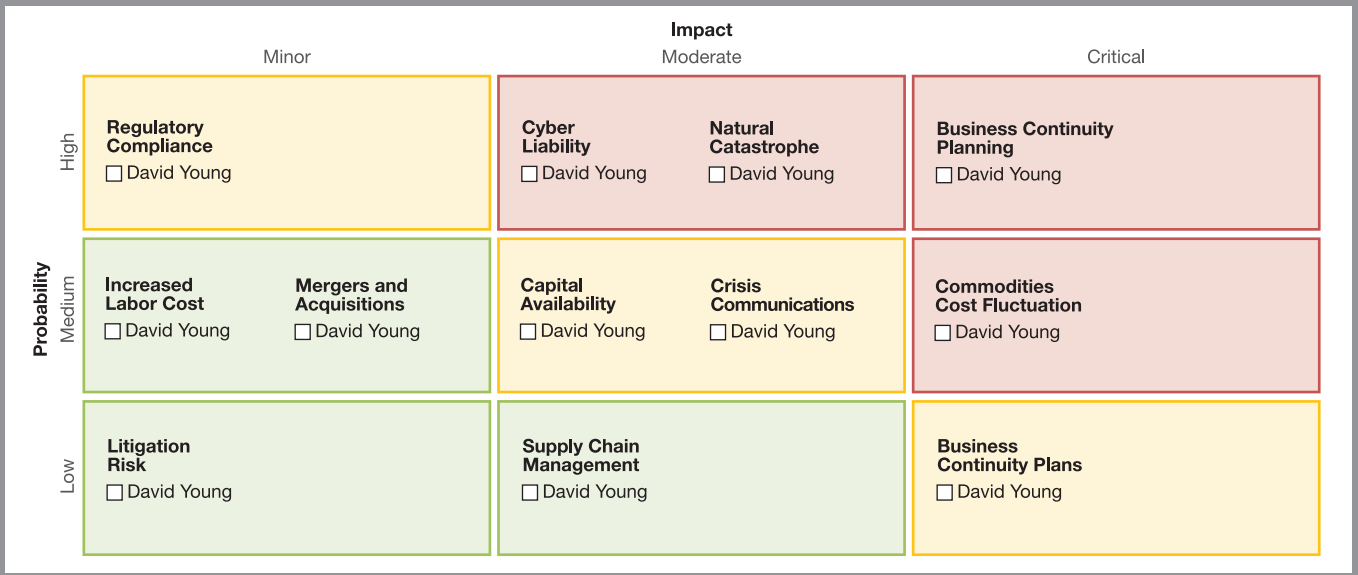
• Key Risk Accountability Matrix by Risk Owner: Building on the Engagement Model, a key risk accountability matrix will allow an organization to track key risks. Organized around critical risks, it helps ensure accountability within an organization for risk ownership.

Sample Key Risk Accountability Matrix

Risk Quadrant	Risk Category	Risk Title	Board	Senior Risk Owner	Additional Risk Owner(s)
High Probability / High Impact	Strategic	Business Model	Full	CEO	Chief Marketing Officer
	Hazard	Political Risk	AC	CRO	Deputy GC
	Operations	Cybersecurity	AC	CIO	CISO
		Recruitment & Retention	Comp	Chief People Officer	HR Director
		Business Continuity	AC	COO	CIO
		Data Privacy	RPP	COO	Chief Privacy Officer
High Probability / Moderate Impact	Strategic	Strategic Investments	Full	CFO	SVP, Business Development
	Hazard	Catastrophic Event	AC	CRO	Director, Risk Management
		M&A Risk/Acquisitions & Divestitures	AC	CFO/CRO	Deputy GC
	Operations	International Operations	AC	COO	VP, International Operations
		Supply Chain	RPP	COO	VP, Supply Chain
		Data Management	AC	COO	CIO
		Customer Relationships	AC	COO	GM, Customer Service & Support
		Regulatory Complexity & Uncertainty	RPP	General Counsel	GC
		Facility Access and Security	AC	CFO	GM, Security
		Operational Infrastructure	Full	CEO	CIO
	Financial	Interest Rate Changes	AC	CFO	Treasurer
		Tax Strategy & Optimization	AC	CFO	Tax
		Currency Fluctuations	AC	CFO	Treasurer
		Credit & Collections	AC	CFO	Treasurer

• Heat Map of Key Risks: The risk heat map continues to be a useful tool for quickly understanding what the key risks are and what value at risk is in the aggregate. Heat maps have come a long way in the last few years and can include the ability to drill down into risk ownership and risk mitigation plans.

Heat Map of Key Risks



• Risk Register with Mitigation Plans by Risk Owner: Most organizations practicing any form of risk management currently use a risk register, which is usually a more exhaustive list of risks, usually in an Excel format. While executive reporting is typically limited to key risks given the time constraints of the C-suite and board of directors, such a list will usually be maintained. Examples of risk registers are extremely varied but need to serve the organization's needs.

DELIVERING KEY RISK MANAGEMENT INFORMATION

The next step is to determine what information needs to be included in a board risk report. In developing a system for delivering key risk information to the board, it must be stated that ERM is not a prescribed science. No two organizations will have the same approach or process for determining what defines key risk information or how it should be delivered.

While not a definitive guideline, suggested key ERM information can be categorized as follows:

- Business context statement: High-level snapshot of the coverage of the report, including part(s) of the organization, timeframes, perhaps brief restatement of top business priorities/key strategic objectives, summary of material business changes such as significant global/industry indicators, major mergers, acquisitions and divestitures activity, big wins or heavy losses, and top leadership changes as relevant to the organization. This focuses the audience and frames the enterprise risk information in business context.
- Risk appetite statement: A clear, written risk appetite statement is essential to any ERM strategy. A responsibility of senior management and the board, this statement definitively states the organization's risk appetite in terms of acceptable and unacceptable risk to organizational strategy and objectives, especially with respect to outside stakeholders. A risk appetite statement should communicate the "tone from the top" and facilitate risk communication and understanding throughout the organization.
- Risk tolerance calculation: The risk tolerance calculation is a determined or calculated amount of risk, expressed financially, that the organization is willing to take on in pursuit of business objectives. It should define both the amount of acceptable risk the organization wants to take on, as well as the upper limit of downside risk it can afford without material financial impact.
- Emerging risk review: Emerging risks may be one of the most difficult of information requirements—an understanding of technological disruption, the velocity of change in certain risks and global trends all need to be considered. The most discussed example in the boardroom of emerging risks is the threat posed by cybersecurity. Any relevant information that can be provided to the C-suite and board of directors should be considered for inclusion in reporting.

ADDITIONAL SOURCES OF KEY RISK MANAGEMENT INFORMATION

In addition to the suggested ERM program information, there are numerous other sources of information that can help develop a risk picture. They can provide insights as to whether management's assumptions about markets, customers, competition, technology, regulations, commodity prices and other external factors remain valid, which could alter the fundamentals underlying the business strategy. A few examples include:

- Job review websites: Perceptions to be gained from employees speaking honestly about their company should not be taken for granted. Employment sites like Glassdoor provide critical information regarding employee sentiment and insider views of the organization.
- Internet/social media sentiment: There are many internet applications to track sentiment regarding an organization or its key members. This function can be automated and allow for real-time feedback regarding what is being said.
- CSR reporting: With the growth of corporate social responsibility (CSR), this is also becoming good information to filter to the highest levels of the organization. Since CSR is becoming a leading indicator of corporate performance, like ERM, it may be the type of information senior management regularly wants.
- Dark web monitoring: One of the most valuable applications of dark web monitoring is identification of compromised assets and information.
- Employee opinion/customer satisfaction surveys: Used by many companies as quality metrics to measure and monitor the effectiveness of the services provided. For example, healthcare systems rely on the Hospital Consumer Assessment

of Healthcare Providers and Systems (HCAHPS) score survey, an instrument and data collection methodology for measuring patients' perceptions of their hospital experience. Results influence Medicare/Medicaid reimbursement.

- Legal actions: Significant legal actions such as pending D&O lawsuits, employment practice disputes, liabilities claims, and FCPA and OFAC violations can be important sources of information to guide future practices.
- Regulations: Emerging regulatory risk that may potentially impact the company.
- Calls to a whistleblower hotline: This feedback can indicate potential legal action, loss event and reputation impact.
- Data analytics: Analytics can surface indicators of anomalous activities in the environment, such as fraud.
- Emergency notification systems: Natural disaster early warning systems can provide valuable information.
- Total cost of risk: The total cost of risk is the sum of major components that are individually measured and quantified including: 1) risk financing costs (items that impact the transfer of risk including insurance premiums, self-insurance funds to captives/trusts, broker commissions, bonds, letters of credit); 2) loss costs (claim costs, deductibles/self-insured retention, attorney fees, uninsured losses); 3) administrative costs (third-party administrator fees, broker fees, risk control services, risk department payroll and material/service budgets, consultants and attorneys); and 4) taxes and fees (surplus lines taxes and fees).
- Claim scorecards: Claim scorecards measure the year-over-year performance of loss control activities by developing an internal matrix specific for your industry. These internal key performance indicators can help identify the strengths and weakness in your programs, help you understand, analyze, track and measure process improvements that reduce the frequency and severity of claims, maximize ROI and increase organizational profitability. Examples of KPIs tracked include cost of workers compensation claims as a percentage of payroll; number of claims per 100 full-time employees; number of vehicle claims per mile driven; average cost of claim; and experience modification rate.
- Benchmarking reports: Brokers and industry groups such as RIMS, Advisen and the American Society for Healthcare Risk Management (ASHRM) publish annual reports that benchmark claims information and the total costs of risk among peer groups.

CONCLUSION

Determining an ERM program's return on investment is difficult. However, research from the Corporate Executive Board shows that strategic or operational risks often cause the biggest declines in shareholder value. According to its 2015 study, *How to Live with Risks*, strategic risks have comprised 86% of the significant losses in organizations' market value in the past decade, with operating, legal and financial reporting making up the difference. However, auditors only spend 6% of their time investigating the strategic initiatives that supposedly hemorrhage funds, and a combined 80% on operations and financial reporting. These findings have prompted more organizations to reexamine their focus on enterprise risks.

The old ways of transferring risk through the purchase of insurance and calling it "risk management" no longer suffices for any organization. Key risk information must be communicated to the highest levels to help the organization reach its objectives. Where once ERM was a supporting function for the board, executives are now charged with the oversight of these programs and are increasingly aware of the consequences of not integrating the ERM process into their organizations' missions.

ERM will continue to evolve, both as a discipline and within organizations to help better manage the volatility of existing and emerging risks. As a result, ensuring that the most effective methods are used to inform senior management of critical ERM information is the surest path to organizational success, stability and resiliency.

RIMS™
the risk management society

1407 Broadway, 29th Floor
New York, NY 10018

www.RIMS.org