NC STATE Poole College of Management
Enterprise Risk Management Initiative

MANAGEMENT LEVEL RISK COMMITTEES: AN EFFECTIVE ERM TOOL

Prepared by: Michael Gore, Lucas Hyde, James Merritt & Na'thia Moses
NC STATE GRADUATE STUDENTS | POOLE COLLEGE OF MANAGEMENT
FACULTY ADVISOR: Bonnie V. Hancock

Table of Contents

INTRODUCTION

The central purpose of the Risk Committee Case Study is to provide examples and analyze how companies across various industries are using management level risk committees as part of a broader Enterprise Risk Management (ERM) process. Companies employ risk committees at the management level for a variety of reasons. One common reason is to bring together a multidisciplinary team to take an enterprise view of the risks facing the company. Risk committees may also be responsible for assessing and/or monitoring risks and risk responses, and providing input into the ERM process itself. This case study will examine the way risk committees are used in each of the six companies represented.

These case studies were conducted by first understanding each company and its strategy, then gaining an understanding of the overall ERM process, and finally, by delving into the specifics regarding the use of risk committees. The companies included in the study have had a risk committee structure in place for a minimum of 5 years, and some as long as 15 years. The review of six different organizations reveals a variety of approaches to risk committee design likely reflecting the differing needs of each company which could be driven by industry participation, strategy, business model, culture, and maturity in ERM implementation

Below is a summary of companies that are represented in this case study:

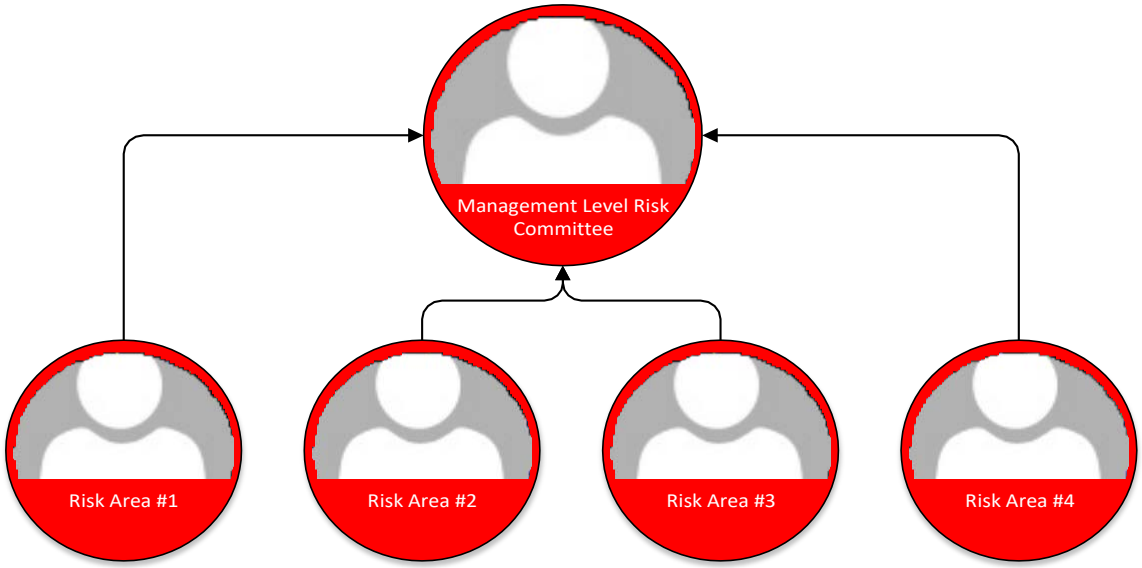
	A	B	C	D	E	F
Industry	*Insurance*	*Drug Manufacturer*	*Savings & Loans*	*Air Delivery & Freight Services*	*Independent Oil & Gas*	*Personal Products*
Revenue	$8.5 Billion	$21 Billion	$350 Million	$60 Billion	$13 Billion	$11 Billion

MANAGEMENT LEVEL RISK COMMITTEE ANALYSIS

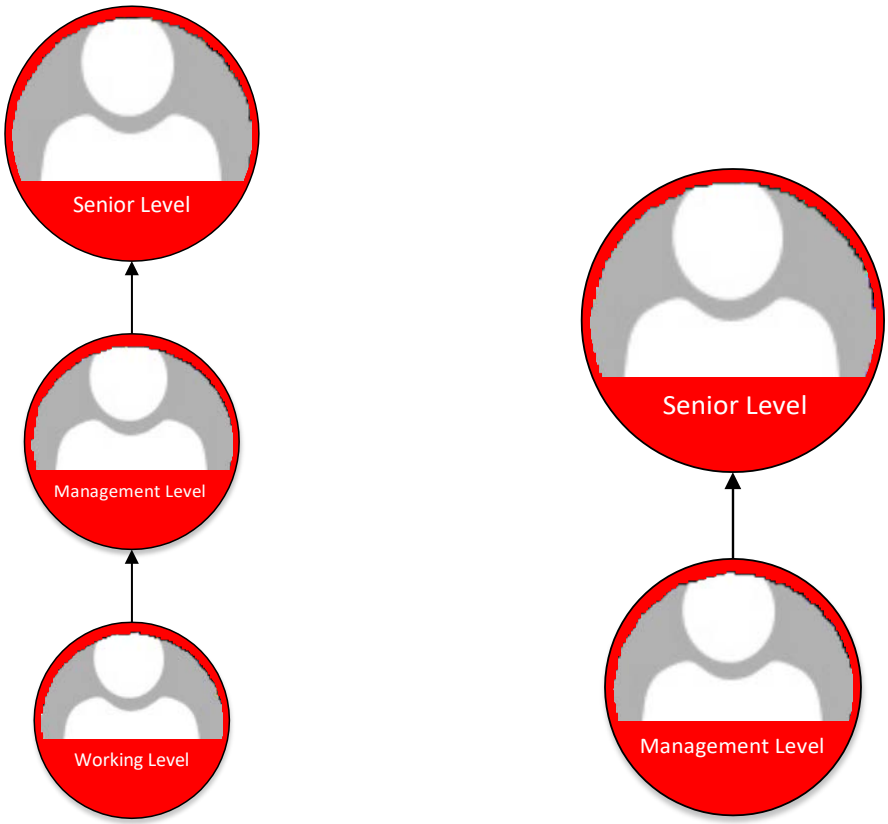
Structure and Composition

All the companies we analyzed had a charter for the management level risk committee. The charter would typically outline the purpose and authority of the committee, its composition and meetings, and its responsibilities and duties. When comparing the companies, we saw considerable variation in the structure, composition, and organization of their management level risk committees. Some of the structures observed included the use of multiple risk committees, typically by using subcommittees focused on specific risk areas within the business that funnel information into an aggregated, enterprise risk committee. For example, C and F's risk committee structure, as depicted below, contains a single

overarching enterprise risk committee, with multiple sub-committees pertaining to distinct risk areas that roll up to it.



In other instances, such as the case of A and D, the organization of management level risk committees was more hierarchical in nature, representing different levels of management. A had two levels of risk committees while B had three levels; both are shown below:



It is important to note that in the above illustrations, each "circle" represents what the company would consider a separate management level risk committee, which is distinct from the corporate risk management teams or individuals in the ERM function who facilitate risk management activities. Throughout the rest of the paper we will be focused on the primary enterprise-wide risk committee that is at the management level.

Ideally, a management level risk committee should be composed of members that can contribute to an enterprise view of the organization and that have a good understanding of effective risk management techniques. While there was a wide range of titles and functions represented in the various management level risk committees in our study, most of the differences were driven by differences in the industry or business models. Although the specific members who sit on the committee are tailored towards the individual business under review, we found that a commonality between the companies was that all the committees analyzed included members that represented each significant line of business and corporate function. The common corporate functions typically represented included human resources, accounting and/or finance, legal, information technology, public policy and internal audit. In addition, some committees included functions like strategy, communications, and quality. It should be noted that when certain corporate functions do not have representation on the committee, corporate ERM personnel often partner or work in conjunction with those functions, particularly when it is a function that performs risk management activities that are pertinent to the responsibilities of the management level risk committee. This cross-functional approach to management level risk committee membership allows for the organization to capture multiple views and expertise in the overall discussion of risks affecting the entire enterprise.

The commonality between the companies was that all committees analyzed included members that represented each significant line of business and corporate function.

Management level risk committees represented in our study were most often chaired by the Chief Risk Officer. In the situations where the Chief Risk Officer was not the chair, the executive named to chair the committee usually had a role leading the compliance, ethics, or legal function. In one case the committee was chaired by the Chief Operating Officer. The duties of the chair were consistent with the typical duties of a committee chair.

Roles and Responsibilities

Across all the companies we studied, the key purpose of the management level risk committees is to initiate a dialogue and provide a forum for members from across the enterprise to openly discuss risks. While most of the risk identification and assessment work is done outside the committee by the corporate ERM function, the committee typically plays a key role in synthesizing and assessing risks to either recommend to a higher-level committee or to approve the list of the most critical enterprise level risks. In some cases, the risk committee would work together to develop for each of those top risks a profile that would contain a description of the risk, the owner of the risk, key metrics, response plans, etc. Once those top risks have been established, the risk committee then plays a key role in monitoring

the risks as well as the effectiveness of response plans. Each organization referenced revisiting, modifying, or updating risk profiles, inventories, and assessments at each management level risk committee meeting. This regular updating process helps to ensure that risk response plans are kept current, and that the risks themselves are kept current so that a risk that may no longer be a threat can be replaced by another risk that may now merit the attention and resources of the committee. The time horizon the committees used when considering risks ranged from 1 to 7 years but was commonly within 3 – 5 years. These timeframes were often subject to change depending on a wide array of reasons from economic forces to environmental regulation.

> The committee typically plays a key role in synthesizing risks, assessing risks, building risk profiles, monitoring the risks, and monitoring the overall effectiveness of the risk response plans.

In all cases, the role of the risk committee was not to develop responses to risks; that was the responsibility of the assigned risk owner. Instead the committee's role, in most cases, was to review and evaluate those response plans and provide feedback to the risk owners. None of the organizations analyzed had quantified risk appetite, however, appetite was indirectly considered when a specific risk and response plan was being determined as acceptable or not. Risk responses would then be re-evaluated periodically to ensure that they are adequately and effectively mitigating the appropriate risks. When the monitoring and evaluation of these responses was not within the scope of the management level risk committee itself, that role was performed by some other business function within the entity, such as Internal Audit.

Another key role of the management level risk committee is to serve as a key reviewer of risk information before it is more broadly disseminated. Though there were disparities in how and to whom information from committee meetings was communicated, in all the companies we studied, the key information, decisions, and takeaways from the risk committee meeting were ultimately communicated to the board of directors or a committee of the board of directors. In most cases either the senior executive responsible for risk management or a committee of senior executives would review the risk information before it went to the board level.

All management level risk committees in our study kept meeting minutes, and typically this function would be carried out by the corporate ERM function. In addition, updated risk profiles would also be documented. Typically, the most important items captured in the minutes were action items or "to-do" lists that members of the committee needed to take back to their organizations or that the corporate ERM team needed to address. The documentation gathered and created by the committee is vital to the risk monitoring process.

Operations

In all cases, agendas were developed in advance for each risk committee meeting. Typically, those agendas would be developed by the corporate ERM function. In some cases, such as C and E, standard agendas were developed at the beginning of the year so that the work of the management level risk

committees aligned with key dates in the entity's overall planning and reporting cycle. In other cases, agendas were more fluid, and were developed with input from committee members and senior management on the issues that needed to be addressed. Among the companies studied, management level risk committees met at least quarterly, except for E which held semi-annual meetings. Companies representing the insurance and savings and loan industries met more frequently than quarterly with A meeting monthly. In addition, all companies noted that "ad hoc" meetings could be called when a significant issue arises.

Keys to an Effective Management Level Risk Committee

Participants in our study cited numerous factors that were key to having a management level risk committee function effectively. The three things that were cited most consistently by the ERM leaders in the study were open dialogue, engagement by committee members, and clear communications. Open dialogue is accomplished by providing a "safe" forum for sharing your risks, one in which the person will not be judged or get a slap on the wrist. The purpose of the committee and the ERM function is to make sure that risks are addressed appropriately, not to assess blame, and that message needs to be emphasized. Keeping the focus of the committee on things that are relevant, updated, and educational will go a long way towards keeping committee members engaged. In addition, engagement can be fostered by the corporate ERM team through building relationships with and educating business leaders on the value that comes from a risk committee. Finally, clear communications can be accomplished by developing transparent and concise definitions of risks, and establishing a line of communication between employees at all levels of the enterprise. The members of the risk committee have an important role in the communication of risk information.

In addition, several ERM leaders pointed to the importance of maintaining structure and protocols in the meetings, including providing agendas and materials in advance to ensure you are making the most effective use of business leaders' time. Consistency in providing these materials, as well as making sure to follow up on any questions that come out of the meetings, sets the tone about the importance of risk to the company. Another factor that was mentioned more than once was the importance of having accountability from risk owners and the full attention of the business decision makers who must ultimately hold those risk owners accountable. As stated by the leader of ERM at E: "Nothing will happen to the risks if you don't have the support of the decision-makers." Accountability from risk owners who are often members of the management level risk committee will also serve to increase engagement with the committee. In addition, there were some important factors in risk committee effectiveness that were unique to individual companies. B believes that having visibility and transparency of the overall risks to the company is important as management constantly battles between which risks should be elevated to the enterprise level and which risks merit the most attention and resources. Having an effective risk

"Nothing will happen to the risks if you don't have the support of the decision-makers."

committee allows for consensus building around the top risks as well as oversight of the implementation of proper control activities. B also noted that having a methodical, disciplined approached to an ERM Program that is heavily integrated into the strategic planning process promotes effectiveness.

C noted the importance of working towards a risk intelligent culture that doesn't just see risks as purely bad, but knows how to embrace certain risks to find opportunities. As part of that, it was also noted that being more directional versus prescriptive improves effectiveness. C observed that going from a qualitative understanding of risk to a quantitative action-oriented view of risks gives consistency across economic cycles. Finally, E suggests leveraging existing processes and carefully pacing the adoption of ERM processes to be sure that you don't add too much too fast. Overextending risks the loss of support at the executive level of the company. For example, if you try to force monthly meetings, or the development of a precise risk appetite statement, then the process could be viewed as too bureaucratic and potentially be shut down before it gets off the ground. Each of these factors play a significant role in determining the effectiveness of a management level risk committee.

CONCLUSION

Risk Committees serve a vital function in the ERM process by bringing together a cross-disciplinary group of people to take an enterprise view of risks and to engage those same individuals to promote risk awareness and sound risk management practices across the organization. Based upon the companies we studied, there were several key considerations in the formation and operation of risk committees.

First, just like most ERM processes, there is no one size fits all approach to risk committees. Some companies found having a single management level risk committee to be very effective, while others had a primary risk committee with multiple sub-committees below it to address specific types of risks, and some others found it effective to have one risk committee at the vice president level and another above it at the senior management level. These structures worked effectively for the companies studied; it is simply a matter of designing a structure that works best in each individual organization.

One very important factor in organizing a risk committee is ensuring that all major areas of the company are represented on the committee so that inter-relationships among risks can be identified, and an enterprise level view with coordinated risk mitigation plans can be developed. In addition, the members of the committee can be used to "spread the word" about risk management across the organization. The important point for all risk committees is to create an open atmosphere where there is no hesitancy to share risk information or concerns over the adequacy of risk response plans. This allows for risks to be given full consideration and provides an opportunity to address any concerns. Another key consideration is maintaining the engagement of risk committee members. The best way to do this is to ensure that committee meetings focus on the most significant risks facing the company and for those risks, keep the information as current as possible. Finally, the risk

An effective risk committee, aligned with the strategy and overall objectives of the company, is a crucial tool that will enhance a company's overall ERM program and its ability to deliver value to shareholders.

committee plays a key role in communicating risk information throughout the company, both formally and informally. An important function of the risk committee is to synthesize and clarify risk information and highlight the most critical risk issues facing the organization. This is vital to communications that may ultimately be shared with employees at all levels of the company as well as those communications that may ultimately be shared with the board of directors. An effective risk committee, aligned with the strategy and overall objectives of the company, is a crucial tool that will enhance a company's overall ERM program and its ability to deliver value to shareholders.

APPENDICIES: INDIVIDUAL COMPANY CASE STUDIES

APPENDIX A

Company Overview

Company A (A) is a Fortune 500 company that operates in the insurance industry with annual revenues of $8.5 billion. A has been dedicated to helping customers achieve and protect the comfort of their financial security, by offering an array of insurance products. A's business model is made up of five operating segments. This diversification of operating segments allows A to embrace strategic opportunities to assist their customers in all 50 states, and more than 25 countries worldwide.

ERM Overview

ERM Framework

A's multi-faceted ERM framework compliments a strategic business risk focus by identifying, assessing, and managing risks to the company's strategic objectives. A's ERM framework consists of six key components that encompass their risk management process: Set Strategies/Objectives, Identify Risks, Assess Risks, Manage Risks, Control Risks, and Monitor and Communicate.

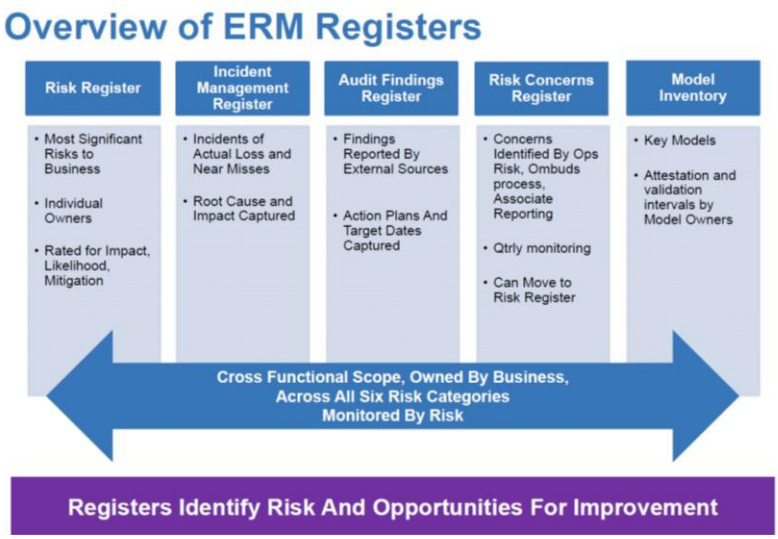
ERM Structure

A's ERM program is led by an ERM director and his staff. The ERM team is one of multiple teams that report to the Senior Director of Risk Management who in turn reports to the Chief Risk Officer. The ERM team performs regular quarterly risk identification and assessment procedures with first line of defense process owners who ultimately own the risks. The ERM director is part of the ERM Working Committee, which is comprised of the director of ERM, the Senior Director of Risk Management, the Vice President of Compliance, the Financial Controller, the IT Controller, and the Chief Information Security Officer. This cross functional team is mainly tasked with reviewing the risk register as well as other information in order to provide input and escalate risks to the board level risk committee. In addition, new risks may be identified in any area of the business and then escalated, as warranted, to be reviewed by the ERM Working Committee. The company's top risks are identified using a standardized internally developed rating scale. The company's top risks, as identified by a risk score, are reviewed during risk committee meetings that occur on a quarterly basis. The risks are displayed in a heat map and the residual risks in the red portion of the heat map are considered to be the "top" risks. At any one time, there are typically 8 to 10 "top" risks. Once the top risks are approved, the management level risk committee will communicate those risks to the Business Unit 3 Risk Committee, who will then share them with the Board of Directors. In addition to the "top" risks; additional risks based on risk categories are discussed at management level risk committee meetings that occur at different times during the year.

ERM Process

A's ERM model has evolved over seven years into a mature model which they define as "a continuous, multi-faceted process driven by business strategy." A has made it a focus to establish risk registers that show a complete portfolio of material risks that the company faces in meeting its strategic objectives. Due to the nature of A's business, they have a prudent risk seeking culture that looks for potential opportunities for growth. The company uses a Specific, Measurable, Actionable, Realistic, and Time-Bound (SMART) framework for describing and managing risks.

A manages its risks using four distinct registers: Risk Register, Risk Concerns Register, Incident Management Register, and an Audit Findings Register. On a quarterly basis, the ERM team performs a risk assessment based on each risk register. In addition, the functional unit leaders are asked if there are any new material risks that should be tracked on the register. The ERM team sends out electronic surveys to the leadership teams of each business function (75 individuals) of their U.S. operating segment, to perform a "systematic and comprehensive review of risks to the company", and to identify any new or emerging risks the company may face going forward. During the surveys, all risks previously identified and any new emerging risks are assessed. The information is then aggregated into the Risk Register in the business' ERM system. The risks are rank ordered on both an inherent basis, (based on impact, and likelihood) and on a residual basis (based on impact, likelihood, and control effectiveness). The ERM Team then presents the top residual risks to the management level risk committee, comprised of the CEO and other chief officers, for their approval. During a risk committee meeting, each of the top risk owners speak to each of their risks and the plans to address said risks. In some cases, the management level risk committee may make changes to those top risks prior to their approval. These top risks are communicated by the management level risk committee to the Business Unit 3 Risk Committee. Ultimately these risks that have been deemed to be the most important are shared with the Board of Directors. All other risks and responses in the risk register are communicated to the proper business process owners who are charged with being the champions for their risks that specifically affect their respective business units.



Throughout the year, A carefully monitors the effectiveness of their risk management process in several ways. First, the company promotes an open risk culture, and implements the use of a risk concerns register to document concerns raised throughout the year by employees. In addition, A maintains an incident management register to compile a list of incidents that have occurred within the company and their actual or potential impacts. This process is facilitated by an incident reporter (the first employee to encounter the incident), who reports the incident to an incident manager (the incident reporter's direct supervisor), and an incident owner (designated by the incident manager) who has the "best line of sight" into the incident. The incident owner will provide feedback and complete an "Action Plan" to give to the incident manager. The incident manager is the first point of contact for ERM, and tracks the Action Plan, as well as performs a root cause analysis to determine the root cause behind the incident. This information is documented in the incident management register and used to formulate key risk indicators (KRIs) that can be used to help preemptively detect and avoid similar incidents in the future. Incidents are mapped back to identified risks and can affect future ratings of those risks. Finally, A uses their audit findings risk register to record any findings from any audits (internal, external, regulatory,

etc.) performed on the business. These findings may help to identify new or emerging risks to the company, or change the residual risk assessment for risks in their other registers.

Management Level Risk Committees

Risk Committee Overview

A consists of three management level risk committees: the Senior Corporate Level Risk Committee, the Management Level Risk Committee, and the Working ERM Committee. These management level risk committees report in a hierarchical fashion with the Working ERM Committee, reporting to the Management Level Risk Committee, who then reports to the Senior Corporate Level Risk Committee, who ultimately reports their findings to the Board of Directors. With this information in hand, the Board of Directors approves the final top tier risks and sets risk limits. The Board then communicates these risk limits down to the Management Level Risk Committee to sets authorization limits for employees who are allowed to override risk limits in certain situations. This information is then disseminated in a similar fashion down the hierarchical ladder. For purposes of this case study we will mainly be focused on the Working ERM Committee and the Management Level Risk Committee.

Working ERM Committee

The Working ERM Committee is the management level risk committee that is the most closely tied to Business Unit 2's ERM program. This committee is made up of five key members, the ERM Director, the Senior Director of Risk Management, the Vice President of Compliance, the Financial Controller, the Information Technology Controller, and the Chief Information Security Officer. The ERM director chairs the Working ERM Committee and records the official minutes. The Working ERM Committee has been in its present form for over 3 years, and meets twice per month for 1 hour sessions. The agendas for these meetings include review of identified risks, issues, or incidents that may occur throughout the business. The cross functional nature of the committee facilitates the identification of enterprise wide issues that should be discussed. The Working ERM Committee typically uses a 1-2 year forward looking lens when examining emerging or strategic risks, but takes a more real-time approach to known operational risks such as market price fluctuation risks. On a quarterly basis, the ERM director sends out surveys to the leadership of each primary business function (approximately 75 individuals) for their U.S. operating segment, to perform a "systematic and comprehensive review of risks to the company", and to identify any new or emerging risks. The results of these surveys are brought into the Working ERM Committee meetings and are discussed throughout the year. The risk register is dynamic and risks can be added or removed throughout the year. The ratings of each risk can also change throughout the year. Risks are ranked by their inherent and residual values related to impact and likelihood. The business is currently tracking approximately 70 risks. A subset of those 70 risks that are above a certain threshold of likelihood and impact are taken into Working ERM Committee meetings and presented by the ERM director to the Management Level Risk Committee.

Management Level Risk Committee

The Management Level Risk Committee meets monthly for 1 ½ to 2 hour sessions. The Management Level Risk Committee is made up of the CEO and their entire direct staff as well as other senior leaders. The CRO chairs the Management Level Risk Committee, sets the agenda, and distributes any pre-reading materials for the meetings throughout the year. The CRO is also responsible for maintaining official risk committee minutes. These minutes are emailed out to all attendees, and outline the topics discussed, decisions made, and any action items that members are responsible for completing before subsequent meetings occurring later in the year.

The Management Level Risk Committee focuses on material risks to the business. The ERM director will present these top, material risks faced by the business, as identified through the quarterly risk surveys and discussions by the business risk owners. In these meetings, the Director of ERM will present the top risks along with their current ratings. The owners of each top risk, will provide an update as to why they believe the risk rating is accurate as well as what action plans are in place to mitigate or accept the risk. The Management Level Risk Committee then decides whether the presented top risks are rated correctly and if they are satisfied with the action plans to address said risks. The committee can also elevate a lower ranked or an emerging risk to priority level during that same risk committee meeting, if deemed necessary. The ERM top risk discussion occurs on a quarterly basis; however, any risk can be discussed at any risk committee meeting as warranted. The top risks are also shared with Business Unit 3's risk committee. In addition to the discussion of top risks, the ERM team will also schedule a discussion of special risk topics to be assessed at the Management Level Risk Committee meetings. Those topic discussions will be led by the appropriate subject matter expert. Business Unit 3 will then share the top risks to the board of directors. The board will set high level risk appetite and authority limits. The risk appetite and authority limits are shared with the Senior Corporate Risk Committee. The risk appetite and delegation of authority is then discussed and approved for Management Level Risk Committee members. The Management Level Risk Committee then translates the high-level risk appetite and delegation of authority into more detailed actionable expectations for Business Unit 2 and the Working ERM Committee. The Working ERM Committee is then responsible for ensuring all primary business functions are made aware of the material risks and ensure that these risks are being managed and/or mitigated. The Management Level Risk Committee ensures that the risks are being managed within Business Unit 2's established "Risk Appetite". Neither the Management Level Risk Committee, nor the Senior Corporate Risk Committee is responsible for setting the overall risk appetite, but they do influence the ultimate decision for the risk appetites of top risks. After the risk appetites are decided upon by the Board, the Management Level Risk Committee is responsible for linking those risk appetites with authority delegations for all leadership functions within the business. In their regular monthly meetings, the Management Level Risk Committee pulls in data from RADAR and the residual risk profiles to assess how well risk responses, formulated by primary business functions leaders, have worked to keep the residual risk scores within their company's accepted risk appetite levels. Also, on a regular periodic basis, the multiple ERM teams within the business will share best practices for assessing, managing, and communicating risks across the businesses.

APPENDIX B

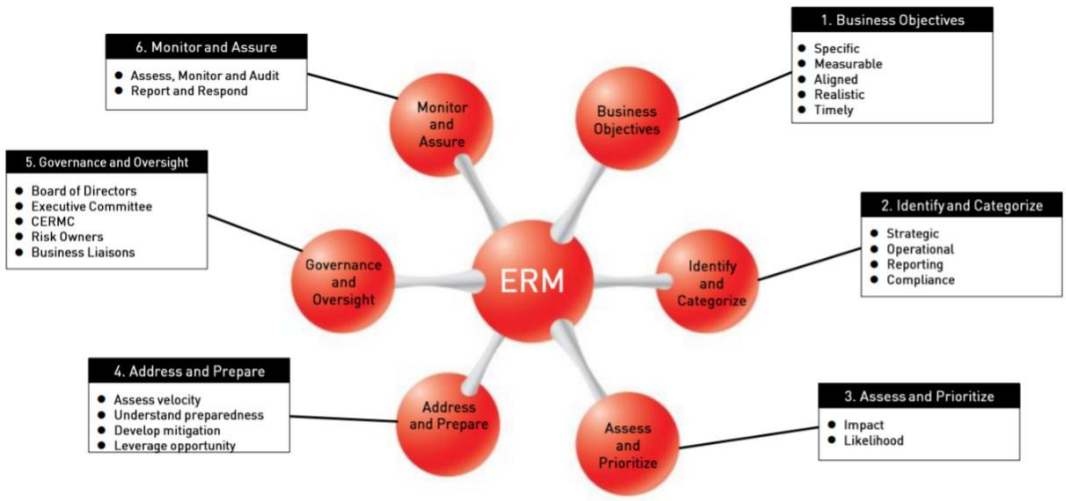
Company Overview

Company B (B) is a global pharmaceutical enterprise that discovers, develops, manufactures and markets both human pharmaceutical and animal health products. Research, development, and the resulting creation of intellectual property or the purchase of other intellectual property such as patents and trademarks, are critical to their ability to successfully commercialize their medical innovations and invest in the future ability of pharmaceuticals. Reported revenues are over $21 billion during the most recent fiscal year.

ERM Overview

ERM Framework

B's ERM framework supports a business-focused risk management process that aligns risk identification, prioritization, and mitigation activities with the company's efforts to achieve key business objectives. As indicated by Figure 1 below, there are 6 major components that guide the development of their risk management process: business objectives, identify and categorize, assess and prioritize, address and prepare, governance and oversight, and monitor and assure.



ERM Structure

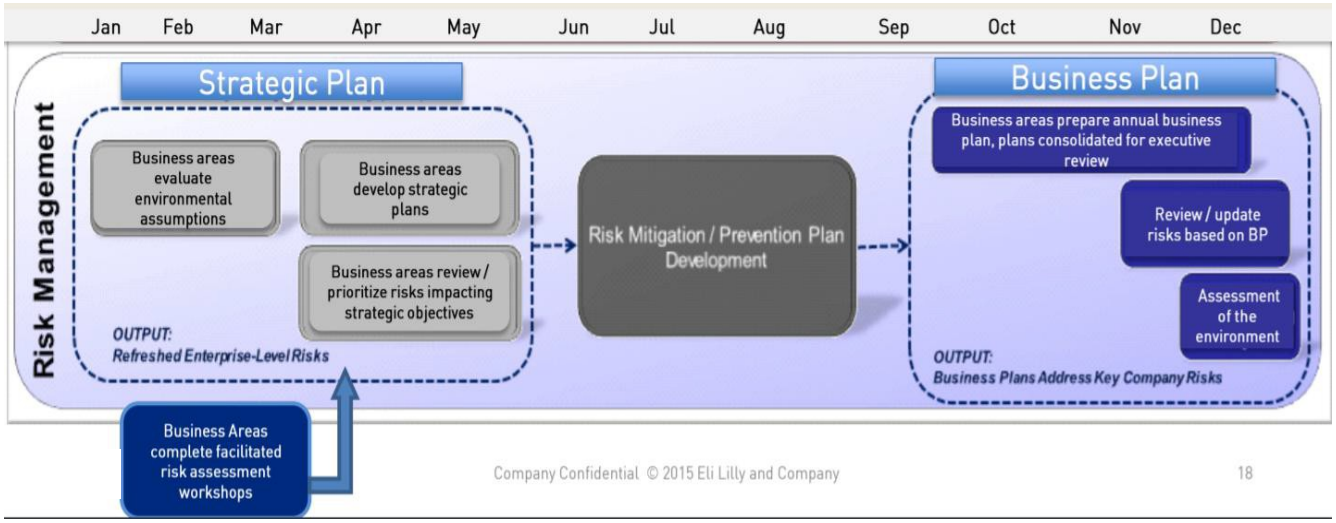
The ERM process is facilitated by the ERM Core Team (ECT) who is responsible for the overall direction of the ERM program. The ECT is a collaborative group that consists of specific members representing various areas within the business. This includes 2 executives in charge of strategy, the Board of Directors Secretary (an attorney of the Law Division), the Chief Ethics and Compliance Officer, and 2 individuals who are responsible for the integration of the company's ERM process. To assist in this initiative, the company has additional committees to further expedite the implementation and integration of ERM.

- The Compliance and Enterprise Risk Management Committee has internal responsibility for overseeing ERM. The CERMC are the risk sponsors and are responsible for monitoring the risks identified as having a high likelihood of occurrence and a high level of impact.
- The Public Policy and Compliance Committee has board-level accountability for the ERM program, and participates at least annually in a full program review.

ERM Process

The ERM program is integrated with the organizations strategic planning process. Aligning ERM with strategic planning allows for a more risk-centric thought process when making critical business decisions that could affect the overall achievement of the company's business objectives. During the ERM process, business areas complete facilitated risk assessment workshops and prioritize risks that may have impacts on the strategic objectives of the entity. After a strategic plan has been developed in conjunction with the gathering and evaluation of enterprise-level risks, a risk mitigation and prevention plan is created. The implementation of the mitigation and prevention plans is an ongoing effort throughout the year. At the end of the year, the ERM process is once again reintegrated into the company's planning process for a review of business plans. When funding decisions based upon those business plans are finalized, the company's risk profile is reviewed again to determine if funding decisions have impacted any of the previously identified risks. If so, risk profiles are updated to reflect those changes. An integration of ERM and planning produces a continuous cycle of risk management processes, such as identifying, evaluating, and responding to risks that can be assessed at any point during a business cycle. The parallels between strategic planning and the ERM processes are best illustrated in Figure 2 below.

Figure 2:



To identify the risks that allow for the creation of such plans, B uses a combination of interviews, surveys, and workshops. The identification process begins with interviewing "risk intelligent sources" such as senior leaders and business area subject matter experts. Inquiries include broad questions concerning the evaluation of the overall business environment and analyzing the specific challenges that may affect the interviewee's business unit. This company also provides a "Risk Survey" to a subset of interviewees who can delegate such questions to their employees so that they may gain a view of business risks from subject matter experts throughout the organization.

After gathering the potential risks recognized throughout the risk interview process, they are consolidated via business area-specific discussions held in a workshop format led by an ERM liaison from within the business area. Proposed business risks are debated amongst members of the risk workshop and prioritized based upon their likelihood of occurrence and the severity of the impact. Following completion of the workshops, business unit risks are evaluated to determine whether they should be

elevated to an enterprise-level. The enterprise risks are monitored based upon their placement on the heat map. The placement of risks on the heat map is an effect of the risk workshops discussed earlier.

Management-Level Risk Committee

General Risk Committee Information

B has 1 overall management-level risk committee, the Compliance and Enterprise Risk Management Committee (CERMC), which is chaired by the Senior VP, ERM and Chief Ethics and Compliance Officer. The CERMC, including the chairman, report to the Public Policy and Compliance committee of the board of directors who are responsible for overseeing the actions of the CERMC.

The CERMC delegates many of its ERM and risk management processes and activities to a lower level risk "team" known as the ERM Core Team. The ERM Core Team is a multi-disciplinary team that includes the chairman of the CERMC and provides for an enterprise wide perspective on both risk identification as well as prioritization and is the staff dedicated to the everyday risk management activities. The CERMC is responsible for advising and supporting the Chairman of the committee in the implementation and oversight of the ethics and compliance program and the ERM program. They also serve as a decision-making forum on cross-business issues involving ethics and compliance. B changed the scope of their Compliance and Ethics Committee to include ERM in 2010, thus transforming that committee into the current CERMC.

Some of the specific responsibilities of the CERMC members are to:

- Provide counsel in their area of expertise to the chairman of the CERMC
- Review management and resource commitment to ethics and compliance activities
- Promote an organizational culture that encourages integrity, ethical conduct, and a commitment to compliance with the law
- Act, as necessary, to improve ethics and compliance program effectiveness
- Ensure effective implementation of the company's Code of Business Conduct, policies, procedures, and business practices within their areas of responsibility
- Review metrics and data, as appropriate, to assess the effectiveness of the ethics and compliance program within their areas of responsibility
- Monitor progress of mitigation and action plans for prioritized enterprise risks
- Identify emerging risks, and mitigate those risks within their areas of responsibility
- Support topic-specific ethics and compliance and ERM initiatives, as needed

The CERMC meets at least quarterly with discussion usually lasting around 1.5 to 2 hours and will also meet ad hoc as specific issues arise. These issues may relate to overall risks that could or may already be affecting the company but may also relate to more specific issues, particularly, ethics and compliance. During ERM discussions, B considers a 5 year risk horizon as an appropriate time frame for analyzing possible future events that may affect the achievement of their business objectives. Though B does not have a stated risk appetite as a threshold for what risks are considered to be worthy of resources, they do consider themselves to be a more conservative company by the nature of the industry in which it operates. Multiple other business functions work in conjunction or in support of the CERMC in order to effectively identify, assess, and manage risks. To support this collaboration, B has individuals from all areas of the organization represented on the CERMC. All business functions play an internal role in sponsoring and owning risks brought to the CERMC by the ERM Core Team.

Risk Committee Membership

Members of the CERMC include the following titles:

Senior VP, ERM, Chief Ethics and Compliance Officer	Senior VP and President, Diabetes; President, USA	President, Manufacturing Operations	Senior VP, Human Resources and Diversity	Senior VP and General Counsel
Executive VP, Science and Technology; President, Research Laboratories	Senior VP and President, Oncology	Senior VP, Corporate Affairs and Communications	Executive VP, Global Services, and Chief Financial Officer	Senior VP and President, Animal Health
Senior VP, Global Quality	Senior VP and President, International	General Auditor	Chief Information Officer	Chief Medical Officer

Members of the CERMC are required to report risk events and other identified uncertainties to the chairmen of the committee, the Senior VP, ERM and Chief Ethics and Compliance Officer so the chairman can properly and effectively facilitate CERMC meetings. The chairman's duties in relation to the CERMC involve setting the agenda of CERMC meetings, facilitating the discussion of risks within these meetings, and seeking guidance on top risk issues from across the enterprise. The agenda, or discussion topics of the CERMC meetings are ultimately set by the chairman but is a collective effort between the CERMC and other members of her organization. Due to the nature of B's ERM program having such an interconnected relationship with ethics and compliance, it is important to note that the agenda for these meetings can vary greatly and in some cases pertain more towards ethics and compliance risks and issues, and in other cases are focused more on broader enterprise risks.

Identification & Assessment of Risks

In regards to the actual identification of risks, the CERMC's role is to review, discuss, and potentially modify (if needed) the identification and assessment of risks conducted by the ERM Core Team. Discussion occurs during the April CERMC meeting, as shown in Figure 2, and results in a recommendation that will be shared with B's Executive Committee.

Communication & Reporting

Once the Executive Committee has reviewed and "approved" the ERM risks, they are presented to the board of directors during this same August timeframe, as previously mentioned. As of 2017, the full board of directors, rather than a sub-committee, oversees the enterprise risk management process. All ERM risks are deemed to be enterprise level, and thus merit the most attention and resources.

Official CERMC "meeting minutes" are created for each discussion amongst members of the CERMC during their quarterly and/or ad hoc meetings. These "minutes" are a record of what was considered and deliberated during their meetings. If needed, a new task force may also be created as a result of CERMC meetings in order to handle or manage particular risks and/or issues that have arisen or been considered during the meeting.

Monitoring & Responses

Mitigation plans specific to identified, assessed, and reviewed ERM risks are developed by their individual risk owners (senior level managers from each business area) during April, May, and June. The ERM Core Team provides feedback from the April CERMC meeting to the ERM Liaisons (subject-matter-experts from across the enterprise and throughout multiple business areas) who then collaborate with risk owners to implement said mitigation plans or changes to such plans. The high, or "red", ERM risks are reviewed and discussed at CERMC, Executive Committee, or the board at least once in a twelve-month period.

B recently introduced the integration of key risk indicators (KRIs) into their risk mitigation plans in order to better understand the factors that contribute to that risk as well as to better monitor the progression of each risk. The risk owners who determine the mitigation plans are responsible for the identification and evaluation of KRIs.

Effective Management Level Risk Committees

B distinguishes 3 key factors that contribute to an effective management level risk committee:

1. Visibility and Transparency – having visibility and transparency to the risks affecting or possibly affecting the enterprise is crucial in maintaining an effective risk committee. Enterprise risks should be transparent in their meaning and easily understood by the Board, CERMC, ERM Core Team, and across all levels and functions of thecompany.
2. Open Dialogue – having open dialogue and clear communication between all employee levels and functions of an enterprise creates a smooth flow of information. Clear and concise meanings of risks and risk vocabulary create better quality feedback and critiques.
3. Methodical, Disciplined Approach – having a methodical, disciplined approach to how risk committees work and communicate, as well as an ERM program that is heavily integrated into the strategic planning process, positively influences the effectiveness of an ERM program and the organization's risk committee.

APPENDIX C

Company Overview

Company C (C) offers a broad array of deposit, loan, and investment products as well as trust, fiduciary, and wealth management services to attend to the financial needs of area businesses, individuals, and families. Through a series of strategic mergers and acquisitions, this company has grown from a community savings bank to a midsize financial institution. C attracts deposits from the public and businesses and uses those funds, together with funds generated from operations and borrowings, to originate commercial real estate loans, commercial business loans, residential mortgage loans, and consumer loans. Reported revenues are over $350 million during the most recent fiscal year.

Overview of ERM

ERM Framework

C's Enterprise Risk Management (ERM) Framework captures the inter-relationship of its values, vision, and strategic opportunities, that, when operating in harmony with its foundational documents, ensure the continued success and ability to exceed market expectations. The primary goal of ERM is not to avoid or eliminate risk, but to avoid unacceptable business risks that may inhibit or prevent the achievement of its overall business goals and objectives, one of which is to operate in a safe and sound manner consistent with the confidence entrusted to them by their customers. This company uses a highly structured and documented approach to ERM and their shared values, mission, and vision and its strategic objectives are linked through its ERM program. Their goal is to correlate the efforts of its risk management activities to facilitate an optimal approach towards achieving its strategic plan while remaining grounded in the pursuit by its guiding principles (shared values). They have adopted the COSO ERM Framework as a basis for its risk management process.

ERM Process

At an entity-wide level, C defines its risk management objectives as the identification of key risks, the formulation of a clearly communicated risk appetite, the capacity to pursue strategic objectives in accordance with such appetite, the optimization of risk and reward decisions by using an organized process, and the engagement of its workforce contributing towards an effective risk management system. Due to the regulatory intensity of the banking industry, they have found it more effective to expand on the categories of risk usually determined to be identified within non-banking organizations. Its risk categories include credit risk, market risk, liquidity risk, operational risk, compliance risk, and reputational risk. These risks are identified and assessed through a series of facilitated meetings with business line managers, executives, and committees that are to the category of risk being evaluated. These "facilitated meetings" are not done periodically but continue through the business's planning and execution cycle. This company begins with an analysis of a specific strategic initiative and the actions that must be done to bring such a plan into fruition. During this time, several of C's management-level committees and subject matter experts are consulted to identify and assess the importance and significance of the risks related to that initiative. It is then the duty of the business line executive, with the assistance of specific committees, to confirm that all risks and impacts are addressed for that project and to advise and execute on the stated course of action for mitigation of those said risks. A description of the roles of key members of the organization is discussed in the following section.

ERM Structure

C subscribes to the widely used 3 Lines of Defense model to promote clear roles and accountabilities of risk management activities to all reporting units within the organization. Within this model, management control is the first line, the various risk control and compliance oversight functions established by management are the second line, and independent assurance is the third line. Selected functions within C's business structure along with the areas of risk for which they are responsible are shown through the 3 Lines of Defense model below in Figure 1.

Figure 1:

Function	Strategic Risk	Operational Risk	Compliance Risk	Financial and Reporting Risk
Internal Audit	3rd	3rd	3rd	3rd
Accounting	1st	1st	1st	1st
Treasury	1st	1st	1st	1st
Vendor Management Office	2nd	2nd	2nd	2nd
Technology	1st	1st	1st	1st
Information Security	2nd	2nd	2nd	2nd
Project Management	2nd	2nd	2nd	2nd
Human Resources	2nd	2nd	2nd	1st
Corporate Compliance	2nd	2nd	2nd	2nd
Legal	2nd	2nd	2nd	2nd
Deposit Operations	1st	1st	1st	1st
Loan Servicing	1st	1st	1st	1st
Credit Risk Management	2nd	2nd	2nd	2nd
Loan Administration	1st	1st	1st	1st
Loan Review	2nd	2nd	2nd	2nd
Credit Department	2nd	2nd	2nd	2nd
Corporate Security	2nd	2nd	2nd	2nd
Sales and Promotions Offices	1st	1st	1st	1st
Trust Sales	1st	1st	1st	1st
Trust Compliance	2nd	2nd	2nd	2nd
Chief Risk Officer	2nd	2nd	2nd	2nd

They provide a formal documented policy for guidance on ERM roles, responsibilities, and activities. They use a typical structured approach as to the arrangement of its designation of risk management responsibilities. The board of directors oversees the risk profile and approves the risk management framework within the context of accepted risk appetite thresholds. Executive management sets the primary risk limits and tolerances that are aligned with the goals, objectives, and risk appetites established by the board of directors. Business line managers are primarily responsible for managing business risks including measuring risk exposures, implementing risk management strategies, and establishing appropriate internal controls.

C supports its ERM activities and appointment of duties through a variety of key management committees that are listed below. These committees are led by an "Executive Leadership Team" that represents 11 executive officers who work with the board to execute on their overall strategic plan within the context of risk appetite.

- Strategic Products and Services Committee – prioritizes scheduling of project based initiatives and provides direction on their IT requirements.
- Senior Risk Committee – serving as the most senior management-level risk committee, the SRC provides a formal periodic system of review, assessment, and management of risk. It complements the various other risk management activities performed by staff and is primarily focused on operational, compliance, financial, reputational and IT related risks.
- Asset and Liability Committee – responsible for the management of interest rate risk, liquidity risk, and market risk.
- Investment Committee – responsible for investment strategies and activities, and borrowing and liquidity positions.
- Credit Committee – responsible for the overall management of credit risk, underwriting standards, and lending practices.
- Compliance Management Committee – provides for the minimization of compliance risk and is responsible for adherence to consumer protection regulations.
- Officers Trust Committee – responsible for reviewing the performance and approval of the significant fiduciary actions of Company C's Wealth Management Group.

Management-Level Risk Committee

General Risk Committee Information

There are 8 "Key Management Committees" that are responsible for the various types of risks potentially affecting C: the Executive Leadership Team, Strategic Products and Services Committees, Asset and Liability Committee, Investment Committee, Credit Committee, Compliance Management Committee, Officers Trust Committee, and the Senior Risk Committee (each committee's responsibilities are detailed in the section above). The Senior Risk Committee (SRC) is the only committee that has an aggregate view of all the types of risks facing the enterprise. The SRC is a smaller group of the most senior managers who are tasked with revealing the layers in the "onion of risks" facing the organization. The SRC, working in collaboration with the Management Risk Committee, are considered to be the forbearers of and responsible for all the risks that may affect the business. The Management Risk Committee is the team assigned to tasks revolved around the everyday ERM and risk management activities while the SRC has a more policy level view of enterprise wide risks.

According to their Senior Risk Committee Charter the SRC's responsibilities are to:

- Discuss the company's overall risk management program in the context of its capabilities and effectiveness in addressing risks
- Offer to executive management, when needed, recommendations to strengthens the company's risk management program
- Assign roles and responsibilities pertaining to the completion of specific risk assessments, and may assess the adequacy of specific risk assessments as it deems appropriate
- Evaluate and coordinate at a high-level the company's risk assessment program, including receiving reports on significant risk assessments and resulting management actions
- Assist the responses to risks by ensuring managements actions provide a consistent approach
- Provide guidance and counsel to the other management level committees

The SRC conducts 8 regular meeting throughout the year with each meeting lasting approximately 60 minutes. In addition, ad hoc meetings may be called as needed.

C started the SRC to manage Sarbanes-Oxley Compliance in 2004. The focus of the SRC is driven off the strategic plan and has a 3 year time horizon that parallels that process. Though C does not specifically state an overall risk appetite, they have set limits or tolerances for specific risks. The SRC does not directly play a role in setting these said limits and tolerance levels for C but does have an influence in its conception. In accordance with the SRC Charter, "The committee is not responsible for determining the overall vision that sets out the expectation of the ERM system, nor shall it set the company's risk appetite and strategy. These responsibilities lie within the authority of executive management, in their respective functions, with the ultimate direction being set by the board of directors." This means that while the SRC does not directly set the "risk appetites", the executive managers who are a part of the committee do determine their own risk tolerances and limits for whichever part of the business they operate, even though the final decision is at the discretion of the Board. Because of the business environment in which C operates is highly regulated, it is critical to the SRC's objective to stress a strong risk management relationship with all other business functions. The "3 Lines of Defense" Model, as shown in Figure 2, implemented by C illustrates all the other business functions that work in conjunction with or in support of the SRC.

Senior Risk Committee Membership

According to the ERM Policy, the SRC committee members include the following:

Chief Risk Officer	Chief Credit Officer	Chief Human Resources Officer	Chief Administrative Officer
Chief Accounting Officer	Chief Wealth Management Officer	Corporate Compliance Director	Chief Lending Officer

The members of the SRC are individually responsible for certain risks that are in their area of expertise and within their respective fields within the organization. This committee is chaired by the Chief Risk Officer of the organization who is designated as the facilitator of the both the SRC meetings and the ERM program. The chairmen's main duties include compiling reports from the other committees for the SRC's discussions and evaluations, sets the agenda and context of the SRC meetings, is the arbiter over accepting risk assessments, and has the ultimate authority of pushing mitigation plans forward to the board of directors. The agenda set by the chairmen is a standard agenda that is set once a year (during the strategic planning process).

The SRC is required to report directly to the Chief Executive Officer, the Chief Financial Officer, and the Risk Committee of the board of directors.

Identification & Assessment of Risks

The SRC occasionally plays a direct role in the actual identification of risks but this task is predominately designated to the Management Risk Committee. The risk assessments created by the Management Risk Committee is brought to the SRC which approves the evaluation and/or any modifications to a previously identified risk. Risks that have been designated as prominent enough to be raised to the enterprise level are discussed at annual meetings with the board of directors. Since members of the SRC

are also members of the strategic planning team, a relationship exists between the actual identification of risks and strategic business objectives. Thus, the SRC contributes significant influence on the identification of enterprise level risks.

Communication & Reporting

Quarterly ERM Reports created by the Management Level Risk Committee are reviewed by the SRC during meetings. The SRC then communicates the information gathered from their meetings with the Disclosure Committee, the Executive Leadership Team (if determined appropriate), and at the end of the year, the Risk Committee of the board of directors.

Official "Senior Risk Committee Meeting Minutes" are created because of information gathered and discussed during SRC meetings. These minutes include such data as members present, non-members present, the agenda, and details of what was specifically discussed.

Monitoring & Responses

Risk mitigation plans are formulated in response to discussions in SRC meetings. These risk mitigation plans produce "take-away tasks" that are communicated back to the owner who is to complete the tasks and implement the plan. The SRC does not specifically assess the effectiveness of these plans being put into action. However, at SRC meetings, the members are updated on the progress of the mitigation strategies put into place by the risk owners.

The process for following up on changes in risks (such as an increase or decrease in their level of impact) that have been identified are directed by the chairman of the SRC and are tailored towards specific risks. However, these changes may fall under the control and responsibility of other risk owners, committees, and any other second-line of defense functions as shown in Figure 2.

At C, KRI's are considered more at the policy level in the form of tolerances and limitations for specific risks. At the enterprise level, KRI's can be more judgmental and variable.

Effective Management Level Risk Committees

C draws upon 2 distinguishing factors that help contribute to an effective management level risk committee:

1. Risk Intelligent Culture – having a risk intelligent culture as opposed to only a risk aware environment allows management level risk committees to consider the opportunities that are coupled with risks rather than fearing risks as purely bad.
2. Qualitative to Quantitative – going from a qualitative understanding of risk to a quantitative action-oriented view of risks which give consistency across economic cycles.

APPENDIX D

Company Overview

Company D (D) is an air delivery and freight service company with reported revenue of over $58 billion in its most recent year and a workforce of over 400,000 employees worldwide. D's services include package delivery and logistics and its customers range from individuals to businesses to governmental entities.

ERM Overview

Enterprise Risk Council (ERC)

While other committees and individual members of the organization play a role in ERM at D, the ERC is the center of the process where inputs are transformed into actionable outputs. The ERC of D is made up of roughly 15 business leaders (VP's) that come together quarterly to discuss risks affecting their respective areas of responsibility. The ERC is designed so that all business units are represented and, as such, allows for an individual member to 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 a 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.

ERM Process

D begins the ERM cycle by identifying risks using an annual survey sent out to approximately 900 business leaders across the enterprise. Identification may also occur at the quarterly ERC meetings although this is considered rare. Another way identification may occur is through direct contact with the Chairs of the ERC. Risks can be brought directly to their attention if thought to be severe enough to warrant immediate ERC action. While the survey serves as the main tool for identifying new risks, D 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 an initial assessment can be performed by the individual who represents a particular business group on the ERC. 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. D 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). D provides a description of each of these points on the scale in order to further assist ERC members in applying consistency 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. The ERC may adjust a specific assessment of 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". D categorizes enterprise-level risks in to 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 would be considered a 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. To further this evaluation, a target rating is assigned to the risk that is based on anticipated effects from mitigation strategies implemented by the risk owner. Some risks that are specific to a single business unit may not fall under the realm of the ERC because they do not have enterprise-wide impacts and thus would 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 should bring the aforementioned target rating. The risk owner will then document the risk and the response plan in a Risk Profile. See example below.

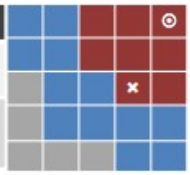
Risk Profile

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

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. Following suit, the risk owner must update the relationship between the current assessment rating and the target assessment rating. This allows the ERC to discuss and evaluate the results of response strategies that have been implemented 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 the Tier 1 risks, but only those Tier 1 risks that the ERC believes are significant enough to warrant notification of the board. The board of directors may also ask management to review certain risks with them when it deems necessary to do so.

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 said presentation to the Risk Committee of the board who then updates the Audit Committee of the board before relaying this information to the full board of directors.

Management-Level Risk Committee

Members of the ERC

The ERC is made of up of 15 business representatives (Vice-Presidents) as follows:

Co-Chair – Chief Legal Officer	VP Engineering	VP Finance & Accounting	VP Human Resources	VP Information Technology
Co-Chair – Chief Audit Officer	VP International Operations	VP Legal & Public Affairs	Director Program Management Group	VP Public Relations
VP Domestic Operations	VP Risk Management	VP Sales / Marketing	VP Security	VP Strategy

Frequency and Focus of Meetings

The ERC meets on a quarterly and, as necessary, an ad hoc basis. These meetings usually last between one and a half and two hours. The Chief Audit Officer usually opens the meetings to set an appropriate tone at the top and keep members accountable. From there the ERM program manager will lead the discussion in the meeting and sets the agenda for these meetings based on risk identification tools as well as topics brought to the attention of ERC members. A typical agenda will make sure to provide discussion time for “hot topic” risks affecting the business. D believes these meetings are of extreme importance because they provide a forum for which leaders within the organization can speak freely about risks impacting their area of the business. Minutes of the meetings are produced by the ERM program manager and sent to ERC members as well as other individuals that would be impacted by the issues covered at the meetings.

Keys to Success

D expressed that the keys to the success of their ERC is that they strive to keep meetings and discussions simple. This ensures that the conversations are moving in the right direction and topics are not too specific to one area of the business making the discussion irrelevant to other members of the committee. Additionally, the ERC is an opportunity to foster communication between business leaders and to educate those individuals on general ERM concepts. ERC members share the insights they have gained from these committee meetings with others in their organization and with their peers. This helps to promote the value in ERM to individuals that might not explicitly consider risk management in their particular business role.

Future Enhancements

Like most companies, D tries to enhance its ERM process, including the function of the ERC and other committees. One planned enhancement of the ERC is to preemptively consider potential outcomes of risk response plans during their quarterly meetings. In addition, D plans to extend the use of cross-functional risk committees further across the organization. These risk committees would serve as a forum for risk management issues and be particularly effective at overseeing risks that are actionable at the business unit level rather than throughout the entire enterprise. These committees provide an

opportunity to educate those across the organization on risk identification and mitigation, and provide the corporate ERM function with a “zoom lens” into specific risks that may be visible in that specific field but are overlooked by the corporate function.

APPENDIX E

Company Overview

Company E (E) is an independent oil and gas company that focuses on onshore drilling. Organization E produces oil, natural gas, and natural gas liquids. Like most oil and gas companies, its revenues are closely tied to market prices and company growth is linked to the discovery of new oil and gas reserves. E partners with contractors to drill and maintain the wells, and sells crude oil and gas to midstream companies and refineries. In its most recent year of operation, E reported over $10 million in revenue and employed a work force of over 5,000 people.

ERM Overview

E had strong risk management practices already in place before ERM was implemented. The ERM process recognizes the value of existing risk management processes across the organization and builds upon those strengths. ERM was initiated by the board of directors in 2009. ERM is driven by the Audit Committee of the board, with support from the CEO and the full board of directors. E's executive team (top senior management) forms the ERM Steering Committee which provides oversight for the ERM process. The Internal Audit department facilitates the ERM process and management owns the individual risks.

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

1. Enterprise risk inventories
2. Enterprise risk documentations
3. Risk group workshops
4. Annual ERM risk surveys
5. ERM Steering Committee

Together, these five components enable this company to seamlessly integrate risk management into daily operations, 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.

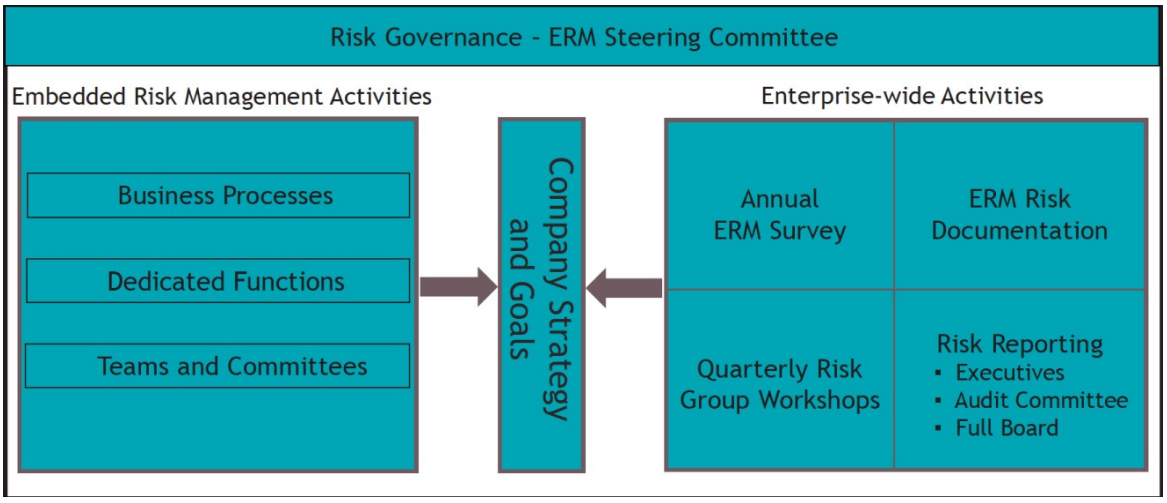


FIGURE 1

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 17 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 those particular 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 detailed information about the risks contained within the enterprise risk inventory. A standardized risk documentation template is used by Internal Audit to collect information about each specific inherent risk within the stated 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 also 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 and is shared with the executive team, audit committee, and the board. Summary reports are updated at least every 18 months in order to reflect the most current risk information.

Risk Group Workshops

Risk group workshops are conducted on a quarterly basis with six to ten executive team members and vice presidents. Typically, two to three similar risk categories are discussed at each workshop which helps to ensure that all risk categories are discussed over an 18-month period. Risk group workshops last approximately two hours and 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 shown below in *Figure 3.*

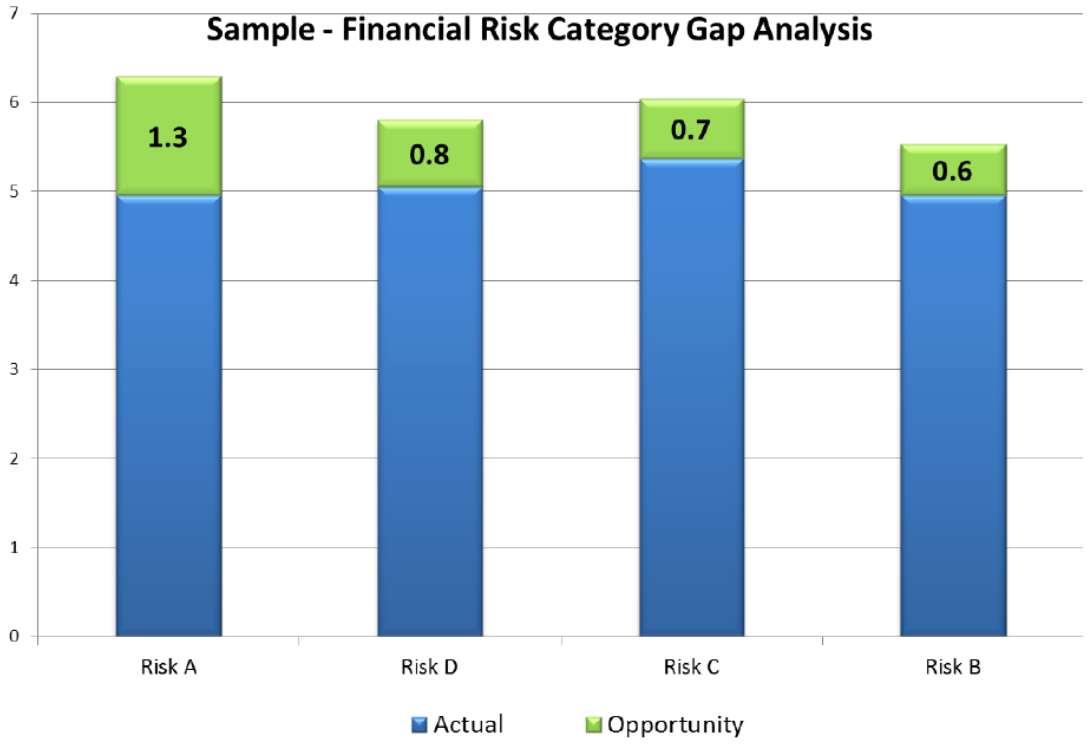


FIGURE 3

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 throughout the organization. Significant risks that are brought up during the group workshops are often discussed even further amongst the executive team members after the workshops have been completed.

Annual ERM Survey

The ERM survey polls roughly 75 leaders in order to prioritize the previously mentioned 17 risk categories. The survey is sent to all Executive Team members as well as various managers throughout the organization. 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, and thus, the more resources the risk merits 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.

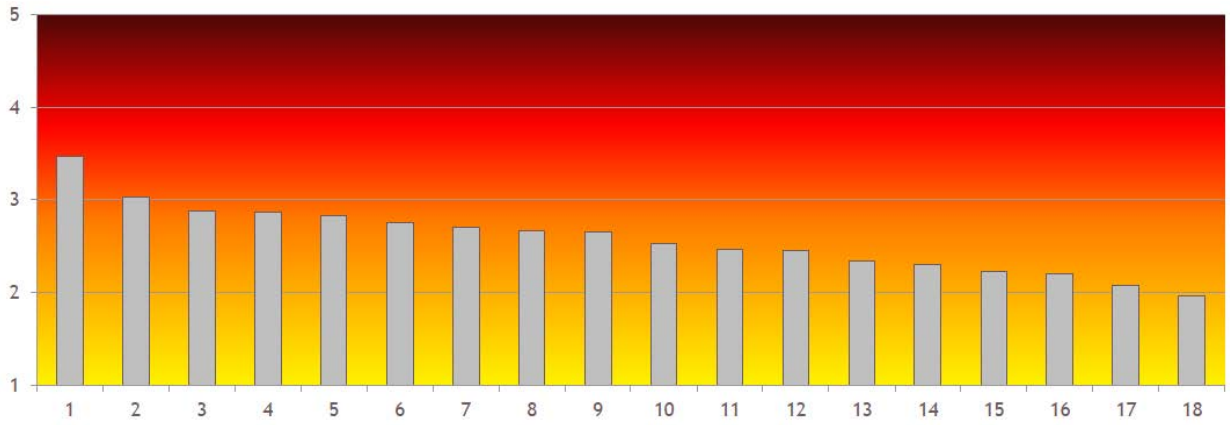


FIGURE 5

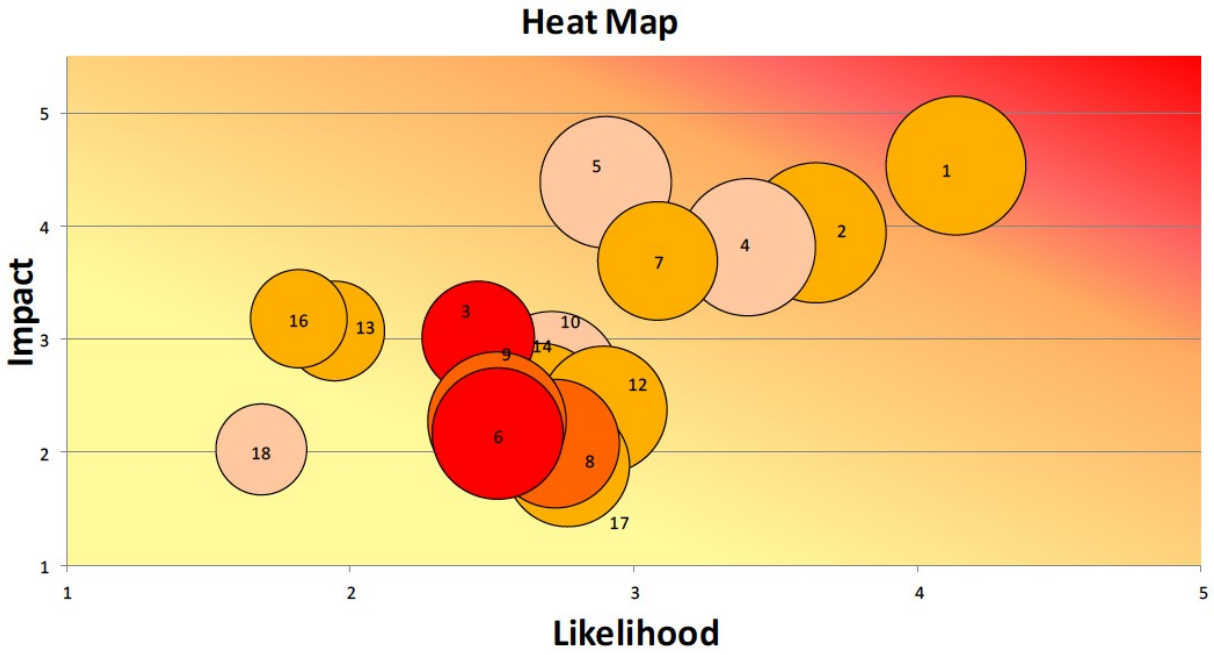


FIGURE 6

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 and to the risk, so that all survey responders are knowledgeable about the events they are evaluating. Survey responders also have the ability to provide new risks for the ERM team to consider.

The data collected through the surveys 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 and the functions of the Executive Team.

Management-Level Risk Committee

ERM Steering Committee (ERMSC)

The ERMSC provides oversight and guidance to the ERM process as it continues to evolve and mature. The ERMSC is composed of executive team members and holds two meetings a year in order to visibly support and confirm the direction of ERM. The ERMSC serves its greatest purpose as a forum for meaningful discussion about the most significant known and emerging risks to the organization. The assessment of risk typically occurs outside of the ERMSC meetings to ensure management responsibility and ownership of risks by management throughout the company. This approach allows Risk Sponsors (EVPs) and Risk Coordinators (SVPs/VPs) to communicate their concerns about risks during ERMSC meetings or any other setting through the natural reporting structure of the organization.

Membership

The ERMSC is comprised of the eight executive-level risk sponsors shown above in Figure 2. The CEO chairs ERMSC meetings and the leader of the ERM function typically leads the discussion in these meetings and shares the information gathered from the annual surveys, quarterly workshops, and ERM documentation activities to particular employees throughout the organization.

Frequency and Focus of Meetings

Two executive meetings per year are designed in order to discuss the results of the risk identification and assessment processes. The first meeting of the year is primarily devoted to discussing how the ERM process may change in the coming year. The second meeting is primarily for discussion of major risks, both existing and new, and incorporates the most recent risk identification results. Neither meeting is bound to the short descriptions above, and are informal in their set agendas such that if an important issue arises, it will be discussed at either meeting. Important to note is that the annual risk assessment is performed via a survey that incorporates ERMSC members, VP's, and other managers across the organization. The results from this tool are brought to the attention of the ERMSC at either the first or second meeting. There is not a formal time horizon considered in the ERMSC meetings, but major risks are presumed to be discussed in the present tense.

Key to Success

E mentioned that one key to their success is keeping the ERM process simple, such as focusing discussions at the ERMSC meetings on the most significant known and emerging risks and trends. This is important to maintain executive management support, and ensure the ERMSC functions effectively as an integrated governance process. This has been the intention since the formalization of the ERM process at E, and still serves its purpose even as the ERM process has grown to a level of significant maturity. Given the nature of the industry in which E operates, such a structure is sufficient to ensure that the ERM process is effective, known risks are seriously considered by the decision-makers, and emerging risks are effectively communicated to the ERMSC.

APPENDIX F

Overview

Company F (F) is a leading manufacturer and marketer of quality skin care, makeup, fragrance and hair care products that are sold in over 150 countries. The company's annual revenues were over $11 billion in the most recent year.

Overview of ERM

ERM Framework

Enterprise risk management (ERM) involves thinking differently about how risks affecting businesses are managed. The objective of ERM is to create a holistic, top-down approach to identify the most significant risks to an entity's objectives. F has adapted its ERM process over the years culminating in the adoption of a "subcommittee" approach to ERM that centers on major risk areas such as strategy, technology, human resources, and supply chain. The subcommittee approach is an enterprise-wide, disciplined approach that aggregates the most critical corporate risks, increases the likelihood of successfully delivering on goals and objectives, reduces unanticipated outcomes, assesses risks associated with changes in the business environment, and presents a detailed description to internal and external stakeholders of what the company is doing to manage risks.

ERM Process

The Risk Sub-Committee's (RSC) risk identification process is the main process for developing an enterprise risk profile for the company, and as such, is a critical part of F's ERM program. The overall RSC risk identification process has several key objectives:

- Identify critical corporate risks
- Identify emerging and escalating risks
- Identify past year's Issues and near misses for analysis

Risk are identified by asking questions such as:

- What are the risks that would affect the strategy?
- What are the operational risks?
- What risks are escalating that will require priority focus in the current year?
- What risks are emerging risks that could have significant impacts in the future?

To assess each individual risk, the risk owners and RSC members are asked to participate in anonymous voting to rank risks based on 3 elements: probability, impact, and velocity. Each element is scored using a 1-5 scale (very low, low, medium, high, very high). A risk score is calculated based upon the scoring of these three elements which is then used to determine the most significant inherent risks.

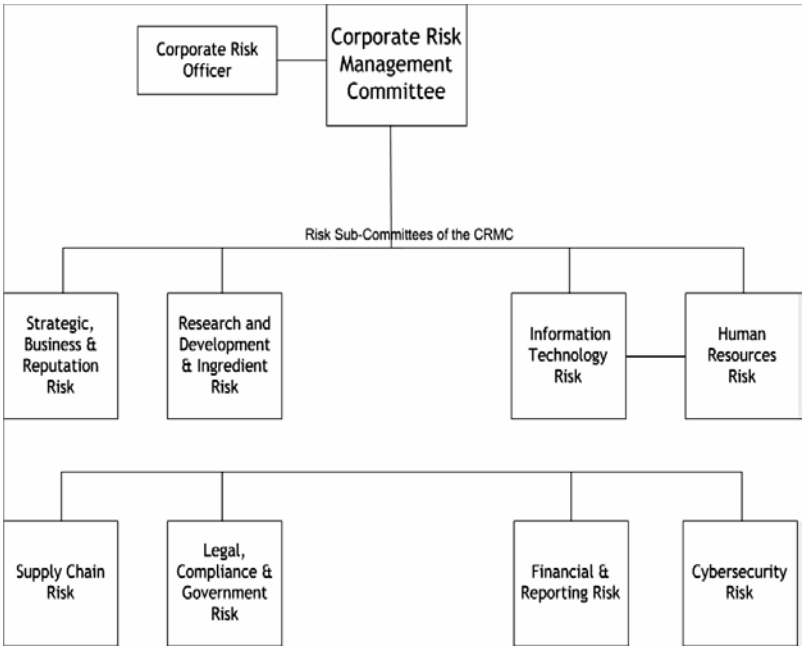
For each critical corporate risk (such as cybersecurity) identified by the RSC, a risk owner must also be identified. Critical corporate risks, are risks that would interrupt business in the succeeding year. A risk owner should be a member of management who has the authority, accountability and resources to provide effective oversight and mitigation of the risk. Since RSC members are senior managers within the company, it is likely that some RSC members will become risk owners based on their normal roles and responsibilities. Risk owners will be responsible for developing appropriate risk mitigation strategies for their assigned risks as well as developing more detailed risk scenarios/descriptions of assigned risks, as necessary. Mitigation tasks are rated using a 1-5 scale (ineffective, somewhat effective, reasonably effective, effective, and highly effective). The risk owner is then given the chance to provide an

explanation for the risk rating score. To know whether the plan will be implemented in the future or whether the mitigation plan has worked, the risk owner must "re-rate" the risk after considering the possible mitigation activity or strategy using the same 3 criteria (impact, probability, and velocity) to arrive at a final residual risk score.

Annually, current strategies and tasks are reviewed and updated, and new mitigation strategies and tasks are developed by risk owners and reviewed by the committee. In addition, risk owners attend committee meetings to discuss, in detail, their existing strategies and tasks. When documenting these strategies, the following information is to be included:

- Name of risk mitigation strategy or task
- Name of person responsible for the risk mitigation strategy or task (owner)
- Detailed description of the existing risk mitigation strategies and tasks
- Effect of the risk mitigation strategy or task on the level of risk
- Overall effectiveness rating of the risk mitigation strategy (average of the risk mitigation tasks effectiveness ratings)

ERM Risk Committee Structure



F has a Corporate Risk Management Committee (CRMC) that is made up of ten senior management level members, as well as the Corporate Risk Officer (CRO). The CRMC includes the Presidents of Brands, Head of HR, the CFO, the Treasurer, and the Head of Operations. Top management discusses critical corporate risks with the board once each year between April and June.

There are 8 subcommittees under the CRMC: Strategic Business and Reputation Risk, Legal Compliance and Government Risk, Research and Development and Ingredient Risk, Financial and Reporting Risk, Supply Chain Risk, Cybersecurity Risk, Information Technology Risk and Human Resources Risk. Each of these subcommittees have approximately 8-12 members at the VP level or above. Each subcommittee is made up of multi-disciplinary members, to help identify risks across the company but specific to the

category of risk designated to that particular sub-committee. Each Sub-Committee will have 4 meetings in an annual cycle.

Management-Level Risk Committee

F's risk committee structure has been in place for at least 15 years. The following chart summarizes the composition, roles, and operations of the CRMC and RSC's:

	Corporate Risk Management Committee	**Risk Sub-Committees**

Role	• Validate and revise, as appropriate, Corporate risk assessment
	• Identify and prioritize critical Corporate risks based on risk assessment
	• Validate and approve:
	  • Corporate risk appetite
	  • Risk mitigation of critical corporate risks
	  • Assigned ownership of risk
	  • Monitoring of corporate risks and metrics
		• Identify and assess critical corporate risks
		• Assess risks using tools and methods provided
		• Validate risk scenarios and Risk mitigation plans developed by risk owners
		• Develop and validate risk metrics and monitoring plans
		• Share critical corporate risks with Crisis Management Team for them to identify the existence of a crisis plan for each

Composition	Presidents of Brands, Head of HR, CFO, Treasurer, Head of Operations and Corporate Risk Officer	8-14 cross-disciplinary members at VP level or above
Chair	CFO	Management level member
Meeting Frequency	Quarterly	Quarterly or more frequently if needed
Meeting Length	1 hour and a half	1-2 hours

The CRO ensures that the risks that are identified in the CRMC are assigned to appropriate individual subcommittees. Once the critical corporate risks are identified, they are assigned to risk owners and presented to the CRMC once a year. A risk list will then be created to catalog each risk. For F, three portfolios of risks are discussed:

- Acceptable risks (risks to monitor whether external or internal)
- Watch list risks
- Critical corporate risks

Each subcommittee is chaired by one of its senior management level members. The CRO, working with the chair of each committee puts together the agenda for the quarterly meetings. In these meetings, the critical corporate risks are discussed, paying close attention to any changes in the risk or its mitigation strategy. For example, cyber risk is one that is consistently present but could change portfolios; therefore, it will be on the list for discussion. Most of the focus is on the critical corporate risks that

could happen within the year, for other risks deemed not critical, a risk horizon of three years is usually considered.

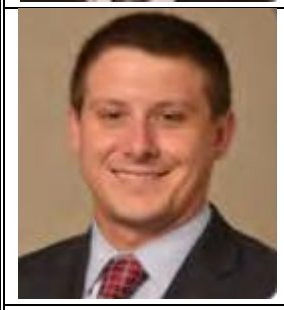
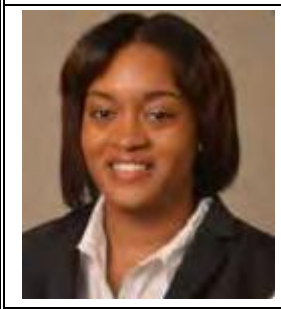
The following chart summarizes the RSC meeting schedule, content and deliverables:

	Meeting 1	Meeting 2	Meeting 3	Meeting 4
Timeframe	August/September	October/November	January/February	March
Meeting Content	• Discuss Risk interview results • Review Risk Template changes and Dashboard • Discuss RSC and Senior Management Risk Identification Process	• Discuss new risks from the RSC and SM Risk Identification process • Risk assessment of new and existing risks	• Discuss RSC and SM Risk Identification results • Riskassessment of new and existing risks	• Review Year-End reporting • Finalize Escalating Risk List
Deliverables	• Identify new critical corporate, emerging and/or escalating risks	• Identify new emerging orescalating risks and update risk templates as required • RSC to complete Risk assessment ratings	• Identify new emerging or escalatingrisks and updaterisk templates as required • RSC to update risk templatesas requiredfornew risk	• Identify new emerging or escalating risks, and update risk templates as required • Final risk template review/update/ sign-off due

At the quarterly meetings of the CRMC, top risks are reported to the CRMC from the subcommittees. Near the end of each year, the CRO will present the top risks identified and the escalating risks to the CFO, CEO, Chairman, the Audit Committee and the Board. The risk owners present to CRMC, and the committees update and assess the effectiveness of what was found and presented on. The keys to having an effective management level risk committee are engagement of committee members, clear objectives for each meeting, consistent protocols, and effective follow-up activities.

About the Authors

NC State ERM Practicum Team Biographies

	**Michael Gore** is a graduate student in the Master of Accounting program at NC State University where he is concentrating in Enterprise Risk Management. After completing his Bachelor degree in Accounting with a concentration in Internal Auditing, he worked for the North Carolina Department of Commerce as an internal auditor before the start of his current graduate program. Upon graduation, he will begin work at RSM in Risk Advisory.
	**Lucas Hyde** is a native of NC and a graduate student in the Master of Accounting program at NC State University where he is concentrating in Enterprise Risk Management. He worked part-time with Falls of Neuse Management, LLC as a General Ledger Intern while completing his Bachelor's in Accounting at NC State. Upon completion of his Master's program he will be joining EY in Charlotte, NC in their IT Risk Advisory program working specifically with Financial Service Organizations.
	**James Merritt** was born and raised in Burlington, NC and is currently a graduate student in the Master of Accounting program at NC State University, with a concentration in Enterprise Risk Management. After graduating with a Bachelor's degree in Political Science from UNC-Chapel Hill, he began working for Wells Fargo Bank, NA, first as a teller, then most recently as a personal banker II. He will be joining Duke University in their Audit, Risk & Compliance office in December 2017.
	**Na'thia Moses** graduated with a Bachelor's degree in both Accounting and Finance before becoming a student in the Masters of Accounting program at NC State University. Her concentration is Enterprise Risk Management. Before attending NC State, she worked in bankruptcy for Wells Fargo. Upon completion of her master's she would like to pursue a career in auditing.