NC STATE Poole College of Management
Enterprise Risk Management Initiative

Extending the Reach of ERM:

Techniques for Engaging More Employees

Prepared by: Stephanie Clark, Wenxin Liu, Russell Thornton
NC STATE GRADUATE STUDENTS | POOLE COLLEGE OF MANAGEMENT
FACULTY ADVISOR: Bonnie V. Hancock

TABLE OF CONTENTS

INTRODUCTION

In many cases, the driver for a company's adoption of Enterprise Risk Management ("ERM") is a request from the Board of Directors acting on its responsibility for risk oversight. As a general rule, the full board has primary responsibility for risk oversight with the board's standing committees supporting the risks inherent in their respective areas of oversight. Actual implementation, however, rests with senior management. Given their enterprise-wide point of view, senior management can ensure that the risk management policies and procedures are consistent with their company's strategy and risk appetite. Over time, companies realized that to be most effective, ERM must reach beyond senior management and engage more employees across the company to gain greater insights into risks and to promote better risk management practices throughout the organization. This case study examines the various techniques that six different companies have adopted to extend ERM throughout the organization.

The six organizations participating in this case study represent a variety of sectors. All of the companies are publicly traded with most falling into the large capitalization[1] category in terms of size. We have kept the participating organizations anonymous to protect any confidential information shared during interviews. Basic organization metrics are presented below.

Companies Represented

Organization	Sector	Market Capitalization
A	Industrials	Large
B	Consumer Cyclical	Large
C	Healthcare	Large
D	Consumer Cyclical	Mid
E	Utilities	Large
F	Consumer Cyclical	Large

The most common way that companies engage employees at lower levels is by requesting their input on risk identification or assessment using surveys, workshops, or one-on-one discussions. Through this process of requesting input from employees in business units throughout the company, each organization gets a better sense of the risk issues that are present at different levels and in different functions across the organization. It is also an opportunity for employees to become more knowledgeable about the enterprise risk management process because these

[1] Large: Greater than $10 billion
Mid: $2-10 billion

methods are not just a one-way street. Leaders of the ERM process also use workshops, one-on-ones, and phone conferences to share updates with employees in addition to seeking input. These updates may cover enterprise risks or be more focused on risks in a particular business unit. By tailoring the content to specific functional areas, ERM process leaders are able to both inform and learn from employees regarding significant risks affecting a particular business unit. In addition, some companies use online portals to house reference materials regarding risk management and publish risk universe listings to educate employees at multiple levels of the company.

In all cases, companies are engaging more employees in ERM. Other techniques that foster engagement include assigning risk owners and naming risk champions. Companies assign risks to "owners" who are responsible for preparing risk response plans and monitoring their assigned risks. Risk champions may be embedded throughout the organization to facilitate ERM practices across the company. The risk champions, who may be individual risk liaisons or collective risk committees, are a conduit for ERM process leaders to gain insights into the unique issues in different parts of a company. Although their roles differ slightly depending on the company, risk champions work collaboratively with each other, within their functional areas and/or with the ERM process leaders to discuss, review, and update ERM risk information. Additionally, risk champions promote effective risk management practices in their part of the company.

In the following sections we will discuss each of these techniques in more detail.

GAINING DIVERSE INPUT

There are many methods companies use to increase risk awareness and drive ERM deeper into the organization. The annual risk identification and assessment process provides an opportunity for the ERM function to get both line and staff functions across the organization involved in the ERM process. As part of the process, each unit identifies its most critical risks and the ERM function compiles that information to develop an enterprise assessment. In addition to informing the enterprise view, this process serves to heighten awareness of key risks and the risk management process across a broader cross section of employees, thus creating a more risk aware culture. As risks are identified, analyzed and monitored, the business units and enterprise risk management teams can connect other risk and control groups to understand how operational and financial risks can tie to enterprise risks.

Most of the companies participating in this case study use some form of surveys or workshops to draw risk information from deeper within their organization. Additionally, some companies use other methods for input such as one-on-one interviews.

Surveys

Many companies utilize surveys as a way to engage more employees in the ERM process by asking for their input in the identification and assessment of risks. The levels of employees that were asked to participate in the surveys vary across the companies. Yet, in all cases, organizations request input from employees across all functions and business units in order to engage employees closer to the risk ownership level of the organization.

With the companies that distribute surveys to lower level employees, the survey questions are more focused on risks within a particular line of business and are customized to each unit. The results are then compiled and compared at the entity level in order to spot trends or connections in risks across the different business units. This is useful in spotting risks that may seem insignificant and possibly escape notice within one business unit, but that could have more significant impacts across the entity. When surveys are directed towards higher-level employees such as those at the business unit leadership level, the questions are more focused on entity wide risks as those employees are expected to be knowledgeable about risks not only within their business unit, but also at the entity level.

One company in the case study sends their surveys to over 900 different business leaders at various levels throughout the company to capture the various viewpoints. Recently, the company has been using targeted surveys that are customized for each business unit. In order to incorporate different forms of risk identification and maximize coverage, the company alternates between two types of surveys each year. The first survey design includes open-ended questions that allow users to give free form responses while the second design provides a list of responses to select. Unfortunately, gathering input from across a large organization can be daunting especially when you want to include open-ended questions. One way a company dealt with that issue was by selecting a sample of divisional business leaders to receive the open-ended survey on a rotating geographical basis as opposed to surveying each divisional entity leader annually. This sampling process allows the company to capture regional risk input from fresh perspectives for each annual survey.

In order to improve participation and provide education on ERM, one company asks potential survey participants to view a short video that explains why risk management is vital and describes their role in managing risk. The video urges employees to complete the survey so that their opinions are heard and emphasizes that responses will remain confidential. The company saw about a 20 percent increase in participation in the survey with the addition of the video.

The use of surveys in risk identification promotes both the discussion of risks from within business units and widely across the different business units of the company. Some companies use the surveys as a guide for subsequent interviews which helps promote more focused risk conversations between the director and managers as well as between managers and their business units. As a result, companies raise risk awareness within the different business units which helps facilitate further discussions regarding risks with employees at lower levels.

Workshops

Another effective method of engaging more employees is to host workshops. Workshops create an environment in which cross functional employees can engage in multi-dimensional discussions of risks. In a way, these workshops act as brainstorming sessions for understanding, identifying, assessing, and mitigating risks. Additionally, they can act as a means for high level business leaders to communicate risk information. Most companies engage a cross functional, multi-level group of employees in workshops in order to better identify and evaluate specific risks. We found Companies B, C, and E draw participation from the business unit management level in their workshops while Companies D and F include business unit teams at various levels throughout the organization. These participants are able to share different perspectives and build on each other's thoughts during the workshops in order to create a more holistic view of risk that can later be shared within business units or functional areas. One company also uses workshops to facilitate consensus on the top 15 risks to the company or business unit—depending on the focus of the workshop—and then discuss focus areas and brainstorm mitigation plans.

One unique type of workshop used to identify risk is a "Blind Spot Analysis." This workshop asks participants to think outside the box and identify risks and opportunities around a certain topic or objective. Before the conclusion of the workshop, some prioritization occurs. Thus, groups of employees can see what those participants deemed to be the most important risks or opportunities that should be considered as the company makes decisions or executes strategy.

Company D uses another type of workshop as a means to better identify tail risks, also referred to as Black Swan risks. The company defines a Black Swan risk as a risk which would have the impact of changing a fundamental business assumption and the potential to build significantly over time. The Director of Internal Audit facilitates a workshop with a cross-functional group of company leaders to identify Black Swan risks that may affect the future success of Company D and compiles the results into a report that is shared with senior leadership.

Most companies host more than one workshop per year, while others may hold several in order to engage multiple business units individually. Each company that hosts workshops attests to the benefits of spreading risk awareness while also getting more robust risk information through engaging employees in groups, regardless of the exact method of conducting the workshops.

One-on-One Interviews

Company F seeks input from lower levels through one-on-one interviews and leadership meetings. The Director of ERM conducts interviews in some cases down to the manager level—4 levels from the CEO. Due to time constraints, the Director interviews selected managers who have particular insights regarding a certain business unit or risk. The purpose of the interviews is to force a dialogue of things typically not spoken. Thus, the Director of ERM uses risk conversation starters to facilitate the discussion. For example, the Director may ask "What do you think is the greatest threat to the company's brand?" or "What significant event risk do you think could jeopardize the company's future?"

Each of these types of interactions serves a dual purpose. In the process of gathering input on potentials risks, the ERM function is also promoting greater risk awareness across a broader group of employees.

Sharing Risk Information

Communication of the results from key steps in the ERM process is one of the main components of extending ERM to engage more employees within the organization. Business units continue to integrate risk management into day to day operations by incorporating risk discussion into established discussions or as many forums as possible. Linking the right risk discussions, at the right time, in the right forum can be powerful and help the business have even more productive discussions around strategy and decision making.

After the ERM function consolidates the input from different levels of employees through the multiple techniques mentioned above, there is an additional opportunity to continue the engagement by sharing the results. The companies in this case study have different approaches for sharing and communicating risk information.

Techniques for Sharing Enterprise View of Risks

When focusing on how different companies share the results of the risk identification and assessment, and communicate updates on risk status, differences exist in the level at which risk information is shared and in the techniques used to disseminate the information. For example, most companies share the entire risk identification and assessment results while other companies may only share the top risks. One company has implemented an online system to identify and track risks within the business units while another uses posters of the entire risk universe to maintain risk awareness.

In Company C, the detailed results from the interviews and surveys are shared down to the division management levels. Survey participants, who are provided with the risk universe prior to taking the survey, will have access to the updated risk universe after the results have been compiled.

Recently, Company E implemented a robust new system for their ERM process which is linked to business unit initiatives and enables business unit management to identify and track risks to achieving their plans. This company also holds semiannual Enterprise Risk Summits to raise awareness and provide updates regarding risk management. Participants in this summit are business unit risk consultants as well as individuals across the risk management department. The ERM team leads the Summit and develops the agenda. The upcoming Enterprise Risk Summit will include a discussion of a recently implemented risk management software tool and a presentation from the security team on both cyber and physical security. Through the Summit, participants gain an understanding of key risk management issues which they can apply to their individual business units thus pushing risk management deeper within the organization.

Company A and C both engage employees through quarterly conference calls providing updates on risk status. To maintain a consistent risk focus across the various business areas at Company A, the lead of the corporate ERM function holds connectivity calls with each business risk committee[2] chair to provide guidance and discuss the ERM process. Similarly, Company C includes divisional officers and management on quarterly conference calls. During these calls, the CEO, President and CFO discusses updated risk results from surveys and interviews and convey appreciation for everyone's involvement in the survey and interview process. The appreciation conveyed helps encourage continued participation in the future. Company C's calls can include over a thousand officers and business unit managers at once. To handle this volume

[2] More on risk committees under "Embedding Risk Owners and Champions"

of participants the company uses a conference line with a moderator to help with questions. The moderator keeps all lines muted until the designated time for questions when specific requests for questions are taken in turn.

Sharing Through Online Portals

Posting information on a company's internal website can be an effective way to share relevant ERM information. Two of the six companies have made ERM information available on their website to serve as a resource for employees. For example, company D posts links to the NC State University's ERM website so that employees would have access to the research and case studies available there. This helps employees see how other companies are managing different aspects of risks and to be aware of trending risk issues. Sometimes, instead of directing employees to the online portal, the Director of Internal Audit at Company D may hand out a physical copy of a highly pertinent case study. The company also uses an online portal to share training materials with employees who have been nominated by risk owners to serve as risk liaisons within their respective business units. Similarly, Company E has the content of the ERM framework shared via the risk management department's page on the company's intranet in order to help employees understand their responsibilities and accountabilities with respect to risk management. One significant benefit of online resources is the ease of accessibility that allows employees to refer to these materials as needed, and, particularly with the educational materials, at their own pace.

Embedding Risk Owners and Champions

A consistent measure found in how companies involve more employees in ERM processes is by assigning individuals risk ownership and delegating risk management responsibilities to those leading individual business functions.

Risk Owners

Assigning risk owners is a means of designating specific employees the responsibility for developing response plans and for monitoring the assigned risks. Usually, a risk owner is in a leadership role of a business unit or function whose duties are related to or could be affected by the risk they are assigned.

Having specific accountability for managing a risk instills a sense of personal responsibility in risk owners that generally extends through the ranks. This helps to invest employees in ensuing risks are properly monitored and managed to minimize any impacts on the achievement of the organization's goals. As risk ownership occurs at the business unit and operational level, risk owners are in the best position to identify the root causes of risks helping to provide better mitigation plans. Risk owners generally report up to enterprise risk teams on their assigned risk. Enterprise wide risk teams are able to use reports from risk owners to give them a line of sight into risks across different business units, which can then be aggregated at the enterprise level.

Risk Champions

Another way companies engage lower levels of the organization in the ERM process is by embedding risk champions who will serve as key points of contact for the ERM function. These risk champions are also a resource and facilitator for risk management activities within their business unit. For example, Company D engages employees—generally at the director level—who are nominated by their risk owner to act as "risk liaisons". When selecting a risk liaison, the risk owner will choose an individual who is closely associated with the particular business unit and knows the details of that unit. The risk liaison understands the business unit strategies and risks and can act as an enabler for their respective function to educate and gather risk information to include in the ERM reporting.[3] When a new risk liaison is appointed, training is provided by a member of the Internal Audit team. The risk liaisons work collaboratively with the other risk liaisons to discuss, review and update ERM risk information. Risk liaisons also provide assistance once or twice a year during the ERM update process. The liaisons review content, including the risk maps and risk dashboard, and provide input for identifying the top 5 to 6 risks for the company. This discussion of risk from a company-wide viewpoint informs the conversations that the Director of Internal Audit has when he reviews the ERM content with the Leadership Team prior to communication with the Board of Directors. The review with the Leadership Team includes review of the risk maps, risk dashboard, risk appetite, top risks, black swan risks, etc. at an overall enterprise level.

Company F also uses the term "risk liaisons" to describe the risk champions from different business units. Although the risk liaisons at Company D are nominated by the risk owner of the unit and are typically at the director level, risk liaisons at Company F may be directors, managers, or VPs who have been delegated or who have volunteered for the role. Similar to Company D, the risk liaison in Company F is someone who knows the strategy as well as the "ins and outs" of his or her particular business unit. Thus, risk liaisons are those that tie the business unit activity to strategy. At Company F, the Director of ERM establishes risk liaisons within business units that serve as key partners in coordinating risk assessments, risk mitigation, and reporting for that function and its risk owners. Although there is no formal training, the risk liaison is familiar with the ERM process. In the most mature examples, each risk liaison will lead his or her individual risk assessment for the business unit and then report back to the Director to integrate the information. Similarly, at Company E each main line of business and functional area has risk consultants who are aligned with a risk liaison from within the risk management area. The risk consultants serve in the key role of maintaining risk registers which track the status of risks and response plans.

Whereas some companies embed individuals as risk champions, Company A utilizes Business Risk and Compliance Committees ("BRCCs"), which give the corporate ERM function a lens into each business area. In its international structure, Company A has pushed BRCCs further down into regional and district committees. Since each region has its own set of risks, each BRCC is responsible for overseeing locally actionable risks and generating local risk registers. In each region, the BRCC is chaired by a manager from the legal or compliance function in that region and the regional president serves as the executive sponsor. The corporate ERM function provides informal training for the chair of each BRCC and is working to develop more formal training procedures to use in the future. The membership of each BRCC consists of the regional

[3] For example, the CFO nominated the Chief Accounting Officer as his risk liaison.

leaders of key functions including finance, human resources, security, etc. The members meet monthly to address the steps in the ERM cycle at the regional level and to discuss current risk issues in their region. The BRCCs formally report through the regional business structure but coordinate activities with the corporate ERM function.

In order to integrate the ERM processes at the regional and district level with the overall ERM process, the corporate ERM function maintains a dashboard to assess the performance and effectiveness of each BRCC. The dashboard is updated on a quarterly basis, and the results are communicated to regional presidents. In addition, the BRCC assessment results will be considered in the overall performance assessment of the regional president. This provides a strong incentive for each regional president to ensure that risks within the region are being managed effectively. By having BRCCs at the regional and district level, regional management can improve the effectiveness of its resource allocation process by recognizing how the top risks may impact strategic objectives and allocating resources in a way that provides greater assurance that objectives will be achieved. At the same time, the corporate ERM function benefits by attaining a more holistic picture of the risk universe by including regional information.

CONCLUSION

While most companies find they would like to extend the reach of ERM even further within their organizations, they have also found some challenges in attempting to engage more employees in ERM processes. In most cases we found the challenges revolved around communication, whether it is how to share the right information with the right employees, how to tailor communications that resonate across multiple divisions and department, or at what level communicating risk information breaches company confidentiality. Additionally, companies have seen challenges with how to connect the granularity of risk issues at lower levels to an enterprise wide view of risks. As the ERM process begins to involve employees at lower levels, it requires that communications be adapted to take into account both the different point of view and the limited experience in risk management of this new constituency.

While there are communications challenges, companies are still seeing benefits from engaging more employees in risk management. With executive management more focused on a high-level strategic view, it is critical that ERM teams work to identify risks facing business units at the operational level. Involving more employees across the business units helps companies identify risks that may seem to have a low impact on individual business lines but combined may represent a significant enterprise risk. Further, lower level employees may see into blind spots that higher level executives may have, and thus have a valuable role in expanding the identification of critical risks.

Companies who participated in the case study and extended the reach of ERM further into their organizations noticed an improvement in their resource allocation processes and an improvement in their business decision-making process. Engaging more employees in the ERM process helps promote sound risk management practices deeper within a company and provides a broader perspective on risk from the local business unit to the global entity wide view. By promoting risk awareness through more levels of the organization, companies can close information gaps between risk identification, analysis and mitigation efforts. These advancements have proven to enhance the overall ERM process and strengthen each company's ability to handle risks.

APPENDIX – A

Organization Description

Company A is a global transportation company operating in the industrials sector with, in its most recent fiscal year, a large market capitalization of over $60 billion and over 450,000 employees worldwide.

ERM Overview

Enterprise Risk Council ("ERC")

While other committees and individual members of the organization play a role in ERM, the ERC is the center of the process where inputs are transformed into actionable outputs. The ERC is made up of roughly 15 business leaders (VPs) that come together quarterly to discuss risks affecting their respective 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 the ERC is to review and discuss the risks identified through the work performed by the ERM functional team. The ERM functional team includes the program manager and his direct reports and works in conjunction with the ERC to profile 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–the 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.

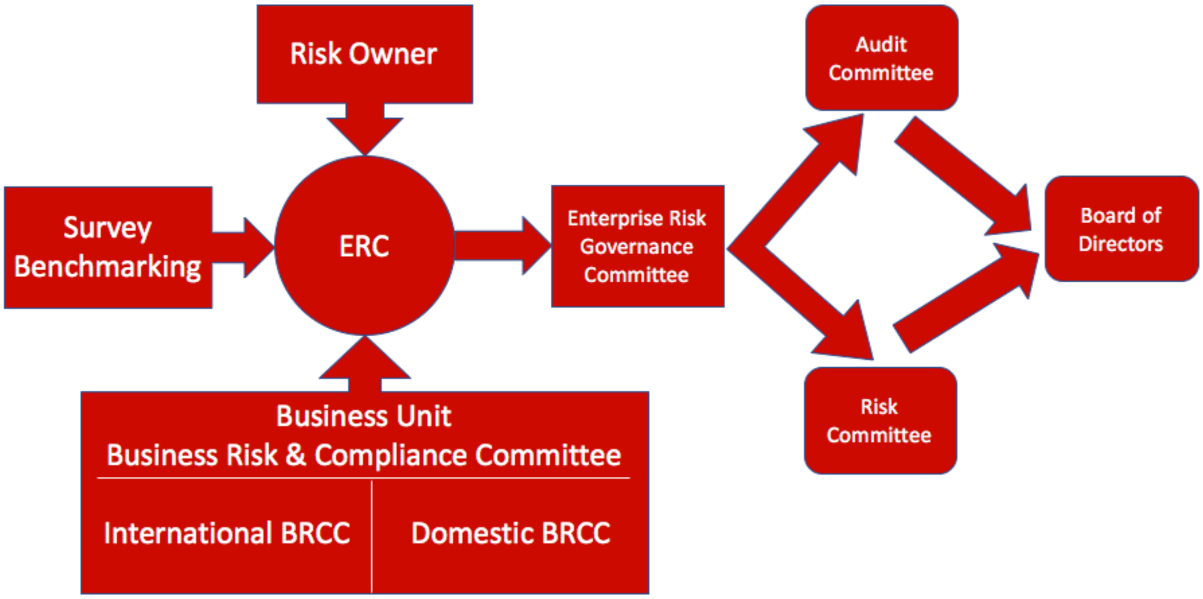


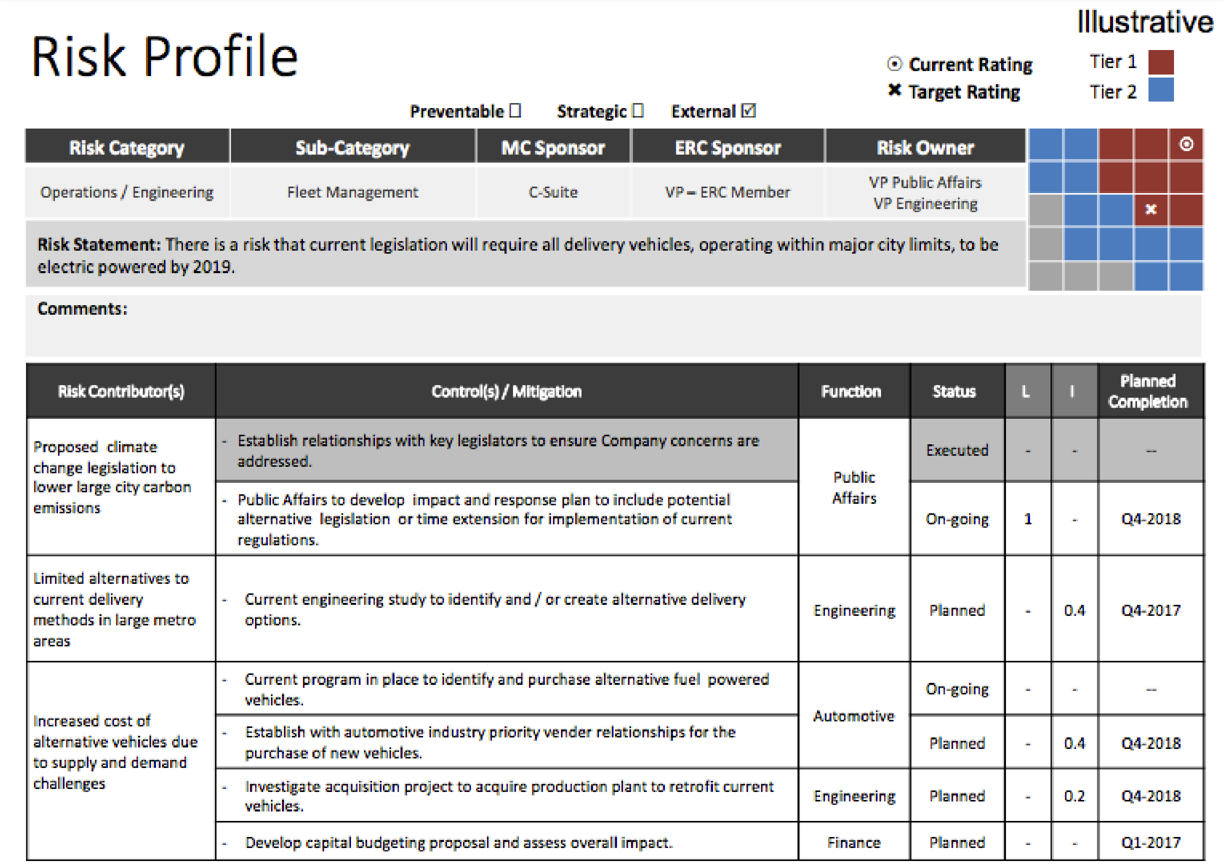
Figure 1

The ERM cycle begins by identifying risks through the use of an annual survey sent out to approximately 900 business leaders across the company. There are mainly two types of surveys the company uses. The first type is open-ended questions that let users give free form responses and the second type provides a list of categories and sub-categories of risks for the respondent to select from. More recently, the company started using more targeted surveys which are customized for each business unit. Company A changes the survey format on a yearly basis in order to incorporate both forms of risk identification and maximize coverage. Identification can also happen at the quarterly ERC meetings; however, 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, Company A also uses external risk studies and peer comparisons such as reports from Protiviti and a regional risk benchmarking group comprised of risk leaders from other companies.

The list of risks identified by this process are compiled by the ERM function and then divided up among the responsible business units. Afterwards, the individual who represents each business group on the ERC, as well as other members of their team, will perform an initial assessment. This employee 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 guided scale is provided 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 description of each of these points is provided on the scale to further assist ERC members in maintaining consistency across their assessments. Once the individual ERC member has narrowed down the risks and provided his or her own assessment, the ERC discusses the risks 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. Enterprise-level risks are categorized into two tiers based on an assessment over two dimensions: likelihood and impact. The risks will further divide into strategic, operational and external areas. 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 risk. 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 an enterprise-wide impact 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" and upload to SharePoint. 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 include all Tier 1 risks and any others that the ERC believes are significant enough to warrant notification to the Board. The Board of Directors may also ask management to review certain risks during the quarterly Board meeting 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. In turn, the Risk Committee will then update the Audit Committee of the Board as well as the full Board of Directors.

APPENDIX – B

Organization Description

Company B is in the consumer cyclical sector and offers a variety of transportation solutions, including products and services. The organization is highly complex and matrixed, operating across five continents and comprised of numerous business units and functions. Currently, the organization is in the medium market capitalization category with total market capitalization between $20 and $60 billion.

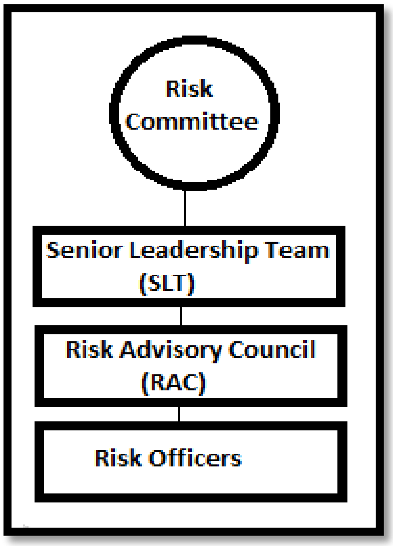
Overview of ERM

ERM Approach and Structure

B's approach to ERM is structured in a way that gives responsibilities from the Board down through the organization. The Risk Committee, a subcommittee of the Board of Directors, is responsible for providing oversight of the company's management of risk and the ERM program and processes. The full Board reviews the results of the annual corporate risk assessment and specific risk topics are reviewed and discussed by the Board or a subcommittee as appropriate.

The company's Senior Leadership Team ("SLT"), which is comprised of the CEO and direct reports, is responsible for the management of enterprise risks and, along with business unit leaders, responsible for the management of business risks. The SLT is also responsible for the management of the ERM program, processes, and integrating risk management into the business.

Each SLT member appoints one of their executives to the Risk Advisory Council ("RAC"). The RAC is responsible for implementing and overseeing risk management processes within the functional or geographical area they represent while also integrating a risk lens into the business. RAC members are also charged to provide timely updates on risks to leadership and escalate items as appropriate. The council meets regularly to discuss current risks, escalate emerging risks and debrief on leadership and Board risk reviews.



Risk Officers are typically leaders and subject matter experts within the business unit or function. They support the RAC, escalating risks as appropriate, assisting in risk assessments, and are responsible for championing risk management into their local areas of the business. Risk Officers are often relied on to bring a deeper, more technical perspective to a risk or mitigation plan given their knowledge within a specific area.

ERM Function

The ERM function in B operates to support the business in their risk management efforts and as an internal consulting group providing unique tools and perspectives. The team contains experts in risks and controls, decision tools and consulting skills. The ERM function also brings in deeper business expertise, relying on knowledge and perspective from those who have been a part of different functions or regions. Overall, the function is centered around three key pillars:

- Embed a risk-aware culture across the enterprise including open, transparent dialog of risk
- Focus on strategic and cross-functional analysis of risk and see around corners
- Ensure consideration of risk and opportunities in decision-making, strategy development, and execution

The ERM function is responsible for conducting the corporate annual risk assessment in order to determine the most critical enterprise risks. This risk profile evolves as data is periodically collected from the business and organized for reporting and monitoring by the ERM team. While the ERM function is playing a key role in supporting each business unit and function, business leaders are ultimately responsible for identifying, assessing and mitigating risks.

ERM Process

The foundational risk management process used by B to identify, assess and mitigate risk is employed during the annual risk assessment and throughout each year as risks arise or need to be refreshed. The general process includes:

- Identify Risks and Scope
- Identify Risk Ownership
- Determine Existing Risk Response
- Assess the Risk
- Determine Mitigation Plans
- Monitor and Report

For each step in the process above, the ERM function has coordinating “tools” in their “Risk Management Tool Kit.” Tools include items such as surveys, workshops, scenario games and analysis. All tools revolve around the concept of cross-functional teams and gathering a variety of perspectives. The tools are discussed below in the context that they relate to the general ERM process.

Risk Identification

As risks are identified, the ERM team reflects on how a risk may tie to the company’s priorities and objectives to determine escalation and the audience that needs to be involved. As previously mentioned, risks are more formally identified during the annual risk assessment in which tools such as interviews and surveys are used but are also bubbled up more informally throughout the year.

One tool the ERM team may use to identify risk is a “Blind Spot Analysis.” This workshop asks participants to think outside the box and identify risks and opportunities around a certain topic or objective. Before the conclusion of the workshop, some prioritization occurs. Thus, groups are able to see what those participants deemed to be the most important risks or opportunities that should be considered as the company makes decisions or executes strategy.

Risk and Strategy Analysis

As previously mentioned, the ERM function uses a variety of tools, or methods, to assist in analyzing risks, opportunities, strategies and decisions. These tools can be used as the business is making an assessment or as they monitor how assumptions or preferences may have changed. While the specific tool applied is based on circumstances and what the business needs deeper insight into, ERM consistently is bringing a cross-functional perspective and pushes participants to consider both internal and external factors.

Tools that are utilized include:

- War gaming
- Game theory
- Workshops
- Interconnected risk analysis
- Social media monitoring

The business has consistently derived value from using skills or tools provided by the ERM team, which is part of the ERM function’s value proposition. The value is also derived from quick turnaround and thoughtful analysis so decisions and actions can be “real time.”

APPENDIX – C

Organization Description

Company C is in the healthcare sector and operates in many states across the country. As a long-standing company in the industry, the company strives to put the patient first and provide quality care. In the most recent year, Company C has a medium market capitalization of between $20 billion and $60 billion.

ERM Overview

Objectives

The ERM program for C focuses on risks at the Executive Management and Board level and is tied to the strategy of the organization. The main objective for the program is to identify and understand significant risks which may affect the achievement of the company's strategic and financial objectives. The Board of Directors provides risk management oversight.

The program aims to strengthen accountability and reporting through the monitoring of risks, remediation efforts, and facilitation of communications across business functions as well as senior management and the Board of Directors. Furthermore, the program helps management rapidly respond to strategic and organizational change. The company is also more adapt at managing emerging risks and gaining competitive advantage when opportunities present themselves. These actions serve to reduce the likelihood and potential consequences of operational surprises.

Structure within C

The CEO is the ERM owner and provides the tone for risk management. The Chief Audit Executive is the executive sponsor of the ERM program and reports to the CEO/Executive Risk Owner. The Assistant Vice President of ERM and Business Continuity Planning has a separate department but reports to the Chief Audit Executive and facilitates the overall ERM process. This office develops and manages the ERM process, including the development of a Risk Universe and the facilitation of the risk identification process through surveys and interviews across the organization. The status of the program is communicated to the Executive Sponsor, Executive Owner, the Board of Directors, and Internal Audit, and is the focal point for ERM activity across the organization.

An understanding of corporate strategy and risk management alignment is crucial to the success of the ERM effort. The facilitator of ERM maintains and tracks ERM trends across the industry by attending ERM conferences, meeting with other companies, and researching best practices to help strengthen and enhance processes and reporting at Company C.

Risk Identification and Assessment

Risk identification and risk assessment are addressed together during interviews of Board members, executive management and division leadership survey risk owners (e.g. entity officers, supply chain officers, and shared services officers, etc.). Survey participation originally only included executive management but has now been expanded to include the Board of Directors, senior management, management, and divisional risk owners from entities. The most recent year engaged 318 participants selected from entities throughout the country. As there are over 175 entities in twenty states, only a few entities are selected per division each year to participate. These entities are chosen on a rotational basis every year, so no entity is chosen two years in a row, but each division is represented for feedback from a wide geographical range.

Surveys and Interviews

Each year the ERM function reaches out to board members, division presidents, CFOs & CMOs, and executive management for a personal interview about risk. In the past year over 120 interviews were conducted. The goal is to interview the leadership of each unit every two or three years. Top executives and key business unit executives are interviewed each year. The process takes around four months.

The surveys are relatively short risk assessment surveys regarding the top three risks, but they provide significant value. The surveys are structured questions with drop down boxes, but also include free form questions. As part of the survey, the ERM group provides a link to a video clip on their website for the survey portal explaining the importance of the employee's participation in ERM which has improved survey response rates. While the video of ERM has increased participation, the surveys still do not have a 100% response rate due to the operational tasks the entities may be facing during the survey period.

The ERM function compiles the interview and survey data and publishes the results anonymously. This publication is then presented to the Board of Directors annually at the company's January board meeting and later distributed to everyone who participates in the interviews. The results are reviewed, and the current action plans and strategies are adjusted as needed. The Board considers the top risks for board and committee agendas during the upcoming year, and they will bring the risk owner to present on the risk and risk mitigation plans. This helps provide a constant assessment of how risks are changing. The Board will provide input on if the risk is put on the agenda, the effectiveness of the risk mitigation plans and offer their opinions if they think the appropriate action is not taking place.

Risk Universe Visualization

Survey participants are provided with a Risk Universe poster prior to taking the survey. The risk universe is a vast document that outlines all risks throughout all the business segments. A special color and number system represent the level of concern and each risk's priority. This tool has been useful to visualize across the traditional business "silos." It helps risk owners to visualize the scope and implication of risks. It is sent with the survey request during risk identification process to set the tone and mindset of risk identification. The distribution of the Risk Universe does not go further than top management at the division level.

Risk Response

It is management's responsibility to manage risks and update response plans as needed. As noted above, risk owners may be asked to present response plans to senior management or the board of directors. The CEO reviews and monitors the most significant risks as well as management's response plans. Additionally, the CEO approves both critical strategic risk responses and critical risk mitigation plans and programs.

Communication and Monitoring

The ERM program aims to strengthen accountability and reporting through the monitoring of risks and remediation efforts. It also facilitates communications across business functions as well as with senior management and the Board of Directors. While risk owners monitor and mitigate the risks they own or can impact, they also provide updates to executive management and the board. They report to the Board of Directors three times a year, and twice a year to the senior and division level management, updating the parties on the status of the identified and emerging risks.

Conclusion

The ERM program's goal is to help the company take a proactive approach to managing risks that may affect the achievement of corporate objectives. The ERM function at C has withstood the test of time, having been in place for over 15 years. While the core elements of the program have not changed, ERM personnel actively work to identify emerging risks and best practices in risk management by attending ERM conferences, meeting with other companies and researching leading practices. This continuous learning process has helped to strengthen and enhance the ERM program over time.

APPENDIX – D

Organization Description

D is a company which operates in the consumer cyclical sector with a market capitalization of under $20 billion. The company also provides financial services such as wholesale and retail financing and insurance programs.

ERM Overview

Risk Management Function: Internal Audit

While other committees and individual members of the organization play a role in ERM at Company D, Internal Audit ("IA") is the group ultimately accountable for the development, implementation, and training of the ERM reporting and update program. In general, IA develops and sustains the ERM process, procedures, tools, and deliverables. Specifically, the Director of IA heads up the ERM process with assistance from the IA team. The Director of IA reports through the CFO.

Risk Management Function: Leadership Team & Strategic Risk Committee

The Leadership Team[4] also acts as the Strategic Risk Committee ("SRC"). Responsibilities of the SRC include the following:

- understanding the risk universe identification, prioritization, and reporting
- overseeing the output of the risk mapping exercises
- periodically reviewing action plans and progress for each business risk
- identifying emerging risks and redirecting resources as needed
- reviewing the risk tolerance framework and metrics
- ensuring risk identification and mitigation is incorporated in the strategic plans
- reviewing the risk dashboard; and determining the frequency and content of reporting

Strategy and Objective Setting

For Company D, the ERM mindset and process is embedded into the company's strategic planning process. In fact, the risk management process informs strategic action. Strategy and objective setting intertwines with ERM in two ways. First, regular risk maps help to inform strategy throughout the annual business planning process. Company D observes the nature and trend of the risks that could impact strategy. Likewise, business units update risks and how risks may impact achievement of objectives. Business units also update any changes in how risks are being mitigated which also informs strategy. Second, Black Swan risk identification helps guide longer term strategic planning. For example, competitor actions and regulatory changes fall under the category of Black Swan risks. Company D takes advantage of opportunities these risks may present as well as thinking through how to mitigate other Black Swan risks.

[4] The Leadership Team includes: the CEO, CFO, COO, VP of Communications, CCO, President of Financial Services, VP of Marketing, and VP of Human Resources, Director of Strategy.

Risk Identification

Company D identifies specific risks through workshop discussions at different levels and within different units of the company. These risks are then grouped at a high level into risk categories such as brand, competition, product, people, legal and government affairs, reputation, etc. Additionally, Company D identifies tail risks also known as Black Swan risks. A Black Swan risk is an event beyond the company's current risk horizon that is not actively monitored (e.g. +5 years). The impact of a Black Swan risk may change a fundamental business assumption, and the nature of the risk could build over time to become significant. The Director of IA facilitates a workshop with a cross-functional group of company leadership to identify Black Swan risks that may affect the future success of Company D and documents the results. Company D has a list of key Black Swan questions that assist in identifying this type of risk.

The Director developed a process for soliciting and synthesizing executive input and prepared pre-read materials that educate participants regarding the Black Swan approach. These pre-read materials describe the risk identification process and include sample Black Swan risks. Finally, the Director assists in preparing a summary report that can be used to brief the Board of Directors.

Risk Assessment

The two primary risk evaluation criteria are the impact of risk and the likelihood of risk. The impact of risk is assessed as either critical, major, or minor. The likelihood of risk is assessed as likely, possible, or remote. To better visualize how these two criteria interact, Company D has placed risks into a heat map comprised of four quadrants. Quadrant I includes risks that are critical and likely. These are high priority risks that threaten the achievement of company objectives. Some of these risks can be outside of the control of management such as regulatory issues. Quadrant II risks are significant risks, but less likely to occur. Quadrant III risks are both unlikely to occur and not significant. Quadrant IV risks are less significant risks but have a high likelihood of occurring.

Risk Response

Company D mitigates risks through the use of "action plans." The risk owners meet 1 or 2 times a year to report on their risks and discuss possible mitigation strategies. D has established action plans for the top three quadrants of risk. Because of their high priority, Quadrant I risks require the creation and ongoing review of action plans. The company facilitates the creation of action plans through the following steps:

1. Describe the action steps in sentences starting with a bullet
2. List as many one sentence, bullet action steps as planned
3. At the end of the action plans, identify the action plan owner name
4. Add the due date for the completion of the action plans

After these action plans are finalized, the risk owner is responsible for implementing the action plan. For Quadrant II risks, action plans have been developed and implemented, and there is evidence that these actions have reduced the likelihood of the risk to "low." Finally, Quadrant

III and IV risks are mitigated through the use of risk monitoring to ensure that the statuses of these risks do not change.

Communication and Monitoring

The SRC, chaired by the (CFO), is responsible for monitoring the ERM process. The SRC is responsible for providing oversight of the risk management, identification, and mitigation processes. It is also involved in the review of adequacy and effectiveness of business risk management throughout the organization. In regard to risks, the risk owners have the role of managing those risks and monitoring mitigation actions, including the effectiveness and validation of those actions. The SRC meets periodically to review action plans and progress for each business risk, as well as ensuring that mitigation is incorporated in the strategic plans.

The SRC facilitates the ongoing monitoring of risks through the use of risk dashboards. Near term risks are those that have an impact on EBIT, and therefore are relevant for the current year. Strategic impact to the business model is more long-term in nature and involves the likelihood of risks occurring that could impact the company's ability to meet their strategic goals. The future risk trend component is used to identify whether the risk's inherent impact and likelihood is increasing, decreasing, or not changing year-over-year. By utilizing this tool, D is able to monitor specific aspects of risks over time. Another way the company continually monitors risks is through risk appetite and tolerances.

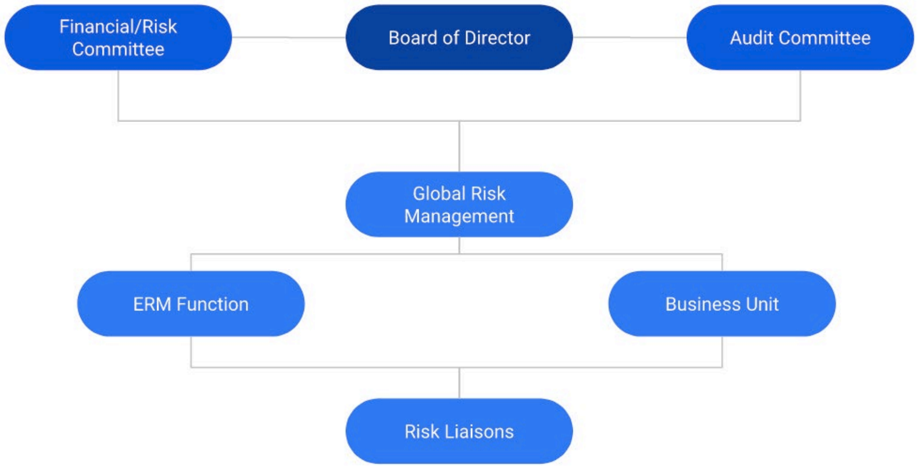
APPENDIX – E

Organization Description

Company E operates in the utilities sector and has a business model that is focused on electric and natural gas infrastructure and comprehensive energy solutions. The company has a medium market capitalization between $20 billion and $60 billion, and over 30,000 employees.

ERM Overview

After a major operational risk event, there was increased focus from the Board of Directors in ERM especially in relation to operational risks. Company E has a policy driven process with the primary risk management committee of the Board approving the overall ERM framework in which senior management individuals focus on areas of risk including project, financial/transaction, strategic, reputational and operational. The Board level finance and risk management committee is charged with oversight responsibility of risk management and observes the risks to the company as a whole. Other committees, such as the audit committee, are responsible for monitoring different aspects of risks. The company has a dedicated Global Risk Management department—including ERM function as subset—which is led by the senior vice president of Global Risk Management who is also the Chief Risk Officer. The Chief Risk Officer reports to Chief Financial Officer. The ERM function collaborates with the business units to identify and monitor risks that impact the enterprise while the business units focus on managing risks that primarily impact their function.



ERM is integrated with the company's strategy and objective setting processes. The risk department partners with the strategy department to make sure the ERM process is aligned with strategy. These two departments also develop potential scenarios in order to conduct stress tests or identify potential opportunities.

Risk Identification techniques are different depending on the type and complexity of a particular risk. Some techniques E utilizes include interviews, surveys, risk workshops, risk bow tie analyses, pre-mortems, and benchmarking. Interviews are conducted at senior management and executive levels to understand the greatest concerns and identify top risks. The business units are not limited by the number of risks that they identify within their area, and the company shares approximately 40 enterprise level risk registers from areas throughout the company. After the identification is complete, risks are entered into the system in an if-then format to communicate a cause and consequence statement of the risk.

Since the end of 2017, the organization has utilized a system from an outside vendor to replace the software solution they used. The new system is robust and includes information regarding the probability and impact of the risk, risk owner, mitigation, response, and evaluation. Risks are also linked to business unit initiatives and this enables business units to identify and track risks to achieving their plan. The software solution also supports a comparison of all risks across the enterprise and helps them to easily identify the major risks to the organization.

Risk assessment is measured through probability and impact. Probability is considered over a five-year horizon which is in line with the five-year business planning cycle. Impact–including financial, reputational and performance (operational, environmental, and compliance) impact–is estimated by the risk owner using historical information, industry data, and experience. The dimensions are ranked on a five-point scale to ensure consistency. The business unit leaders are asked to update the risks at least annually, but preferably quarterly, and more critical risks such as cyber security are updated monthly. Once the company updates the business unit risk registers, a risk matrix is created within the risk system to be utilized processes such as business planning, decision making, resource deployment, allocation of resource, etc. The ERM group has regular discussion with risk liaisons within the business units. They also collaborate with Corporate Communications to assess reputational impact for each risk. The leaders in charge of the top risks will have discussions with executive management on an annually, quarterly or monthly basis depending on the significance of the risks.

The organization uses a top-down and bottom-up approach in its risk assessment. The interviews conducted at executive levels mentioned above provide assessment from the top levels. That top-level assessment of risk is then paired up to the bottom up results from the register reviews to create the top enterprise level risks—around 12—annually that are presented to the Risk Committee of the Board of Directors. Many of these top enterprise level risks are broader categories that encompass a number of lower level risks.

After the company's major operational risk event noted above, the company placed increased focus on identifying tail risk which is a low likelihood and high impact risk. These are noted during the risk assessment process in the risk system and there are currently 44 tail risks. Mitigation strategies have been developed for the major tail risks. Company E sees great value in monitoring tail risk. By mitigating some of the tail risks, E 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 concerns.

Company E uses KPIs to monitor business performance, and they can serve as early warning signs for potential risks to trigger. The business units handle monitoring procedures and the 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. They monitor the risks trends and discuss with risk consultants to look at various KPI's.

An Enterprise Risk Summit is held twice a year to discuss risk management. The ERM team within Global Risk Management leads the Summit. The business unit risk consultants and individuals from risk management department participate in the Summit and have discussions about key topics regarding risk management. For the upcoming Enterprise Risk Summit, Company E will have a discussion of the new risk management software tool recently implemented and will also host a presentation from the security team on both cyber and physical security.

APPENDIX – F

Organization Description

Company F is in the consumer cyclical sector and has a business presence in the US, Canada and Mexico. Currently, Company F has a large market capitalization of over $60 billion.

ERM Overview

ERM Function

At Company F, the ERM function is led by the Director of ERM who reports to the VP of Risk Management within the Finance organization. While he has the help of a "team" of other employees who support risk management efforts, the ERM Director is the sole facilitator of ERM activities across the organization. The "team" refers to informal risk liaisons and formal risk owners found in other areas of the company. For example, a manager working in international sourcing may serve as a principal risk liaison (coordinating risk assessments, risk mitigation and reporting for that function and its risk owners) and have regular communications with the ERM Director. The ERM Director also has a strong partnership with Internal Audit and its risk assessment and audit planning work as well as officers in the Legal Department.

Strategy and Objective Setting

In addition to its partnership with Audit and Legal, the ERM function at Company F works with the strategic planning group throughout the entire planning cycle. The strategic planning group includes a team of employees who think through trends, evaluate competitive markets, and business development opportunities. Working with that group, the ERM Director looks at the inherent assumptions and risks of the current strategy such as competitors, disruptors, market conditions, internal capabilities, etc. Routinely, Company F, through strategy sessions, risk workshops and other events, engages leadership in discussions around future planning and emerging risks for up to the next three to five years. Afterwards, the Director meets with the risk-facing business units to think through underlying assumptions and inherent risks to the strategies defined.

Risk Identification

In regard to risk identification, the Director of ERM conducts a survey once every other year. These surveys are typically sent to as many as 700 managers/directors and above from multiple business units and functions from across the company. Generally, the surveys ask targeted questions relevant to the specific business unit or strategy or through open-ended questions exploring issues like emerging risks or risk blind spots. The survey responses are used to identify new risks and help to define the scope of follow up discussions, interviews and workshops. The purpose of the interviews is to force a dialogue of things typically not spoken. Thus, the Director uses risk conversation starters to facilitate the discussion. For example, the Director may ask "What do you think is the greatest threat to the company's brand?" or "What significant event risk do you think could jeopardize the company's future?" It is not unusual for the Director of ERM to engage as many as 40-50 stakeholders over the course of a month to review or report on risks and risk mitigation activities.

Risk Assessment

Company F has developed a formal risk assessment methodology. This methodology begins with articulating the company's strategy and objectives and the key risks that the company faces. The pursuit of some opportunities or strategies give rise to certain risks, while in some cases strategies may be defined to address risks or threats identified. These risks are gauged on along several scales:

- Likelihood – how probable or frequent is the potential risk?
- Impact – what is the magnitude of the risk?
- Capability – how prepared or vulnerable is the organization?
- Velocity – how rapidly might this risk change?

Once assessed, the risks are placed into a hierarchy. At the top, risk categories are the highest-level groupings of risks reflected in risk tiers of significance. Next, component risks are a more detailed set of risk definitions, or risk universe, that make up the risk categories. Last, risk drivers are statements that capture the specific risks and issues; they are what risk owners address directly. These tiers can either be order ranked or placed in a "heat map" considering the interdependencies between risks.

It is paramount that the company "gets the best" out of both the quantitative and qualitative factors. Sometimes an employee may bring up an issue that might not be big picture enough to be considered a true risk. To ensure that no one is ignored, the Director will make a note of the more granular issues and communicate that such note has been made to the reporting employee.

Risk Response

Each risk is assigned a risk owner or owners, who are typically the head of the specific business unit principally affected by the risk. Each risk owner is responsible for developing and reporting on appropriate risk responses with the ERM Director serving in a facilitator role.

Communication and Monitoring

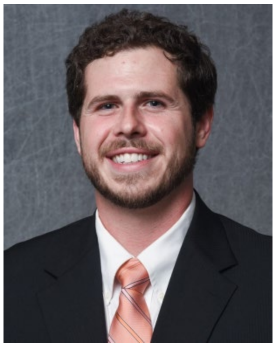
Through the use of risk driver dashboards, Company F connects risks to their specific owners and monitors trends in the risks and the results of risk mitigation activities. The risk dashboard separates the risk into its tiers—category, component, and driver—and illustrates trends associated with each risk category and risk driver. The dashboard notes the overall trend, the trend of internal capabilities, and the trend of external threats. In addition to noting the separate trends, the dashboard also highlights the speed of onset associated with each risk category or risk driver.

Risk owners report to the ERM Director regarding top risks and risk mitigation activities on a quarterly basis. This report includes any major implementations or improvements and what risks can be addressed through these improvements.

Risk Culture and Leadership

Company F exhibits a strong-values based culture that really drives the perspectives and approach to ERM. The company has a strong sense of its purpose in serving customers and supporting employees. With such a positive, focused mission and a strong risk management culture endorsed by leaders at all levels, ERM at Company F has the support it needs to continue to mature.

ABOUT THE AUTHORS

	Stephanie Clark is a graduate student in the Master of Accounting program at NC State University where she is concentrating in Enterprise Risk Management. Upon completion of her Bachelor degree from North Carolina State University, she accepted a position as an Accounts and Operations Manager for a local manufacturing company where she has worked for four years. After graduation, she will be working as a Risk Advisory Associate with a public accounting firm in Charlotte, NC.
	**Russell Thornton** is a licensed attorney and graduate student in the Jenkins Masters of Business Administration (MBA) program at NC State University where he is concentrating in Financial Management. After earning his Bachelor of Arts degree in Economics with a minor in Spanish from the University of North Carolina at Chapel Hill, he matriculated into Campbell University Norman Adrian Wiggins School of Law. He earned his Juris Doctor (JD) in May of 2017 and passed the North Carolina Bar Exam the following summer. As a dual degree student, he is now completing the remaining requirements for the MBA and will graduate in December of 2018. Upon graduation, he hopes to work in corporate law and possibly in the areas of mergers and acquisitions or privacy and data security.
	Wenxin (Laura) Liu is currently pursuing her Master of Accounting degree with a concentration in Enterprise Risk Management at NC State University. She is originally from Xi'an, China, where she earned her Bachelor of Economics degree. Before she came to NC State, she earned a Master of Science in Finance degree from the University at Buffalo, State University of New York and worked in the New York area for a year as a Financial Analyst. After graduating from the MAC program, she plans to pursue her career at a public accounting firm.