

THE ERM JOURNEY

White Paper Series

St. John's University
Tobin College of Business
Center for Excellence in ERM

NOVEMBER 2018

THE ERM JOURNEY

ALTHOUGH ERM HAS GROWN SUBSTANTIALLY AND NUMEROUS COUNTRIES HAVE ADOPTED SOME VERSIONS OF EITHER ERM OR BOARD RISK OVERSIGHT REQUIREMENTS, ERM SEEMS TO BE AT A CRITICAL MOMENT FOR MANY COMPANIES.



Will ERM step it up and consistently get linked to performance and value? Both of the major ERM Frameworks (COSO and ISO) were recently updated and provide an opportunity to make those steps. But first, companies need to understand their current practices, successes, value, and challenges. From there, they can begin to move forward on their journey.

As part of the ERM Summit at the Center for Excellence in ERM at St. John's University, we explored several organizations' ERM journeys and how they built and sustain ERM. Additionally, we surveyed the participants in order to dig deeper into these companies' journeys to try to understand the connection between higher performing companies and ERM. The ERM companies at the Summit were in various places in their journey, but all were experienced in the game as evidenced by the 74% that said they had an ERM process for longer than three years and the 36% that said they had a process for longer than seven years.

Of course, managing risks is not getting any easier because risks are not shrinking away. A large majority (87%) believed their organizations' risks were growing (Figure 1). Furthermore, many of the risks facing organizations are not easy to identify or assess and can be related to large losses in value. For example, Figure 2 shows that although over half of organizations' risk are operational, 27% are strategic, and 8% are emerging risks. Up until 2017's COSO ERM Framework refresh, there has not been a lot of guidance on strategic risks.

There are many reasons to build ERM other than just a growing set of risks. There is a growing body of empirical evidence showing that ERM is associated with higher short-term and long-term value metrics and some other research that shows that ERM leads to better decisions. However, regulatory and other pressures came up at the Summit as the top reason/driver of an ERM program. Specifically, Figure 3 shows that over half of organizations state that regulatory pressures and board requests are the primary drivers of ERM. Interestingly, almost half also state that ERM is driven by some incident or event—perhaps one that got the attention of the right people and put pressure on ERM to fix things (whether that's possible or not). As is clear, ERM can't solve all of a company's problems, but the prior Chair of COSO, Bob Hirth, was known to say quite frequently that ERM can help you "meet more of

ALMOST HALF ALSO STATE THAT ERM IS DRIVEN BY SOME INCIDENT OR EVENT—PERHAPS ONE THAT GOT THE ATTENTION OF THE RIGHT PEOPLE AND PUT PRESSURE ON ERM TO FIX THINGS.

your objectives more of the time." The high percentage of incidents and events as drivers just might suggest that quite a few folks agree with him. Other top drivers of ERM included C-level pressure, competition, and culture problems. This could be one of the first times that companies noted culture incidents as driving ERM. Both of the new ERM frameworks by ISO and COSO have linked ERM to culture more than their prior frameworks. For example, COSO's 2017 ERM Framework mentions culture over 130 times and has two ERM principles that focus on culture.

BUILDING THE COMMITMENT AND ERM INFRASTRUCTURE

The prior section noted that risks are growing, that companies are categorizing risks, and that companies know the drivers of their risks. This section explores the ERM infrastructure and other ERM aspects that companies have built. Additionally, the companies were asked to judge their own performance. Using this data, we can highlight and get a sense of the difference between ERM at high-performing organizations vs non high-performers. Although it is always wise to be cautious about causation of the performance gaps, the results and data split are still interesting.

For example, Table 1 shows that 54% of non high-performer responding companies believe they have the necessary ERM infrastructure but that 70% of high-performers believe the same. Stated differently, high performers are more likely to have their ERM infrastructure set up. The lesson: build your ERM program and get the right aspects in place. Furthermore, Table 2 shows another performance difference. Although most companies integrate ERM with compliance and audit, high-performers have much higher percentages of integration with strategy, operations, and finance. Another key performance lesson: where possible, try to integrate ERM into these other areas.

Figure 4 reveals other performance differences. For example, high-performers appear more likely than non high-performers to have an emerging risk process and they appear more likely to have a process that holds management accountable for the risks. The 2017 COSO ERM Framework makes a big push for linking ERM to performance and this data appears to support the value-added link.

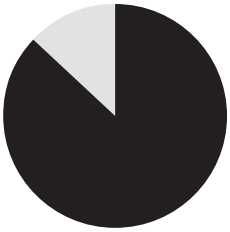


FIGURE 1
RISKS ARE GROWING
The risks facing our organization are growing significantly.
STRONGLY AGREE
OTHER

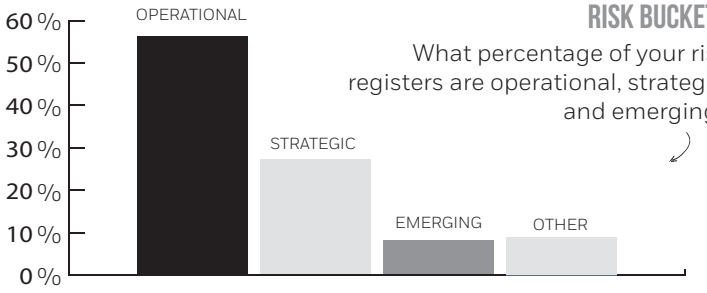


FIGURE 2
RISK BUCKETS
What percentage of your risk registers are operational, strategic, and emerging?

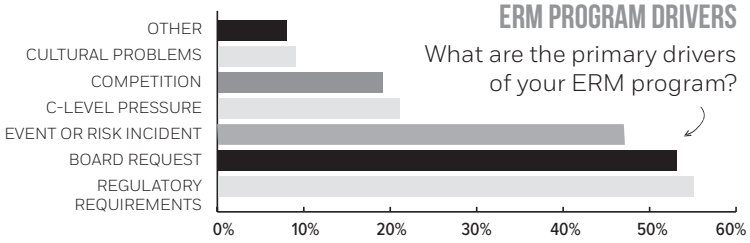


FIGURE 3
ERM PROGRAM DRIVERS
What are the primary drivers of your ERM program?

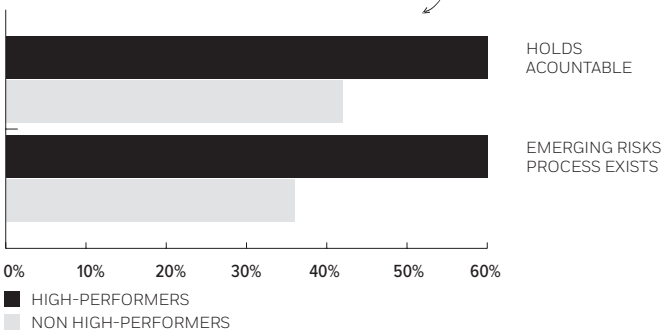
TABLE 1: NECESSARY ERM INFRASTRUCTURE

We have the necessary infrastructure to support the ERM process.	54% % of the non high-performers sample that agree	70% % of the high-performers sample that agree

TABLE 2: INTEGRATION & PERFORMANCE

Where is ERM Integrated?	IA	COMP	STRATEGY	OPR	FIN
HIGH PERFORMERS	85%	70%	80%	65%	65%
NON HIGH PERFORMERS	92%	81%	58%	54%	50%

FIGURE 4
INFRASTRUCTURE & PERFORMANCE GAPS





ERM VALUE INSIGHTS

Despite the performance differences there were many companies that had built serious ERM infrastructure and, as the following data shows, this makes a difference in other ways. Figure 5 reveals that 65% believe their ERM program is effective and Figure 6 reveals that 63% also believe they are adding value. Figure 6 further reveals additional insights into the value added. For example, 54% believe that they added value because they helped their organization identify previously unknown risks and 76% stated they believed they added value by helping their organizations understand the real risks. Identifying these unknowns or perhaps moving unknown unknowns into the known realm has been discussed by many. Risks are difficult to manage unless they can be seen so this performance gap is not too surprising. One view of this data is that there is still a lot of work to be done and value to be gained by simply identifying the risks and helping management to understand those risks.

ERM ASSESSMENT AND SATISFACTION

Many organizations also have their ERM process assessed or judged. For example, Figure 7 shows that 61% of organizations assess or benchmark their ERM process to ensure its effectiveness and that 65% have their management and board evaluate their ERM process. Overall, 72% of ERM organizations believe that their leaders are satisfied with their process.

To highlight some of their success stories the respondents were asked to share their "best wins" in ERM. Table 3 lists most of the comments. There are several comments about the infrastructure but there are also comments about resource gains, opportunities, training, and culture. Numerous respondents also commented on the changes in the mindsets and thoughts with comments about "aha moments," building relationships, and being asked for help. These types of wins are not necessarily written down in ERM frameworks but they are listed in the comments as "best wins" as often as the infrastructure. This is a great reminder to ERM leaders that more is needed than just building the components of ERM. As one ERM leader recently stated, "You've got to get out of your office for ERM to be successful."

CULTURE

One dimension that almost everyone agreed on was that they try to drive a risk aware culture—87% agreed with this statement (Figure 8). Respondents also offered their best way to drive a risk aware culture (see Appendix A). The pattern that emerges seems to be communication with a big emphasis on ERM education and training. Another pattern for driving a risk aware culture appears to be focused on performance linkages, incentives, and accountability.

LEAKS IN THE ERM BOAT?

Despite all the positive results above, there were some leaks in the ERM boat and some other areas to improve.

When specifically asked which area to improve the top five areas (in descending order) were:

- The strategy risk connection
- Building resiliency

- Measurement
- Understanding impact
- Monitoring.

In addition to improving these areas some potential leaks in the ERM boat include:

- 33% did not agree that their risk assessments were accurate.
- 48% had not looked at risk connections and correlations (which COSO Principle 14 suggests)
- 58% agreed that "unidentified risks have impacted our organization in recent years;" in essence, they had been surprised by a risk.

Several questions also addressed decision making and suggested additional leaks in the ERM boat, including (Figure 9):

- Only 34% say ERM gets involved up front in major decisions (although the data show that high-performers are more likely to be involved up front)
- Only 46% agree that decision making involves explicit consideration of risk
- Only 48% believe the risk information that is reported is enough to enable better decision making.

THE ERM CHALLENGES

The Summit participants were also asked their ERM challenges going forward (see Appendix B). The patterns that came up included the value proposition, management (working with them, educating them on the value, turnover, etc.), integrating ERM (into strategy, into operations but also distinguishing from operational risks, and into decisions), and building the ERM infrastructure.

Perhaps the most interesting challenge of all is that only 50% believe their organization is resilient enough to withstand a major risk. In other words—given the leaks, surprises, and not incorporating risk into decision making up front, etc., it is quite possible that a large risk will get unnoticed or mis-assessed early. Combine that with the lack of confidence in resilience, and some are gambling with their future. Boards and leaders, beware! Ensure your ERM is effective and communicate what you need to manage your risk.



FIGURE 5
ERM EFFECTIVENESS
Our ERM program is effective.

FIGURE 6
ERM AND VALUE PERSPECTIVE

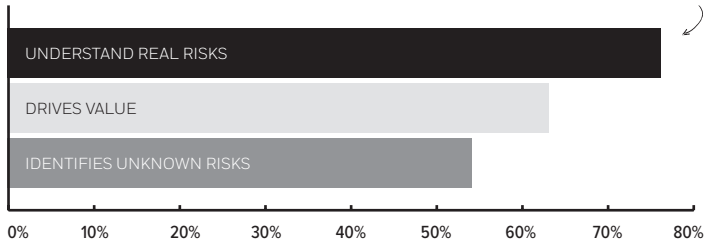


FIGURE 7
ERM ASSESSMENT AND SATISFACTION

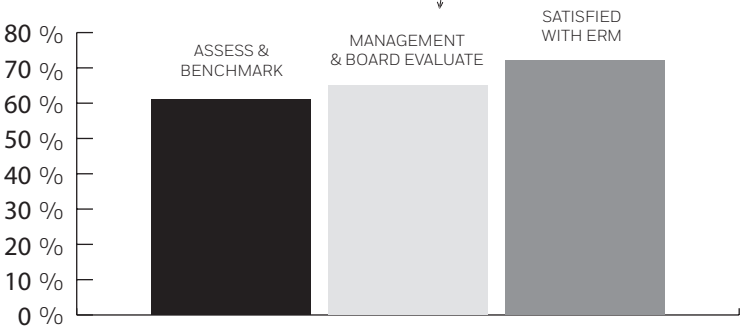


TABLE 3: BEST ERM WINS

Getting started	Affecting organization structure to best address operational risk	Building a relationship with risk owners and having them see a holistic view of the risks
CEO and CFO allocating more resources	Driving the business to successfully position and address an (unfolding) emerging risk	To bring an 'a-ha' moment to management on risks they did not previously have insight into.
Changing the culture to see risk as opportunity	Developing a risk tracking dashboard embedded in operational business units	Having the business call us prior to something going wrong!
Facilitating management dialogue to get alignment and clarity on major risks	Illustrating for executive management (EVP) a real "disconnect" between some of their opinions on the top risks and the opinions of the SVP and VP level	Having business leaders promote and embed risk management in their respective areas as a value add
Getting accepted throughout the organization		Being asked to help evaluate and having a seat at the table at strategy
Having senior management acknowledge the need for rigorous ERM		
Helping the culture become more risk aware		
Deploying training on ERM		

FIGURE 8
DRIVE RISK AWARE CULTURE



Our organization strives to drive a more risk aware culture.

FIGURE 9
ERM & DECISIONS





APPENDIX A – HOW TO DRIVE A RISK AWARE CULTURE

Active engagement and always showing the value add of risk management

Based compensation on whether or not including risk in decision making and whether or not adhering to key control practices

Communication and training

Communication from top down of risk parameters and communication of examples of success stories from the bottoms up

Constant dissemination of information and face-to-face meetings to drive engagement

Constant education and awareness efforts to help individuals realize the risks they manage in their roles each day

Drive accountability and transparency

Driven from top down awareness and involvement

Educate, establish ownership of risks and regular cadence of reporting with good accountability and governance from the board

Education, training

Embed risk concepts in the business and tie risk management activities to performance.

Enabling strong third line and a stronger second line of defense who partners and supports the organization's risk takers

ERM personnel meeting face to face with all levels of mgt

Fully integrating enterprise risk management in business processes with strong linkages to the organizations' strategies and business performance

Good communication strategies and execution

Incentives

Incorporate risk-related activities into managers' goals and include as part of year-end evaluations

Integration of the ERM process at all levels of the organization.

Learning by example: Raise awareness of experience of external organizations, both successes and failures

Learning by experiences (i.e. participating in a workshop or similar experience)

Promote speak up culture, two-way communication, and transparency

Pull from the board level into the organization

Risk awareness is everyone's responsibility. It should be part of a mission statement, employee reviews and regular communication throughout the organization

Senior management expectation of risk discussion, inclusion of risk in operational and strategic forums, broad education and awareness initiatives

Sponsorship from senior leaders, training, recognition of risks well mitigated.

Stay consistent in the messaging

Through a bottom-up ERM approach; performance review element; education -- "Risk is everyone's business!"

Through communication from leadership

Through training and ensuring adherence to corporate standards

Through training, tools and integration with operations

Tone at the top

Top management needs to live it and hold everyone accountable

Training and consequence for risk failure

Training and more frequent touchpoints with management



APPENDIX B – ERM CHALLENGES GOING FORWARD

Senior leadership socialization

Integration into the Strategy Formulation process

Measuring the value of ERM

Benchmarking the thoroughness of the program

Applying consistent and/or universally-accepted risk assessment criteria across different business units/contexts

Building awareness of the integration between ERM and Strategy

Competitor innovation

Consistent implementation of new ERM-related policies and procedures

Credit for the work that is done

Customer attrition

Deepening organizational understanding of risks, and framing such in a way that facilitates Decision making

Determining the purpose and "value add" of the ERM program and gaining C-Suite level support for ERM initiatives

Differentiation between ERM level risk and operational risk

Education on ERM to middle management

Ensuring the business actively monitors risk

Ensuring underlying assumptions, modeling and forecasts are adequate to meet our short and long-term obligations and regulatory mandates

Establishing an ERM system

Formalizing ERM throughout the organization.

Getting involved in strategy setting and decision making

Getting the attention of staff at all levels of the agency

Keeping the appropriate balance between profitability and growth

Maintaining a regular cadence of engagement - engagement tends to vary by the risk stakeholders

Maintaining Consistency

Moving from an ERM program that has a higher focus on reducing negative outcomes and managing risks to one that is fully integrated with the business and strategies, increasing the range of opportunities linked to performance ... creating, preserving and realizing value

Not enough resources around model, vendor and ops risk functions

Responsiveness from several business units

Risk appetite

Showing or proving how we add value

Siloed risk activities; no CRO

Standardize ERM governance across all regions. Insert ERM or its principles into the strategic planning process across at regions

Talent management

Time to work in ERM to decision making process

Too many silos

CENTER FOR EXCELLENCE IN ERM BOARD

John Adams (PepsiCo, retired)
Kristie Bidlake, General Motors
Russ Charlton, WeWork
Blake Eisenhart (Unisys, retired)
Rob Gould, Harley-Davidson Inc.
Stu Horn, IBM
Deon Minnaar, KPMG
Rich Muzikar, Long Island Power Authority
Matt Perconte, Protiviti
Henry Ristuccia, Deloitte
Kathy Robinson, ADP
Chris Ruggeri, Deloitte
Gerry Spry, Estee Lauder
Zach Wolff, Con Edison
Arya Yarpezeshkan, Western World
Stephen Zawoyski, PWC

2018 ERM SUMMIT SUPPORT

The Spring 2018 ERM Summit was supported by funds from Protiviti.

ST. JOHN'S UNIVERSITY



DR. PAUL L. WALKER, PH.D., CPA
JAMES J. SCHIRO / ZURICH CHAIR – ENTERPRISE RISK MANAGEMENT
EXECUTIVE DIRECTOR, CENTER FOR EXCELLENCE IN ERM

ST. JOHN'S UNIVERSITY
TOBIN COLLEGE OF BUSINESS