Strategies for Designing a Lasting ERM Process: A Case Study

Andrew J. Farris | Jacqueline C. Gaine

John A. Humienny | Zihang Yin

Faculty Advisor: Bonnie V. Hancock

NC STATE UNIVERSITY

Table of Contents

INTRODUCTION

Implementing Enterprise Risk Management (ERM) within an organization can be challenging; it can be even more difficult to create the traction necessary to ensure that ERM will be an effective process over the long run. This case study delves into the key factors that have enabled six organizations to sustain an ERM process over a period of time. The purpose of the case study is twofold: first, to gain an understanding of key processes and factors that contributed to the on-going success of the ERM process at these organizations and, second, to share advice from ERM leaders that may be useful for other organizations with an ERM process.

This case study examines six organizations which have had ERM in place over a long period of time or have a process so embedded in the organization that it is expected to be sustained over the long run. The ERM processes evaluated have been employed from five to fifteen years and are critical components of operations. For each organization included in this case study, we have included a separate appendix summarizing the key steps in its ERM process, as well as the success factors that enabled the organization to sustain its process.

The paper is organized into two main categories: common sustaining factors and additional insights. Common factors were present in all, or the majority of, the six organizations' ERM processes and would most likely be applicable to other organizations looking to analyze the sustainability of ERM. These common success factors included support from senior leadership, a simple, easy-to-understand process that fit the organization's culture, effective communication of risk information, customizing ERM to the organization and evolving the process. Additionally, some organizations cited success factors that were specific to the individual company or industry, providing unique insights that may be useful to other organizations.

ORGANIZATION OVERVIEWS

The six organizations volunteering to participate in this case study represent a variety of industries and have annual revenues ranging from $3 to $60 billion. We have kept the participating organizations anonymous to protect any confidential information shared during interviews. Basic organization metrics are presented below.

Companies Represented

Organization	Industry	Revenues	Number of Employees
A	Air Delivery & Freight Services	$60 billion	400,000
B	Beverages	$42 billion	100,000
C	Electric Utilities	$12 billion	15,000
D	Higher Education/ Hospital System	$3 Billion	50,000
E	Electric Utilities	$23 billion	29,000
F	Independent Oil & Gas	$12 billion	5,000

COMMON SUSTAINING FACTORS

While studying each of the six participating organizations, several commonalities were discovered regarding sustaining ERM. This section of the case study describes the common factors that exist across multiple organizations. These factors include obtaining support at the top, simplifying the process, communicating effectively, tailoring ERM, and constantly evolving the process. ERM programs exhibiting these components are more likely to continue over time.

Gain Support and Engagement at the Top

Support at the top of an organization refers to the leadership and commitment towards ERM by those at the apex of the organization. As ERM is enterprise-wide, it is virtually impossible to begin, much less sustain, an effective ERM process without support at the top level of an organization. This responsibility primarily rests with the board of directors and senior management. That support should be exemplified both in words and actions, with those at the top of the organization not only communicating the importance of ERM, but also demonstrating their commitment by engaging in key ERM activities. Thus, it is not surprising that the board and senior management drove and actively supported the ERM process in each of the organizations participating in this case study. Support from the top was the sole factor cited by all six organizations as critical to sustaining ERM over the long term.

There were some differences across the organizations in the way that support from the top of the organization was exhibited. In most cases, ERM began, and was sustained, from a request and continued engagement by the board of directors. The boards and senior management teams in all of the organizations regularly received reports and engaged in discussions regarding the status of the top risks facing the company and the effectiveness of the risk management process.

In the case of D, implementation of ERM coincided with the appointment of a new president who was eager to use ERM to gather insights. B was slightly unusual in that support for the program initiated from a business unit that embraced ERM, demonstrating its usefulness to other business unit leaders. ERM was gradually adopted by other business unit leaders after seeing this success of ERM in the business unit, spreading ERM horizontally across operational business units.

Simplify and Standardize

ERM can be a difficult subject to explain to those unfamiliar with the concept. Thus, it is crucial to keep both the ERM process itself, as well as the terminology used, simple to make ERM easier to explain, understand and implement.

Using more complex concepts made ERM more difficult to understand and created an impediment.

As an example, A experimented with several assessment criteria, such as velocity. The organization also explored some fairly intricate interconnected risk models. It found these complex concepts more difficult to understand, creating an impediment to obtaining engagement from the members of its Enterprise Risk Council. As a result, A simplified its assessment criteria to include only two criteria: likelihood and impact. This allowed the assessment process to be more easily understood and management to feel confident in providing input to risk assessment.

F simplified its ERM process for documenting risks. The company created a standard definition for each risk to develop a consistent understanding among employees. In this way, when surveys were administered or risks were discussed in workshops, there was a common knowledge of each risk. As a result, the accuracy and relevance of the information gathered in those processes was improved.

C created a standardized risk report for annual presentations to the board of directors. The standardized format presents top risks using a nearly identical template year-over-year, allowing recipients of reports to quickly find desired information. Thus, board members can spend more time analyzing the information rather than attempting to understand the reporting format. Risk information can be analyzed from risk-to-risk and year-to-year in a consistent manner. Simple, direct reports are better understood and promote readability at the board level.

While a less complex ERM process is easier to implement and gain initial traction, it does not have to remain simple perpetually. E successfully implemented maturity models to map out the status of the process. Then, E considered the current state of the company's culture and designed

a process to bring the organization up the maturity curve. However, early in the ERM process development, E attempted to implement overly complex tools without first assessing the status of the program and whether the changes fit with company culture. From this experience, the ERM team learned that the organization must be ready before moving to more sophisticated processes.

Communicate Effectively

A key component of any successful ERM program is open and effective communication. F stated that ERM should communicate the right risks to the right people at the right time. Ideally, risk information regularly flows between employees, management, senior management and the board of directors. Communication is vital to establishing a relationship built on trust between the ERM team, business units and functions across the organization. Since ERM relies on employees sharing risk insights openly, a safe environment is necessary to facilitate communication. Business unit leaders are more apt to proactively share risk information if they believe the ERM team's goal is centered on improving risk management, rather than distributing blame.

Communicate the right risks to the right people at the right time.

A safe platform exists at A for business units to communicate risks to the ERM function. The ERM team makes a point to promote its goal as aiding business units facing major risks, not chastising them. A large factor in building trust between the ERM team and individual business units is evidenced by word of mouth referrals. If one business unit leader has a positive experience while sharing risks with the ERM team, he or she is inclined to describe the experience to other leaders. The ERM team understands this communication flow and strives to assist business units in any way possible. Over time this enhances trust and cements the relationship between the ERM function and the business units.

B has a similar approach to enabling risk information sharing. B focuses on communicating the value proposition of ERM to business units, taking a "carrot approach." This practice has proved successful, evidenced by the business units' adoption of ERM processes before such measures were ultimately required by adoption of a company-wide ERM policy. This implicit communication of ERM value is supplemented by the ERM policy, which explicitly conveys ERM requirements within the company.

As mentioned previously, C developed standardized risk reporting templates, enhancing communication between senior management and the board of directors. The standardized templates allow for consistent risk information reporting. This provides more time for risk discussion and facilitates additional communication on ERM topics.

Tailor ERM to Fit Your Organization

Each individual ERM process must be tailored to fit the culture and the business needs of an organization. For example, a highly regulated company will likely adopt a structured and quantitatively focused ERM process. Conversely, an organization operating in a less regulated environment may have less structure and may approach ERM more qualitatively. Each participant in this case study developed its own unique ERM program consistent with its organizational culture and built on existing processes to meet its unique ERM needs.

An example is E, an electric utility company. The organization is highly structured due to its regulated operating environment. Thus, the ERM process implemented at the company mirrors its operating environment. The program was designed around an established ERM framework, creating a structured and policy-driven process. ERM is successful partly due to its ability to assimilate into the organization's operating culture. Management and employees familiar with structured daily operations are more comfortable with integrating similar ERM processes into regular tasks.

On the other hand, D is a less regulated private university maintaining a collaborative process. If D's ERM process was as structured as E's process, it may have been met with resistance. Instead, D's ERM process is mostly qualitative in nature, with key processes, such as risk identification and assessment, being more discussion-driven. ERM works well at D due to its focus on dialogue that provides leaders with an opportunity to seek feedback when developing mitigation strategies. The ERM process also creates a forum to raise concerns that may represent emerging risks.

Enhance the Process Over Time

ERM process evolution refers to improvements made to ERM as part of facilitating program advancement. ERM requires constant attention and adjustments to be effectively sustained over time. Although each organization participating in this case study maintains a sustained ERM process, none of the organizations are content with the current rendition of their program. The case study participants have future plans to enhance ERM by adding new elements, removing ineffective components and/or implementing technological upgrades.

Implementing enhancements to the ERM process aims to keep the process fresh and at the forefront of employees' minds.

Accordingly, C adds at least one new wrinkle to its ERM process each year to facilitate program evolution. For example, the ERM department recently added the concept of high impact, low likelihood "black swan" events to its risk inventory. In the future, the ERM department will offer to discuss emerging black swans, as well as their causes, with company departments annually. C obtains ERM insights through benchmarking its process against the ERM programs of other organizations. Benchmarking is performed in relation to companies both inside and outside of the organization's industry. Gradually implementing enhancements to the ERM process aims to keep the process fresh and at the forefront of employees' minds.

As part of its evolution, D is in the midst of removing heat maps from its ERM process. Over time, the organization realized that heat-mapping risks has become rote without providing desired insights. Currently, nearly all top risks appear in the upper right quadrant of the diagram, resulting in little discrimination between the risks. As a result, the ERM director decided to retire heat maps, pursuing a more qualitative risk prioritization method. Implementing the new risk prioritization process will encourage leaders to assess risks from a fresh perspective.

Organizations A and E each plan to pursue technology to advance existing ERM processes. A is seeking to implement an information technology system to enable business units to directly upload risk information to a common platform. Thus, a two-way transfer of risk information between the ERM team and business units will take place. Efficiency gains will be realized as business units facing similar risks can quickly access information about how other business units have successfully mitigated the risk. E is pursuing data analytics software to improve its inventory of key risk indicators (KRIs). The software will allow risk owners to be alerted to potential emerging risks affecting their area of responsibility. This will help the ERM team to devise risk mitigation strategies in anticipation of approaching risks.

F focuses on the proper pacing of ERM evolution. Although adding new elements to an ERM process is helpful, too many changes in a short amount of time can disrupt the process. Company personnel require time to adjust and correctly implement process changes. ERM changes should be deliberate, with consideration given to the organization's culture and operating environment. Accordingly, F strengthens its existing ERM processes at a calculated rate to create a smooth transition to an increasingly robust process.

ADDITIONAL INSIGHTS

In addition to citing specific critical success factors for establishing ERM, case study participants offered advice for organizations implementing or seeking to mature ERM processes. While these suggestions were not uniformly cited by case study participants, they reflect valuable lessons learned. A sampling of that advice is summarized below.

Have an ERM Champion

An ERM Champion is a vocal advocate and leader of ERM within an organization. An ERM Champion can be an individual or group. The Champion serves as a "cheerleader" emphasizing the important contribution ERM makes to the organization. This is especially important during the implementation phase of ERM, when initial pushback may be experienced. Having a vocal leader to promote the value of ERM, explain its benefits and communicate its purpose contributes to the program's success. Additionally, the Champion should be a continuous force for improving existing ERM processes. Often, management can become content with processes already in place without seeking improvements. The ERM

The Champion serves as a "cheerleader" emphasizing the important contribution ERM makes to the organization.

Champion can offset any complacency by evaluating current processes and suggesting changes to benefit the program.

Consult an Expert on ERM

The ERM leader of one case study participant suggested that engaging an ERM expert could be valuable during the initial ERM launch and in sustaining the program over time. The ERM expert could be hired into the company or engaged as a consultant. The value created is the independent and unique perspective on ERM processes that comes from someone with diverse experience in risk management. This knowledge base can be tapped to provide a company with solutions tailored to its industry and operating characteristics. An expert can minimize the trial and error phase of ERM process implementation for companies embarking on an ERM journey. Likewise, an expert can provide guidance for continual improvement of established ERM processes.

Focus on the Major Risks

When focusing on the most significant risks facing an organization, senior leaders are more likely to be engaged and the value of ERM is better communicated. If ERM is viewed as being too compliance-focused or overly detailed, it may be regarded as a "check the box" exercise rather than a strategic tool. In addition, if organizations devote too much time to less significant risks, there is potential to overlook major risks. This inevitably minimizes the discussion of the top risks that should command the most attention. Keeping the emphasis on top risks helps ensure ERM meetings target the most critical risks and produce effective mitigation strategies.

Allocate Sufficient Resources to ERM

In order to operate effectively, ERM should be allocated appropriate resources. Senior management is primarily responsible for resource allocation, further illustrating the importance of executive support. Expectations for ERM should be appropriately balanced with the resources committed to the function. As ERM grows, increased resources should be available to expand the ERM department. Additional staff and enhanced risk management software are two examples of common resource allocations for organizations growing an ERM process.

Establish Clear Risk Ownership

Several organizations noted the importance of clear risk ownership. Assigning accountability for managing specific risks provides greater assurance that risk response plans will be developed and executed. Also, clear risk ownership is another way for top leaders to demonstrate their support of ERM by holding individuals across the company accountable for risk management. In addition, it was noted that assigning accountability by position, as opposed to by name, ensures that risks continue to be managed even when turnover exists in key positions. Providing training for new risk owners also helps risks to be managed in the face of employee turnover.

Provide ERM Training

At A, having employees across the organization who understand and appreciate the value of ERM is crucial to sustaining the ERM process. To this end, the corporate ERM function works to ensure

that individuals in each business function are knowledgeable about the company's ERM program and their responsibilities for identifying and managing risks. Accordingly, the ERM function ensures that each new management level risk committee member receives the appropriate training to carry out their role. Typically, the ERM function will spend 30-40 minutes explaining the process to new members of the committee, providing basic information necessary to perform ERM duties.

CONCLUSION

Implementing ERM within an organization can be challenging. The purpose of this case study is to offer insights related to improving ERM implementation and current ERM processes by sharing common success factors. These common success factors have been aggregated from interviews conducted with six different participating organizations. Additionally, some organizations provided unique insights for improving ERM based on their individual ERM journeys. Given that ERM is typically tailored to fit individual organizations, these unique factors provide valuable insights specific to industry and operating environment.

Obtaining support and engagement from the board of directors and senior management is a success factor shared by all organizations participating in this case study. Due to ERM being enterprise-wide, key leaders possessing an enterprise view are vital to both the initial implementation as well as the long-term success of the process. Additionally, one organization in particular has an ERM Champion that serves as a "cheerleader," emphasizing the important contributions ERM makes to the organization. The ERM Champion promotes ERM's value, explains its purpose and combats complacency by suggesting improvements to the process.

ERM may be a difficult subject to explain those unfamiliar with the concept. Thus, the majority of ERM processes studied are simple and relatively standardized in many facets. By keeping ERM processes and related terminology simple, ERM becomes easier to explain, understand and implement. One organization articulated its efforts to keep the ERM process simple by focusing on major organizational risks. This ensures that ERM resources are directed at the most crucial risks and removes the distraction of less significant issues. Another organization simplifies its ERM process through standardized risk documentation. This creates a common understanding of each risk and, as a result, the accuracy of the information gathered by its ERM processes is improved.

Open and effective communication is another success factor shared by organizations participating in the case study. Communication is vital to sharing risk information as well as establishing trust between the ERM team and company personnel. Several organizations noted the need to create a "safe" environment for sharing risks, as well as the importance of promoting the potential value of ERM.

Each organization in this case study developed its own unique ERM process tailored to fit its culture and business needs. ERM processes do not lend themselves to a one-size-fits-all approach. One organization hired an ERM expert to tailor its process to fit company culture. The

expert's knowledge base can provide solutions tailored to the industry and operating characteristics of the organization, while minimizing the trial and error phase of ERM implementation. Others relied on internal talent that leveraged knowledge of organizational culture and existing processes to develop an effective approach to ERM.

Continuous ERM process evolution is the final common success factor shared by organizations in this case study. ERM requires constant attention and adjustments to be effective over time. Each organization in the case study has made changes to its ERM process over time. Future plans to enhance ERM include adding new elements, removing ineffective components or implementing new technology. One of the organizations is focusing on allocating more resources to ERM as the process grows. Another organization is improving ERM training for business unit leaders.

We hope that readers will benefit from gaining an understanding of the unique ERM processes and success factors of these six participating organizations. Each of the success factors identified in this study provide insights that could be applied to other organizations seeking to establish or enhance their ERM processes, sustaining them over time.

APPENDIX – A

Organization Description

A is an air delivery and freight services company with reported revenue of approximately $60 billion in its most recent fiscal year, with over 400,000 employees worldwide. A's services include package delivery and logistics and its customers range from individuals to businesses to government entities.

ERM Overview

Enterprise Risk Council (ERC)

While other committees and individual members of the organization play a role in ERM at A, the ERC is the center of the process where inputs are transformed into actionable outputs. The ERC of A is made up of roughly 15 business leaders (VP's) that come together quarterly to discuss risks affecting their areas of responsibility. The ERC is designed so that all business units are represented on the council and thus an individual member can be deemed a Risk Owner. The central duty of this group is to review and discuss the risks identified through the work performed by the ERM functional team. The ERM functional team works in conjunction with the ERC to profile these risks and to ensure that risk profiles are kept up to date. The outputs produced by this group are then sent to the C-Suite level risk committee, Enterprise Risk Governance Committee (ERGC), which provides its own assessment of notable risks, before a presentation is made to the risk committee of the Board.

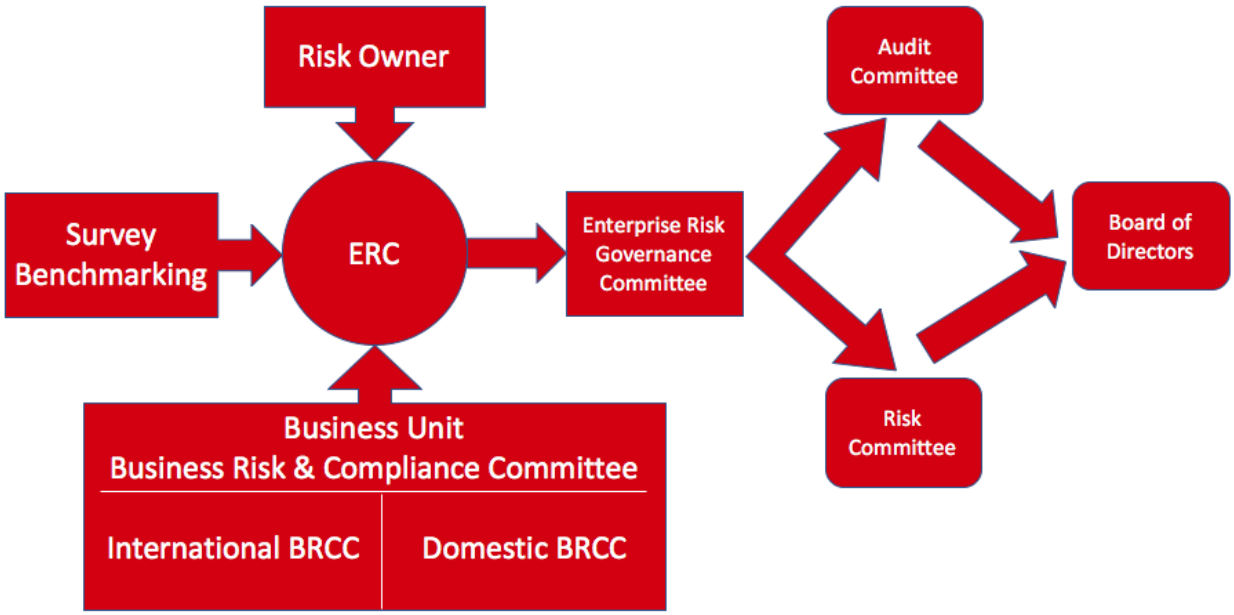


Figure 1

A begins the ERM cycle by identifying risks through the use of an annual survey sent out to approximately 900 business leaders across the company. Identification can also happen at the quarterly ERC meetings although this is rare. Another way that identification can occur is through direct contact with the Chair of the ERC. Risks can be brought directly to his or her attention if thought to be severe enough to warrant immediate ERC action. While the survey serves as the main tool for identifying new risks, A also uses external risk studies and peer comparisons.

The list of risks identified by this process are compiled by the ERM function and then divided up among the responsible business units so that an initial assessment can be performed by the individual who represents each business group on the ERC as well as other members of their team. That person will ultimately narrow down the individual risks identified on the survey into a few key risks that can be assessed more easily by the ERC. A provides a guided scale to help these individuals assess risks. Both likelihood and impact are considered on a five-point scale ranging from Very Low (Insignificant) to Very High (Severe). A provides a description of each of these points on the scale to further assist ERC members in being consistent across their assessments. Once the individual ERC member has narrowed down the risks and provided his or her own assessment, the risks will be discussed by the ERC as a whole. The ERC may change the assessment of the risk if, after discussion, it is agreed that an adjustment is necessary from the initial assessment.

The agreed upon assessment given by the ERC will be used to place the risks into tiers. A categorizes enterprise-level risks into two tiers based on their assessments for likelihood and impact. The number of risks included in Tier 1 is based on the product of the two assessed scores for likelihood and impact. A product of 12 is needed for the risk to be included in Tier 1. For example, a risk that has an assessed likelihood of 3 and an impact of 4 will result in a product of 12 and will be considered Tier 1. A risk that has an assessed likelihood of 3 and impact of 3 will have a product of only 9 and therefore would be considered Tier 2. At the same time, a target rating is assigned for the risk that is based on anticipated effects from the mitigation strategies chosen by the risk owner. Some risks that are specific to a single business unit will not fall under the purview of the ERC because they do not have enterprise-wide impacts and thus will not be considered in the above assessment process.

Each Tier 1 and Tier 2 risk is assigned a Risk Owner that is also a member of the ERC. Each Risk Owner is then responsible for developing a response plan that will bring the risk to the target level assessment. The risk owner will then document the risk and the response plan in a Risk Profile. See example below.

Risk Profile

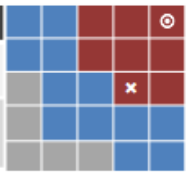
Illustrative

⊙ Current Rating
✖ Target Rating

Tier 1
Tier 2

Preventable ☐ Strategic ☐ External ☑

Risk Category	Sub-Category	MC Sponsor	ERC Sponsor	Risk Owner
Operations / Engineering	Fleet Management	C-Suite	VP – ERC Member	VP Public Affairs VP Engineering



Risk Statement: There is a risk that current legislation will require all delivery vehicles, operating within major city limits, to be electric powered by 2019.

Comments:

Risk Contributor(s)	Control(s) / Mitigation	Function	Status	L	I	Planned Completion
Proposed climate change legislation to lower large city carbon emissions	- Establish relationships with key legislators to ensure Company concerns are addressed.	Public Affairs	Executed	-	-	--
	- Public Affairs to develop impact and response plan to include potential alternative legislation or time extension for implementation of current regulations.		On-going	1	-	Q4-2018
Limited alternatives to current delivery methods in large metro areas	- Current engineering study to identify and / or create alternative delivery options.	Engineering	Planned	-	0.4	Q4-2017
Increased cost of alternative vehicles due to supply and demand challenges	- Current program in place to identify and purchase alternative fuel powered vehicles.	Automotive	On-going	-	-	--
	- Establish with automotive industry priority vender relationships for the purchase of new vehicles.		Planned	-	0.4	Q4-2018
	- Investigate acquisition project to acquire production plant to retrofit current vehicles.	Engineering	Planned	-	0.2	Q4-2018
	- Develop capital budgeting proposal and assess overall impact.	Finance	Planned	-	-	Q1-2017

Figure 2

It is the responsibility of the Risk Owner to track the effects of the response and to update their assessment of the risk before each quarterly meeting. The Risk Owner must update the relationship between the current assessment rating and the target assessment rating. This allows the ERC to discuss the results of the response strategies moving forward.

The ERM function recommends to the ERC specific risks that it believes should be discussed with the Board of Directors. The risks taken to the Board are not simply all of the Tier 1 risks, but only those that the ERC believe are significant enough to warrant notification of the Board. The Board of Directors may also ask management to review with them certain risks when it deems necessary. Prior to any presentation to the Risk Committee of the Board, the ERC will review the presentation with the ERGC. The General Auditor will make that presentation to the Risk Committee of the Board which will then update the Audit Committee of the Board as well as the full Board of Directors.

Evolution of ERM

The company launched ERM 10 years ago and gradually built momentum as it became apparent that the process and the mindset it created were valuable to the organization in managing the risks it faced. In addition, as the company's senior management and board members gained experience with ERM and saw it in place at numerous other companies, their support of the

program grew. That support at the highest levels of the organization is a critical component of a successful long-term ERM program.

Over the past ten years, the ERM process has evolved and grown. The company has had three different individuals leading the ERM process, and each new leader saw opportunities to enhance the process. Some of those changes were designed to align the company's process with industry standards. The central value of an ERM process is found in its ability to capture and make the Aware of potential risk events. As the company found gaps between expectations and reality, in capturing and addressing potential risk events, additional processes were added to address those gaps. Even after 10 years, the company is continuing to make improvements to build a more effective ERM process.

Key Factors for Sustaining ERM

A cited six factors that were important to its ability to sustain an ERM program over time, with the first three being cited as the most critical factors:

- Creation of an Enterprise Risk Council
- Simplification
- Feedback loop
- Clear risk ownership
- ERM training, and
- Evaluation and continuous improvement.

Creation of an Enterprise Risk Council

The Enterprise Risk Council (ERC) is the heart of the company's ERM program. This group formed in 2008 and began meeting in 2009. As discussed above, the ERC is made up of leaders from all major disciplines across the company and meets quarterly to discuss risks facing individual areas within the business as well as enterprise-wide risks. Having an ERC has been valuable in that it helps individuals to see across the organization and understand the interrelationships of risks and how those risks, if not managed effectively, could impact the organization overall. Another key aspect of the ERC is the creation of a safe environment to communicate issues and risks. Having the ERC separated from day-to-day functional activities removes some of the pressure of revealing bad news or concerns. In this way, council members were more willing to open up. As the organization recognized the safe environment within the ERC, individuals outside the ERC have become willing to come forward to identify particular risks or seek help in managing risks.

Simplification

In the early stages of its ERM program, the company experimented with different risk assessment techniques like velocity, and complex interconnected risk models. What it found out was that these techniques were too complex and difficult to understand and it risked having its ERC members disengage from the assessment process as a result. From this, the company learned that keeping the process simple and at a level where it could be widely understood was key.

Currently, the company assesses risks only based on likelihood and impact, maintains concise profiles for its top risks, and produces an overall heat map of tier 1 and tier 2 risks.

Feedback Loop

Over the course of the ERM process evolution, there were some implementations that significantly enhanced the effectiveness of the ERM process. The implementation of a company-wide risk survey about 6 years ago was a key enhancement that began a feedback loop between a broader group of individuals across the company and the ERC. Initially, the survey was just targeted to a small group of the most senior personnel but over time it gradually expanded to 930 people across the entire company. The purpose of this survey is to not only to gather risk information, but also provide insight into how personnel across the company are thinking about risks. Frequently there are risks which can be undetected if there is a weak communication between enterprise level and operational level. By connecting numerous similar individual comments from an operational level, the organization may be able to detect a larger enterprise risk that may have otherwise gone unnoticed.

In addition to the use of the survey, the company also employs interviews with members of the ERGC to ensure it is capturing the views of the top risks and to build risk awareness at that level. The Business Risk & Compliance Committees (BRCC) are another part of the feedback loop which are housed within each business unit and operate similarly to the corporate level ERC. These committees communicate regional level risks on a monthly basis.

Establish Clear Risk Ownership

Another key to the effective long term operation of the ERM program at A is establishing clear risk ownership within the business functions. First, the risks have to be clearly defined and then a risk owner must be designated. The members of ERC own the risks in their areas of responsibility. Those risk owners are held accountable for establishing and maintaining the appropriate controls and mitigation strategies. Risk ownership is embedded in specific positions as opposed to specific individuals in order to ensure clear accountability even when there are leadership changes.

Provide ERM Training

Having people across the organization who understand and appreciate the value of ERM is an important part of sustaining the ERM process. To this end, the corporate ERM function works to ensure that individuals in each business function are knowledgeable about the company's ERM program and their responsibilities for identifying and managing risks. Accordingly, the corporate ERM function ensures that each new ERC member gets the appropriate training to carry out their role. Typically, the ERM function will spend 30-40 minutes explaining the process to new ERC members.

Evaluation and Continuous Improvement

The ERM program provides updates to the ERC and the Risk Committee of the Board of Directors on a quarterly basis. The update not only includes information on the top risks, but also includes any changes or enhancements to the ERM process as well. In this way, both the ERC and the

board's risk committee are formally reviewing and evaluating the ERM process. In addition, personnel in the company's ERM function are regularly comparing notes with peers and experts in the ERM profession to identify practices that may enhance the ERM program.

Currently, the company is working on several enhancements to its ERM program. The first is the implementation of an enterprise-wide IT platform for ERM that will bring together all of the risk information from the various business functions. In addition, the company is working to enhance its annual risk survey by making some questions more specific. Finally, the company is trying to get ERM more embedded in day-to-day operations by working more closely with the BRCC to encourage business unit managers to employ risk management principles.

Conclusion

A has been able to establish and evolve its ERM program over a 10-year period. While support from senior management and the board of directors is crucial at the launch of an ERM program, it will be challenging to sustain unless the program operates effectively. The company's use of the ERC was vital to the effective functioning of the ERM program. In addition, creating a feedback loop to receive and share risk information across the organization was also critical. An important related factor is the ability to keep things simple. If the process was overly complicated it would have made it very challenging to engage the ERC or create a meaningful feedback loop across the organization. The company has recognized and built upon the key strengths of its program and continues to evolve to meet the risk challenges of the future.

APPENDIX – B

Organization Description

B is a large beverage company that markets over 500 nonalcoholic beverages globally. The company has $87 billion in assets, posted net revenues of $42 billion in its most recent fiscal year and employs 100,300 individuals worldwide. The company's beverage empire has been built through its massive network of bottling companies.

ERM Overview

ERM Roles – ERM Function

The enterprise risk management (ERM) process begins with the Corporate ERM Function, which is made up of two full-time employees and facilitates risk management processes. The ERM team's responsibilities fall into two major categories, strengthening risk management governance and building risk management capabilities. Further, the ERM team provides a global risk management framework, improves and shares ERM competencies and reports risk information. The ERM framework is the foundation upon which ERM has been built. Although the company's business units and markets are numerous and varied, the framework delivers consistent internal expectations for ERM across the entity. Now that the framework has been deployed, more sophisticated ERM tools are being implemented. One of these tools is Riskonnect risk management software, which is used as a repository for risk registers and as an ERM communication channel.

Strengthening Risk Management Governance

Strengthening risk management governance involves monitoring ERM policy compliance, performing semi-annual strategic risk assessments and promoting risk culture. As stated above, in 2016, an ERM policy was implemented, explicitly stating the company's requirements and expectations for risk management. The ERM function's efforts to obtain policy compliance are fundamental to maintaining a robust program. Beginning in 2017, the Corporate Audit Department (CAD) will audit individual business units and functions for compliance with the ERM policy. In addition, semi-annual strategic risk assessments, a joint effort by the ERM team and CAD, are performed to certify that top risks are identified and assessed. The performance of the ERM function, business units and other company departments is measured with respect to ERM duties. Updating of risk registers within the Riskonnect software and refreshing associated heat maps is another aspect of this process. Finally, generally promoting risk culture is a major governance function of ERM.

Governance roles exist both internally and externally. Internal governance includes ensuring both corporate functions and business units understand their top risks and report ERM progress to the Board. External governance requirements relate to the company's status as a public corporation, such as risk disclosures displayed in SEC 10-K filings. The ERM team verifies that top risks are prioritized, risks have clear owners, mitigation plans are documented for top risks and a regular dialogue exists with business units. The governance role of ERM positions the program as a strategic resource.

Building Risk Management Capabilities

Building risk management capabilities involves consulting with business units and corporate functions. It also relates to performing risk workshops, facilitating risk management capability assessments, distributing ERM best practices and providing advanced risk data analytics. Risk workshops are one-time events where the ERM team makes an initial visit to a location to implement ERM. The business unit president, CFO, strategy lead and local ERM process leader must all be present for a workshop to take place. Business unit leaders are offered a list of over 300 risks that affect various areas of the company to provide a beginning point for risk identification. Business units then assess and prioritize identified risks into a list of the top five to fifteen risks. Deliverables from this two-and-a-half-hour meeting are a risk register highlighting top risks, along with assignments of top risks to singular risk owners. Afterward, the ERM team holds discussions with business unit leaders concerning causes and consequences of top risks, as well as mitigation plans. The risk workshop serves primarily as a strategic exercise, as risks are deliberated in the context of business objectives. Business units are tasked with refreshing and submitting their risk registers semi-annually, focusing on top risks. The local global ERM process leader is accountable for this requirement.

Risk management capability assessments (*Figure 3*) are completed at the business unit level every two years to communicate what constitutes effective ERM. This assessment is one of five ERM policy requirements, defines expectations for risk management and sets an effectiveness baseline to measure progress maturity and progress. A few of the dimensions of the assessment seen in *Figure 3* below are management commitment, framework and tools and risk assessment processes. Participants in the assessment must include the president, CFO, strategy lead and ERM process leader within individual business units. These leaders undergo a self-assessment consisting of 22 specific risk management attributes that define an effective and holistic ERM approach. After completion of the self-assessment, the Corporate ERM team leads a follow-up conference call with the leadership team to calibrate responses and confirm the baseline. Importantly, the Corporate ERM team also assigns the leadership team two to three tailored recommendations. Per the ERM policy, all recommendations made by the ERM team must be implemented. This commitment ensures that each location continues to mature its risk management program. If recommendations for improvement are necessary, the focus is on only a few that will add the most value for business units. Due to the periodic nature of these assessments, business unit progress is monitored and ERM evolution can be measured. Performing the risk management capability assessment at the local level ensures that operations and business units can collectively contribute to advancing the maturity of the company's enterprise-wide ERM program.

In its consulting role, the ERM team disseminates best practices across the organization. These best practices are routinely shared internally by the ERM team with global ERM process leaders through their ongoing interactions. Methodologies are also discussed externally at a regional risk council, a meeting of the minds held by large companies headquartered in the company's region. Finally, risk data and analytics are increasingly used by the company to provide insights related to developing trends that impact the company.

ERM Roles – Other Personnel

Risk management is performed at all levels of the company, including employees further down the corporate ladder. At the operational and business unit levels, several positions are crucial to sustaining ERM, including the president. When the ERM team travels to a business unit location to perform ERM duties, obtaining support from the operational and business unit president is the top priority. Consequently, those within the business unit recognize the importance of ERM when their leader is on-Board. Next, the ERM process leader is designated as the ERM contact, with a related assessment following to ensure this individual is sufficiently supported. The ERM process leader is the "local" risk owner for the business unit. These process leaders are located within corporate functions, business units and bottlers groups and dedicate about five to ten percent of their time to ERM. The ERM team maintains regular contact with all 65 process leaders, ensuring ERM is effective within business units. Business unit leaders know their function better than anyway and do not usually contact the Corporate ERM Function for concerns due to the enormity of the company. It is imperative that leaders within units are competent with respect to ERM, as leaders of business units essentially run their own miniature ERM program. Then, the ERM team brings the overall process together across the enterprise.

B maintains an ERM governance structure consisting of the Board of Directors, executive management, Risk Steering Committee, Corporate ERM Function and global ERM process leaders. The audit committee of the Board ultimately oversees ERM, with other Board committees providing supervision over respective top risks. The CFO and COO serve as executive risk sponsors for ERM. The Risk Steering Committee, comprised of roughly 20 senior leaders just below the C-suite, represents the governance assurance body overseeing the company's top risks. Respective risk owners must present their top risks, along with related mitigation strategies, to the steering committee if the risks land within the top two tiers of the risk hierarchy. Major risks are allocated to three tiers, with tier one risks being the most material. This process is performed monthly, focusing on a couple major risks topics at each committee meeting. This ongoing, monthly routine of top company managers discussing risks inherently sustains the program. The objectives are to provide assurance that top risks are managed effectively and to leverage the collective expertise of the cross-functional committee to identify potential gaps and opportunities. Before respective risk owners discuss risk information in front of the steering committee, the ERM team coaches them due to the severity of any risk going before the committee. Steering committee members bring an enterprise-wide lens to the top risks of business units.

Internal Environment and Connection to Strategy

The internal environment and risk culture at the company is fundamental to its ERM journey. Success in maintaining a strong risk culture and internal environment is closely related to the approach originally taken in introducing ERM to the organization. The company took a "carrot" approach to implementing ERM by establishing and communicating the value of the program. This technique allowed company leaders to understand ERM and its benefits to areas they led.

Although the company's ERM process is linked to strategy, it is admittedly a work in progress. Maintaining an interplay between ERM, strategy and operations is central to sustaining ERM over

time. The connection between ERM and strategy can be viewed through two lenses. First, a business unit perspective can be taken, where routines to ensure sustaining of ERM are in place. Accordingly, ERM is an input and output of the strategic planning process for business units. For instance, the unit's strategic plan is compared to its risk register to determine whether risks are addressed by strategic objectives. Then, any newly identified risks are added to the risk register. Second, a corporate perspective can be taken to understand the linkage between ERM and corporate strategy. A connection between ERM and strategy is being built through working with the corporate strategy team, including regularly communicating and sharing top risks. For example, ERM has become an agenda topic during the strategy team's global meetings. During this meeting, the Corporate ERM team is able to share risk insights, include geographic risk profiles, which becomes a key input to augment local strategic planning efforts. ERM is embedded into routines for both one-year business plans and 3-year strategic plans.

Embedding ERM principles into existing business processes and planning cycles has also aided in linking ERM, strategy and operations. The process is sustained as an aspect of regular operations, with business unit leaders making an explicit commitment to the program. There is little to no distinction between risk management and business planning. The company has found that executives are considering risks while making strategic decisions, albeit on an implicit basis. The ERM team would like to see growth in the explicit contemplation of risks by senior management. The risk management capability assessment, described above, is performed at the business unit level and is another way to link ERM with ongoing operations.

Identification and Assessment

B employs several techniques to identify risks at multiple levels of the company. Identification methods, number of risks identified, frequency of risk updates and other factors vary based on the location of business units. The company mainly utilizes surveys for its risk identification process. Surveys allow specific risks to be identified for business units, with those risks being consolidated across the enterprise. The most recent survey uncovered roughly 350 risks to be included in the risk universe. Surveying functional leaders is typically completed as part of risk workshop pre-work activities. The ERM team recommends that business units only perform these comprehensive surveys every four years or when a substantial business change occurs. Operational units are given flexibility in determining survey frequency, allowing business unit leaders to decide what adds value. For company locations that have not previously performed risk identification, the ERM team teaches business unit leaders best practices during risk workshops. Often, business units inquire about other locations' top risks to understand what could be a top risk for themselves. After the workshop, business units are better equipped to independently perform risk assessments.

Once surveys are completed, the identified risks are discussed with cross-functional business unit leaders. By design, no one person completes the entire survey. Risks are allocated to the departments in which they impact and logically assigned to individual risk owners. Typically, 20 to 40 risks are assigned to each department. Then, departments filter and prioritize their own top risks. After this initial process, the collective knowledge and experience of those participating in the meeting is leveraged in a "whiteboard exercise." This exercise elicits a discussion about top

risks of the entire company. Debate ensues until consensus is reached on the top five to fifteen entity-wide risks. Within the Riskonnect software tool, top local risks can be consolidated and summarized into company-wide broader risk themes, a more digestible format for the Board. Although input from business unit locations is considered when prioritizing top entity-wide risks, business unit risks are not necessarily directly rolled into the top 32 risk themes. Instead, the ERM team examines top risks affecting company departments, understands which risks impact the entire company and uses this information when prioritizing top risks. Tier one risks, the most severe, are reported to the Board annually. Tier two risks, a step below, are only reported to the Board as needed. In addition to top risks, the report to the Board covers the overall ERM process, successes and areas for improvement and an output from strategic risk assessments. As seen above, business unit leaders may be requested to present before the Risk Steering Committee on top tiered risks.

Assessment of risks is performed using dimensions of likelihood and consequence on a five-point scale. Velocity has recently been introduced as a third assessment dimension at the corporate level on a three-point scale. Velocity identifies risks that require proactive risk treatment strategies to be in place and ready for immediate implementation, such as natural disasters. The use of velocity is limited to the corporate level for simplicity.

Risk Responses, Communication and Monitoring

Due to the Corporate ERM Function's primary role as ERM facilitator, the function does not own specifics risks, respond to risks or perform monitoring. Risk owners, who are assigned risks related to their business unit, are responsible for managing, responding to and allocating resources to mitigate specific risks. They also monitor risks relevant to their business unit. Business unit leaders are required to maintain documentation related to mitigation of their top risks. Risk owners are monitored by CAD to ensure proper risk management accountability and risk responses.

Risk information is communicated across the entity by aggregating information collected from individual business units and locations. B's size and complexity makes it essential to provide business unit locations with flexibility in reporting risk information.

Evolution of ERM Process

B employs a robust ERM process today. First introduced by an executive over ten years ago, the concepts embedded in ERM gained the support of numerous managers over time, who applied the principles of risk management into their areas of responsibility. Since the program's beginning, the company has formed a Corporate ERM Function, developed an enterprise-wide process and evolved ERM to the point of being sustained. The original goal was to prove the value of an enterprise risk approach and then expand the budding risk management process into an entity-wide global ERM program. After demonstrating its value, program progress began to accelerate with the hiring of two dedicated resources, including an ERM Director in October 2010. Undertaking this process evolution required the support of many within the organization, including executives and leaders of key functions. ERM development was driven primarily by these leaders in concert with the Corporate ERM Function. Around this 2010 timeframe, B's

Board of Directors began independently engaging in discussions about ERM and requiring an annual report-out, signaling an organizational trend. The program was not spawned as a mandate from the Board, but rather, out of a groundswell of support from many at the top of the company.

B's ERM program has evolved over the years by tailoring the process to fit the company's culture. Accordingly, the company began with the ISO 31000 ERM framework, building upon this literature and modifying the program to fit the company. At the genesis of the program, ERM did not connect with business units and was simply a corporate process. A major factor in the evolution of ERM relates to pushing the program down into operations, including the business units. The future progression of ERM at B surrounds the use of risk data. Now that the ERM framework has laid the foundation for the program, the ERM team is pursuing data analytics and the development of Key Risk Indicators (KRIs). The ERM team will be able to anticipate risk events more precisely.

ERM process evolution can be viewed in a timeline format in *Figure 1* below.

Key Factors for Sustaining ERM

B has identified several success factors that have been essential to sustaining ERM. These key factors include implementing the company-wide ERM policy, maintaining connections with business units, advancing risk culture, obtaining executive buy-in and communicating the value proposition of ERM. A section for lessons learned is also included to highlight additional success factors that the company has experienced over time.

Implementing an Enterprise-Wide ERM Policy

As previously described, the company-wide ERM policy put into action in 2016 sets out specific requirements related to risk management for all operations, which is comprised of 65+ locations. The policy was jointly announced by the CFO and COO, demonstrating to employees its entity-wide nature. Explicit expectations for risk management are presented in the policy, which is reinforced by the involvement of C-suite executives. The uniform, enterprise-wide approach to ERM that the policy provokes will work to sustain the program. Employees will understand ERM and their roles within the process. With its value proposition and requirements firmly established, the ERM policy will be sustained going forward as a normal part of operations. The major five requirements laid out by the ERM policy can viewed in *Figure 2* below.

Maintaining Connections with Operations and Business Units

Sustaining ERM is one of the primary objectives of the risk workshops held by the ERM function. As part of the workshop, business unit leaders are required to make a commitment to ERM and to input procedures to sustain the process. This commitment entails an agreement to include ERM as an explicit agenda topic in quarterly meetings, consider the business unit's risk register in strategic planning and undergo a risk management capability assessment every two years. ERM becomes a regular piece of operations for business units after risk workshops are completed. Identified and prioritized risks are documented in the risk register and a routine is installed to discuss top risks in the future. Thus, ERM is integrated into existing business routines. Additionally, a baseline for ERM capability is established, ensuring that all business units can

effectively participate in a truly entity-wide program. Due to the commitment made by business unit leaders to include ERM as a normal part of on-going management routines, the program is naturally sustained at the business unit level.

Preserving a connection between the ERM function, business unit leaders and global ERM process leaders is vital to sustaining ERM, especially in a company the size of B. Each quarter, the ERM team meets with 65 global ERM leaders to share best practices and build risk management capabilities. All ERM leaders meet with the ERM function through a videoconference, with three sessions held in a single day to accommodate time zone differences. These meetings cover process topics and risk topics. Process topics focus on necessary ERM procedures and duties to be performed by business units. For example, discussions about using risk management software to generate simple reports to support leadership risk discussions would be considered a process topic. Next, risk topics emphasize particular risks that are selected and communicated to meeting participants in advance. In the previous quarterly meeting, a series of risk topics are presented to and voted on interactively by ERM process leaders. Votes are tallied and the risk topic with the most votes is selected for discussion in the following quarterly meeting. In that next meeting, the ERM team coordinates with the company's subject matter experts, who educate the group, provide best practices and answer questions on the chosen risk topic, followed by an open conversation on the matter. For example, during one quarterly session, the global ERM Process leaders selected Currency Exchange risk as the risk topic so the Corporate ERM team worked the Treasury department SME to address this timely risk topic. This quarterly process plays a major role in sustaining ERM, as an ongoing communication channel is established with business unit leaders. These employees are on the front lines and help ERM to be applied in day-to-day operations, sustaining the program.

Advancing Risk Culture

Furthering risk culture has been a point of emphasis for B, especially in regards to sustaining the ERM program. Risk culture is defined by the company as proactively managing risks to the company. Therefore, risk management should be naturally intertwined with making decisions to achieve business objectives. Risk culture also holds all within the Accountable for their risk management duties. Advancing risk culture has taken place through various forms of training. The use of B's ERM e-learning course has been an avenue for educating employees on ERM and spreading a common risk language. To date, over 2,500 global leaders have completed this on-line training. Additionally, substantial in-person ERM training is performed through global lunch-and-learn web-ex sessions, finance training classes and supply chain leadership development classes. Employees are continually trained to sustain ERM in the face of any employee turnover that may occur. Outside of education and training, the Risk Steering Committee, risk management capability assessments and risk workshops emphasis risk culture. Evidence of success in promoting risk culture is evident by B's CEO emphasizing a "culture of driving risk" in meetings.

Obtaining Executive and Business Unit Leadership Buy-in

Receiving support from executives has been pivotal to the company's success in sustaining ERM. Without top executives understanding the value of ERM and pursuing a robust program, sustaining ERM would not be possible. The attitude executives take toward the process

significantly impacts risk culture and opinions of employees below. The tone at the top and executive leadership's support for ERM was reinforced when the COO and CFO announced the ERM Policy in 2016.

In addition to executives, business unit leader buy-in was also crucial to promoting and sustaining ERM. Initial success in obtaining buy-in from business units began with a Production and Operations Group (POG) from 2010 to early 2012. POG consists of bottlers that were originally separate entities from B, but that were acquired by the company. The CFO of POG was the first high-level executive within the organization to request ERM's services. The ERM team seized this opportunity and implemented ERM at 15 POG global locations, which helped to bring "operational credibility" to the program in its developmental stages. After implementing ERM in all POG locations, the ERM team expanded its reach to other sectors of the company and have now employed ERM in all global manufacturing locations and nearly all business locations. Prior to executing ERM with POG, the ERM program only had a corporate focus. However, successful implementation of ERM within POG caused executives and business unit leaders to realize the potential value of ERM, helping to expand and sustain the program. By the end of 2016, an estimated 95% of all global operations had implemented ERM, capping a three to four-year process. The ERM team has established routines and monitors ERM policy compliance to ensure the program will be sustained at each of these locations. To date, the ERM team has not found it necessary to revisit these locations.

Communicating Value Proposition

For those within an organization to view ERM as more than a compliance exercise, the value of the program must be communicated. B has overcome this obstacle by underscoring a "carrot approach", illustrating the value of ERM at both corporate and business unit levels. Utilization of a carrot approach is apparent by the voluntary cooperation of operational units. Operations and business units recognized the value of ERM and often sought Corporate ERM team support to implement ERM before being required to do so by the ERM policy. Thus, the implementation of the policy served as the "stick approach" portion of the equation, while initial efforts to sustain ERM represented the "carrot." A carrot approach is particularly important when engaging a business unit location for the first time, usually as part of the preliminary risk workshop. After the value of ERM is displayed, the program is more likely to be sustained, as employees will desire the program's benefits in the future.

Other Success Factors and Lessons Learned

During its ERM journey, B has learned various lessons relevant to sustaining a program. The major takeaway is that simpler is better for ERM. For example, pushback was experienced from employees when traditional ERM language was disseminated throughout the organization. The ERM team abandoned this overly complex verbiage and embraced a simple, non-academic risk language. As an example, the company eliminated the term "residual risk", instead using "current state." Also, inherent risk has been completely removed from ERM terminology because it was too theoretical. Simplifying risk language encourages employees to regularly use risk management terms without being overwhelmed. Keeping this language alive helps to strengthen and sustain ERM going forward. Simplification has also occurred through replacement of complex

risk management software with less complicated and more user-friendly Riskonnect risk management software that employees can better handle.

In addition to simplification, understanding that "process leads technology" has been important to B's ERM journey. Once an ERM process is defined, technology can be implemented that accentuates strengths of the program. This has been done at the company with the deployment of the Riskonnect software. The new software is used by employees to submit risks to their risk register, reinforcing the ERM framework. Employing appropriate technology only after the ERM process is established is fundamental to sustaining a program.

Conclusion

B employs a robust ERM process and has significant measures in place to ensure that the program will be sustained into the future. With the key success factors stated above, B has positioned itself to maintain an impressive ERM process going forward. Cultivating a strong relationship with company departments, obtaining organizational buy-in and furthering risk culture are a few crucial components to sustaining an ERM program. B has developed a mature and sustained ERM program by implementing these success factors.

Figure 1 – Timeline of Major ERM Events

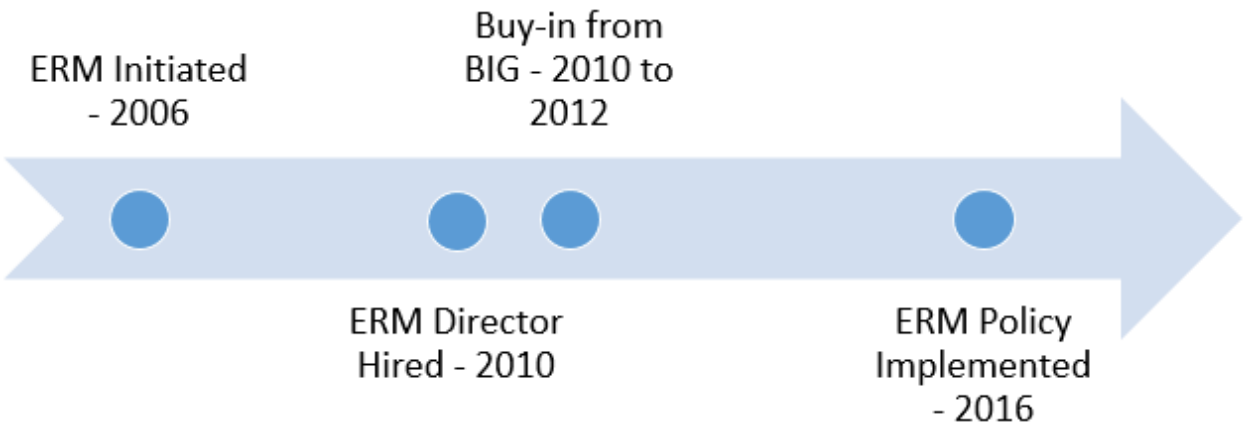


Figure 2 – ERM Policy Components

ERM Policy Requirements
(1) Maintain prioritized list of risks
(2) Actively manage & monitor risks
(3) Report risks to Corporate twice per year
(4) Functioning ERM Process Leader
(5) Complete a capability assessment every two years

Figure 3 – Risk Management Capability Assessment Example

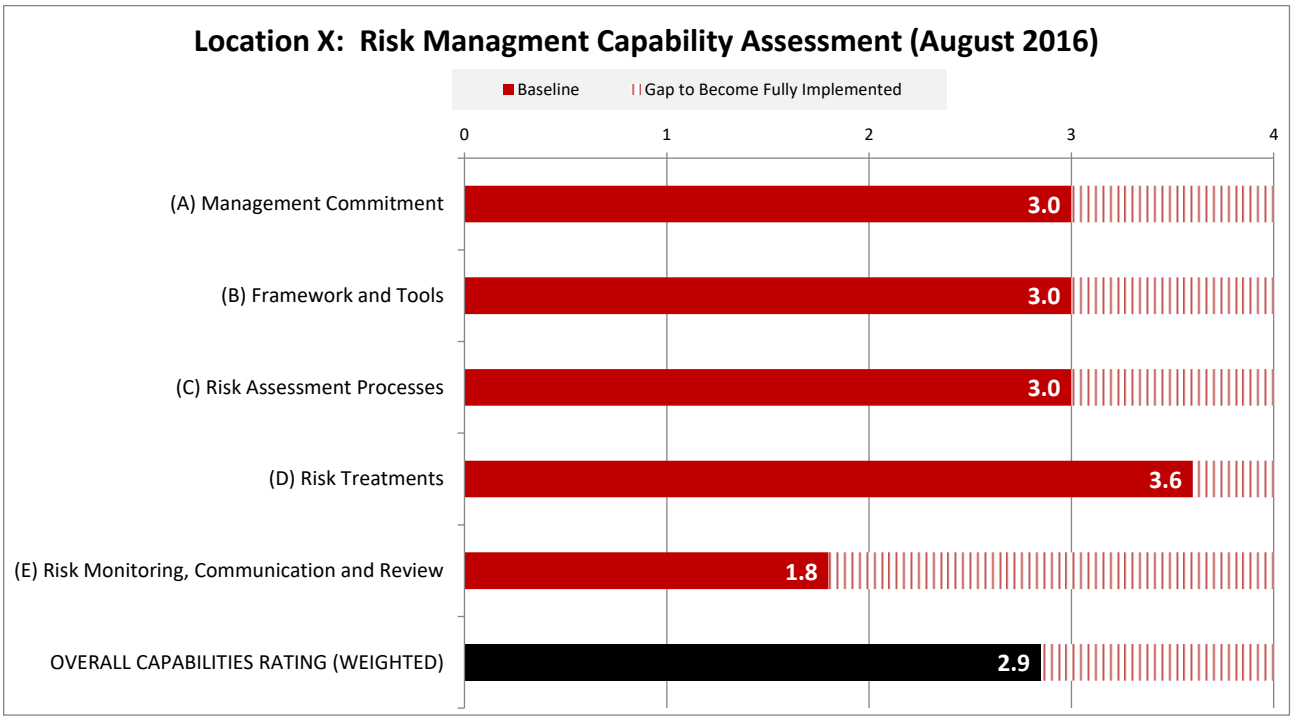
Location X: Risk Management (R/M) Capability Assessment Summary	**Dec 2016**

Location X leadership team completed a risk management capabilities self-assessment and participated in a 'calibration' conference call facilitated by the Corporate Enterprise Risk Management (ERM) team in Corporate City X. These notes supplement the actual Risk Management Capability Assessment that was completed. The calibration call consisted of a brief review of the Company's ERM program as well as a review of the five ERM policy requirements outlined in SPP 2.1:

1. Maintain a prioritized list of top risks
2. Actively manage and monitor risks
3. Report risks to corporate twice per year
4. Assign a functioning ERM process leader
5. Complete a risk management capabilities assessment once every two years

The completion of this self-assessment, the completion follow-up calibration meeting, and then taking action on the specific recommendations outlined below will fulfill the risk management capability assessment requirement outlined above. Call participants included (insert name) - BU President, (insert name) - Vice President Finance, (insert name) - Vice President, Strategy & Insights), (insert name) – ERM Process Leader and Corporate Director Enterprise Risk Management.

After the introduction of ERM and the policy, the discussion shifted to the results and findings of the recently completed Risk Management Capability Assessment. Location X self-assessed a score of 2.9 on a scale of 1 to 4 which is an improvement over their 2014 score of 1.9. The key strengths and opportunities documented within the Risk Management Capability Assessment are detailed on the next page.



Key Strengths – Effective Risk Management Processes Working Well Today:

- **Increased Awareness Amongst Leadership Team and Bottling Partners** – The risk workshop conducted in June 2015 played a key role in developing proactive mitigation plans for Location X top risks. The proactive plans put in place to manage business disruptions due to monsoons worked quite well. Other companies in for Location X did not fare as well and had a lack of water supply which was not an issue for Location X.

- **Proactively Managing Taxes and Regulation Risk** – Project Sparkle helped build risk mitigation plans to manage these risks by enabling a cross-system team to manage tax and regulatory risks. More recently Project Sparkle has been integrated into the Renewing Category Growth routine which is supported by (1) weekly reporting via the GSD update and (2) a monthly global call led by the global PAC organization.

- **Risk Sensing Capabilities** – Real-time and quarterly routines are in place to help inform risks that could impact the business. The routines help Location X more proactively manage PR-related risks. APCO is a PR consulting firm that sensitizes the Company to government-related risks on a real-time basis. In addition, two Advisory Boards (Community & Environment and Science and Regulatory) provide insights into what they are seeing in terms on new regulations, NGO activities, new packaging laws, solid waste management, etc.

Specific Recommendations to Increase Risk Management Capabilities (to be completed by Location X):

1. **Implement Scenario Planning Routines:** Building upon existing planning routines, scenario planning will be implemented to help manage business uncertainty for key risks (e.g. local competitors increase their market share) in the 2017 annual business planning process. This approach will enable the development of proactive mitigation plans and supplement corporate reporting routines.

2. **Add ERM as an explicit topic in quarterly Leadership Team meetings:** While functional teams are really good at managing their respective risks (e.g. legal has monthly routines in place), establishing an integrated leadership routine focused on risk management will improve overall risk visibility and ensure top risks are discussed cross-functionally and included in business planning routines. Moving forward, ERM will be included as an explicit agenda topic in quarterly LT meetings. Location X's risk register will be updated as needed, documented, and submitted in Riskonnect.

3. **Establish A Regular Continuous Improvement Routine:** At least once per year, select a recent IMCR or business disruption event, conduct a key learnings sessions, and document key findings (e.g. simple 1-2 pager of what worked, didn't work, and process enhancements). Share and discuss key findings, both internally and with bottling partners, and align on process improvement action items. In addition, share documented key learnings with the Company's global IMCR process coordinator, and the Corporate ERM team to facilitate global best practices sharing.

APPENDIX – C

Organization Description

C is a holding company, consisting of several wholly-owned subsidiaries in the electric utilities industry. The various subsidiaries provide electricity, natural gas and steam to customers in the northern United States. Subsidiaries also participate in energy infrastructure projects and provide energy-related products and services throughout the United States. C employs nearly 15,000 individuals, has $48 billion of total assets and posted $12 billion of net operating revenues in its most recent fiscal year.

ERM Overview

C has employed an enterprise risk management (ERM) process since 2004. The program was initiated as part of a request from the Board of Directors, which set a strong tone at the top in support of ERM. The early renditions of ERM targeted operational energy-related risks, which is common in the highly regulated utility industry. Although risk to operations is still the centerpiece of the process, C has transformed an energy-focus, operational risk management approach into a mature ERM program.

The ERM Process at C is maintained through an interplay between the Board, ERM Steering Committee, ERM Corporate Risk Committee and the ERM department. The governance structure of the program begins with the Board, which provides oversight of the process and top entity-wide corporate risks. The ERM department meets with the Board annually to present ERM-related information. The ERM department includes the ERM director and four other employees, who jointly facilitate the program. The ERM director is responsible for providing leadership over the program, implementing ERM initiatives and training employees. Next, the ERM Steering Committee, chaired by the CFO, is comprised of Senior Vice Presidents from various departments and leaders of corporate legal, audit and compliance functions. The Steering Committee meets bi-monthly to discuss current trends, ERM process changes and fluctuations in risks. Major changes to the ERM program require approval from the Steering Committee.

The ERM Corporate Risk Committee, consisting of officers, general managers and departmental directors, meets quarterly to discuss risk matters and emerging risks. Risk committee members are usually at the General Manager/Director level and are closer to operations. Corporate Risk Committee meetings are held to update corporate risks and evaluate risks that may be elevated to the corporate level. At the meeting, votes are casted to come to consensus about assessment of risks. If a risk is determined to be worthy of being elevated to the corporate level, the relevant risk owner would be called upon to present before the ERM Steering Committee.

Risk identification occurs using both top-down and bottom-up methods. Risks are identified from the top down by the ERM Steering Committee, which scans the landscape for higher-level emerging risks. Benchmarking against other companies is another way to identify risks from the top down. Meanwhile, departments across the organization identify from the bottom-up lower-level risks affecting particular business units. A bottom-up approach is also utilized by the ERM

Corporate Risk Committee. As described above, a risk coming from directors of operational units can be elevated to the status of "corporate risk" based on a qualitative analysis of the risk issue and a vote of Risk Committee members. Thus, risks can receive corporate-level attention through a bottom-up risk identification and assessment process. These two levels of identified risks are subsequently merged together to provide a broad risk perspective. Roughly 400 departmental risks have been identified within the risk universe, with many repeating across business units. The ERM department meets with all approximately 30 business units annually to update risk profiles and determine whether risk assessments need to be adjusted. Identified risks are categorized based on the corporate sector impacted by the risks. Then, the ERM department considers the way in which risks assigned to a particular category can affect other categories, adding an enterprise-wide perspective. After consolidation of similar risk wordings, about 260 unique risks exist in the organization's risk register.

Identified risks, both corporate and departmental, are assessed and prioritized. Risks are assigned to a risk owner, who is responsible for managing the risk. The risk owner is generally a subject matter expert (SME) well-equipped to manage the risk. Using the most-probable worst-case scenarios, each risk is assessed on three dimensions: severity, likelihood and controllability. Severity factors include financial, safety and reputational components. Likelihood factors are determined by looking at past events as well as current probabilities. Finally, controllability evaluates the Organization's ability to prevent and detect an event. Each dimension is scored on a 10-point scale. Then, the severity, likelihood and controllability scores are multiplied together to generate an aggregate score for each risk on a 1,000-point scale. A blank template of this risk assessment tool, as well as a further explanation of its operation, can be viewed in *Figure 1* below. This quantification helps to prioritize risks effectively. SMEs contribute qualitative input to aid with risk prioritization, as operational risks can be difficult to quantify. C not only manages risks that are likely to occur, but also identifies and assesses high impact, low probability risk events, often termed "black swans." C-suite executives and SVPs are asked to identify black swans relative to their department and may report their findings to the CEO.

Appropriate risk management strategies are developed based on risk assessment. Root cause analyses are fundamental to eliciting a proper risk response, as the identification of the sources of risks leads to more effective mitigation. The company makes use of a bow-tie analysis, which promotes thinking about the "causes" of risks and current preventive measures. However, if little control can be exercised, focus shifts to minimizing the "consequential impact" of potential events. The bow-tie analysis aligns with the controllability dimension in risk assessment. Accordingly, an informed decision can be made as to whether risk responses will center on causes or consequences. The bow-tie has facilitated creation of key risk indicators (KRIs) based on identified risk root causes. A KRI dashboard has also been formed to monitor risk trends. The company thinks of KRIs as a stoplight, with the colors of the light signaling whether a risk requires more attention. A risk's cause, mitigation strategy and KRI are all linked, allowing for an organized and timely response. A risk's mitigation strategy is less of a risk response, and more of an ongoing activity in place to address risks continually. KRIs and bow-tie analyses indicate whether additional mitigation efforts are necessary. KRIs and bow-tie analyses also provide quantitative, data-driven monitoring over significant risks. This quantitative data is combined with qualitative

input solicited from SMEs to determine a proper risk action. Together, these data-driven and subjective perspectives merge as part of monitoring practices.

C uses a variety of methods to communicate risk information, including a risk dashboard and an annual report to the Board of Directors. The Board report, presented annually to the Board by the ERM director, details the top 14 corporate risks identified and monitored by employees and the ERM department. Each key risk is reported in a single-page, standard template. The chosen risks rotate from year to year, except for a few recurring, pivotal risks. Each of the 14 corporate risks are generally included in a presentation given by risk owners at the officer level at least once in a three-year cycle. Presentations and related materials are provided to the Board in a consistent reporting format to promote readability and Board engagement. C performs monitoring over its ERM program through both subjective and data-driven perspectives. Subjective, qualitative input is solicited from SMEs to determine when risk action should be taken. Conversely, data-driven monitoring techniques are also utilized, such as bow-tie analyses and KRIs, discussed above. Subjective and objective information is combined to perform effective monitoring.

To ensure that ERM influences strategy, the ERM department holds regular conversations with the Vice President of Strategic Planning. These ongoing meetings contribute to sustaining ERM, as a constant interplay between ERM and corporate strategy is created. ERM is also involved in department-level strategy. ERM is embedded into operations in a variety of ways, including the engineering aspect of the company's operations. Engineers design programs to address risks by utilizing quantitative analysis. Resulting data is input into the ERM process to craft tailored solutions to risks. Solutions are implemented at the day-to-day operational level. For instance, particular attention is paid to underground gas pipes located in high-traffic areas. These pipes are prioritized over gas pipes in less risky areas when updating equipment.

The way in which the ERM program is viewed within the organization is inherently tied to the ERM director, making the perception of this individual important to sustaining the process. The ERM director position is viewed favorably at C, as is illustrated by the director's ability to contact anyone within the About a risk concern. Specifically, the director's monthly meetings with the President, semi-annual reports to the audit committee and annual reports to the Board represent vital channels of communication. Outside of operations, the corporate audit and compliance functions are also heavily involved in executing ERM. The audit department uses a program created by the ERM department to plan its work for the year, taking a risk-based approach. The compliance department is intertwined with ERM due to C's industry, as well as the increased regulation seen overall. Even research and development uses ERM data by developing solutions for major risks tracked by ERM.

ERM is integrated within many facets of the company, one of which being the budgeting process. A risk factor is considered by the company when determining funds to be allocated to various projects and departments, speaking to ERM's involvement. Additionally, ERM engages in annual meetings attended by top officers and company departments. After these meetings,

departments make presentations before the CEO and President, requesting funding for projects. Thus, ERM is fully embedded within the budgeting process of C.

Evolution of ERM

C has employed a formalized enterprise risk management (ERM) process since 2004. The program was initiated as part of a request from the Board of Directors, which set a clear tone at the top in support of ERM. Afterward, several executives strongly supported the program, namely the CEO and CFO at the time. Each successive CEO has embraced ERM to an even greater degree, naturally sustaining and strengthening the program. Having the top corporate officer in-tune with ERM is fundamental to facilitating a desirable risk culture.

The initial perception of ERM focused on the fact that the Board initiated the program. Thus, it was essential that executives demonstrated buy-in and were not simply following orders from the Board. Early adopters of ERM within the company effectively described the value of ERM in taking an enterprise view and leveraging existing risk management processes. That message helped the company obtain buy-in from executives and managers across the organization over a three to five year-period after initial implementation. At that point, it became clear that the ERM process was permanently embedded in the organization.

Much of the success in eliciting acceptance of ERM stemmed from middle managers. These individuals were frequent participants in ERM committees and worked intimately with the ERM director. As these middle managers grew into more senior positions, they continued to support the program, helping to elevate ERM to the top of the organization. This assisted in sustaining the program, as well as creating a risk culture that recognized the value presented by ERM. Support from the organization's general counsel was another important factor in the advancement of ERM. Originally, the company's legal team was concerned about the possibility that the documentation of risks could be used against the company in a legal proceeding. However, the legal team discovered that documenting risks and mitigation strategies could be useful as a litigation defense, creating evidence to support the company's legal positions. Finally, the timing of ERM adoption by C provided a unique opportunity. The Commenced an ERM program in 2004, well before most utility companies were interested in the topic. At the time, the company did not have access to rich ERM information that has been produced during recent years. However, initiating a program 13 years ago allowed for the design of a more tailored process.

Prior to the Board's initiation of ERM, risk management strategies existed within the organization, but were enhanced by an organized ERM effort. The early renditions of ERM primarily focused on energy-centered operation risks, while secondarily covering strategic, reporting and compliance risks. Risks are now classified into the following categories: Operations, Regulatory/Compliance, Financial/Strategic, People and Technology. In addition to the COSO framework, benchmarking was key to launching ERM, with processes of other companies serving as a starting point. As the program has matured, internal risk conversations have increased in focus and frequency.

Key Factors for Sustaining ERM

C has identified several success factors that have been fundamental to sustaining ERM. These key factors include focusing on major risks, constantly evolving the process, holding discussions with executives, utilizing risk data and effectively presenting risk information to the Board.

Focus on Major Risks

C has found that concentrating on top corporate risks works to create and sustain an effective ERM process. After top risks are identified and assessed, risk mitigation strategies are central to realizing a program's value. Tying budget dollars to the mitigation strategies of top risks ensures an effective risk response is applied. Additionally, including mitigation plans in the strategies of business units allows for a granular risk response, while sustaining ERM's place in operations. For example, budgeted resources are allocated to the mitigation of top risks, such as updating equipment to alleviate the overall risk of a hazardous event occurring.

Constantly Evolve ERM Process

C attempts to add new elements to its ERM process each year, making constant improvements. As an example, the ERM department introduced the concept of high impact, low probability "black swan" events last year. Going forward, the ERM department will offer to discuss emerging black swans, as well as their triggers, on an annual basis with company departments. C develops many of its new ideas through benchmarking with ERM programs of other companies, both inside and outside of its industry. The Focuses on keeping an open mind to identify best practices, regardless of the maturity of the ERM programs studied. The ERM department attempts to keep the program fresh by encouraging employees to take a new perspective on previously identified issues.

Evolution and sustaining of the ERM process has been realized over time through standardization. An example is the use of an e-learning course. The course is available online to employees and communicates a uniform ERM message across the enterprise. Due to its success, the ERM department encourages use of the e-learning module as part of the onboarding process for new employees. The module is promoted to all employees, which is particularly valuable as ERM is integrated into many aspects of the organization. Standardization is also infused with the ERM department's annual Board presentation.

Hold Discussions Between the ERM Department and Executives

Connecting the ERM department with executives is pivotal to keeping ERM involved with strategy and operations. C's ERM department partakes in an annual meeting with the President, CEO and COO, along with other company departments. Additionally, the ERM director meets with the President monthly to discuss risk issues. These meetings serve to maintain a relationship between ERM, strategy and operations. Also, the meetings allow the President to alert the ERM director of any risk items covered in meetings attended exclusively by executives. With this knowledge, the ERM director can ensure that the relevant department is notified of potential risks to solicit an appropriate risk mitigation. This is crucial to the program, as C-suite executives often discuss risks in meetings that do not include an ERM department representative. Regular

communication between the ERM department and top executives helps to sustain the program by maintaining a constant risk dialogue.

Utilize Risk Data

Collection and use of risk data is another sustaining success factor, providing insights that can be leveraged to improve the program. C utilizes data analytics and KRIs to monitor and improve its process. Data analytics are used by engineers to quantify risk information, including measurement of mitigation activities. KRIs, employed by the company since 2011, can be thought of as a "stoplight." Based on historical and analyzed data, an evaluation occurs to determine if a risk's status is green, yellow or red. The causes and consequences of risks are identified to create KRIs. Then, KRIs are monitored quarterly as a measure to indicate the status of risks. KRIs are formulated for corporate risks, which have the potential to impact the entire entity. Together, knowledge coming from these sources creates a common flow of communication for risk data. Processes surrounding this data become regular parts of operations and assist in sustaining ERM.

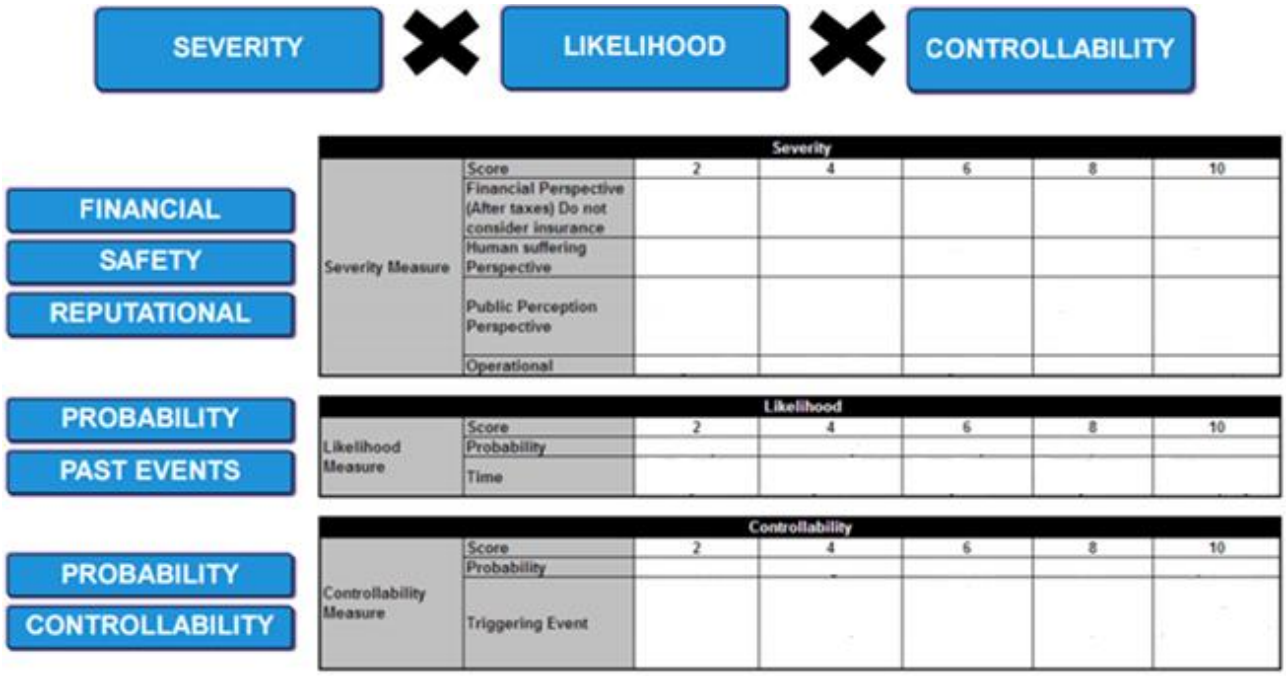
Present Risk Information to the Board Effectively

C has found that its method of annually presenting ERM information to the Board has added substantial value to sustaining the process. Top corporate risks are covered during these presentations, with each major risk discussed at least once every three years. The unique aspect of C's Board risk presentation centers on its standardized format. Both written materials and oral presentations have consistent formats from year-to-year, avoiding any possibility of overwhelming or confusing Board members. This standardized format also allows the Board to compare risks on an even scale. The content of the presentation focuses on the current status of corporate risks, any changes since the previous ERM presentation and mitigation strategies undertaken. Maintaining a standard format aids Board members in understanding ERM topics.

Conclusion

C maintains a healthy ERM process that is structured to facilitate sustaining of the program. Over the 13-year life of the program, ERM has evolved greatly and is now embedded in many aspects of the organization. The sustaining ERM success factors stated above have been essential to continuing an effective and ongoing ERM process. In summary, focusing on major risks, communicating risk information and continuously evolving ERM are crucial to sustaining any process. The company has successfully built its ERM program on these fundamentals.

Figure 1 – Risk Assessment Factors



The maximum score for a risk is 1,000, with the highest possible individual score for Severity, Likelihood and Controllability dimensions being 10. Within each dimension, the highest scoring component is selected to represent the entire dimension. Using Severity as an example, if Financial, Safety and Reputational have scores of 5, 8 and 7 respectively, Safety's score of 8 would represent the entire Severity dimension. This is done for Likelihood and Controllability dimensions as well. Then, the score for each dimension is multiplied to calculate the overall score for a risk.

APPENDIX – D

Organization Description

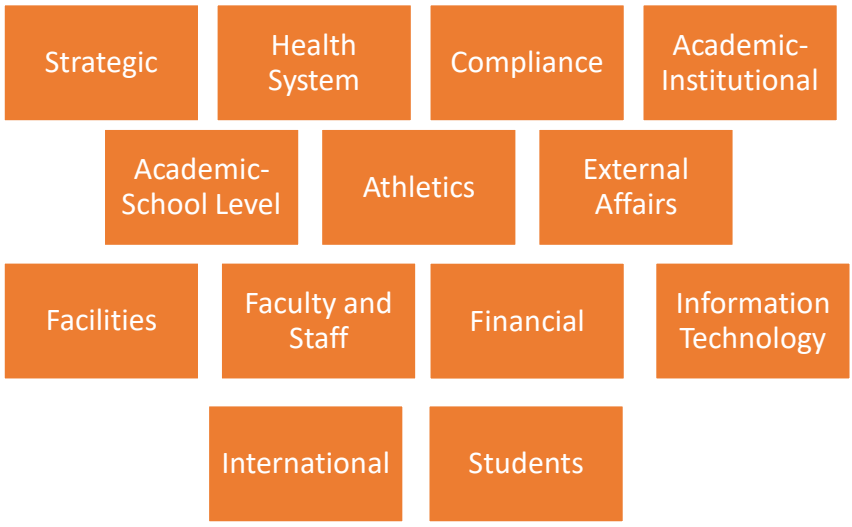
D is a private research university and health system with over 15,000 students including both graduate and undergraduate students. The University is active internationally through conducting business with over 125 countries and even has campuses internationally. D receives annual revenue of $5 billion from the University and Health System.

Organizational Culture

D's risk culture can be best described as a risk awareness culture. Because universities are subject to many standards and regulations, risk management processes can become too rigid and stagnant. Therefore, in order to achieve the agility and flexibility desired to sustain an ERM system, a less robust, more fluid ERM process is utilized. There is no regulation requiring the use of ERM, rather the organization uses it purely for the strategic value it adds to decision making.

ERM Overview

D's ERM process receives ample support from its Board of Directors. Many of the organization's Trustees were aware of ERM, which was helpful during the initial implementation of ERM. The organization introduced ERM by defining all risks and establishing risk owners for each respective risk. ERM was implemented using a traditional top-down approach. The University's ERM structure is currently broken down into 13 functional areas, as shown to the right, and its risks are aggregated into 4 major categories: strategic, operational, compliance and academic risks.



Identification of risks are done at the executive and functional area levels. Functional leaders use a multitude of techniques including risk workshops, interviews, and surveys to identify new emerging risks. It is up to the functional area leader to choose an identification technique that works best in each situation. Risks are updated annually or biannually. It is important to note that strategic risks are not rolled up from the functional areas. Rather the strategic risks guide the functional area assessments.

D's Executive Director of Audit, Risk, and Compliance will meet with the executive team to update the strategic risk statement and agree on prioritization. The full board will review the top institutional risks annually. For risks related to a particular operational area there are two levels of review. First, there is a management level review by the Risk and Compliance Steering Committee where executives and senior leaders vet the priorities. Then, the top risks are mapped to a board committee or to the full board for transparency and governing oversight. Either annually or biannually the risk owner will make a presentation to that board committee or full board. For example, the organization's Athletic functional area will give a risk presentation to the Audit, Risk, and Compliance Committee of the Board biannually.

Throughout the year, it is up to the risk owner to actively monitor the risks in its jurisdictions. Functional areas have different monitoring techniques and no standard monitoring procedures are set in place entity-wide. Monitoring is linked more to the overall strategy than to any particular risk. Some of the organization's functional areas that are more quantitative, such as its research cost compliance office and central finance, has been able to develop and track key risk indicators utilizing Tableau and SAP software. Meanwhile, other more qualitative risks are tracked using key performance indicators.

D also has just recently implemented a risk appetite scale that has low, medium, and high levels to show risk owners what the organization's risk appetite for top enterprise risks when making business decisions. Another measure the University added was adaptability which indicates the speed or ease with which we can implement mitigation actions. The University's Executive Director of Audit, Risk, and Compliance will have meetings with risk owners at their discretion to further communicate risk guidance, but it is ultimately up to the risk owner to execute decisions within the University's risk appetite.

Evolution of ERM

D's process was initiated in 2006 by its Executive Director of Internal Audit. The ERM program achieved a strong buy-in right away from a recently appointed president who was eager to see what the organization's top risks were and what mitigation strategies the University had in place to handle these risks. Throughout D's journey to sustaining ERM, milestones were achieved in different areas of its ERM process. The University considered its process to be sustained at a strategic level after two or three years of strategic risk assessments, whereas ERM was considered to be an accepted management responsibility approximately four to five years after its initial implementation. D is still attentive to continuing sustaining its ERM program through process evolution and utilizes feedback loops with risk owners to look for new improvements in its ERM process.

This is the first year the University has made major changes to its ERM process since ERM's inception. D has recently stopped utilizing a heat map to rank risks in terms of likelihood and impact and moved to a different risk prioritization method. The University implemented this change to make its dimensions less quantitative based and, instead, match risks to strategic plans utilizing a risk prioritization method. The organization decided to make this decision because the culture was becoming too comfortable with the mindset of already knowing their risks and

moving plots around the heat map to show progress. The heat maps were not creating the conversations of emerging and growing risks it was intended to produce and were becoming a stagnant part of the organization's ERM progress that needed to change.

A major success the program has achieved is creating a common risk language among the senior leadership team, and providing indirect support for emergency management and risk management committees. This success was further reinforced by the added benefit it created when actual risk events affecting the organization required response and the University was prepared to respond.

Key Factors for Sustaining ERM

D's advice for companies moving to implement, grow, and sustain an ERM process is as follows:

- Use a collaborative process to develop a reporting framework
- Keep the assessment process simple
- Ensure executive and board buy-in
- Look for the value added in the process

Collaborative Process

Creating a collaborative process to develop a reporting framework has been a critical part of D's ERM process. The key element needed to create a successful collaborative process is having a safe environment where employees feel comfortable enough to be vulnerable and express potential weaknesses and concerns they are facing without fear of penalties or being deemed as failing at their job. It's hard to convince middle management that it is not a performance evaluation and to be open and honest in these facilitations in front of their bosses. That acceptance will come with time and D stresses the importance of creating an open culture. Collaboration needs to be viewed in the organization as an opportunity for leaders to discuss weaknesses and seek feedback from other leaders to develop better strategies to mitigate risks or to raise new concerns the organization should address.

Simple Process

D sees the value in simplifying its process through a less policy driven, group collaboration strategy. The University focuses on group discussion as a way to get all functional leaders to agree on the entity's top overall strategic risks. This utilization of group discussion helps engage senior management regarding the University's strategic risks through meaningful discussion and debate. D sees sustainability of ERM through a culture of awareness rather than through compliance and relies on its employees to execute business decisions within its risk appetite. The organization describes its risk owners as the individual driving the bus and it is everyone else's responsibility to make sure they are not distracting the bus driver so the bus does not drive off the road. This depiction shows the reliance on the risk owners of the University to be actively managing their own risks with the utilization of ERM function intervention as deemed necessary. D also employs less policies and procedures to allows its ERM function to be adaptable and flexible to the risk owner's needs thus simplifying the process to suit the needs of the organization.

Executive and Board Buy-in

It is no secret that in order to achieve success in implementing or sustaining an ERM process you need a strong motivating force behind that ERM process. Strong buy-in from both top level executives and the board of directors removes a lot of barriers to implementation and sets the proper tone the organization needs to sustain ERM for the future. D was fortune that the timing could not have been better for the initial implementation of ERM. The University had just hired new president who was in the process of learning more about how the organization handles its risks. He saw ERM as a great opportunity for the organization and as a means to help familiarize himself with the University's risk information. The president's eagerness coupled with a strong board buy-in gave ERM the right footing to have a successful implementation process. D cannot stress the importance of achieving a strong buy-in at the top of the organization and how critical it is for the future success of any ERM program.

Look for Value

D's Executive Director of Audit, Risk and Compliance continues to look for new value-adding improvements to its ERM program and is also evaluating its current process to ensure it is being utilized for its intended purposes. This was the main rationale behind retiring the heat map as a tool for reporting its risks. Organizations should assess whether their current process is adding to the value chain of the organization's ERM program. In D's case, the heat map was not being utilized as a resource by the organization's employees and was a distraction to the prioritization of risks. Retiring the heat map and utilizing a more qualitative risk prioritization method will allow the University a new way to provide insight on its risks. In addition, this has allowed D's employees to think critically about what they desire from a risk assessment process and refocus on the objectives of the assessment. In order to keep an ERM program relevant over the long run, organizations should be actively assessing and looking for new ways to add to the value chain of their current process to adapt to a changing business environment.

Conclusion

D has been able to establish a less policy driven, more group collaboration strategy in managing risks. The University has seen success in keeping the assessment process simple by giving more discretion to the risk owners with less executive monitoring. ERM gained traction through its strong executive and Board buy-in which gave the program the proper footing for its continued success. The organization strives to look for new ways to add value to its ERM process ensuring its success for the future.

APPENDIX – E

Organization Description

Organization E is an electric utilities company in the United States with a business model that is focused on electric and natural gas infrastructure and comprehensive energy solutions for customers. The company has annual revenues of over $25 billion, a market capitalization of over $50 billion, and over 30,000 employees.

ERM Overview

After a major operational event, the Board of Directors became very interested in Enterprise Risk Management (ERM) especially in relation to operational risks. After that incident in 2013, E's ERM process includes a bottom up and top down assessment of risk with enterprise wide focus for the company. E has a policy driven process with the Board approving the overall ERM framework, whereas senior management individuals focus on areas of risk including project, financial/transaction, strategic, and operational. This creates a lasting framework and defines expectations with the Board of what ERM will do.

Risk Identification techniques are different depending on the type and complexity of a particular risk. Some techniques E has utilized include risk workshops, risk bow tie analysis, pre-mortems, benchmarking, and surveys as useful tools. The organization utilizes an in-house developed software solution (named RIMS) that allows risk owners to update the risk inventory electronically. Risks are entered into the system in an if-then format to communicate a cause and consequence format of risk identification. The risk register tracks risks as they relate to business unit goals.

The register also includes information regarding the probability and impact of the risk, mitigation, response, and evaluation. Probability is considered over a 5-year horizon and impact is estimated by the risk owner using his or her best judgement. Both of these dimensions are ranked on a 5-point scale for the purpose of better consistency in estimations. Some risks are updated annually, and more critical risks like Cyber Security are updated on a monthly basis. Once the business unit risk registers are updated a risk matrix is created in RIMS to be utilized in the business planning process.

E uses KPIs to monitor current risks. Monitoring procedures are handled by the ERM and the traditional risk management departments to steer the monitoring process and make sure there is effective follow through on mitigation strategies. The ERM department has an active role in the business planning process so once a year they are assessing progress on business unit mitigation strategies. Forums also exists to discuss risk management as needed throughout the company to ensure everyone is on the same page.

After the company's operational incident, the company also wanted to focus on identifying tail risk, which is a low likelihood and high impact risk. The organization has created a separate risk registry for tail risk and currently has 55 tail risks. Mitigation strategies have been developed for some of the major tail risks. E sees great value in monitoring tail risk and has seen that by mitigating some of its tail risk, it has also helped prevent more highly probable adverse risk

events. In addition, this activity has brought about a cultural change where the organization is now more open to identifying and escalating risk.

The organization uses a top down and bottom up approach to its risk assessment. To get an assessment from the top levels of the organization, interviews are conducted of the top business unit leaders of the company. That top level assessment of risk is then reconciled to the risk registers that contain the bottom-up view to create the top 12 to 15 enterprise level risks. Those top enterprise-level risks are reported to the board annually. A lot of these top enterprise level risks are broader categories that encompass a number of lower level risks. Other significant risks may be periodically selected for a deeper review and a presentation to the board.

Evolution of ERM

E considers its ERM process to be maturing and on its journey to be considered a "sustained" process. The organization has been analyzing its risk since the 1990s, and formalized a robust ERM process in 2014. E has implemented clear documented policies regarding roles and responsibilities of all levels of employees and has created a risk aware culture that strives for all employees to consider themselves as risk owners. These documents and procedures have been made with the mindset of creating a common risk language across the organization. The organization has seen major strides in achieving this task due largely to the CEO using risk language in front of the company's leaders and being utilized more throughout the organization. E benchmarks its process with other comparative companies in relation to size and industry and conducts companywide surveys to solicit internal feedback regarding its ERM process.

Major successes the program has experienced is having the organization recognize the value added from the ERM process. This was largely achieved by building trust with the business units and by having the capability to do certain things that the business units can't do for themselves. The company's CRO is always challenging the business units and helping create a pull for the utilization of the ERM department with business decisions. The organization's business units are now reaching out to the risk team to be involved with large transactions and other projects which signals that ERM is being viewed as adding value to their decision making process and is seen as a strategic resource. Creating a separate risk inventory in the RIMS software for tail risks have also been deemed a success of the process and really highlighted the value of ERM to the board and is utilized as a way for employees to think critically about worst case scenario risks that can occur.

Key Factors for Sustaining ERM

E's advice for companies moving to implement, grow, and sustain an ERM process are as follows:

- Marrying ERM with Strategic Business Planning Process
- Building Trust with Business Units
- Culture and Driving Forces
- Celebrating Small Victories

Marrying ERM with Strategic Business Planning Process

E recognizes the need for connecting ERM through its business planning process. By establishing a close link between a company's strategic planning and risk management processes, management can ensure that new strategic initiatives are connected to appropriate risk mitigation strategies, and that changes in the company's strategic direction are accompanied by timely assessment of new or emerging risks making the company better prepared to identify risk-related competitive advantages. The organization is still evolving the process to fully integrate ERM with corporate strategy. The company is in the process of building a five-year plan to better integrate ERM and strategy. Currently, ERM is well integrated into the strategic business planning process at a business unit level.

Building Trust with Business Units

In order for an ERM program to achieve its desired results and truly be utilized for strategic value involves the organization's ERM department to gain the trust of the risk owners and business unit leaders. Leaders and risk owners cannot view ERM as an audit function and be believed to enforce penalties on employees. The ERM department's role is to help the organization achieve business objectives through aiding risk owners and business leaders in solving problems. This trust in some company cultures is hard to achieve and involves the ERM leader to build relationships with business units and risk owners. This relationship is critical in implementing an ERM department that actively helps business units and risk owners examine opportunities that exist from taking risks as opposed to viewing risk as purely a negative, which is one of the main objectives of Enterprise Risk Management. The organization has been very successful in establishing this trust, which is evident by business units actively seeking out the ERM department to be involved in their decision making process.

Culture and Driving Forces

Due to E's culture and the industry it operates in, the organization is very policy and procedure driven so the written ERM framework policy and standards worked really well for the organization. You can't just implement everything you read in COSO without considering the impact of the culture of your organization. Having a firm grasp of your culture is critical to implementing the right policies for your organization and knowing what will work well for your company. The company sees value in creating a strong risk culture and embodies the mentality that all employees are risk owners. To achieve a risk awareness culture E created a risk culture survey in 2015 to see how all of its employees view its risk culture. The survey revealed that almost all employees feel responsible for taking actions when they identify a risk and are confident in their abilities to report that risk There is not a one size fits all when it comes to the right ERM process, but failure to recognize when a framework or process isn't adding value to your ERM process may lead to wasting employees time and a check-in the box mentality of complying with your ERM process. Any ERM process needs the proper driving force to be able to create a sustaining process that lasts overtime. Having this driving force sets the mindset of the company and requires both board and executive leadership buy-in. E was lucky to have a strong CEO and board buy-in which is what allowed them to create a robust ERM process in 2014.

Celebrating Small Victories

As the saying goes, Rome was not built in a day and neither are lasting ERM programs. One of the key pieces of advice E offers to companies expanding or creating an ERM program is that greatness is not achieved in one day and patience is needed to implement the process that works best for your organization. The organization achieved successful implementations in areas where they focused on maturity models to map out where the process was, how the company's culture is, and designing the right implementation process for the organization. E learned that lesson from trying to introduce a few processes that were a few years ahead of where the company currently was which backfired in terms of producing the results they had anticipated. They tried to implement too complex of tools without assessing where the organization was and whether that fit with the culture and the speed of adoption of the company. Sometimes your organizations progresses with one step forward, two steps back and celebrating the victories and prioritizing what process is necessary is critical for successful implementations.

Future Improvements to the Process

- Formalizing enterprise wide risk appetite and risk tolerances
- Understanding risk inter-dependencies between different departments
- Ingraining ERM more into the strategy process

The list above are future goals and areas where E would love to see improvement in its ERM process. Currently risk appetite is determined at a business unit level. Functional levels are responsible for selecting the proper risk response and mitigation strategy using their personal judgement and following company policy for certain operational risks. The company currently has risk appetite integrated on a transactional basis, but sees the growth potential for an enterprise wide risk appetite that extends through the business units. An effort to develop an enterprise wide capital optimization process will further drive defining trade-offs in the company's risk appetite and tolerances. ERM is ingrained more into functional areas with risk-strong departments such as nuclear more than other departments. E believes that by having small victories within business units by improving definitions of risk appetite the company will be able to better align ERM with the strategy process.

Conclusion

E's ERM process can be characterized as a structured, policy-driven process for managing risk. The program has experienced major success by having the organization recognize the value added from the ERM process. This was largely achieved by building trust with the business units and by considering the organization's culture in implementing and improving its ERM structure. E continues to look for ways to improve and sustain its ERM process for the future long-term success of the company.

APPENDIX – F

Organization Description

F is an independent oil and gas company that focuses on onshore drilling. F produces oil, natural gas, and natural gas liquids. Like most oil and gas companies, its revenues are closely tied to oil and gas prices and company growth is tied to discovering new oil and gas reserves. F partners with contractors to drill and maintain the wells and sells crude oil and gas to midstream companies and refineries. F has a market cap of $22 billion with revenues of $12 billion and 5,000 employees.

ERM Overview

F had strong risk management practices before ERM was implemented. The ERM process recognizes the value of existing risk management process across the organization and builds upon those strengths. ERM was requested by the Audit Committee and Board of Directors in 2009 and visibly support from the CEO and executive team (top senior management). F's executive team forms the ERM Steering Committee which provides oversight over the ERM process. The Internal Audit department facilitates the ERM process and management owns the individual risks.

F's ERM process utilizes five fundamental, interrelated components:

1. Enterprise Risk Inventory
2. Enterprise Risk Documentation
3. Risk Group Workshops
4. Annual ERM Risk Survey
5. ERM Steering Committee

Together, these five components enable F to identify existing and emerging risks and communicate the right risks to the right decision makers at the right time. *Figure 1*, below, provides a graphical representation of the key elements of F's ERM process.

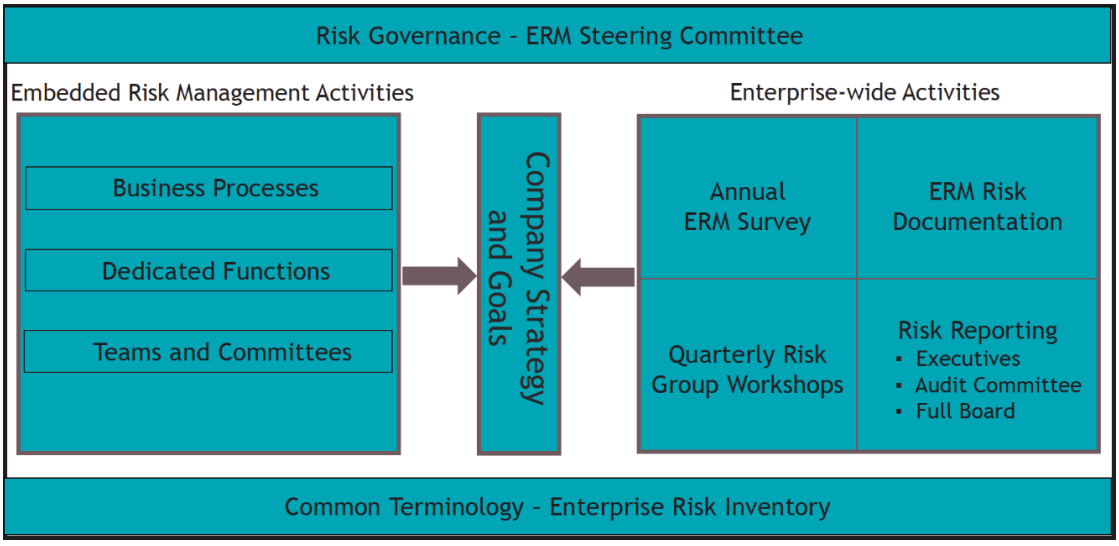


Figure 1

Enterprise Risk Inventory

The enterprise risk inventory is an integral component of the ERM process because all other ERM components build upon the risk inventory. The risk inventory is a collection of 18 risk categories and approximately 50 specific inherent risks to the company's business and culture. Each risk category contains two to four inherent risks specifically defined by the leaders who are considered subject matter experts on the risks.

Each risk category is also assigned an executive level risk sponsor. A risk sponsor is an executive team member who is responsible and accountable for all inherent risks within the enterprise risk category. The designation of a risk sponsor is important to the ERM objective of communicating the right risks to the right decision makers at the right time. *Figure 2* illustrates an example of the assignment of executive team members to risk categories.

Examples of Enterprise Risk	Executive Risk Sponsor
Strategy, Global Macro	CEO
Operational Cost, EH&S	COO
Financial, Reserves	CFO
Public Policy	EVP Public Affairs
Market Access, Commodity Price	EVP Midstream & Supply Chain
Recruitment and Retention	EVP HR
Legal/Regulatory	EVP General Counsel
Information Technology, Disasters	EVP Administration

Figure 2

Enterprise Risk Documentation

Enterprise risk documentation collects more detailed information about the risks in the enterprise risk inventory. Internal audit works with over 100 leaders and managers across the company to gain a better understanding of each risk category and inherent risk. A standardized risk documentation template is used to collect information about each specific inherent risk within the risk categories. The risk template includes:

- Inherent risk overview (risk name, definition, sponsor)
- Contributing factors (root causes that drive risk)
- Risk management activities (processes and controls in place to mitigate risk)
- Opportunities & Issues (risks that need attention)
- Risk management plans

Based on the information collected in the risk template, the ERM team develops customized reports. Executive overviews are developed for each risk category. Additionally, a one-page summary is written for each inherent risk incorporating the information documented in the risk

template. This summary report highlights the most important changes in each risk category. This report is shared with the executive team, audit committee, and the board. Summary reports are updated every 18 months to present the most current risk information.

Risk Group Workshops

Risk group workshops are conducted on a quarterly basis with six to ten vice presidents. Typically, two to three similar risk categories are discussed at each workshop. This ensures that all risk categories are discussed over an 18-month period. Risk group workshops last approximately two hours. The first 15 minutes are used to prioritize the inherent risks within each risk category. Anonymous votes are cast to determine the "actual" and "desired" risk management effectiveness for inherent risks based on a seven-point scale. The gap between "actual" and "desired" is used to prioritize the risk discussion, as seen in *Figure 3.*

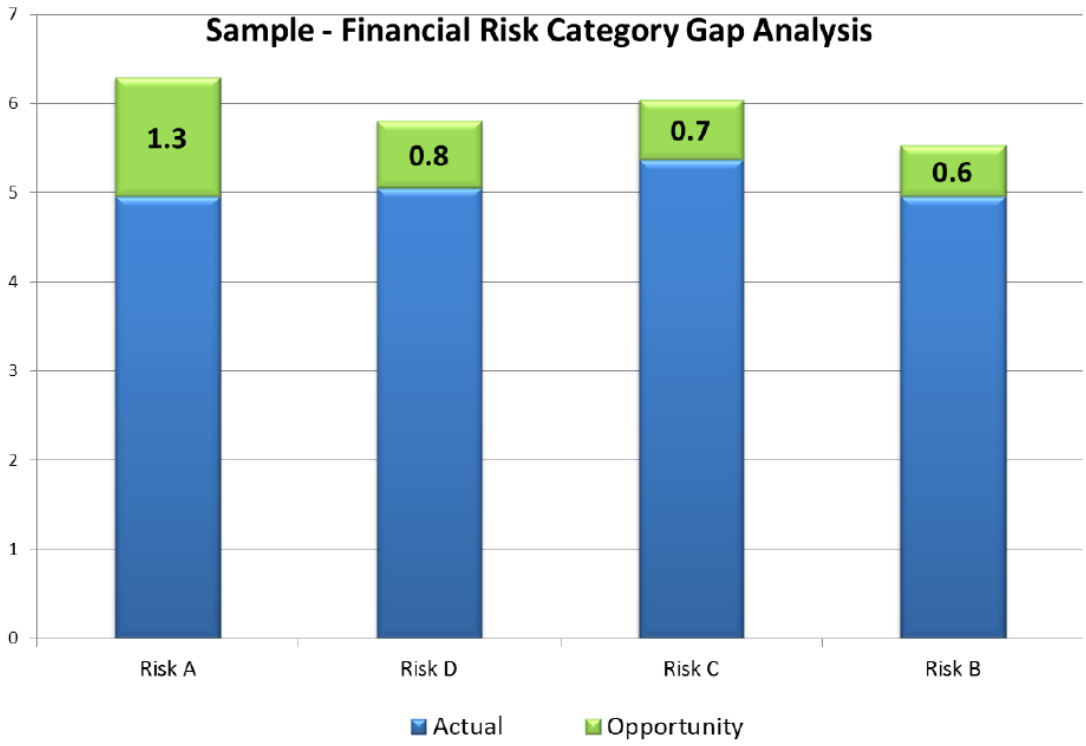


Figure 3

The larger the gap, the sooner the risk is discussed. The risk discussion focuses on identifying factors causing the gap as well as the corresponding opportunities to shrink the gap. The top changing and emerging risks for each risk category are also communicated. Significant risks that are brought up during the group workshops are often discussed further amongst the executive team members after the workshop.

Annual ERM Survey

The ERM survey polls roughly 75 leaders to prioritize the 18 risk categories. The survey is sent to all executive team members as well as vice presidents throughout organization. The survey is

conducted electronically and 100% survey participation is common. Risk category prioritization is based on four metrics illustrated in *Figure 4* below:

Management rate risks based on 4 metrics

Financial Impact

1. <$50 million
2. >$50 million < $500 million
3. >$500 million < $1 billion
4. <$1 billion < $5 billion
5. >$5 billion

Velocity

1. Greater than one year
2. One Year
3. Weeks to Months
4. Days to Weeks
5. Hours to Days

Likelihood

1. Highly Unlikely
2. Somewhat Unlikely
3. Neutral
4. Somewhat Likely
5. Highly Likely

Preparedness

1. Very Prepared
2. Prepared
3. Neutral
4. Unprepared
5. Very Unprepared

Figure 4

Risk prioritization is derived from adding the point totals from each of the four risk ranking metrics. The higher the point total, the higher priority the risk receives. Survey results are often presented in visual charts or heat maps to depict risk prioritization. *Figure 5* displays risk prioritization in the form of a bar chart and *Figure 6* displays risk prioritization with a heat map.

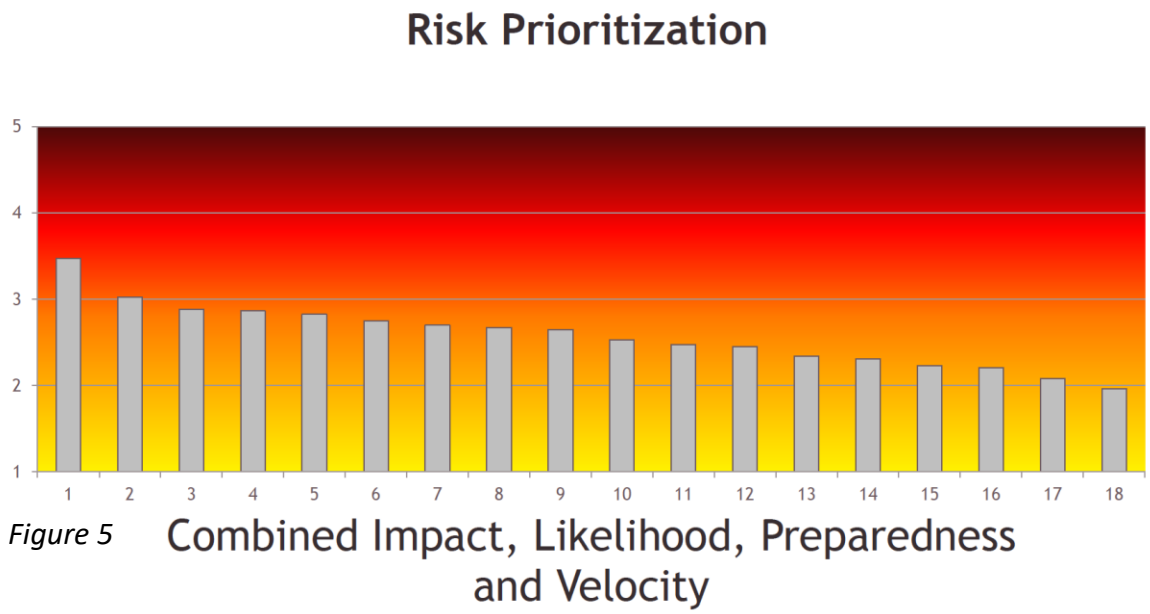


Figure 5

Practical ERM lessons and tools

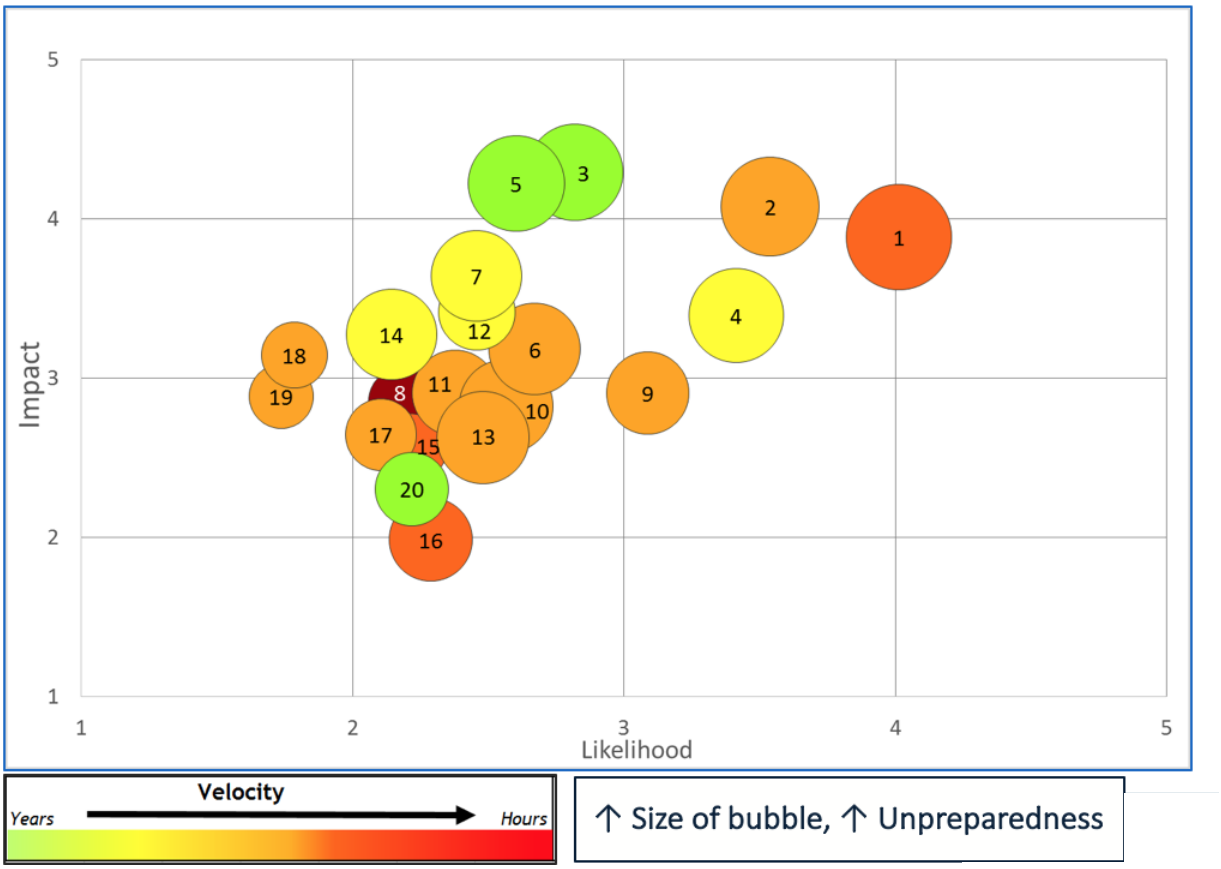


Figure 6

To aid survey participants, the one-page summary reports developed during risk documentation are included for reference during the survey. Summary reports outline the risk definition, scope, and any important changes in the risk so that all survey responders are knowledgeable about the risks they are evaluating. Survey responders also have the ability provide new risks for the ERM team to consider.

Survey data collected is discussed with the executive team. The executive team risk rankings are compared directly to risk rankings amongst management to note any major discrepancies. Survey results are provided to the Audit Committee and the Board of Directors. The Internal Audit department leverages risk information collected from the survey to design annual audit plans to further facilitate ERM.

ERM Steering Committee

The ERM Steering Committee provides oversight and guidance to the ERM process. The Steering Committee is composed of executive team members and holds two meetings a year to set the direction of ERM. The ERM Steering Committee communicates the ERM direction with the Audit Committee and the Board of Directors.

Key Factors for Sustaining ERM

F's ERM process formally began in 2009. Today, the ERM process is still operating effectively and has weathered volatile oil prices. F attributes its ERM success to several key factors:

- proper tone at the top of the organization
- experienced ERM champion
- proven, customized ERM processes
- evolving ERM at the right pace

Tone at the Top

Tone at the top refers to the Board of Directors' and the executive team's attitude towards ERM. While ERM was implemented in 2009, discussion about ERM began several years earlier between the Board and CEO. The Board of Directors initially requested ERM within the organization due to the emerging identification of ERM as a best practice. F's CEO fully supported the decision as well because he knew ERM would add value to the organization by mitigating top residual risks.

An ERM advisor was hired from outside the organization to fill the position and jumpstart the ERM process. The precedent set by the Board of Directors and CEO about the importance of ERM quickly spread throughout the organization. Having the correct tone at the Board and executive level instilled a risk aware culture that ensured the ERM process would take hold. Buy-in from the Board and the executive team places emphasis on the importance of ERM throughout the organization.

Experienced ERM Champion

The ERM process needs at least one experienced leader to promote the benefits of taking an enterprise view of risk. The ERM champion, or leader, is necessary to sustain the ERM process, especially at large organizations where employees may not have daily contact with ERM. F brought on board a full-time ERM advisor to fill this role. Having an experienced ERM advisor on the ERM team enabled F to begin with proven and meaningful ERM tools, techniques, and processes. The key to any ERM process is to link objectives, risks, and risk management activities. By starting the ERM process with proven and effective ERM tools to make this connection, the organization was able to quickly gain traction with its ERM process.

The ERM Champion should be aware of the organizational culture and the users of the ERM process when designing the ERM approach. F's executive management did not want a big, bureaucratic ERM process with a Chief Risk Officer. Instead, F wanted its ERM process to quickly address issues without getting in the way of daily operations. Additionally, F's management felt

that existing risk management practices were effective. In fact, an initial concern was that ERM was going to unnecessarily impact the existing risk management processes and begin with a clean slate.

Proven, Customized ERM Processes

F's annual risk survey was the initial tool used to launch ERM and remains a standard component of the ERM process. The annual risk survey is an effective ERM tool because it is consistently applied year-after-year, allowing for identification of risk trends and expectation gaps between the risk management team and executive management. The survey polls roughly 75 leaders, including the VPs through the CEO. To ensure consistent understand of the risk being surveyed, standard risk documentation is provided to the leaders as a reference tool prior to completing the survey. The survey includes four risk criteria, impact, likelihood, and readiness. The risk survey has 100% participation because it is woven into the organization's culture—everyone knows that he or she is expected to complete the survey.

The ERM advisor was mindful not to reengineer the survey but rather evolve the survey process over time. In addition, other ERM tools such as a customized enterprise risk inventories, a standardized enterprise risk documentation, and quarterly workshops all complemented each other including the survey. The survey is an interactive tool that enables management to really comprehend the importance of managing risks. Survey results are published in a risk booklet that is presented to the Audit Committee and the Board of Directors to ensure a common understanding of risks between management and the Board of Directors.

Evolving at the Right Pace

A critical factor is the pace of change to ERM, especially when ERM is first implemented. F makes a specific point to strategically introduce ERM processes with careful consideration given to organizational culture. Many of the ERM components that are successfully sustaining ERM such as enterprise risk documentation using standardized templates, quarterly risk group workshops to facilitate risk discussions, and the enterprise risk inventory were introduced to the organization one at a time.

Taking the time to organize the timing and priority of ERM process implementation is important. Implementing too many processes too quickly will have negative effects on the sustainability of ERM. Employees are likely to push back to too much change too fast. F strives to pace its introduction of new ERM processes over a one to two-year time frame. Further it is important that each ERM processes builds upon the previously implemented processes. For instance, at F it would not make sense to implement standardized enterprise risk documentation without first creating an enterprise risk inventory of risks to document. Designing ERM processes that complement and improve existing processes is necessary to sustain ERM.

Conclusion

F's ERM process revolves around its five integrated components: the enterprise risk inventory, enterprise risk documentation, risk group workshops, annual survey, and the ERM Steering Committee. Each component builds on the previous component in order to create a more robust ERM process. F's ERM processes is sustained largely due to support from the Board of Directors and its CEO as well as its ERM Champion. The integration of the ERM processes is the most impactful ERM tools at F further communicating the value of ERM to many organizational leaders. Lastly, the proper pace of ERM is necessary to sustain the process. Changes should be deliberate and consideration should be given to executive management and culture as you introduce new ERM processes.

ABOUT THE AUTHORS

Andrew Farris is a graduate student in the Master of Accounting program at NC State University, with a concentration in Enterprise Risk Management. While obtaining his Bachelor's degree in Accounting from NC State University, he developed in interest in auditing financial statements. This interest was carried to a Winter 2016 audit internship with Johnson Lambert LLP. After graduating from the Master of Accounting Program, he will begin full-time employment with Johnson Lambert LLP.

Jackie Gaine is currently earning her Master of Accounting with a concentration in Enterprise Risk Management at NC State University. She is originally from Virginia, where she earned her Bachelor of Science in Business Administration with a concentration in Accounting from Christopher Newport University. While working towards her graduate degree, she is currently a graduate assistant for the Enterprise Risk Management Initiative and helps write abstracts for the program. After graduating from NC State University, she will begin full-time employment with Dixon Hughes Goodman in the fall.

John Humienny is currently earning his Master of Accounting Degree with a concentration in Enterprise Risk Management at NC State University. He is a native of Raleigh, NC, and previously attended the University of South Carolina for undergrad where he majored in Accounting and Global Supply Chain and Operations Management. In 2015, he interned at Roche Pharmaceuticals in the Accounting department which sparked his interest in public accounting. After graduating from NC State, he will begin full-time employment at Ernst & Young in Raleigh.

Zihang (Rick) Yin is currently enrolled in the Master of Accounting Program, concentrating in Enterprise Risk Management at NC State University. He is originally from China and attended Ohio University where he earned his Bachelor's degree in Accounting, Finance and Business Pre-Law. In 2012, he had an internship with Shanghai PwC in the assurance service line. In 2014, he had the opportunity to have another internship in global accounting department with Driscoll's, the biggest berries selling company in the United States. After graduating from the program, he plans to pursue his career at a public accounting firm.