Embedding ERM into the Organization

White Paper Series

St. John's University, Tobin College of Business

Center for Excellence in ERM

Dr. Paul L. Walker

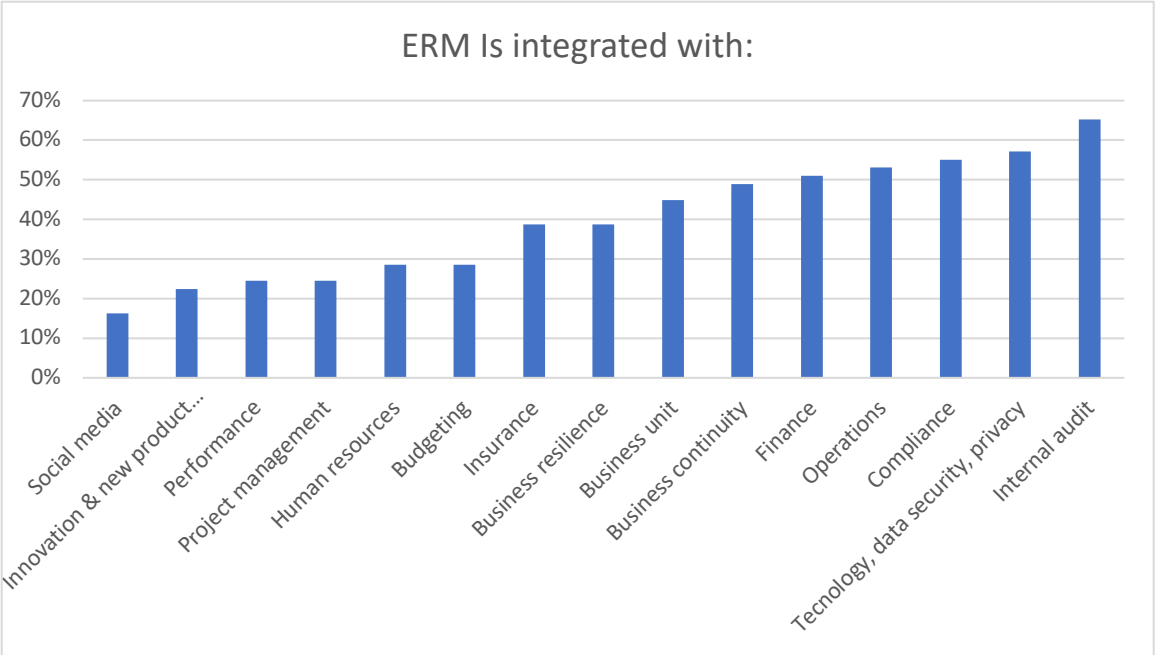
Embedding ERM into the Organization

It has always been "enterprise" risk management and not "do-it-on-your-own" risk management. But how is an ERM program taken from launch, to various levels of maturity, and then integrated more and more into the organization? ERM leaders from nonprofit, for profit, and from around the world gathered at the Center for Excellence in ERM at St. John's University 2019 Fall ERM Summit to discuss these and other ERM integration approaches. The big question was about how to embed ERM into the organization.

Among the diverse group that attended the ERM Summit, there were some serious ERM leaders and leading-edge practitioners. A few of the participants have even won ERM awards from RIMS. Additionally, almost half of those attending stated their ERM program was effective and, almost half also reported their organization was a high-performer, and well over half reported that their ERM program was delivering value. The registrants graciously participated in a preconference survey to supplement the conversation and help identify the trends and areas where embedding ERM worked and what was needed to improve embedding ERM.

Where ERM is Currently Integrated

Most of the Summit participants have experience with ERM integration as evidenced by how many reported that ERM was integrated to some extent both in their organization and within multiple areas and units (see the figure below). There were five areas where about 50 (or higher) percent of leaders agreed that ERM was integrated. Internal audit led the way, followed by the area of technology, data security, and privacy. Compliance, operations, and finance rounded out the top five areas where ERM is integrated.



The ERM integration effort needs to be continuous too, it is not something that organizations can ever stop pursuing. For example, one ERM leader shared how his company continuously tries to increase the level of integration between risk, integrity, and controls. To increase the integration, his company developed guiding principles to achieve that vision including things such as being bold and innovative in driving efficiency in end to end processes, leveraging technology, and sharing lessons across the company to keep up the improvements.

Areas with the least amount of ERM integration included project management, performance, and innovation and new product development – each area showing up at just over 20 percent integration. Given the amount of disruption and innovation that so many companies are reporting today, the fact that so few are integrating ERM into new product and innovation is surprising. There is a growing body of work being done in this area that shows how to identify risk in innovation and expand beyond normalized stage gate approaches and NPV, ROI or other financial metrics. In fact, one CFO noted that strategic position is the preferred way to judge risk around an innovation – not necessarily the risk of losing dollars.[1]

[1] See *Innovation and ERM – Partners in Managing the Waves of Disruption*, by Paul L. Walker and published by the IMA and ACCA in 2012. Seminal work such as Clayton Christenson's *Innovators Dilemma* also note the importance of understanding innovation from a disruptive or sustainable perspective, suggesting that the disruptive risks can threaten the entire organization.

The social media approach used by the enterprise showed up as the least likely area to be integrated, with an integration level of just 16 percent. Since it is likely that few companies would deny the importance of reputation risk, it is somewhat surprising that integrating ERM into social media approaches is the least integrated area.[2] Given the number of high-profile companies that have had major reputation risk blunders, this could be an opportunity for improvement for embedding ERM thinking and discipline. A common pattern in these reputation risk blunders seems to be that the overall risk impact is under assessed and seems to not factor in just how prodigious of an impact reputation has on future contracts, relationships, revenue, etc.

Risk Awareness

But how much risk thinking progress has been made and how much do these enterprises understand the upside of risk? To determine this, the ERM leaders were asked about overall risk awareness and about who sees the upside. Specifically, the Summit participants were asked which of the groups in their organization were risk aware. Getting them to at least be risk aware is a big step in the right direction of embedding ERM. The areas considered to be the *most risk aware* are listed below (in descending order):

- Senior management
- Technology
- Board
- Internal audit
- Compliance
- Business units
- Management

It's encouraging to see organizations believe that senior management is risk aware and that the board is not far behind (over 90 percent agreed that both senior management and the board

[2] Some companies, such as Barclays, have developed separate reputation risk approaches, that feed into the ERM process.

were risk aware). Slightly over 80 percent agreed that their management and business unit were risk aware. This almost 10-point gap suggests there are some opportunities to get the management level more risk aware and potentially on a level more consistent with senior management and the board. An additional perspective is that those in management may want to become more risk aware since senior management and the board are ahead of them in that capability and thinking. Other opportunities to improve risk awareness are evident by looking at the least risk aware area. The five least risk aware areas were budgeting, performance, innovation, human resources, and employees, which was ranked dead last as the least likely area to be risk aware. **Only 24 percent of ERM leaders believe the employees are risk aware**. The 69-point gap between senior management and employees is startling (93 percent vs 24 percent, respectively). Embedding ERM beyond senior management and towards employees will be a huge task.

The Upside

When asked who is more likely to see the *upside* and opportunities of risk management, the top three areas identified by ERM leaders were

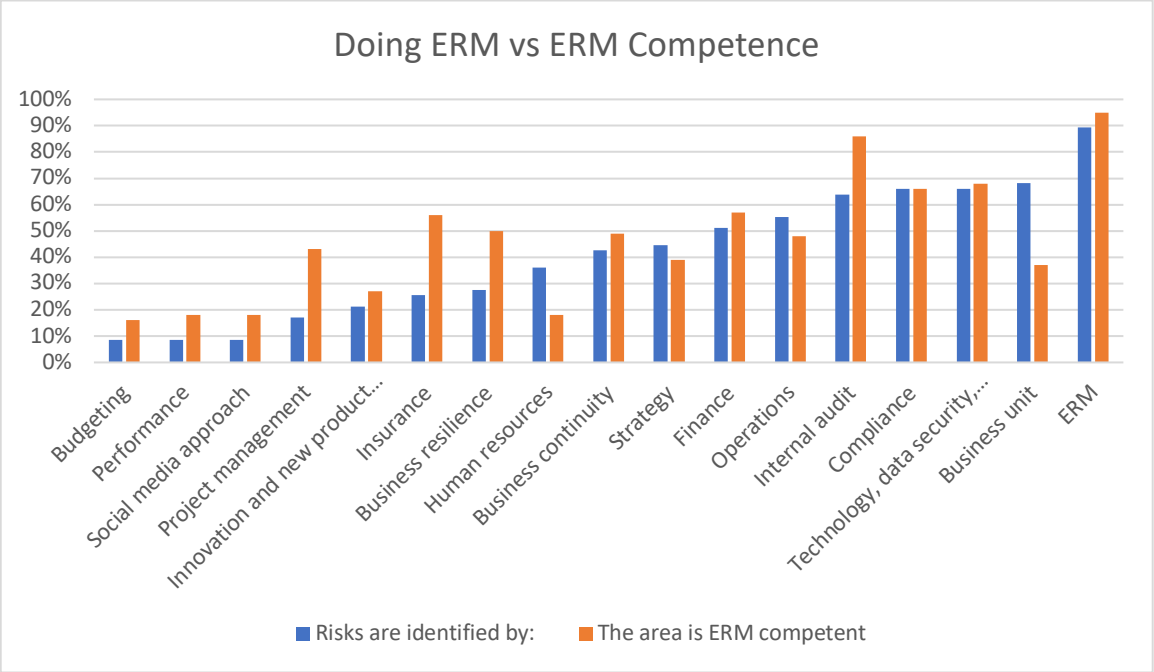
- senior management (80 percent agreement)
- management (41 percent agreement)
- strategy (39 percent agreement).

Given how many ERM programs ask the value of ERM question, one way to interpret this data is that it suggests the value (and related upside) might best come from and be seen by these three groups. Those working in the ERM trenches should do what they can to engage these groups when tackling and developing the value proposition.

Doing ERM vs ERM Competence

ERM development and integration must always learn to work with what they are given and within the organization's current capabilities. As such, leaders were asked where else in their organization risk identification and assessment was already occurring. Further, they were asked

how competent they believed those organizations were at risk assessment. The results are shown below.



The graph is sorted based on which groups are doing risk assessments, with the lowest number on the left and the highest number on the right (the blue data lines). As the results show, some type of risk identification and assessment is done by many units in organizations. In fact, over 50 percent of ERM leaders agreed that some type of risk identification was already occurring in finance, operations, internal audit, compliance, technology, business units, and, of course, in ERM. This is a reminder to those building ERM to learn what the organization is already doing with respect to analyzing risks. It might be a lot easier to leverage or adapt work already being done than to start from ground zero. Very few organizations are doing risk assessments in budgeting, social media, innovation, and surprisingly, business resilience and continuity - areas where risk assessments would appear to be quite indispensable.

The orange data in the graph show whether ERM leaders believe that area is ERM competent. Excluding the ERM group, the most ERM competent groups are internal audit, compliance, and technology. The five least ERM competent areas are innovation, social media,

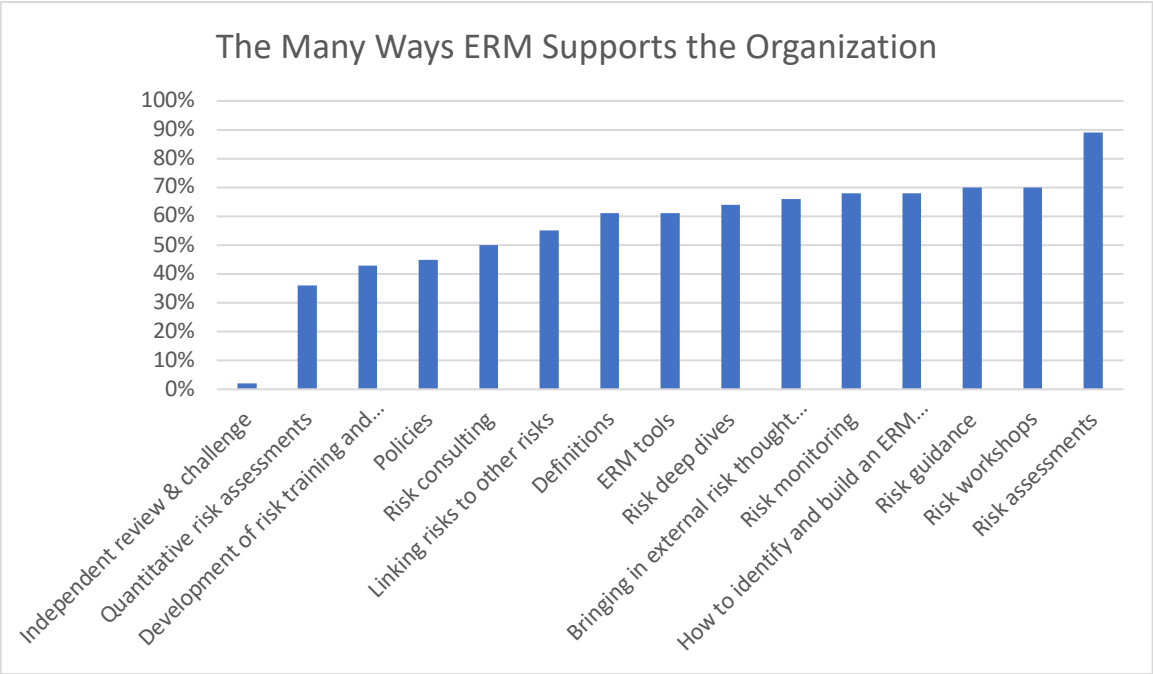
human resources, budgeting, and performance. However, the business units and strategy run close behind these groups in terms of low levels of ERM competence, which is a bit of a concern. **Specifically, slightly less than 40 percent of organizations thought their business units and strategy units were ERM competent**. Of course, a likely solution is ERM training for these groups, but it could be a sign of other problems. The business unit is especially troubling since 68 percent of them were identified as doing risk assessments (the second most of all the groups) and yet they are one of the lowest ranked on ERM competence. One ERM leader noted his operations around the world conduct their own risk workshops but that he had also spent considerable time training the units. The operations (production, quality, HR, legal, etc.) at his organization identify, assess, and prioritize the risks and these risks are then rolled up to the top company/enterprise level risks. This works best if the ones conducting the risk assessments are properly trained.

How ERM Supports the Enterprise

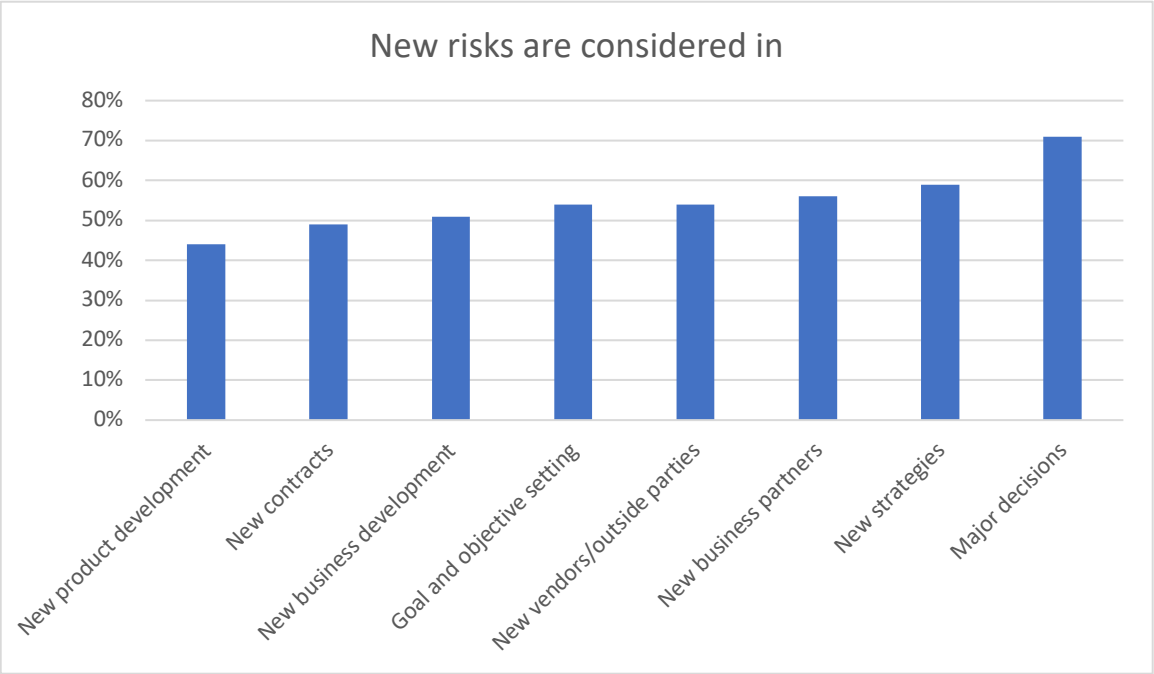
In addition to general ERM competence the ERM leaders also reported the top ERM ways they support their organizations. One ERM leader noted that they provide gap/risk assessments to business units *before* new systems and programs are deployed. Another ERM leader stated they do pre-business partner risk assessments, and another has ERM get involved in projects above a dollar threshold. As seen in the figure below, around 60 percent or more of ERM leaders provide definitions, tools, deep dives, and bring in external thought leaders. Others help with monitoring, building ERM, and offering risk guidance, risk workshops, and risk assessments. ERM has clearly become a busy job with many tasks and an expanding job description. **Gone are the days of the annual survey being the only thing some ERM leaders achieved.**

One ERM leader highlighted that the tools not only enable ERM but they also change the culture, specifically noting that the tool helps them drive focus and message and also help communicate risks. Another ERM leader shared the importance of a risk taxonomy and how it can be used to create transparency across processes, thereby furthering ERM integration. Other

interesting ERM offerings include independent review/challenge, quantitative assessments, and linking risks to other risks (emphasized in the new COSO 2017 Framework).

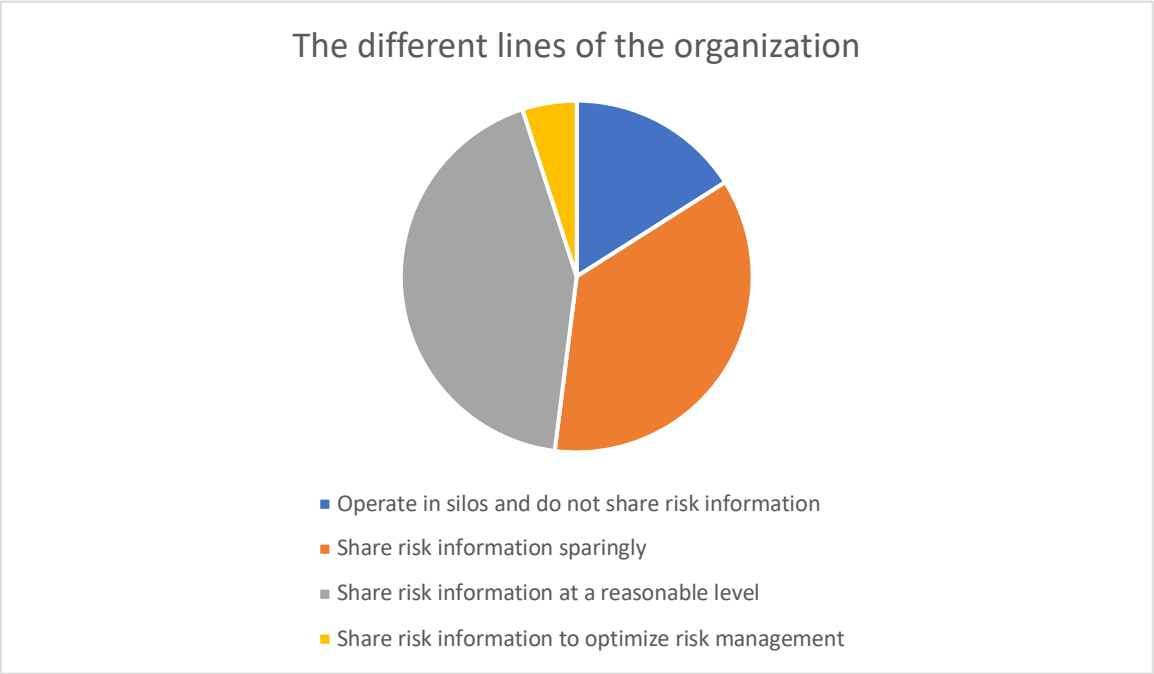


Interestingly, when asked where new risks are considered, there appears to be more areas where ERM could get involved. The figure below shows the good news is that 70 percent consider risk in new decisions and almost 60 percent in new strategies. Still, however, only about half consider risk in the other areas. To some these are further ERM embedding opportunities especially since some believe there is a lot of risk in these areas, including areas such as outside parties. **Since both COSO and ISO emphasize the importance of risk to objectives, the only 54 percent reporting that they consider risk in goal and objective setting is a bit of a surprise.**



Identifying and Eliminating Silos

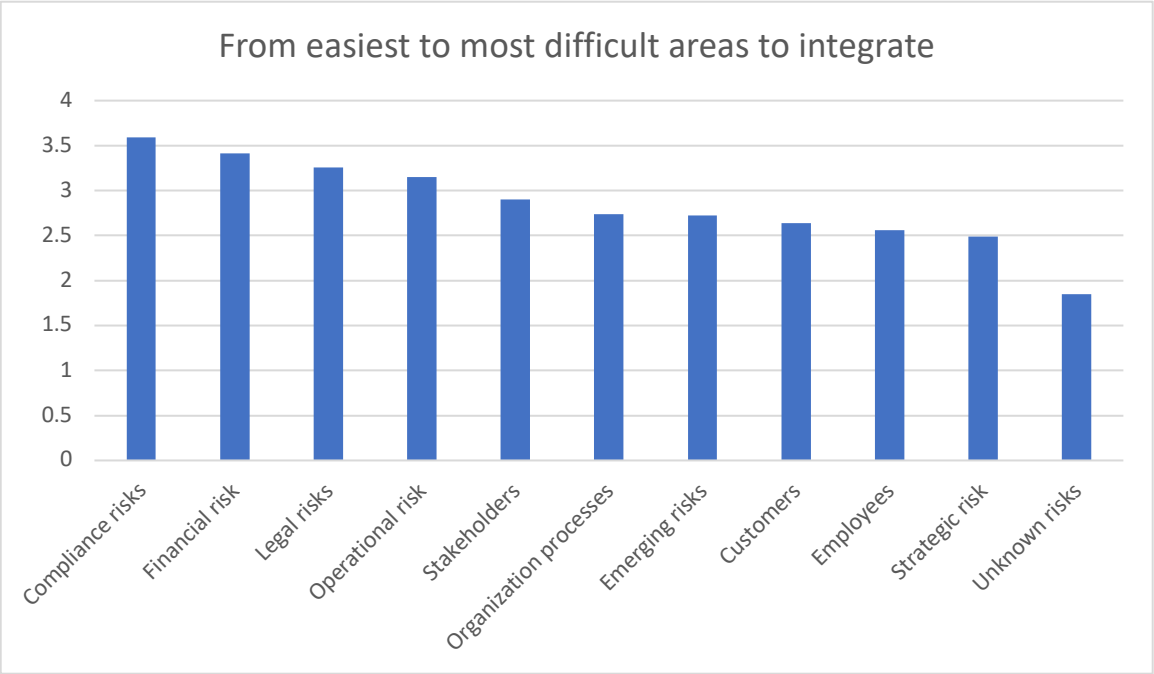
Specific questions about unit coordination (within organizations) were also sought to determine the extent that units talk to one another and whether ERM is able to be part of that process. The findings (shown below) suggest some significant opportunities for improvement. **Over 52 percent either operate in silos or share risk information sparingly.** While 48 percent sounds good, it still seems odd that so many are not able to get the units to share risk information. Additionally, only 5 percent agree that they share to the point of optimizing risk management. Perhaps the answer is a unique approach highlighting how risk information impacts other parts of the organization along with focused meetings to solve those shared risks.



Furthermore, when asked an additional question regarding whether integrated risk conversations are occurring, only slightly above half of organizations reported that any of businesses, managements, or boards are having integrated risk conversations. Whether this implies that ERM becomes more siloed at the board or at the management level is not clear but it is a potential barrier to effectively manage a portfolio of risks with a value-oriented approach.

The Most Difficult Areas to Embed ERM

The difficulty in integrating and getting different areas to talk is of utmost importance to understand. But it's not just the nature of the people and units in the organization that make ERM integration more difficult - there are some areas that are just inherently more difficult than others. For example, the figure below shows the response to a question about whether the area was difficult or easy to integrate ERM. The lower scores are considered the most difficult areas to integrate and the chart is ordered from left (easiest to integrate) to right (most difficult to integrate).



The results in this figure show that the easiest areas to integrate ERM are compliance, financial, legal, and operations. Those building ERM programs may want to take note that these are some potential easier wins. The most difficult area to integrate ERM is the unknown risks. Even though that seems obviously difficult or impossible, organizations are attempting to identify unknowns using a variety of tools and techniques. The NACD and others have been pushing for boards to step up their efforts in disruptive and exogenous risks, and also to step up with respect to legacy business models. Tools such as in-depth emerging risk searches, risk comparison/benchmarking, scenario analysis, design thinking, game theory, black swan workshops, pre-mortems, and strategic disruption workshops can all be used to help identify potential unknowns. Additionally, as noted earlier, some are bringing in external thought leaders. These and other tools can also be used in helping to identify the second most difficult area to integrate - strategic risk. For example, some link their (identified) risks to strategic plans and objectives in an effort to view and better understand the risk – strategy connection. Of course, this is not the same as a strategic risk analysis around the business model and strategic risk dimensions but it is a starting point.

Getting both employees and customers to understand risks is a big job and ranked third and fourth most difficult, respectively. **There has been talk of organizations trying to understand risk to the extended enterprise and that is a worthy effort because the most difficult risk to manage is the risk an organization bears from the behavior of others.** The complexity of getting customers to understand risk and manage them is tricky. One presenter at the ERM Summit noted the importance of thinking about this by putting risk in categories that help explore the various types of risks. In that company's case they apply the risk categories to data as listed below

- data risks associated with entities supplying data to you
- data risks associated with your processing of data, and
- data risks associated with entities receiving your data.

According to this ERM leader, one of the keys to treating these risks was to build partnerships with the business. Partnering with them helps to integrate ERM further into the business. In these partnerships, ERM could offer some of the services listed above such as risk assessments, risk workshop, etc.

Improving Coordination of Risk Efforts

Sophisticated ERM programs recognize the difficulty of integrating and coordinating risks and are trying to improve those connections. When asked about the key to improving the risk management "between the organizational areas" the responses fell into a variety of areas or themes (the full list of responses to this question are listed in Appendix A). One theme that came out addressed the top of the organization - specifically mentioning the tone at the top and management buy-in. One respondent went further than just top support and stated, "Standing up an Executive Risk Council - to ensure that the ELT is thinking about the organization's risks holistically and from the point of view of what it means to the organizational strategy." Another noted the importance of adding risk culture and integration into the roles and responsibilities of risk and leadership councils. Other more straightforward suggestions included:

- Getting over politics

- Be open and honest
- Educating them on ERM
- Being a trusted partner
- Constant communication, and
- Changing the risk culture.

Taking a more direct approach, another theme seemed to be to get them together to have meetings, have conversation, develop approaches, etc. One respondent pointed out the importance of showing them risks cannot be managed "solely within a business unit/function because of interdependencies." In other words, show the areas where it cannot be done and then maybe they'll be willing to get together. Another stated the importance of "setting up enterprise-wide mechanisms to get cross-function teams to think specific risks from different perspectives." Along this theme of getting them together came up related topics/ideas suggesting:

- Having cross-functional workshops
- Sharing the vision
- Having cross-functional dialogue
- Having risk forums
- Having integrated workshops
- Promoting knowledge sharing
- Having collaborative meetings

The central idea, according to one ERM leader, is to "create opportunities and platforms for collaboration and communication."

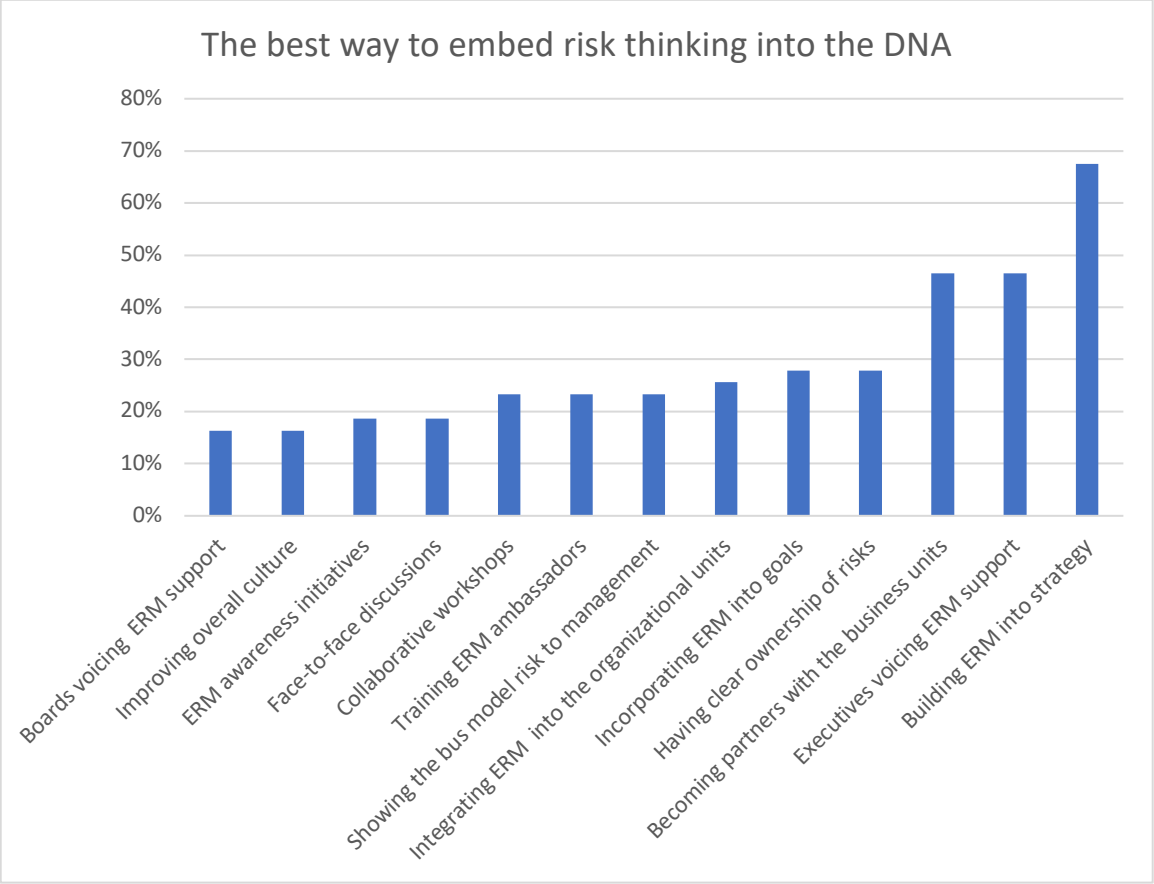
Embedding Risk Thinking into the DNA

Other ways to improve risk coordination came out in the answer to a question asking how to best embed risk thinking in the DNA of the organization. The responses are shown below. It is interesting that the most frequently chosen reply was to build ERM into strategy. It's likely that some chose this because when ERM is built into strategy it both sends a message and makes ERM involved at the beginning instead of in efforts to later identify risks (after strategy is

set). The other top two methods for embedding risk into the DNA were executive support and becoming partners with the business units. Having clear ownership of risks and incorporating ERM into goals round out the top five. One ERM leader discussed the importance of clearly defining the risk roles and responsibilities including ERM, legal, business, and internal audit.

Improving overall culture was mentioned too. Whether it is a "risk culture" or not, improving overall culture can go a long way. Other notable answers that came up but did not make top answers include:

- Sharing success stories
- Making management and employees accountable
- Establishing a clear governance model, and
- Leading through risk events and helping solve risk issues.



In one question, the ERM leaders were asked to identify the best way to integrate ERM. Although this question is somewhat duplicative of embedding risk thinking into the DNA, there were some good insights shared (the full list of responses can be seen in Appendix B). One ERM leader felt a change management approach is needed. When asked how to best integrate ERM they stated, "Through a well-articulated and properly planned change management process, where the change in culture, which may be very significant, is managed well." Another insight was to avoid the technical ERM jargon, "Stay away from the technical ERM lexicon/jargon when engaging the organization. Be flexible to adapt to their existing business rhythms and the manner in which they natively think and talk about risk…" Another ERM leader emphasized the importance of management assuming their responsibility, while another noted, "Have everyone own something related to risk, and have everyone understand how they can participate."

One ERM leader stated that integrating ERM is assisted by also being collaborative in other areas such as governance or in taking a risk-based approach in compliance. Another ERM leader noted that they approached improving ERM integration by asking both the senior leaders and the audit committee chair how to improve and optimize ERM. They also sought input from external consultants. As a result, they made improvements in getting risk thinking into the business design (meaning more upfront) and also raised accountability by getting risk and treatment plans to be included in quarterly business reviews.

Conclusion

In a prior Center for Excellence in ERM white paper it was noted that higher performing organizations tend to embed ERM more into the enterprise and embed ERM into more and different areas that non-high performing organizations. This white paper extends that progression and peels back the many layers of embedding ERM. Some key findings include:

- Organizations are embedding ERM more and more into their organizations, especially into areas where it fits more naturally. Over 50 percent of ERM leaders agree that ERM is integrated into finance, operations, compliance, technology, and internal audit. However, there were some critically important areas (e.g., innovation, performance, business resilience) where ERM did not appear to be integrated.

- Senior management and the board are highly risk aware. Others in the organizations need to step it up to get on the same page.
- Senior management, management, and strategy are the three areas most likely to see the upside of ERM. ERM leaders should partner with them in developing the value proposition.
- Many parts of organization are already doing some form of risk assessment. ERM leaders may want to leverage those efforts to get buy in and avoid duplication. Other areas need additional training.
- The top ways ERM supports the organization are assessments, workshops, guidance, identifying and building ERM, and risk monitoring. There are many other tools in the ERM toolbox. ERM leaders should choose the tool that best fits their organizational needs and culture.
- New risks are being considered more and more, with major decisions, new strategies, and new partners showing up at the top.
- Silo risk management is still a problem and a significant barrier to overcome. Several techniques for improving the integrated risk conversation were identified.

Appendix A- The key to improving risk management between the organizational areas is:

Better integration.
Collaboration through meetings to discuss risks and strategies.
Common language and understanding of central processes.
Communication and collaboration.
Communication; central ERM team needed to drive alignment and set common language/goals.
Constant Communication.
Creating consistent opportunities (quarterly meetings) for ERM topics and issues to be discussed.
Creation of opportunities and platform for collaboration and communication
Cross-functional dialogue.
Cross functional risk workshops/discussions.
Group discussions of risks.
Having a risk leader bring the appropriate functions together to discuss the risks in their own functions or common amongst them.
Integrated workshops / training.
Lines of communication.
Management buy-in, planning, execution, communication.
Open and honest discussion/ assessment.
Open and transparent dialogue.
Risk forums and discussions between organizational areas.
Sharing information and continuous dialogue.
Transparency and awareness.
Better communication. Show the business value for each organization. Make it simple to use and report on.
Clarity of top objectives and trust.
Continuous discussion, demonstrating value through the ERM process, and data sharing.
Education.
Education, awareness and integration. Being a trusted and valued business partner in their decision making and planning processes.
Driving awareness and demonstrating value.
Promoting knowledge sharing.
Building off of existing practices instead of forcing a new way of working
Demonstrate that risks cannot be managed solely within a business unit/function because of interdependencies.
Developing risk culture.
Getting over politics.
Governance, defined processes, and technology.
Having executive sponsors who understand the significance of risk management.
Incentives and performance measurement objectives in leaders across lines of defense position descriptions and annual appraisals.
Metrics, performance monitoring, and linkage.
More centralized management with a core group of top level, centralized functions, terminology and oversight.

Setting up enterprise-wide mechanisms to get cross-function teams to think specific risks from different perspectives, and risk owners of similar risks in different business units together to compare mitigation and control strategies.
Shared vision of risk management and ERM and operational cohesiveness of risk management.
Standing up an Executive Risk Council - to ensure that the ELT is thinking about the org's risks holistically. and from the point of view of what it means to the org strategy.
Showing interdependencies.
Tone at the top and ERM being viewed as part of "leadership" (however that might be defined in a particular organization).

Appendix B - The best way to integrate ERM into the organization is:

Be a core part of the strategic planning process.
Dedicated ERM team, CEO tone, coordination with 2nd line of defense, and clear alignment with key business processing, such as strategic budgeting.
Facilitated workshops, discussions with other groups (IA, Strategy, Budgets, et al.), continuous improvement.
Incorporate into the company's strategy and budgeting process.
Integrate ERM into strategic and performance processes.
Strategy.
Through budget.
Understand the organization's mission and strategy and provide thought leadership to achieve or support them.
Buy-in by executive management.
By making risk informed decision making in day today activities in all the three tiers of management.
Continuous improvement sessions with all business heads.
Discussion and deep dive analysis.
Embed one level below the Executive Committee.
Explicit governance includes the integration and communications.
Find a friend . . . ERM needs executive champions who are willing to experiment with sometimes unfamiliar concepts toward a benefit may not be tangible as the next revenue dollar generated.
Getting buy in from AC and ELT.
Have everyone own something related to risk, and have everyone understand how they can participate understand the risks from the top, key employees of the company, getting their input on the top risks and buy-in on prevention, minimization or remediation of those risks.
Leadership sponsorship.
Obtain strong support from top leadership and tie ERM back to strategy and growth objectives where possible.
Orient management to their responsibility for ERM within the business.
Regular meetings and analysis with business units.
Risk assessments and regular interactions with the business.
Stakeholder engagement - I think what this means though is different for each of the various functions within our organization.
Start with leadership support and accountability.
Stay away from the technical ERM lexicon/jargon when engaging the organization. Be flexible to adapt to their existing business rhythms and the manner in which they natively think and talk about risk, even if they don't explicit title their activities risk management.
Through executive sponsorship and integration with key central processes.
Top down and bottoms up approach. Get commitment from executive team and then embed erm team into projects with heightened risks.
Clear value statement, building a trust-based partnership with the Business Unit.
Continual education and awareness along with responsiveness and value-added activities (i.e., helping the business deal with risk and better manage it.)
Driving culture evolution.
Endorsement from an engaged executive leader to champion the process, philosophy and methodology. If it's too truly be integrated, it must be incorporated into most senior levels of

leadership and their dialogue as a leadership team... not just an agenda item from time to time for updates.
GRC Tool and Culture.
Proving value.
Making it valuable for the organization.
Risk Culture and awareness training, Risk Assessments, Risk 101 sessions, and Risk identification workshops.
'Road Shows' educating about the function, various risk disciplines - and, most importantly, by promoting a culture of accountability.
Showing the business value.
Strong partnerships and executive support through goals and objectives.
Through a detailed, well-articulated and properly planned change management process, where the change in culture, which may be very significant, is managed well.
Tone at the top. The culture around ERM.
Using the culture/normal management process to drive risk management capabilities into the business instead of creating new demands or tasks for them to provide data for someone else's use.

Center for Excellence in ERM Advisory Board

John Adams, Retired VP Global Enterprise Risk Management, PepsiCo

Russ Charlton, Chief Audit Executive, Advance

Blake Eisenhart, Retired Chief Audit Executive, Unisys

Geralyn Fanelli, Global Enterprise Risk Management Sr. Director, PepsiCo

Stuart Horn, IBM, Director of Enterprise Risk Management

Athina Kontouli, Business Development and Operations Analyst, Frenkel & Co

Joshua Mahnke, Director of Internal Audit, Harley-Davidson, Inc.

Deon Minnaar, KPMG, Global Leader for Internal Audit, SOAS, and ERM

Adrian Mueller, Vice President, Risk Management, Enterprise Risk Management, MasterCard

Rich Muzikar, Enterprise Risk Management Advisor, Long Island Power Authority

Matthew Perconte, Managing Director, Protiviti

Steve Richard, Senior Vice President, Chief Risk Officer, Becton Dickinson & Co

Chris Ruggeri, National Managing Principal Risk and Financial Advisory, Deloitte

Kelli Santia, Risk Manager, Strategic Risk Management, General Motors

Denise Sobczak, Global Enterprise Risk Management Sr. Director, PepsiCo

Spry, Geraldine, Vice President, Enterprise Risk Management & Global Insurance, Estee Lauder

Wolff, Zach, Con Edison, Director of SOX & Enterprise Risk Management

Arya Yarpezeshkan, North America Specialty Risk Officer, AIG

Stephen Zawoyski, Partner – Internal Audit, Compliance, Risk Services – ERM Leader, PWC

Dr. Paul L. Walker, Ph.D., CPA

St. John's University, Tobin College of Business

James J. Schiro / Zurich Chair – Enterprise Risk Management

Executive Director, Center for Excellence in ERM