

The Value Proposition for ERM: From Intangible to Tangible



Prepared by: Adrienne Shoaf, Ben Boudreaux, and Shovan Bhatta
NC STATE GRADUATE STUDENTS | POOLE COLLEGE OF MANAGEMENT
FACULTY ADVISOR: Bonnie V. Hancock

Table of Contents

- INTRODUCTION2
- Case Study Process and Participants2
- Value Added by ERM3
- Increasing Risk Awareness3
- Focusing on What Matters3
- Targeting Longer Term Emerging Risks4
- Consulting on Risk Issues.....5
- Improving Resource Allocation.....6
- Enabling Proactive Responses6
- Spotlighting Hidden Risks7
- CONCLUSION8
- APPENDICES: INDIVIDUAL COMPANY CASE STUDIES.....10
- APPENDIX A11
- APPENDIX B14
- APPENDIX C17
- APPENDIX D22
- APPENDIX E25
- APPENDIX F.....30
- About the Authors.....36

INTRODUCTION

The growing popularity of Enterprise Risk Management (ERM) has given many organizations the opportunity to observe and experience the tangible advantages it can provide. In the pursuit of value, executives know that they must take risks to be successful in the highly competitive global arena. Although it is widely acknowledged that the volume and complexity of risks facing companies today are increasing, there are still a significant number of organizations that have not adopted ERM, citing concerns about bureaucracy, resource constraints, and the difficulty of measuring the value being derived from ERM. The difficulty in identifying value lies in the fact that it is challenging to directly measure the value of not having an event occur or having the impact of an event minimized, and to definitively tie that benefit to the ERM process.

Nonetheless, companies who have adopted ERM cite numerous benefits that have been realized through the implementation of the enterprise wide approach to risk. The main purpose of *The Value Proposition for ERM: From Intangible to Tangible* case study is to analyze and provide examples about how companies across various industries have experienced significant benefits from a robust ERM program. The findings from this case study suggest that there are several different aspects in which ERM adds value. One common finding is that it increases risk awareness and communication throughout different levels of the company. There were also interesting and unique findings, such as the use of ERM as a tool to aid in the allocation of resources. This case study will examine the way in which each of the six companies represented have experienced the advantages of ERM.

There are six overarching sources of value discussed in this case study; they are organized from the most “intangible” to the most “tangible.” In other words, the intangible sources of value are those that are more broad and general in nature. These sources are also the ones that seem to be experienced by the majority of the companies that participated in the study. Conversely, the tangible sources of value are ones that are more clear-cut and impact specific areas within the organization, exemplifying the most concrete observations in regards to the value that ERM can provide to an organization.

Case Study Process and Participants

These case studies were conducted by first gaining an understanding of the overall ERM process at each company, and then exploring the specifics regarding the benefits gained from ERM. The review of the six different organizations reveals both common themes and a variety of unique experiences with ERM adding value. These experiences were likely affected by differences in industry participation, strategy, business model, culture, and maturity in ERM implementation.

To ensure anonymity of the participants, we identified each company by sector and market capitalization (market cap). The market cap was broken down into three ranges: small (<\$2 Billion), mid (between \$2 Billion and \$10 billion), and large (\$10+ Billion). Below is a summary of companies that are represented in this case study:

	A	B	C	D	E	F
Sector	<i>Healthcare</i>	<i>Consumer Cyclical</i>	<i>Consumer Cyclical</i>	<i>Energy</i>	<i>Utilities</i>	<i>Financial Services</i>
Market Cap	Large	Large	Mid	Large	Large	Small

VALUE ADDED BY ERM

Increasing Risk Awareness

One of the most widely mentioned benefits of ERM from the participants in this case study is that it creates a structured approach to risk communication and awareness. More specifically, it gets individuals from the organization that truly should be engaged in risk management, more involved. Multiple companies mentioned how their ERM process allows risks to be effectively communicated between management levels, the executive level, and the Board of Directors (Board). Some companies use a dashboard tool to share key information on significant risks in a user-friendly manner.

Company E stated that ERM creates a forum to discuss risks, allowing everyone's opinions to be heard and compiled in one place. This allows E to compare issues across the entire company and direct management's attention to specific risk areas. Similarly, Company F mentioned that ERM enables management to work in unison to identify both threats and opportunities, and then aids in the ability to manage and exploit them in a timely manner. Company D discussed how ERM provides management with "actionable data" that can be used to mitigate and manage risks.

Participants mentioned how the use of dashboards has improved the effectiveness of risk communication within the organization. Company C utilizes a risk dashboard tool which creates a snapshot of both near-term and longer-term potential risk impacts all on one page. The information provided by these dashboards includes the prior period assessment of risks, how they have changed over time, and the future risk trends. By utilizing this tool, C is able to easily communicate an abundance of information regarding each identified risk. This information facilitates the development and execution of effective plans to manage risks and meet goals. In a similar fashion, Company E utilizes a key risk indicator (KRI) dashboard that monitors risk trends and provides an early warning for risks requiring more attention. It is evident that ERM can heighten the efficiency and effectiveness of risk awareness and communication throughout any organization.

"A structured approach to risk communication and awareness"

Focusing on What Matters

Time and resources are a universal constraint in any organization. One of the last things a company wants to do is to invest their limited time and resources addressing risks that have an insignificant impact on the company. ERM functions within companies can provide value by assisting decision makers in prioritizing risks so that more of the company's time and resources are spent addressing risks with the highest potential impact. By prioritizing high impact risks, the company and the decision makers are better able to allocate their resources and invest more of their attention on achieving strategic objectives, rather than attempting to minimize impacts from risks that were not identified in time to be avoided or mitigated effectively. Several companies stressed the importance and value of risk communication and awareness at the Board level, and the focus it provides. Company A alluded to the fact that ERM ultimately drives the Board's agenda.

The work the group does in identifying, assessing, and ranking the high impact risks, helps shape the topics that the Board discusses during their meetings. The top risks are typically strategic in nature, and likely to have a significant effect on the company's success in reaching its objectives. While many of these risks have already been on the minds of senior management and members of the Board, the annual assessment process helps to focus attention on those risks most likely to affect the company's ability to achieve its strategic goals. Similarly, Company C states that it relies on its ERM function to facilitate the discussion of risks from the executive level up to the Board. Because of this, the Board is reassured that it has the information it needs to provide effective oversight over the management of the organization's top risks.

Although the annual risk update process takes only a few months, Company A uses a Risk Universe tool to provide focus throughout the year. The Risk Universe is a collection of all risks that are affecting the organization and is typically updated four times a year. Through these regular updates, emerging risks are added, changes are tracked, and significant issues are prioritized. In another example, the ERM function at Company B strives to apply a risk lens that has the benefit of creating a holistic view of risks that others in the company may not see from their vantage point. At Company B, executives may reach out to the ERM team to provide structure in analyzing a significant issue or decision and apply a risk lens to the situation. Finally, E has found that one crucial benefit from the ERM process is the creation of a risk management methodology and thought process throughout the company. Through ERM, E is able to set boundaries for risk discussion and focus on the opportunities and threats that are truly important to the organization.

“ERM ultimately drives the Board’s agenda”

Overall the ERM function can provide decision makers with an enterprise-wide view of risk, which will highlight the concentration of risks, interconnected risks, and situations where there may be a natural offset for the risk in another part of the enterprise. In this way, decision makers are focused on those risks that are highly consequential to the company. This, in turn, means that the organization will be better able to allocate its limited time and resources to addressing matters of utmost concern.

Targeting Longer Term Emerging Risks

ERM provides value by identifying emerging risks and analyzing them across the business horizon. Company D describes ERM as “a forward view, not a rear view” and tries to incorporate that principle into the ERM process by increasing the risk horizon. All companies in our case study have processes in place that focus on identifying risks with a longer horizon. The longer the outlook, the more time a company will have to prepare and mitigate the risk exposure. There are a variety of ways that companies have accomplished this; including scenario analysis, which typically takes the form of a Black Swan analysis. Other examples include gathering information throughout the organization, tracking new risks year after year, benchmarking, and linking risks to strategic objectives.

Company C uses a specific tool referred to as a “Black Swan” analysis to look “beyond the horizon.” C defines a Black Swan event as a risk that is not on the current horizon, not actively monitored, and likely to accumulate to a significant level. The analysis is led by the Director of Internal Audit and ERM, and the process involves an open discussion of possible risks and opportunities facing the company. The risks and opportunities that are identified during the discussions are compiled in a report that is ultimately presented to the Board of Directors. This analysis focuses on both sides of ERM; the opportunities and the risk areas. Executives have described the process as “giving the confidence to pursue opportunities.” One example of an outcome from the Black Swan analysis is the decision to increase the use of prototypes as part of the new product development process. As a result, the organization has improved the design process.

***“A forward view,
not a rear view”***

Company A also uses a Black Swan analysis. A’s analysis is focused on identifying risks that are fast paced, low probability, and high impact. A faces a wide range of potential Black Swan events given its geographic diversity and the rapidly changing industry in which it operates. Most recently, the organization was faced with two Black Swan events at one time, a natural disaster that demanded evacuation and a terrorist event that created a high demand for patient care. Using the negative experience as an opportunity for growth the ERM function amended the scope of the Black Swan analysis. Now, when analyzing Black Swans and future events, the ERM function will pair drastically different risk events together when performing emerging risk and business continuity analysis.

This is particularly helpful for larger companies that may face risk with various business ventures. Combining two drastically different events in the scenario exercise provides the opportunity to discover risk overlaps that may not have previously been considered. Company B uses scenario-based tools such as war gaming and game theory to identify risks in the external world and industry. Both tools have been uniquely adapted from traditional economic analysis to the ERM perspective.

Company A extends the risk horizon during their annual risk identification (surveys and interviews) process where any new risks or opportunities are analyzed and organized to show the top emerging risks. Emerging risk can include trends in the business environment and may be listed as emerging for several years. Each year emerging risks are accumulated, and the list is included in the presentation to the Board of Directors. If the emerging risk has a horizon across several years, the position of importance is tracked and reported to the Board each year. This process keeps the company aware of emerging risks and opportunities year after year.

Company E identifies emerging risk in two parts; long and short horizon risk identification. Long horizon risks are tasked to the ERM Steering Committee. This committee scans the landscape for higher-level emerging risks and benchmarks against other companies. If a valid corporate level risk is identified in either process, a risk owner is assigned. The risk owner does more research and is responsible for the mitigation and monitoring of the risk. Short horizon risks are identified by the ERM Corporate Risk Committee that meets quarterly to discuss the risk environment and any trends that may be emerging. The committee includes officers, general managers, and departmental directors from across the organization. The information discussed quarterly comes from their bottom-up and top-down approach to risk identification. Bottom-up risks are reported from the various departments in the organization through the quarterly meetings, while top-down approaches include surveys and interviews.

“...giving the confidence to pursue opportunities.”

Company F exists in the highly regulated financial services sector. As a result, F has a very structured approach to risk identification and similar companies face almost identical risks and environmental factors. Currently, emerging risks are monitored at the three-year level to match their strategic plan. The company uses externally available information to benchmark others in the industry. By analyzing and acting on industry trends F can maintain growth, seize opportunities, and avoid risk areas.

Consulting on Risk Issues

Consultancy is one of the new perspectives for an ERM function identified during the case study. Taking the role of a consultant has many positive benefits, including an “external” viewpoint. This external viewpoint provides the ability to focus resources on emerging risks and special processes and creates the ability to tailor risk analysis into a specific story and visualization. At the same time, this internal consultancy has the advantage of a deep understanding of the company and its culture. For the consultant element to be successful, each business unit needs to have its own ERM process or risk awareness. For example, in Company B, each business unit has an employee trained in ERM. This is also true for Company E, where each unit is responsible for finding risks within the business unit. The unit should also be mindful and monitor changes in existing risks.

Value is also added through ERM’s consulting capabilities in the way that the team conducts analysis and turns around information in “real time.” With the consultant mindset, risk visualization is created to cater specifically to the business unit or leaders that request the analysis and provides insights about certain decision, strategy, problem or risk. In addition to risk visualization, B finds that narratives and written communication are effective for risk communication. The ERM team creates value by providing a “toolkit” to the business as they analyze risks, assess strategies, and make decisions. Techniques in the toolkit range from specific management workshops, to stress testing, and to war gaming. Specifically, war gaming has been successful in providing the decision makers with practical information by considering the actions of external players. Reports from this process have helped to avoid negative risk scenarios and have also highlighted positive opportunities.

Company D's ERM function operates as a combination of consultant and risk monitor. As a function of internal audit, they are involved in the risk identification and monitoring process for each business unit. They are also available to help with special projects and emerging issues. One such case involved an industry trend in which many companies were transitioning to outsourced logistics. The logistics leader from the company requested an analysis of the risk and reward profile for the logistics function. After an in-depth analysis, they found that the logistics program was a competitive advantage, which if outsourced, would potentially destroy value. As a result, it was not outsourced.

Improving Resource Allocation

One unique finding from the case study was the use of ERM as a tool incorporated within the budgeting process. This was cited by two of the companies studied and is a key takeaway for how ERM can add value to any organization's budgeting process and resource allocation methodology.

Companies E and F both utilize risk management to aid in the allocation of resources. Company E's ERM process is directly involved in the budgeting process, specifically regarding the cost of risk mitigation strategies. During the planning process of the budgeting cycle, each department reevaluates for the most significant risks, the changes made to risk scores, relevance, and mitigation strategies. The budget is then updated to reflect necessary mitigation costs and the company attempts to link every risk to a line item in the budget. After the update is complete, there is an evaluation of the planned spending on the mitigation of a risk relative to the potential impact of that risk to ensure that the spending is appropriate. Therefore, the departments use risks to shape and prioritize the budget.

Furthermore, each department at E meets with the ERM group separately to discuss how they have incorporated risks within the budget. Then, each department meets with the CEO to have a discussion that is strictly risk related. This includes examining the different risks, funding plans, past occurrences related to risk events, and any new forward-looking changes that have been incorporated. Input from the CEO is incorporated into the plans before they are presented to the Board for final approval. Company E recognizes that effective planning must include consideration of significant risks and the allocation of resources to address those risks. On the other hand, Company F takes a higher-level approach to the incorporation of ERM into the resource allocation process. As is common in the financial services sector, Company F uses a risk-based approach when calculating return on investment. They also utilize ERM when approving expenditures on new projects. Each project's expenditures must go through a stage-gate process of approvals, one of which is focused on risks.

Both E and F provide great examples of how companies can involve ERM in their resource allocation methodologies without completely changing the budgeting process that is currently in place. While the two companies took different approaches to the incorporation of ERM into budgeting, both have devised a way to think about the actual cost of risks and how it should affect the allocation of resources. Although it is not extraordinarily popular, we believe companies that utilize ERM have an opportunity to seriously benefit from the formal incorporation of risk considerations within budgeting and resource allocation.

Enabling Proactive Responses

Throughout the case study, many companies stressed the importance of a proactive approach, rather than a reactive approach, to managing risks. Managing risks reactively could be extremely costly and may even hinder an organization's continuity. Improving awareness of potential harmful events has been shown to prevent or minimize business losses and disruptions. Through ERM, companies are able to prioritize the most significant potential risks, evaluate their impact, and develop a strategy to monitor and respond to the risks in a timely manner.

An effective tool that has proven to enhance a company's ability to proactively address risks is the Key Risk Indicator (KRI). KRIs are forward-looking measures that can be used to help predict when risk events are more

likely to occur. KRIs can be developed by evaluating root causes of risks, and then analyzing those root causes to identify metrics that have predictive value. Several companies in the case study utilize KRIs to monitor risk trends.

Company E developed a KRI dashboard that acts as a “stoplight” with different colors signaling whether a risk requires more attention. When a risk is flagged, the company can update their mitigation efforts before the event causes any major impact on the organization. Company D also uses KRIs to give early warning signs that the potential risk events are becoming more likely to occur or are increasing in significance. When a KRI reaches a certain level, management can take immediate action to address the risk, which greatly reduces the impact of the risk event. The use of KRIs in ERM is an excellent example of how companies can become more proactive and avoid any significant risk impacts.

Even without a formal KRI system, a proactive ERM function can serve in a valuable risk monitoring function. In the case of A, the ERM function was monitoring patient volumes related to specific strategic initiatives. When the company experienced declining patient volumes, the ERM function identified the likely root cause as not focusing enough on meeting the needs of their physicians. This risk was mitigated by addressing targeted areas such as equipment, facilities, and training programs to provide more resources to physicians, thus improving patient volumes.

Spotlighting Hidden Risks

A proactive and robust ERM function allows for a company to identify and mitigate risks that may be unknown or overlooked. A few participating companies were able to provide tangible examples of risks that were uncovered, analyzed, and effectively treated directly as the result of the ERM process.

In one example, ERM identified a concern bubbling up from the lower levels at Company A. The concern was that the eventual retirement of tenured executives would change the tone at the top and the culture of the company. Having heard this concern multiple times, the ERM function followed up and found that succession plans were outdated. Subsequently the company acted to improve its succession planning process to address this risk. As shown in this example, the ERM function cultivates a transparent flow of information throughout the organization, which leads to timely, practical risk responses.

Company A’s ERM function was able to use their enterprise wide view, to identify the depth and breadth of the potential nursing shortages. While this was a risk that had been on management’s radar, it had not been given a high priority because executive management did not expect the risk to have a significant impact at the time. When results from the annual risk identification process were compiled, it was evident this risk was starting to be felt across the organization and was more significant than previously considered. The ERM function was able to research the forces driving the shortages and present their findings to the executive management and the Board. The company then implemented a mitigation strategy to improve retention rates.

Overall, the most significant example was that of the logistics function at Company D mentioned earlier, where many companies in their industry were transitioning to outsourced logistics. After the ERM function performed an in-depth analysis, the logistics program was found to be a competitive advantage that was better maintained in-house. The finding allowed for management to preserve the competitive advantage.

CONCLUSION

ERM functions differ in maturity, structure, and objectives from organization to organization. Throughout the case study, the six different participating organizations showed common themes of how a strong ERM process added value to their organizations. Several of the participants also had unique insights into how their ERM function, tailored to their company and industry, has added value in different ways. We also observed that the most commonly cited benefits were more intangible in nature, but there were also some specific examples of tangible benefits that were shared.

The value provided by increasing risk awareness is more intangible, yet each company in this case study recognized the importance of having an ERM function serve as the focal point for two-way communications regarding risk. The ERM function, having a view of the critical enterprise risks, is uniquely able to promote risk

“It is challenging to directly measure the value of not having an event occur or having the impact of an event minimized”

conversations across different departments and business units throughout the organization. In this way, the ERM function is able to disseminate information

about the critical risks facing the enterprise while also helping management at all levels of the company manage risks and opportunities within their own area.

Through the process of assessing risks, the ERM function focuses the organization’s attention on what matters the most, the most impactful risks. One participant described the ERM function’s ability to “drive the Board’s agenda” by providing them information about the most immediate and significant risks affecting the company’s ability to achieve its strategic objectives. This is extremely valuable in enabling directors to effectively carry out their oversight responsibilities.

Some of the more tangible elements of value were the use of the ERM team as internal consultants and the ERM function’s ability to shift an organization’s focus from short-term to long-term view of risk. Different areas of the company may call on ERM, in its consulting capacity, to help them identify and assess risks related to the execution of a major project or initiative, as well as suggest techniques for monitoring risks. The fact that the organization calls on the ERM function in this way indicates that the function is valued for the unique insights it brings that may not be available with an external consultant. In addition, the ERM function facilitates a longer-term view of risks through tools such as the Black Swan analysis that is used to identify and monitor the rare risks that may have low likelihood of occurring but could have a material impact on the company. The ERM function is valuable in pushing management to focus on the longer-term risks that may not seem significant today but are building in significance over time and may require more lead time to prepare a response.

The ERM process can also add tangible value to an organization by bringing risk information into the resource allocation process. Some of the companies in our case study considered the potential impact of risks, and the resources needed to address those risks, in the budgeting process alongside the more traditional requests for resources to further the company’s goals and objectives. By linking risks to budget requests, management is ensured that they are looking at the entire picture of what is required for the organization’s success. Having an ERM process in place also promotes a proactive approach to identifying and managing risks which provides tangible value in reducing operational surprises and the negative consequences of risk events. The use of KRI’s provides a more disciplined approach to monitoring and addressing risks. This advanced warning system can be combined with preset triggers to ensure that risk response plans are activated at an optimal time. The companies in this case study that utilize KRIs have been able to significantly reduce the impact of various risk events.

Ultimately, the most tangible examples were the instances where ERM could be directly linked to a specific action. Those examples show that ERM has an important role in accumulating and synthesizing data from throughout the organization to provide strategic and actionable insights to senior leaders and the Board of Directors. We hope that readers will benefit from gaining an understanding of the different ways that value is provided by ERM at the organizations we studied. Each of the value propositions identified in this study provides insights that could be used to either convince an organization to initially invest in a robust ERM program or to extend an existing program to realize more value.

**APPENDICIES:
INDIVIDUAL COMPANY CASE STUDIES**

APPENDIX A

Company Overview

Company A (A) is in the healthcare sector and operates in many states across the country. As a long-standing company in the industry, A strives to put the patient first and provide quality care. A has a market capitalization of over \$30 billion.

Overview of ERM

Objectives

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

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

Structure Within A

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

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

Risk Identification and Assessment

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

Surveys and Interviews

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

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

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

Risk Universe Visualization

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

Risk Response

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

Communication and Monitoring

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

How ERM Adds Value

Company A has realized value from its ERM program through the identification and proactive response to risks that otherwise may not have been recognized and addressed in time to avoid negative consequences. This was made possible by the ERM function's ability to break down silos and facilitate the exchange and compilation of risk information across the company.

An example of the value proposition described above was evident when the ERM function identified a common concern at the lower levels of the company related to succession planning. Employees at the lower levels were concerned about how the tone and culture of the company would change when the tenured executives left the company for retirement. These concerns lead the ERM function to discover the outdated succession plan that was in place at the company.

The executives had been with the company for such a long period of time that they had not given much thought to a formal succession plan. The situation was remedied after the ERM function presented the concerns over succession planning, discovered through surveys implemented during the risk assessment and identification process, to executives and those charged with governance. Thereafter, a formal and up to date succession plan was put in place and more resources were allocated to leadership development programs mentoring of middle management to help fill those roles as they opened. The ERM function was able to identify and communicate the concerns over succession planning early, allowing management to proactively address the issue.

A second example of the value ERM provides relates to the risk of shortage of nurses that hospitals currently face. In a similar manner as was described in the previous example, the ERM function discovered through their annual surveys of the operational level management, that the hospitals were encountering significant nursing shortages. While this was a risk that had been on management's radar, it had not been given a high priority because executive management did not expect the risk to have a significant impact at the time. However, the surveys revealed that the shortage of nurses was already being felt in many hospitals throughout the United States. The ERM function, working with Internal Audit, was able to research the forces driving the shortages and recognized that there were several different factors including a shortage of new nurses coming out of college as well as an improving economy that increased wage pressures and made it easier for nurses to change jobs. The findings were presented to the executive management and the Board and the company developed a response plan. The ability of the ERM function to facilitate the information exchange concerning risks throughout the organization helped to provide executive management with information that enabled a more proactive stance in addressing risks, as was the case with the two examples discussed above which were identified and addressed before they had the chance to materialize into a significant risk event.

Yet another example of the value ERM provides was apparent as they identified some issues with the company's strategy around physician alignment. Most physicians are not employed by the hospitals they practice in. The physicians choose which hospitals they want to practice in based on the quality of nursing care that will be provided for their patients, the availability of the equipment and facilities required for them to practice, the preferences of their patients and the insurance those patients have, the ease and experience of working in those hospitals, etc. The doctors are clients of the hospitals. If a hospital's goals are not aligned with those physician's needs, the doctors may choose to direct their patients to another hospital. The company's hospitals were seeing some declines in patient volumes in some markets that they felt were the result of not focusing enough on the needs of the doctors. More focus was placed on listening to the doctors, making it easier for them to practice in the company's hospitals, updating equipment and facilities that they use in surgeries, adding a Chief Medical Officer at the hospital level to work directly with the doctors that practice at their hospitals, providing well trained nurses and demonstrating high quality standards, etc. to better meet their needs so they will want to practice in those hospitals. More focus has been placed on this through investment in equipment and facilities upgrades, process changes, specialized nurse training programs and a high focus on quality and measurements around quality standards.

ERM also helps the company dissect and learn from risk events that have already occurred to better prepare management for future risk events. After every significant risk event, the ERM function examines the risk event to identify root causes so that management can better monitor and prevent future impact from similar risk events.

Conclusion

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

APPENDIX B

Company Overview

Company B (B) is in the consumer cyclical sector and offers a variety of transportation solutions, including products and services. The organization is highly complex and matrixed, serving across five continents and being made up of numerous business units and functions. Most recently, the organization has a market capitalization of over \$30 billion.

Overview of ERM

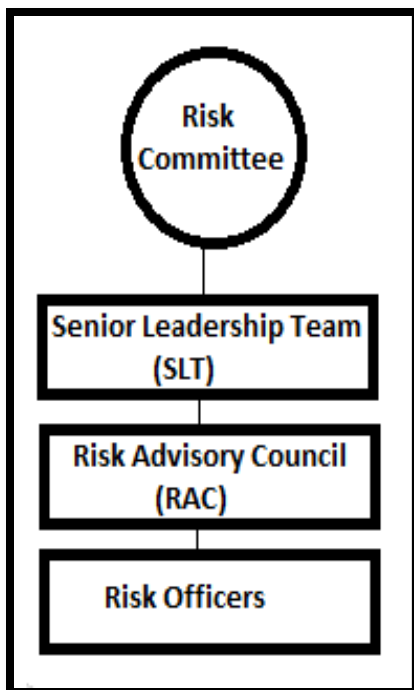
ERM Approach and Structure

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

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

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

Figure 1



Risk Officers are typically leaders and subject matter experts (SMEs) within the business unit or function. They support the RAC, escalating risks as appropriate, assisting in risk assessments and are responsible for championing risk management into their local areas of the business. Risk Officers are often relied on to bring a deeper, more technical perspective to a risk or mitigation plan given their knowledge within a specific area. The relation of all committees, teams, and councils are shown in Figure 1.

ERM Function

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

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

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

ERM Process

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

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

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

Risk Identification

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

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

Risk and Strategy Analysis

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

Tools that are utilized include:

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

How ERM Adds Value

B is a global company operating in a dynamic and changing industry, facing many risks as well as opportunities. ERM works with the business and external resources to identify critical risks and support leaders in the analysis of those risks and ongoing monitoring. This risk information also works to inform leaders as strategies or developed, reevaluated or key decisions are made. The ERM team is suited with consulting capabilities that allow that information to be expanded upon to achieve that greater value for leaders. At company B, executives may reach out to the ERM team to provide structure in analyzing an issue or decision and apply a risk lens to the situation.

Value is also added through ERM's consulting capabilities in the way that the team conducts analysis and turns around information in "real time." With the consultant mindset, risk visualization is created to cater specifically to the business unit or leaders that are asking for insights around a certain decision, strategy, problem or risk. In addition to risk visualization, B also finds that narratives and written communication is equally effective for risk communication.

The ERM team also creates value by providing a "toolkit" to the business as they analyze risks, assess strategies and make decisions. Techniques in the toolkit range from specific management workshops to stress testing to war gaming. Specifically, war gaming has been successful in providing the decision makers with practical information by considering the actions of external players, including other companies and governments. Reports from this process have not only helped to avoid negative risk scenarios but have also highlighted positive opportunities that could be exploited to further strategic goals.

Working with the business outside of traditional risk assessment and analysis has allowed ERM to further risk awareness into more practical applications with business leaders and continue to apply a risk lens in decision making and strategy development. In addition to the risk lens, the ERM team works to bring a cross-functional perspective to risk analysis and the application of techniques from their toolkit. This includes identifying and bringing people together as well as sharing knowledge gained from other work performed. ERM continues to evolve its value proposition, anchored in risk management but applying a risk lens while serving as strategic consultants to their business partners and leaders.

APPENDIX C

Company Overview

Organization Description

C is a company operating in the consumer cyclical sector and has a market capitalization less than \$15 billion. The company also provides financial services such as wholesale and retail financing and insurance programs.

ERM Overview

Risk Management Function: Internal Audit

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

Risk Management Function: Leadership Team & Strategic Risk Committee

The Leadership Team¹ also acts within the Strategic Risk Committee (“SRC”) Responsibilities of the SRC include the following:

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

Strategy and Objective Setting

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

Risk Identification

Company C identifies specific risks through workshop discussions at different levels and within different units of the company. These risks are then grouped at a high level into risk categories such as brand, competition, product, people, legal and government affairs, reputation, etc. Additionally, Company C identifies tail risks also known as Black Swan risks. A Black Swan risk is an event beyond the company’s current risk horizon that is not actively monitored (e.g. +5 years). The impact of a Black Swan risk may change a fundamental business assumption, and the nature of the risk could build over time to become significant.

¹ The Leadership Team includes: the CEO, CFO, COO, VP of Communications, CCO, President of Financial Services, VP of Marketing, and VP of Human Resources, Director of Strategy.

The Director of Internal Audit facilitates a workshop with a cross-functional group of company leadership to identify Black Swan risks that may affect the future success of Company C and documents the results. Company C has a list of key Black Swan questions that assist in identifying this type of risk.

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

Risk Assessment

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

Risk Response

Company C mitigates risks through the use of “action plans.” The Strategic Risk Owners² meets 1-2 times a year to report on their risks and discuss possible mitigation strategies. C has established action plans for the top three quadrants of risk. Because of their high priority, Quadrant I risks require the creation and ongoing review of action plans. The company facilitates the creation of action plans through the following steps:

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

After these action plans are finalized, the risk owner is responsible for implementing the action plan. For Quadrant II risks, action plans have been developed and implemented, and there is evidence that these actions have reduced the likelihood of the risk to “low.” Finally, Quadrant III and IV risks are mitigated through the use of risk monitoring to ensure that the statuses of these risks do not change.

Communication and Monitoring

The SRC, chaired by the (CFO) are responsible for monitoring the ERM process at C. The SRC are responsible for providing oversight of the risk management, identification, and mitigation processes. They are also involved in the review of adequacy and effectiveness of business risk management throughout the organization.

In regard to risks, the SRM Owners have the role of managing those risks and monitoring mitigations actions, including the effectiveness and validation of those actions. The Strategic Risk Committee meets periodically to review action plans and progress for each business risk, as well as ensuring that mitigation is incorporate in the Strategic Plans.

The SRC facilitates the ongoing monitoring of risks through the use of risk dashboards (see Figure 2 below). Near term risks are those that have an impact on EBIT, and therefore are relevant for the current year.



² Their role is to facilitate a process to manage and monitor the identification and mitigation of business risks for each strategic risk category.

Strategic impact to business model is more long-term in nature and involves the likelihood of risks occurring that could impact the company’s ability to meet their strategic goals. The future risk trend component is used to identify whether the risk’s inherent impact and likelihood is increasing, decreasing, or not changing year-over-year. By utilizing this tool, C is able to monitor specific aspects of risks over time. Another way the company continually monitors risks is through risk appetite and tolerances.

Figure 2 – Risk Dashboard Template

Risk Category	Risk Description	Risk Owner	Last Assessment Date	Near Term Risk (Ability to Deliver Plan)	Strategic Impact to Business Model	Future Risk Trend (1-3 Yrs)	Overall Future Assessment (1-3 Yrs)
Strategic	Brand						
	Competition						
	Product						
	Americas Sales Region						
	International Sales Region						
Financial	Financial						
	HDFS						
Operational	Information Technology						
	Manufacturing						
	Parts and Accessories						
	General Merchandising						
	People						
Compliance	Supply Chain						
	Legal & Government						
	Reputation						

Company Performance Attribute and Definitions		Time Frame
Near Term Risk (Ability to Deliver Plan)	Impact on EBIT Low, Medium, High	Current Plan Year
Strategic Impact to Business Model	Likelihood of risk occurring that could impact our ability to meet the strategic goal of the company Low, Medium, High	3-5 years

Future Risk Trend (1-3 yrs) Definition:	
	Inherent impact and/or likelihood of risk is increasing
	No change in inherent impact and/or likelihood
	Inherent impact and/or likelihood of risk is decreasing

C creates risk appetite statements and risk tolerances for each individual risk. In order to facilitate this, the Strategic Risk Committee utilizes a “risk management metric” with the following components: quantitative risk, qualitative risk, risk appetite statement, acceptable risk, and status. This metrics is reviewed and updated as needed to reflect the company’s current risk appetite,

tolerance, and status levels. The Audit Committee is responsible for reviewing the risk appetite and ensuring that they reflect the Board’s vision for the business.

On a more high-level, the Internal Audit department is responsible for the oversight of the SRM framework and

supporting processes, procedures, tools, and training. Continual monitoring of each of these aspects is crucial to ensure the sustainability of the company's ERM process.

The Internal Audit function is also responsible for interpreting, producing, and facilitating the annual summary report for the Board and Audit Committee. The organization also uses a SRM Liaison group to identify and share risk management best practices. The purpose of the SRM Liaison group is three-fold. The first being to promote risk awareness within the different functions across the company. The second being to help ensure consistent understanding of risk management processes and initiatives. Finally, this group supports risk informed decision-making.

Risk Culture and Leadership

A major key to the success of any ERM process is a strong risk culture and leadership. C exemplifies this through a values-based tone-at-the-top and a strong network of internal controls. The company's leadership and top management show full support for the process, which is imperative for the buy-in from all other individuals throughout the organization. The Board, Audit Committee, Strategic Risk Committee, SRM Owner, Internal Audit, Corporate Strategy and SRM Liaisons all play a crucial role in the ERM process at C. By comprising almost every facet of top management and implementing ERM specific roles, it is evident that the company fully supports the importance of a strong tone-at-the-top.

C has also implemented specific steps to facilitate a strong risk culture and buy-in throughout the organization. One example of this is the development of an on-line ERM training program for the Strategic Risk Owners and Risk Liaisons⁴. In the following year, the company enacted a feedback mechanism to facilitate program evaluations and improvements from ERM stakeholders. More recently, the company has created an on-line risk management training program for those individuals who are actively involved in managing risks. Through each of these actions, C has ensured the development of a rich risk culture.

How ERM Adds Value

The ERM process at C is viewed within the organization as a source of considerable value. They truly believe the process adds significant value and both identifies opportunities that may have never been pursued otherwise as well as increases the confidence that risks are appropriately managed and communicated across the company. When speaking with C, they believe there are two main advantages of ERM. The first being that it facilitates risk communication and focus, especially between the executive level and Board of Directors. The second key takeaway from C is the opportunities that have presented themselves through the Black Swan analysis.

Risk Communication and Focus

C perceives that the primary benefit of ERM is creating a structured approach to risk identification, evaluation and communication from the executive level up to the Board. This allows the Board to focus attention on the most significant risks, their nature, and events that could materially impact the success of the company. Because of this, the Board is reassured that the company is identifying and communicating critical risk information and is doing a diligent job in managing those risks. Specific examples of the types of information that is communicated with the Board include:

- A summary of the critical risks for the company and the reasons why they are critical
- Status of risk mitigation efforts, including significant gaps in capabilities for managing risks and status of initiatives to address those gaps
- The effect of changes in core assumptions underlying the company's strategy
- Changes in the overall assessment of risks over time

It is imperative for different levels of the company to come together and freely discuss risks. This allows for the sharing of ideas and opinions that may have never been heard otherwise. ERM involvement also enables integration with the Internal Audit risk assessment so there is a consolidated view of risk and alignment with the Internal Audit plan for visibility at the Board level. The internal audit function also facilitates the communication of Black Swan risks to the Board, which is described in the second section.

When communicating risks, C utilizes a risk dashboard tool. These dashboards create a snapshot of both near-term and longer-term potential risk impacts all on one page. The information provided by these dashboards includes the prior period assessment of risks, how they have changed over time, and the future risk trends. By utilizing this tool, C is able to easily communicate pertinent information regarding each identified risk, which facilitates the development and execution of effective plans to manage risks and meet goals.

Furthermore, the risk management process provides insight, promotes debate, and adds to the collective understanding of what is really important for the business to be successful. By focusing their attention on the events that could have a true impact on the success of the business, C is able to be more proactive and mitigate important risks in a timely manner. It can be quite easy for businesses to get bogged down over certain events that have a minor impact and require much less attention. By utilizing ERM, C is able to focus their attention to those risks that truly matter to the company's success. It is evident that the ERM process at C has enabled a structured approach to risk communication and focused attention on the most critical risks across the organization.

Black Swan Analysis

C identifies certain risks known as "Black Swan" risks. The company defines a Black Swan risk as an event that is beyond the company's current risk horizon, not actively monitored, and likely to build over time to become significant enough to change a fundamental business assumption. The Director of Internal Audit collaborates with the strategic planning function to facilitate a workshop to identify Black Swan risks that may affect the future success of C and documents the results. Planning for the workshop included developing pre-read materials that describe the risk identification process and include sample Black Swans, which is used to educate participants who may be unfamiliar with the process. The workshop solicits and synthesizes executive input in order to facilitate an open dialogue, specifically focused on Black Swans. The workshop output is summarized for in a form that can be used to brief the Board. This relates to the previous topic as it enables greater comfort within the Board that the company is looking around the corner and considers potential impacts to the company business model. This provides increased confidence that the company is proactive in thinking through the implications of Black Swan risks on strategy. It provides a forum for discussion with the Board on company actions to mitigate risks or leverage potential opportunities identified from the Black Swan process.

The main advantage of utilizing the Black Swan analysis is that it gives the company confidence to pursue opportunities they would not have otherwise. One example of an opportunity pursued through the Black Swan analysis is the use of a prototype before officially introducing a new product. The company had never utilized prototypes for any of its previous products but decided to for a recent product innovation. The display of their first ever prototype produced valuable feedback from customers all around the world. Without the use of ERM and the Black Swan analysis, the company may have never considered such a beneficial opportunity.

APPENDIX D

Company Overview

Company D is in the utilities sector and has a market capitalization between \$16 and \$30 billion.

ERM Structure

The ERM function at Company D is led by the Director of Risk & Advisory Services who has four direct reports, three ERM leads and a senior analyst. The Director in turn reports to the Chief Audit Executive (CAE) at the company. At the top of the hierarchy of the ERM function sits the CFO, to whom the CAE administratively reports.

ERM Process

Prior to 2005, D hired external consultants to perform annual risk assessments. However, management desired a continuous ERM process and wanted to avoid expensive external consulting fees for a one-time assessment. Management felt that the company would be able to develop the talent needed to establish a sustainable ERM function in-house and therefore created D's ERM function in 2005.

Early Years

In the early stages of D's ERM program, the company sponsored a simple "Ad Hoc" process that aimed to identify and assess the top ten inherent and residual risks based on interviews with senior leaders. The process was limited to management's perspective of risk, which resulted in narrow and siloed views on the risks facing the company. These risks were then mapped on a heat-map. Output from the ERM program was limited to a small audience via reports to executive management and the Board of Directors. The ERM program was under-utilized within the company, as many were not able to see the benefits of ERM right away. From there, the company evolved its process to include quarterly assessments and updates on the risks previously identified. This assessment was accomplished through interviews conducted by ERM. In addition to interviews, the ERM group gradually implemented surveys to solicit likelihood and impact ratings. However, the process of risk identification and assessment continued to involve only senior management, effectively keeping the siloed view of the risks facing the company intact, which resulted in a limited focus on the linkage between risks. The company continued to further grow the ERM process by expanding the number of risks being assessed, including more senior leaders in the risk identification and assessment process, using heat maps with risk ranking, and adding qualitative factors such as reputational impact onto the surveys. The top ten risks having highest impact on the company are also presented in a heat-map to show the likelihood and impact. As the ERM process continued to mature, new tools, such as dashboards were added to better organize and present the identified risks. With the new tools, the company was better able to identify specific, tactical risks and how they affected the company as a whole, providing a comprehensive approach to the ERM process.

Current Process

The current ERM process at D is described as "comprehensive." The current assessment process is conducted annually, and it begins with the identification and assessment of top risks affecting the company, which is accomplished through interviews, workshops, and surveys of senior level employees. Most recently, the survey targeted 70-75 leaders, which include top executives, Senior Vice Presidents, Vice Presidents, Executive Directors, Directors, and subject matter experts. The survey included both open-ended questions and simple scoring scales so as not to take up much time of the respondents, who receive other internal surveys from other departments. The survey asks the respondents to describe, in their own words, the risk scenarios they think are currently facing the company and any specific examples they can cite. Since some of the survey questions are open ended, the responses are not structured for quick analysis, so the ERM function assesses and evaluates each survey to spot common themes or concerns throughout the organization. Typically, the surveys identify 30-40 risk themes. The risks identified are then put into 18 different categories and ranked. After the risks have been identified, assessed, categorized, and ranked, they are presented at several levels of the organization.

The risks are first presented to functional leaders in small group meetings. Ultimately the risk themes are included in a report and presented to the Executive Committee (CEO and his direct reports), the Board of Directors and the Audit Committee. The executives typically discuss the top 10 to 15 identified risks, spending about 80 percent of their time discussing operational risks with high impact, low likelihood of occurrence. The remaining 20 percent of their time is spent discussing strategic risks with the highest likelihood of occurrence and high impact. These risks are then monitored by risk owners and updated on a quarterly basis. Historically, D has monitored 30-35 risks on an annual basis. Although the risks are the primary responsibility of the risk owners, the ERM function helps risk owners monitor risks throughout the year.

Future Goals

D hopes to mature its program into an “integrated” approach. This approach is characterized by coordinated risk management activities, enterprise-wide risk monitoring and measuring, and linkage between assurance functions. D has identified some opportunities for improvement in their process, particularly with respect to better coordination of risk oversight, alignment of functional and corporate goals, and an enterprise view of risk and assurance. The “integrated” approach hopes to address some of these issues and breakdown the silos that limit an enterprise-wide views of risks.

How ERM Adds Value

The value of ERM at Company D comes from the program’s ability to facilitate risk conversations within and throughout different business units, which ultimately helps to break down the siloed view of risk. The facilitation of the risk conversations is accomplished through various interviews and workshops conducted during the risk identification and assessment phase of the ERM process. Although the interviews are conducted, and the results shared with those in management positions, the ERM function sees the concerns of leaders in different business units and provides a more holistic view of risk in which risk is interrelated rather than isolated. The advantage of a holistic view is that risks are no longer viewed and dealt with in isolation at the business level; this prevents redundant efforts to address the same risk across multiple segments. An important value proposition of the ERM function at Company D includes the effort and focus to support the need for “real-time, actionable data” to improve decision-making. The ERM program monitors risks and opportunities associated with different projects at the company and provides decision makers with information that enables more effective decisions.

An example of the value provided by ERM came when an operational manager contacted the ERM function when he was considering expanding the proprietary transportation business instead of increasing reliance on third-party carriers. At the time, the industry was moving towards increasing their reliance on third-party carriers to reduce expenses. However, the operational manager believed Company X’s proprietary transportation business was a competitive advantage. The ERM function worked with the operational manager and his team to analyze the risks and opportunities associated with the transportation business, supplemented by performance metrics. By providing a holistic view of the project’s risks aligned with the strategic objectives of the company, the ERM function provided different risk perspectives and identified opportunities to enhance value for the company and its stakeholders. The operational manager presented the recommendation, supported by the risk analysis, to senior leadership for approval. The recommendation was approved and implemented.

This example shows how the ERM function at Company D facilitates risk conversations throughout the organization to break down silos and provide analytical support to decision makers. The operational manager may not have had a balanced view of risks and opportunities to present to the executive decision-making level and could have faced resistance to proceed. The ERM function provided additional analysis, so that the company was able to seize an opportunity that may have otherwise been unknown, except at the operational level.

Another value adding proposition the ERM function at Company D provides is the group’s ability to furnish decision makers with real-time, “actionable” data. When large projects are underway, the ERM function assists management in monitoring the environment around the project to identify and assess risks that may emerge

during the project's life.

In doing so, they help decision makers to address issues that may jeopardize the completion of a project. In a recent example, Company D has been expanding its operations outside the United States. The ERM function is working with the business development function at the company to understand and capture the risks associated with various proposals. They are surveying the environment in different locations and monitoring the changes in economic and regulatory conditions. The purpose of this activity is to help decision makers identify and address risks that may impact the strategic objectives of the expansion efforts so that they have a more comprehensive view as strategic decisions and trade-offs are made.

APPENDIX E

Company Overview

E is in the utilities sector and has a market capitalization between \$16 and \$30 billion.

ERM Overview

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

Structure Within E

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

The ERM Corporate Risk Committee consists of officers, general managers and departmental directors. These members meet quarterly to discuss various risk matters and emerging risks. Risk Committee members are usually at the General Manager/Director level and are closer to operations. Corporate Risk Committee meetings are held to update corporate risks and evaluate risks that may be elevated to the corporate level. At the meeting, votes are cast to find consensus and appropriate risk assessments. If a risk is determined to be worthy of elevation at the corporate level, the relevant risk owner would be called upon to present before the ERM Steering Committee.

Risk Identification

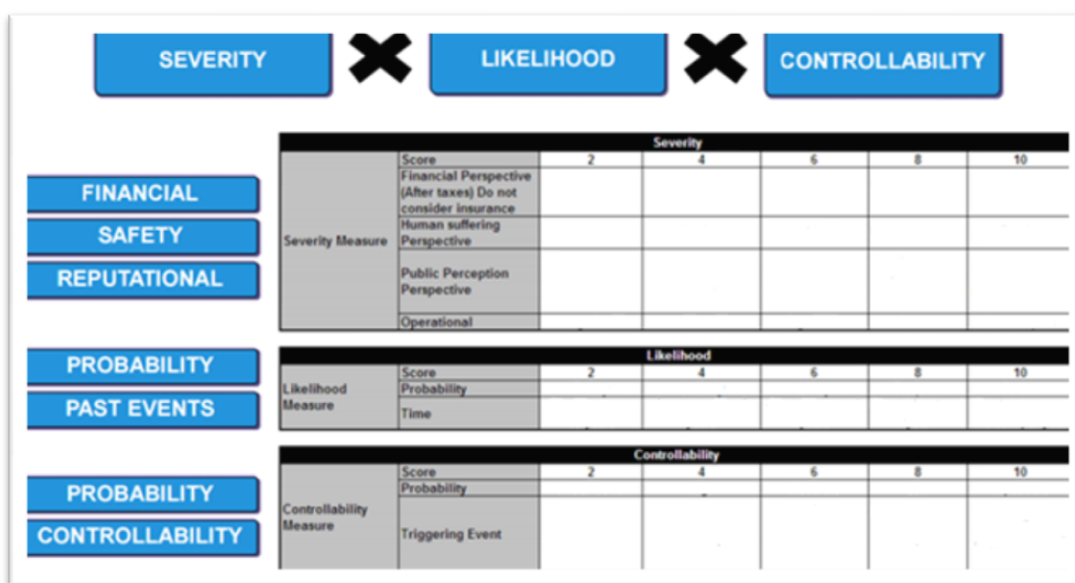
Risk identification occurs using both top-down and bottom-up methods and is facilitated through meetings with various business areas. Top down approaches include input from the ERM Steering Committee, which scans the landscape for higher-level emerging risks, and benchmarking against other companies. Meanwhile, departments across the organization identify from the bottom-up lower-level risks affecting particular business units. The ERM Corporate Risk Committee also utilizes a bottom-up approach.

As described above, a risk coming from directors of operational units can be elevated to the status of “corporate risk” based on a qualitative analysis of the risk issue and a vote of Risk Committee members. Thus, risks can receive corporate-level attention through a bottom-up risk identification and assessment process. These two levels of identified risks are subsequently merged together to provide a broad risk perspective. Roughly 400 departmental risks have been identified within the risk universe, with many repeating across business units.

The ERM department meets with all approximately 30 business units annually to update risk profiles and determine whether risk assessments need to be adjusted. Identified risks are categorized based on the corporate sector impacted by the risks. Then, the ERM department considers the way in which risks assigned to a particular category can affect other categories, adding an enterprise-wide perspective. After consolidation of similar risk wordings, about 260 unique risks exist in the organization’s risk register.

Identified risks, both corporate and departmental, are assessed and prioritized. Risks are assigned to a risk owner, who is responsible for managing the risk. The risk owner is generally a subject matter expert (SME) well equipped to manage the risk. Using the most-probable worst-case scenarios, each risk is assessed on three dimensions: severity, likelihood and controllability. Severity factors include financial, safety and reputational components. Likelihood factors are determined by looking at past events as well as current probabilities. Finally, controllability evaluates the organization’s ability to prevent and detect an event. Each dimension is scored on a 10-point scale. Then, the severity, likelihood and controllability scores are multiplied together to generate an aggregate score for each risk on a 1,000-point scale. A blank template of this risk assessment tool, as well as a further explanation of its operation, can be viewed in Figure 3 below. This quantification helps to prioritize risks effectively. SMEs contribute qualitative input to aid with risk prioritization, as operational risks can be difficult to quantify. E not only manages risks that are likely to occur, but also identifies and assesses high impact, low probability risk events, often termed “Black Swans.” Although this is still a work in progress, C-suite executives and SVPs are asked to identify Black Swans relative to their department and may report their findings to the CEO.

Figure 3 – Risk Assessment Factors



Appropriate risk management strategies are developed based on risk assessment. Root cause analyses are fundamental to eliciting a proper risk response, as the identification of the sources of risks leads to more effective mitigation. For the most important and imminent risks, the company makes use of a bow-tie analysis, which promotes thinking about the “causes” of risks and current preventive measures. However, if little control can be exercised, focus shifts to minimizing the “consequential impact” of potential events. The bow-tie analysis aligns with the controllability dimension in risk assessment. Accordingly, an informed decision can be made as to whether risk responses will center on causes or consequences. The bow-tie has facilitated creation of key risk indicators (KRIs) based on identified risk root causes.

A KRI dashboard has also been formed to monitor risk trends. The company thinks of KRIs as a stoplight, with the colors of the light signaling whether a risk requires more attention. A risk’s cause, mitigation strategy and KRI are all linked, allowing for an organized and timely response. A risk’s mitigation strategy is less of a risk response, and more of an ongoing activity in place to address risks continually.

KRIs and bow-tie analyses indicate whether additional mitigation efforts are necessary. KRIs and bow-tie analyses also provide quantitative, data-driven monitoring over significant risks. This quantitative data is combined with qualitative input solicited from SMEs to determine a proper risk action. Together, these data-driven and subjective perspectives merge as part of monitoring practices.

Risk Communication

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

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

Integration and Perception

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

ERM is integrated within many facets of the company, one of which being the budgeting process. E currently utilizes a 1-year budget and a 5-year look-ahead overview budget. With the help of ERM, the company plans on documenting budget data for all 400 department-level risks across the organization. A risk factor is considered by the company when determining funds to be allocated to various projects and departments, speaking to ERM's involvement. ERM allows E to generate better budgeting data, as focus is geared towards risk mitigation strategies and the actual costs of those strategies.

This allows for the analysis of whether or not the company is using its resources in an efficient manner. Additionally, ERM is engaged through annual meetings attended by top officers and company departments. After these meetings, departments make presentations before the CEO and President, requesting funding for projects. Thus, ERM is fully embedded and adds value within the budgeting process of E.

E plans to implement several changes to their ERM process in the current and coming years. One important plan is the way in which they identify emerging risks, which is currently facilitated through meetings with various business areas. By the end of 2018, E plans to develop a more structured approach to their emerging risk identification process by including surveys, interviews, and possibly a web interface for sharing inputs.

They are also interested in an integrated IT system to track and communicate risks. Currently, E uses electronic paper, such as spreadsheets and e-documents, to accomplish this. Implementing this type of system is something the company is looking into throughout the next few years in an effort to continue the improvement of their ERM process.

How ERM Adds Value

When speaking with E, it was evident that they cherish the values provided by their ERM process. In fact, they believe it would take an abundance of hours to fully discuss and embrace the true breadth and depth of how the process impacts the company. However, E provided several key takeaways of how ERM adds value to their organization, including eliciting risk communication, expanding anticipation, and implementing ERM into their budgeting process.

Eliciting Risk Communication

One crucial benefit from their ERM process is the creation of a risk management methodology and thought process throughout the company. Through ERM, E is able to set boundaries for risk discussions and focus on the opportunities and threats that are truly important to the organization. They accomplish this by centering their discussion around a paradigm of three risk assessment factors: severity, likelihood and controllability.

In addition, ERM creates a forum to discuss risks, allowing everyone's opinions to be heard in one concentrated area. This also allows E to compare issues across the entire company and direct management's attention to specific risk areas. Furthermore, risk communication at E enables a heightened awareness and focus on risks that are inherent to the business and has allowed risk owners to use a residual approach to evaluate risk mitigation strategies. The company utilizes ERM to monitor and assess how certain risks are currently affecting the company and how they are changing year-over-year.

Risk awareness and communication at E is facilitated at different company levels through both a top-down and bottom-up approach. Top-down approaches include input from the ERM Steering Committee, which scans for higher-level emerging risks, and benchmarking against other companies. On the other hand, departments across the organizations create risk awareness by assessing and identifying lower-level risks that affect particular business units. By using these techniques, E is able to communicate an array of risks at both the corporate and department levels.

Furthermore, E utilizes a bow-tie analysis and key risk indicators (KRIs) in order to create a more organized and timely response to risks. The bow-tie analysis promotes awareness about the causes of risks and how the company is currently preventing them. This analysis is aligned with the controllability risk assessment factor. Through the use of the bow-tie analysis, E has created KRIs in order to identify the root causes of specific risks. The company utilizes a KRI dashboard to monitor risks trends and identify which risks require more attention. The bow-tie analysis and KRIs are a great combination of tools that effectively monitor risks over time and indicate whether additional mitigation efforts are necessary.

The ERM process at E not only enables risk management, but also structures the communication and awareness of risks throughout different levels of the organization. By utilizing the bow-tie analysis and KRIs, the company can proactively address risks that require additional mitigation efforts. As a result, the company is further prepared for numerous events that could occur across the organization and can monitor risk trends year-over-year.

Expanding Anticipation

Another advantage generated by the ERM process at E is the expansions of anticipation of possible events that may occur in the long-term. It is evident that almost all ERM processes tend to focus on risks that are on the current horizon. However, E believes ERM is more than just a tool used to manage today's risks and can provide value as a forward-looking process.

Anticipating the unforeseen and focusing on what could have a negative impact on the company in the long-term can decrease the likelihood of a possible catastrophic surprise event. This is something E believes is a true value of ERM, which may have never been considered as in-depth otherwise.

ERM in the Budgeting Process

One of the most beneficial aspects of E's ERM process is how it is embedded within their budgeting process. More specifically, the company quantifies the cost of risk mitigation strategies and feeds these amounts into their budget. In order to fully understand how this works, it is important to gain a grasp of their budgeting cycle.

In general, E creates both a 1-year budget for each year and a rolling 5-year plan. The company also utilizes a trailing 4-year budget plan in order to facilitate the creation of the current budget. Each of the 32 departments within the organization manage their own profiles and budgets. The finance department sets guidelines and provides list of what needs to be considered by each department. The planning process begins in the first quarter, during which ERM is a main input into the budget considerations.

During the planning process, the departments consider both the corporate-level risks that trickle down, as well as their specific department-level risks. These risks are reevaluated through the ERM planning activities, during which the scores, relevance, and mitigation strategies for each risk is updated. Once this update is complete, the departments make changes to the budget as needed. The company attempts to link every risk to a line item in the budget. They then evaluate whether or not they are spending too much for any particular risks and assess any changes that may be deemed necessary. In essence, the departments use risks in order to shape and provide a form for the budget.

The ERM group then meets personally with each department head and risk owner. During this meeting, the department head agrees to all of the risks that they own and how they are incorporated into the budget. Next, all 32 departments meet with the CEO in July to have a discussion that is strictly risk related. This includes examining the different risks, funding plans, what has occurred in the past, and any forward-looking changes that have been made. The CEO then makes comments on the proposed plans and the departments make any necessary changes. Finally, the budgets are passed in September after Board approval and the cycle restarts in January.

Evidently, E makes it a priority to embed the ERM process as a part of their budgeting cycle. With both the ERM team and CEO involved, each department produces their budget with a clear focus on risks. This is a perfect example of how valuable an ERM process can be to an organization.

APPENDIX F

Company Overview

Company F (F) is in the financial services sector and offers a broad array of deposit, loan, and investment products as well as trust, fiduciary, and wealth management services. They cater 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. F accumulates deposits and generates funds from operations and borrowings. The income is used to originate commercial real estate loans, commercial business loans, residential mortgage loans, and consumer loans. Most recent market capitalization is between \$1 and \$15 billion.

Overview of ERM

ERM Framework

F's Enterprise Risk Management (ERM) Framework captures the inter-relationship of its values, vision, and strategic opportunities. When the ERM processes of the organization operate in harmony with its foundational documents, it ensures the continued success. It also increases the ability to exceed market expectations for the company without introducing unwanted risk. The ERM process was initiated at the request of the Audit Committee and the Board of Directors, it has evolved over the last 10 years. As a mature program it is highly structured, well documented, and in compliance with industry regulation. The Board of Directors later established a separate Risk Committee to govern the ERM process. 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 the company's overall business goals and objectives. A fundamental objective is to operate in a safe and sound manner that delivers on the level of confidence entrusted to them by their customers. Their goal is to correlate the efforts of various 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 the basis for its risk management process.

ERM Process

At an entity-wide level F defines its risk management objectives as:

- Identification of key risks
- Formulation of a clearly communicated risk appetite
- Establishment of strategic objectives in accordance with the risk appetite
- Optimization of risk and reward decisions using an organized process
- Engagement of its workforce contributing towards an effective risk management system

Due to the regulatory intensity of the banking industry, they have found it necessary to expand on the core categories of risk usually identifiable within non-banking organizations. The organizations risk categories include credit risk, market risk, liquidity risk, operational risk, compliance risk, reputational risk, and strategic risk. Risk categories are tied closely to FDIC regulation to provide effective demonstration to the regulators of the company's compliance with laws and regulations.

The strategic plan is created for 3-year periods and is updated annually. The related risks are identified and assessed through a series of facilitated meetings with business line managers, executives, and committees who are the primary overseers of the category of risk being evaluated. These "facilitated meetings" are conducted in a team setting and occur throughout the business's planning and execution cycle.

The meetings discussions focus on the functionality and viability of existing controls. The existing controls are evaluated to ensure they properly mitigate the potential that strategies will fail in planning or in their execution. The company’s risk categories are used to provide the necessary structure in these discussions. The meetings are regulated for potential audit or review by the regulating bodies of the industry.

The strategic planning process begins with an analysis of each specific initiative and the coordinating actions that must be in place to bring such a plan into fruition. During this time, several of F’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.

The ERM function records the top-level risk management activities in its documentation. ERM also facilitates communication throughout the organization by providing a forum where management-level committees can discuss their risk management plans in greater detail. The increased communication warrants that various committees and service lines are better prepared and protected against risk activities. A description of the roles of key members of the organization is discussed in the following section.

ERM Structure

F subscribes to the widely used 3 Lines of Defense model. This model helps to promote clear roles and accountabilities of risk management activities, to all reporting units within the organization. The first line of defense is management control, which includes business lines and support lines. The second line contains the various risk control and compliance oversight functions established by management. These second line controls can be separated into two groups: ERM Related Functions and Non-ERM Related Functions. Figure 4 below gives more detail to the various functions in the second line of defense. The third line consists of independent assurance, for company F this is Internal Audit.

Second Line of Defense	
ERM Related Functions	Non ERM Related Functions
ERM	Human Resources
Operational Risk Management	Legal
Third Party Risk Management	Finance/ Budget Control
Model Risk Management	Insurance
Policy Control/Administration	Physical Security
Information Security	Privacy
Cyber Security	Business Continuity
Incident Response	Change Management
Data Governance	Enterprise Stress Testing
Compliance Management	Sarbanes-Oxley Testing

Figure 4:

A specific example of the 3 Lines of Defense model is the Compliance Committee. The first line is self-review that certifies that self-assessment has been done. The second line contains programs that trigger the review process. The third line is handled by the Internal Audit program.

The company maintains a formal documented policy for guidance on ERM roles, responsibilities, and activities. They use a typical structured approach for the arrangement and 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. The Chief Risk Officer reports quarterly to the Risk Committee of the Board of Directors to confirm what they are hearing from other committees and business lines regarding risk exposures, and to provide a quarterly enterprise risk scorecard.

Executive management recommends 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.

F 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 Management Team” that represents the executive officers who work with the Board to execute on their overall strategic plan within the context of risk appetite.

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 Company F:

- IT Steering 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.
- Management Risk Committee - Group assigned to tasks that revolve around the everyday operational risk management activities (Similar to SRC, but a less policy view).
- 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, as well as 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 F’s Wealth Management Company.

Senior Risk Committee Information

Each committee has a charter that is approved annually. The Senior Risk Committee (SRC) is the designated management-level committee that has an aggregate view of all the types of risks facing the enterprise. The SRC is a smaller group of management that meet each quarter after all other committees have met. They discuss the company’s overall risk profile and corresponding programs.

According to the 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
- Provide recommendations to strengthen the company’s risk management program to executive management

- 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 management's actions provide a consistent approach
- Issue guidance and counsel to the other management level committee

F started the SRC to manage Sarbanes-Oxley compliance in 2004. The focus of the SRC is now driven by the strategic plan and has a 3-year time horizon that parallels that process. The SRC works in collaboration with the Management Risk Committee, who together are the forebears of and are responsible for discussing the aggregate of risks that may affect the business.

The SRC conducts 8 regular meeting throughout the year with each meeting lasting approximately 60 minutes, additional ad hoc meetings may be called as needed. Official “Senior Risk Committee Meeting Minutes” are prepared and cover the 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.

The Management Risk Committee is the team assigned to tasks revolved around the everyday operational risk management activities while the SRC has a more policy level view of enterprise wide risks. The Management Risk Committee works together once a quarter in a formal setting. The formal meetings are used as a reporting vehicle for ongoing work outside of the committee. To account for managers not involved in the Management Risk Committee a quarterly questionnaire is sent to all managers, so they can report any issues to the committee.

F is currently drafting a statement of overall risk appetite to guide and work with the strategic planning process. The SRC does not directly play a role in setting these limits and tolerance levels for F. In accordance with the SRC’s 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.

Senior Risk Committee Membership

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

Figure 5:

Chief Risk Officer	Chief Credit Officer	Chief Human Resources Officer	Chief Administrative Officer	Chief Information 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, setting the agenda and context of the SRC meetings, is the arbiter over accepting risk assessments, and has the ultimate authority of tracking mitigation plans, in some cases with reports moving up to the Board of Directors. The agenda set by the chairman is a standard agenda that is set once a year (during the business 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 are 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 periodically with the Risk Committee of 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 Executive Leadership Team (if determined appropriate), and at the end of the year the Risk Committee of the Board of Directors.

Monitoring & Responses

Risk mitigation plans are formulated in response to discussions at both the Management Level Risk Committee and SRC meetings. These risk mitigation plans produce "take-away tasks" that are assigned to the owner who is to complete the tasks and implement the plan. The SRC assesses the overall effectiveness of these plans being put into action and 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 4. The CRO consolidates the actions of these groups so that the SRC receives a holistic view of these changes.

At F, KRIs are considered more at the policy level in the form of tolerances and thresholds for specific risks. At the enterprise level, KRIs are more judgmental and variable.

Effective Management Level Risk Committees

F 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 and comparison across economic cycles.

The ERM function at F is mindful of other ERM processes in the industry. The CRO has worked to build a network of other CRO's and meet with them semi-annually to share lessons learned and process enhancements from other organizations. The industry knowledge combined with an environment of risk intelligence makes the ERM initiative at F successful.

How ERM Adds Value

Company F believes that the true value of ERM is “tethered to its ability to entrench itself into the operations of the company,” the more deeply involved ERM is, the more value it will bring. The nature of business operations is volatile and dynamic, ERM process's that F uses to promote structure and stability. Stability is created when management across the company is organized and coordinated to mitigate and respond to risk. ERM acts as an underlying system of information that is gathered across the organization. In an ideal state, that company F aspires to be, anyone in management can easily access the data and there is no need to rely on one person or process to provide information.

When building an effective systems of company risk data, the increased availability of information is vital. Its valuable because in such a highly regulated industry it increases the effectiveness and accuracy of responses to regulator request and inquiry. Financial service providers that are proactive in responding to regulatory changes have a competitive advantage over peers who run afoul in regulatory compliance. Financial institutions who demonstrate sustainability in their risk and compliance management program often have regulatory applications delayed and expansion opportunities denied. With more information the company can also identify and respond more quickly to recover from business missteps and address challenges.

Separately from management information, ERM has also provided positive opportunities to F by demonstrating the business value of increasing customer data. As more data is collected the goal to “know the customer's needs and wants” is more easily achieved. With a better understanding of the customer base, the company can make more informed decisions of which business opportunities to pursue.

ERM also makes an appearance in the budgeting process for the company. F uses a stage-gate process of approvals for the annual budget. One stage in the process is specifically devoted to risk-based return on investments, and analysis of risks.

Future Goals and Changes for ERM

One current goal of the ERM function is to increase the use of data analytics. As more analytics are used, larger sets of data can be analyzed. Larger datasets make it easier to see trends and create more objective data. As data becomes more objective, the decisions made by the company are less influenced by individual bias and judgement. This is being implemented specifically into the cyber security aspect of online financial services. The cyber security system includes authentication protocols and monitoring. The system is fortified using a variety of third party cyber specialist firms. The choice to engage these third parties was made to utilize the expertise and experience that each provides. This is specifically helpful with technology updates and changes in today's fast-paced society.

The second element of data analytics is to modernize the data that is shared and the manner in which the data is presented. Currently, the ERM group is dependent on traditional methods to gather data that is a byproduct of business activity and share the data through Microsoft Word, Excel, or PDF. The most helpful visualizations are those that show trends over time, especially when compared or benchmarked against other companies in the industry.

About the Authors

NC State ERM Practicum Team Biographies



Ben Boudreaux is a graduate student in NC State's Masters of Accounting program with a concentration in Enterprise Risk Management. While obtaining his bachelor's degree in accounting from NC State, he completed an audit internship with Dixon Hughes Goodman in the Spring of 2017. As an intern, he gained valuable audit experience in the financial institution and real estate industries. He has accepted a full-time position with the firm and will begin his career as an audit associate in October of 2018.



Shovan Bhatta is a graduate student in NC State's Masters of Accounting program. While obtaining his bachelor's degree in accounting from NC State, he completed an internal audit internship with Extended Stay America in the Summer 2016. As an intern, he gained valuable audit experience in the hotel industry. He has accepted a full-time position with Ernst & Young and will begin his career as an Assurance Staff in Summer 2018.



Adrienne Shoaf is pursuing her Masters of Accounting at NC State University and expects to finish in May of 2018. She attended NC State for undergraduate education and was awarded a bachelor's degree in Accounting with a concentration in Managerial Accounting. While in her undergraduate program she interned with Self-Help Credit Union and specialized in process documentation. Adrienne has accepted a full-time auditing position with Blackman and Sloop CPA in Chapel Hill and will begin in August 2018.

