

The Art & Science of Key Risk Indicators: A Case Study Analysis



Prepared by: Truth Chou, Jordan Fulbright, Campbell Irwin, and Michael Patch

NC STATE GRADUATE STUDENTS | POOLE COLLEGE OF MANAGEMENT

FACULTY ADVISOR: Bonnie V. Hancock

TABLE OF CONTENTS

INTRODUCTION 3

 Case Study Process and Participants 3

TIMING OF KRI IMPLEMENTATION..... 4

DEVELOPMENT OF KRIs..... 4

 Role of ERM Function vs. Risk Owners 4

 Workshops 5

 Interviews..... 6

SOURCES OF DATA 6

TYPES OF KRIs..... 7

MONITORING & REPORTING OF KRIs 7

THE FUTURE OF KRIs 8

CONCLUSION 9

APPENDICES 10

 APPENDIX A 11

 APPENDIX B 13

 APPENDIX C 17

 APPENDIX D..... 23

 APPENDIX E 33

ABOUT THE AUTHORS 40

INTRODUCTION

Enterprise Risk Management (ERM) is an ongoing process that applies a holistic, portfolio approach to the most significant risks to the achievement of the entity's business objectives. In general, most ERM process implementations begin at a very basic level and evolve over time. Typically, as the ERM process matures, more sophisticated elements like the use of Key Risk Indicators (KRIs) are implemented. KRIs are metrics used by organizations to provide an early signal of increasing risk exposures in various areas of the enterprise. In some instances, they may represent key ratios that management throughout the organization track as indicators of evolving risks and potential opportunities, which signal the need for actions to be taken. Others may be more elaborate and involve the aggregation of several individual risk indicators into multi-dimensional scores for emerging events that may lead to new risks or opportunities.¹ Implementing and effectively using KRIs brings additional challenges to the ERM function given the in-depth analysis that the process typically requires.

The main purpose of *The Art & Science of Key Risk Indicators: A Case Study Analysis* is to analyze and provide examples of how companies across various industries have designed, monitored, and reported KRIs. The company participants we interviewed have taken different paths to arrive at the KRI reporting they use within their ERM process. In addition to analyzing the common themes and challenges that the companies faced, our goal is to provide examples that could be used as guidelines for organizations seeking to implement or improve their KRIs.

Case Study Process and Participants

This case study was conducted by first gaining an understanding of the overall ERM process of each company, and then exploring the process of developing, monitoring, and reporting KRIs. Interview questions were designed to identify the timing and reasons for companies to implement KRIs, the methods each used to develop KRIs, and the subsequent reporting and monitoring of KRIs. The questions also included how companies improve their processes and where they want to go in the future. A comparison of the five different companies reveals common themes and unique attributes around implementation and execution of their KRIs.

A common theme is that industry participation affects the way companies adopt and use KRIs. For example, organizations that participate in highly regulated industries typically have greater access to external information and more quantitative information based upon the nature of their industry when compared to industries that are not subject to heavy regulation. While these inherent differences exist, companies in this case study also exhibited common themes in their KRIs. Examples include the importance of using high quality data, effective communication as well as buy-in from the business side of the organization in addition to the ERM department.

To ensure anonymity of the participants, we identified each company by sector and revenue. Company B represents a subsidiary that does not provide financials separate from its parent; therefore, its revenue is not comparable. Below is a summary of companies that are represented in this case study:

	A	B	C	D	E
Sector	<i>Retail</i>	<i>Financial Services</i>	<i>Financial Services Insurance</i>	<i>Utilities</i>	<i>Hospitality</i>
Revenue	\$9 Billion	\$49 Billion	\$22 Billion	\$12 Billion	\$9 Billion

¹ COSO. Developing Key Risk Indicators to Strengthen Enterprise Risk Management. *How Key Risk Indicators Can Sharpen Focus on Emerging Risks*.

TIMING OF KRI IMPLEMENTATION

There were two different points in the evolution of the ERM process that companies introduced KRIs: at the same time as the ERM process was started or after the ERM process was fairly well established. Companies A and B implemented key risk indicators at same time as their ERM processes. The two companies operate within the retail and finance industries. Given the highly regulated nature of the financial industry, there is a plethora of information readily available to use as risk metrics and therefore Company B was able to select the metrics that best tracked its risks right at the start of the ERM process.

Company A, on the other hand, chose to use existing key performance indicator (KPI) information which was already being reported on a single dashboard. These KPIs were reworked into KRIs, where appropriate, in order to leverage risk management information that had already been gathered for other purposes. By including all the KRIs in a single dashboard, a holistic view of the company's risk portfolio is presented. Given the availability of existing data, companies were able to implement the KRIs at the same time as the ERM process. There was no need to delay the implementation to collect information on the risks.

Interestingly, Companies C and D also operate in highly regulated industries but did not implement KRIs at the same time as their ERM process. Companies C, D, and E implemented KRIs after their ERM process was well established. Those companies did not add KRIs initially because they did not have the required resources to develop and report on KRIs. By waiting until the ERM process was more developed, these three companies had a foundation upon which they could build out KRIs.

DEVELOPMENT OF KRIs

There are no set methods for developing KRIs. The first step in the development of KRIs is to identify who is responsible for the risk and then to establish the roles of the risk owners and the ERM function in the KRI development process. Companies that participated in the study then used workshops and/or interviews with risk owners to develop their KRIs.

Role of ERM Function vs. Risk Owners

Three companies had risk owners take responsibility and accountability for developing KRIs while the ERM team played a supporting role. Risk owners in companies A, B and D took control of KRIs, with the ERM team playing an advisory role, sharing insights on optimal approaches. In some cases, like Company D, the ERM team facilitated workshops to assist the risk owners in developing KRIs. The employees within the business units are responsible and accountable for the KRI, while the ERM team plays a background role. This reflects the use of subject matter experts within each department, and ensures buy-in from the business side.

Companies C and E took a different approach with the ERM team leading the development of KRIs. Although there is still significant involvement from the risk owners, the effort to develop KRIs is driven primarily by the ERM team. Company E realized the risk owners did not have bandwidth to take on this effort and therefore the ERM team took the lead in developing the KRIs. In that process it was the ERM team's job to gain input and buy-in from the business unit leaders by demonstrating that KRIs would be a valuable tool in achieving business objectives.

After the companies determined the appropriate roles for the development of their KRIs they then began the process of identifying the appropriate metrics to use for KRIs. Companies used both workshops and interviews to identify those metrics.

Workshops

Workshops were used to develop the KRIs in order to gather input and generate discussion from a broad group of stakeholders, including risk owners and subject matter experts. Company D was able to effectively utilize workshops to analyze its risks. Risk owners that have been assigned a risk gathered information prior to the workshop. Included within this information are potential causes that could lead to the risk event at the center of the Bowtie analysis. The ERM director then organizes a series of workshops that usually included six to eight subject-matter experts to keep the discussion focused and encourage debate. The director determines the right combination of people and the appropriate level of preparation can create the kind of atmosphere that would drive the creativity needed to focus on the relevant root causes of the major risks of the organization.

Company D uses a “Bowtie” analysis technique in its workshops. The illustration below portrays the bowtie analysis process in more detail. It starts with the risk at the “knot” of the tie, and then moves to the left to identify and describe the events or circumstances that may cause the risk event to occur, paying particular attention to root causes. Once those causes have been identified, the analysis then identifies preventive measures that could be implemented. At this point there could be an evaluation of the actual preventive measures that the organization has in place to determine whether additional measures should be put in place. The analysis then moves to the right to look at the potential consequences that would result after the risk event happens, and the plans the organization either has or should have in place to minimize the negative effects of the risk.

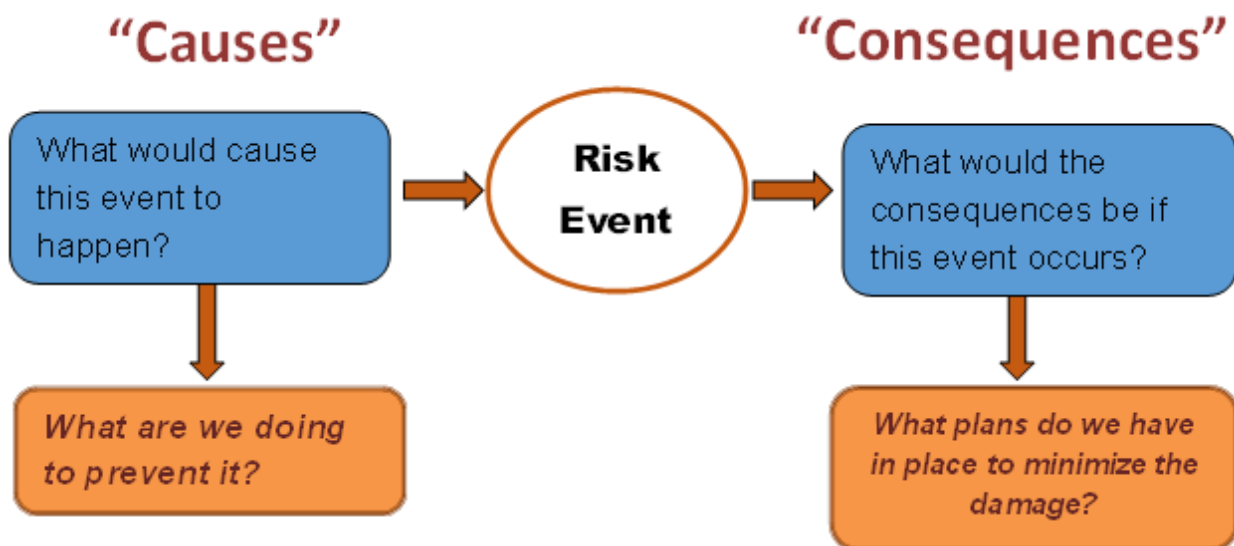


Figure 1: Bowtie analysis

In the workshop, participants first focus on the events that could cause the risk to happen. Once the cause events have been identified and agreed upon, the risk owner and subject matter experts consider the potential consequences of the event. Based upon the identified consequences, the group reviews mitigation strategies currently in place or need to be developed for each cause. Each workshop would last two to four hours and, depending upon the complexity of the risk, the number of workshops needed to vet each risk could range from two to four. The ERM director found that these workshops had to be broken down in this way in order to be more effective due to the exhaustive nature of the approach.

Interviews

Interviews are used to gain perspectives from individual risk owners and subject matter experts. In particular, the use of interviews allows both the ERM team and the business unit leaders to avoid the potential for groupthink and identify unique perspectives. One-on-one interviews are used by Company A and E to start the discussion of proposed metrics with business unit leaders. The use of interviews is beneficial in that the ERM team and the business unit leaders share their perspectives on proposed metrics and challenge each other. Company A also uses interviews but takes a more informal approach. The ERM leader begins the interview process by sitting down with the risk owner to gain a thorough understanding of what is being done to manage the risk. Once an in depth understanding of the risk is obtained, a follow up interview is then conducted to develop a KRI that will be effective. Company A chose to complete their interview process in this way because it encourages the risk owners to take accountability for their KRI.

SOURCES OF DATA

An important element of any KRI is the quality of the available data used to monitor a specific risk. Attention must be paid to the source of the information, either internal to the organization or drawn from an external source. Sources of information that are available help inform the choice of KRIs to be employed. Figure 2 below shows companies A, D, and E using mainly internal data while companies B and C use a fairly even mix of internal data and external data.

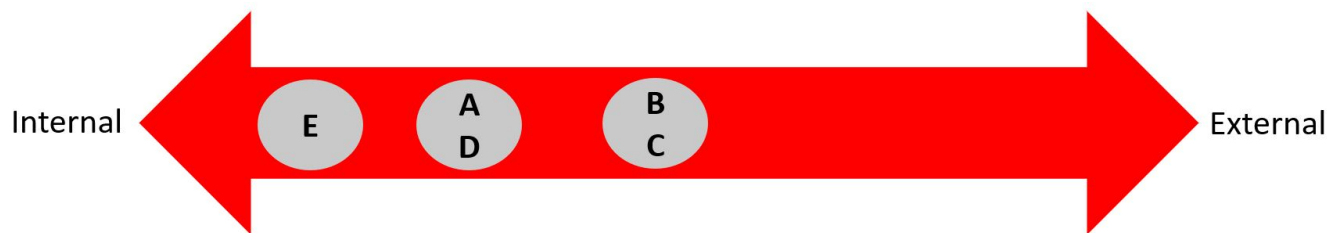


Figure 2: Sources of Data

The three companies using mostly internal data are in the following industries: retail (Company A), utilities (Company D), and hospitality (Company E). These companies operate in industries that sell services or products directly to consumers, so they use their internal data to measure company ratios and compare to prior year metrics and industry benchmarks. For example, Company D was already collecting data concerning risks affecting the organization as a part of the ERM process and to help succeed in the highly regulated industry. Thus, the existing data doubled as information for developing KRIs and for determining KRI thresholds. These three companies are also highly seasonal so historic internal data can be used to indicate when changes are approaching. The downside of using internal data is that it tends to be lagging in nature and may not provide insights on emerging risks.

Two of the five companies were more balanced in their mix of internal and external data. These two companies operate in the finance (Company B) and financial services insurance (Company C) industries. A core element to B and C's business models is buying and selling risks of others, therefore it is logical that many of their key performance measures (KPIs) lend themselves naturally to being reused as KRIs. Additionally, there are many benchmarks inherent to those industries such as London Interbank Offer Rate (LIBOR) that are both easily accessible and provide valuable information to the firms. As a result, macroeconomic data and other external data is valuable for creating KRIs. B and C operate in highly regulated industries dictating the need to handle high volumes of data and respond quickly to regulatory changes.

TYPES OF KRIs

There are two types of KRIs: leading and lagging. Leading KRIs provide indications that risks may be emerging. The closer the KRI is to the ultimate root cause of the risk event, the more likely the KRI will provide management time to proactively take action to respond to the risk event. Lagging KRIs monitor data retrospectively to identify changes in the patterns or trends within the data that will affect the risk. These types of indicators shed insights about risk events that have already affected the organization. The use of leading and lagging KRIs are specific to the company rather than the type of data used to develop the indicators. This observation is supported by comparing leading KRIs between A and E, both of which operate in highly seasonal industries and rely heavily on internal data as indicators of risk. However, Company A developed greater number of lagging KRIs than Company E. The use of more external data, as seen in B and C, did not result in more leading KRIs. Interestingly Company D, which relies heavily on internal data, has the same KRI mix as companies which use equal ratios of internal and external data.

Companies A and B repurposed KPIs into KRIs which led to the dominance of lagging over leading indicators within their KRI mix. The definition of a KPI is a quantifiable measure used to evaluate the success of an organization in meeting objectives for performance. The benefit of using KPIs is that these measures were already accepted and will increase buy-in. This is appropriate if they are related to key risks.

With regards to leading and lagging KRIs, a company is looking for trends, patterns, and interdependencies in the data. Whether the company uses internal or external data depends heavily on the industry the company operates within as well as other factors. Certain industries that are highly seasonal and consumer-centric may require the company to use more internal data. Companies operating in highly regulated industries that are affected by macroeconomic events need to supplement their internal information with external data. What matters the most in designing and implementing KRIs is that companies focus on risk indicators that can signal management to take action.

MONITORING & REPORTING OF KRIs

Monitoring KRIs is an important aspect of ensuring the effectiveness of these indicators. The risk information communicated to decision makers should be relevant, reliable, and timely. Using timely risk information allows the organizations to ensure their respective KRIs are impactful to decision makers. Companies stressed the importance of trends within risk information. Typically, the threshold numeric values are less important than the overall trend of the risk information. If risks trend in the wrong direction, then the risks are escalated up to senior management and executives. ERM leaders highlighted the unproductiveness of focusing on the numeric values that underlie each threshold because it led to discussions with executives that were too detail oriented. Thus, losing the enterprise level view desired.

Company policies dictate a formal annual update of KRIs with respect to thresholds. There are many channels to communicate the updates, such as dashboards, workshops, and memorandums. Companies B, C, and D communicate via dashboards that are available on a shared site. This means that a risk owner in a business unit would be able to pull information regarding the identified risks, the key risk indicators and their thresholds, the mitigation plan, and the trend of thresholds that is relevant to his duties.

Each company reports their KRIs quarterly to a risk committee or council. The Board of Directors from some of the companies receive these updates while some do not. In the quarterly reports, The Board of Directors receive high-level risk information that ties directly to strategic success. Company B relates their KRI reports to respective strategic pillars and any differences between the two would be brought to the attention of the risk council.

CHALLENGES TO THE IMPLEMENTATION OF KRIs

With every new process, there are challenges and obstacles which must be overcome. There are three key areas that the companies faced in implementing KRIs. These include: a lack of quantitative information, manual processes, and business buy-in.

Each challenge was present in at least one of the companies throughout the development of KRIs. There is a greater amount of qualitative data than quantitative data used within each KRI. The challenge with qualitative data is that it is inherently subjective and can be interpreted in different ways. In some settings, the lack of quantitative data has led to slower business buy-in. Failing to realize the opportunities effective KRIs can bring, risk owners may miss a valuable way to improve performance in meeting business objectives. Companies would like to use more quantitative data with the goal of eliminating some of the subjectivity that is inherent to KRIs.

Another challenge that companies face is the financial and time pressures of adopting emerging technologies. This has led to manual processes of data entry and collection being used when these processes may have the potential to be automated. This can allow risks to slip through the cracks or could delay response times. However, it is also important to note that all processes cannot be automated. For example, workshops and interviews allow risk owners to bring out important, qualitative context to the KRIs. To overcome this challenge, one of the companies will be introducing “playbooks” to provide more comprehensive risk information and improve communication of risk information across the organization.

THE FUTURE OF KRIs

All the participants identified areas in which their KRIs could improve. The identified areas are data analytics and automation, greater use of quantitative data, more transparency and better communication. Adding automation and data analytics will provide more timely information and greater insights into risks. Furthermore, companies are striving toward incorporating more quantitative data in order to make less subjective indicators. With reduced subjectivity, ERM leaders expect increased buy-in from all levels.

One company is working towards implementing a “playbook” that contains information on each KRI with the goal of distributing the information on the company’s dashboard. This is an automated process that will provide more robust information beyond just the KRI data. This includes but is not limited to the risk register, thresholds, the mitigation plan, and the trend of KRIs. The purpose of this is to increase communication of KRIs across the company and to help employees see the value of managing and tracking risks through the use of KRIs. Ultimately, the playbook enhance transparency and engage more employees in the risk management process. All companies saw the need to continuously build upon their KRIs in a transparent manner and are moving towards a similar direction.

Through improved data analytics and automation, communication, transparency, and a greater use of quantitative data, companies expect to continue to refine the metrics used to track risks and improve the speed at which they can respond to risks.

CONCLUSION

All the companies in this case study have a structured ERM processes in place that facilitated the development of KRIs and held the common goal of improving risk management capabilities. In each of the companies, we noted the importance of effective communication, readily available, credible data and buy-in from the business side of the organization. While not every organization had the initial implementation of KRIs go as smoothly as planned, companies were able to overcome challenges to establish meaningful measures of risk to provide warnings when action needs to be taken to address potential risk events.

Each company has taken a different path in the development, implementation, and refinement of its KRIs to fit its needs and capabilities. Their respective industries have influenced the way their KRIs were developed and used. This report and the detailed examples provided in the appendices should serve as a tool for other organizations that are looking to build out their ERM process by adding or improving KRIs.

APPENDICES

APPENDIX A

Company Overview

Company A is a specialty retailer with stores and branches across North America. Company A had revenue of more than \$9 billion in its most recent fiscal year.

ERM Overview

ERM Function

ERM is led by an employee with a dual role as both the Chief Audit Executive and Chief Risk Officer. The CRO reports on risk directly to the CEO. Currently, ERM consists of the CRO, one manager, an analyst and a data scientist. A Risk Advisory Council meets every four weeks to discuss risk and is comprised of C-Suite risk owners within the organization, including the CEO, EVP of HR, EVP of Supply Chain, Chief Procurement Officer, Chief Information Security Officer, Chief Technology Officer, Chief Audit Executive, VP of Safety and the EVP of General Counsel. The purpose of the Risk Advisory Council is to oversee risk in a holistic manner across the Company.

Strategy and Objective Setting

The ERM function within Company A is working to make strides in influencing the annual strategic and objective setting process within Company A. The company had previously used a consulting firm to assist in developing its strategy. The ERM function started with that strategy document and simplified it into 6 core pillars driving the company's success. Risks are presented to executives within the context of how they could adversely affect each of those core pillars.

Risk Identification

The company uses a combination of interviews, workshops and surveys to identify risks. 75 interviews from executives down to employees at manufacturing plants were conducted last year, and that number has grown to 200 this year. The interviews are open ended with risk themes utilized as topics of discussion. Risk workshops are also utilized for analyzing risk implications for joint ventures. Additionally, surveys are employed to aid in the risk identification process. Questions and risk themes explored within the workshops, surveys and interviews are updated on an ongoing basis as the ERM function gains a better understanding of risks over time.

Risk Assessment

The ERM function ranks risks over two measures, impact and likelihood, and is considering the addition of a third measure, residual risk, to take risk response measures into account. A five-point scale is used to rank each measure used. The ERM function uses visual tools such as heat maps to help aid executives in seeing their risk assessment process.

Risk Response

Risk responses are the responsibility of risk owners who are typically the executives in charge of each strategic pillar of Company A or the most senior official within the relevant department. The ERM function focuses on the most critical areas of risk where the company's risk tolerance has been exceeded which are indicated by a 'red KRI'. These are the risks that are most critical to the achievement of strategic objectives and may be escalated to the CEO for further discussion over how to best formulate an appropriate response.

Communication & Monitoring

Risks are communicated to the board using dashboards. Executives within the organization prefer to see a risk dashboard that shows the firm's risk positions at a high level. Workshops are utilized more often to incorporate employees who are out in the field managing the risks themselves. In general, the ERM function seeks to tailor their communications to risk owners and managers with their audience in mind. KRIs are also utilized within the monitoring process to ensure that each key risk is being managed sufficiently. Each KRI has three ranges associated with them: green, yellow, and red with red indicating that risk has exceeded tolerance levels. The thresholds used to determine the red, yellow, green ranges and mark escalation to higher levels are designed by risk owners with input from the chief risk officer or ERM manager.

Risk Culture & Leadership

Company A has a strong silo-based risk culture that is transitioning to a more enterprise level of risk culture. The firm displays a sense of pride in their craft and the fulfillment of their vision of providing auto parts and the requisite knowledge to fulfill their customer's needs. With the support of executives and top management like the CEO, the risk owners should continue to buy into ERM, and the function is expected to continue to mature.

Development of KRIs

Company A began developing its KRIs two years ago when it re-started its ERM process. KRIs were designed with input from risk owners through a risk interview with a focus on using KRIs to measure risk only where useful and relevant. Some categories where KRIs were particularly useful were safety and shipment accuracy. There were some areas that did not lend themselves to the use of KRIs, and so those types of risks did not have corresponding KRIs.

As the risk owners themselves set, communicate and monitor the KRIs on their own, they have a lot of ownership in the process thereby improving buy-in. Typically, risk owners report KRIs on a monthly basis. The ERM department, has pushed to automate the data collection process particularly where a risk owner has difficulty collecting the data to report KRIs on time. The ERM department recently hired a data analyst to accomplish this objective. Most of the information used to create the KRIs is internally generated and there is an even split between leading and lagging KRIs.

KRIs are communicated mostly between the risk owners and ERM team. At the board level this information is summarized within the risk dashboard to highlight trends. In addition, the board will receive information regarding "red" KRIs and the risk owner's response plan to get their KRI below the red threshold.

APPENDIX B

Company Overview

Company B is a finance subsidiary of a large firm in the technology industry. The parent has a global footprint that has a majority of its revenues of almost \$50 billion coming from the Americas and a market capitalization of approximately \$198 billion. The subsidiary provides financing solutions to the parent company's clients such that they are able to fund the innovative solutions provided by the parent company.

ERM Overview

ERM Function

A global risk manager leads the ERM function, reporting up to an executive with the dual role of SVP of Company B's parent and the president of Company B (the subsidiary). The SVP then reports to the CFO of Company B's parent who then reports to the CEO meaning there are three layers of reporting to the parent and two layers to the subsidiary. The company also has in place a Risk Council, that includes a senior executive of the parent company and Company B and support function (HR, IT, Legal, etc..) employees and focuses on how the risks within the subsidiary may affect the parent company. At one time, as ERM was initially be implemented there were up to four individuals on the ERM team but since that time there have been budgetary cuts that have reduced the team to one global risk manager. However, there are various rotation programs that provide periodic headcount and support to the global risk manager. The global risk manager consults directly with risk owners to help advise them on how best to manage their risks. She also has close ties with the internal audit department of the parent corporation.

Strategy & Objective Setting

The company operates within a proprietary framework which connects each risk theme to strategic objectives. The strategic planning group, which includes the senior leadership of Company B as well as, support function staff from the parent company (HR, IT, Legal, etc.) reviews the objectives the parent company has set for the subsidiary and the related risks that may impact the parent company annually as part of the planning cycle.

Risk Identification

A comprehensive risk register was developed upon the formation of Company B's ERM function 5 years prior. The comprehensive risk register gives more detail to the overall risk themes of Company B and an annual risk review sets the top 10 to 15 risks themes. Company B's detailed risk register is updated through an annual risk review in which risk owners participate. This year the global risk manager will send out a new risk survey to identify any new or changing risk themes that may have occurred since their initial survey. This survey will ask senior management within Company B to name 5 to 15 key risks that could impact the achievement of objectives.

Risk Assessment

After the survey results have been collected and summarized, the members of senior management of the parent company will meet to determine the key risks for which a response plan will be formulated. This is accomplished using a forced ranking system. Risks are then assessed by Company B's senior leadership using a 5-point scale for both impact and likelihood. Company B began building their risk assessment ideology 5 years ago and the ERM function's understanding of the risks has improved throughout this period. Recently the assessment was expanded to include velocity and directionality. Company A uses heat maps, scorecards and other visual aids as part of reporting for senior management.

Figure 3 describes Company B's 5 Point Scale:

Rank	Degree of Impact / Severity	Financial Impact, including Misstatements & Penalties or Fines	Customer Satisfaction Impact	Brand/ Reputation Impact	Negative media attention	Relationships with Governments / Regulators	Impact to business objectives / Disruption of operations	Internal impact [E.g., employee relations, recruiting, retention; policy changes, increased future costs,]
1	Minimal	Minimal (<=\$25M)	Low	Questioned, but easily recovered	Limited or no local	Heightened government & regulatory scrutiny	Little to no impact to any single objective or operation	Minimal internal impacts
2	Marginal	Marginal (>\$25M-\$50M)	Moderate	Some impact, limited to customer or market	Local	Warning Letters & Non-Standard Audits	Moderate impact to any single objective or operation	Moderate internal impacts
3	Critical	Critical (>\$50M-\$100M)	Significant	Significant impact w/ Loss of revenue	Extended local or regional	Deteriorated relationships. Hostile engagement.	Impact to multiple objectives; disruptions of isolated operations	Significant internal impacts
4	Severe	Severe (>\$100M-\$600M)	High	Significant Impacts, earnings impact	National	Loss of regional relationship w/ impact on objectives	Significant impact to multiple objectives; disruptions of isolated operations	High internal impacts
5	Catastrophic	Catastrophic (>\$600M) or Freezing of assets or bank accounts	Material	Catastrophic Impact – total loss of reputation & market share	Global	Damaged relationships; Criminal & Civil Charges; Lawsuits; License Suspension; Business Stoppage	Failure of multiple objectives or operations; continuing disruptions to material operations	Substantial, extended internal impacts

Figure 3: A 5-Point Scale

Visual heat map of Company B:

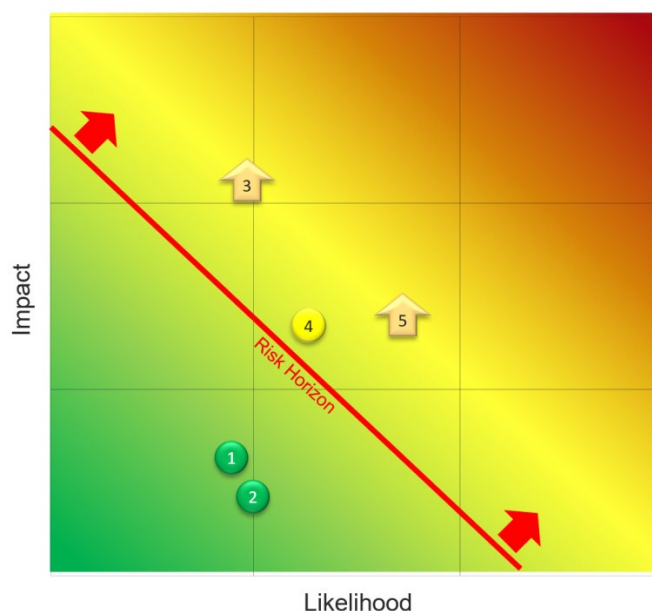


Figure 4: Heat Map

Risk Response

The global risk manager consults a RACI (Responsible, Accountable, Consulted, Informed) chart to determine the most appropriate position to assign as risk owner. The risk owners are typically the most senior manager within each department of Company B. Those owners will consult with the global risk manager to evaluate risk response plans. The global risk manager will meet with each of the 10-15 risk owners at least once a quarter, with additional meetings for risk owners of Company B's top risks, in order to assess the status of risks and response plans. The global risk manager highlights any of the top risks that require additional mitigation and works with the risk owners to ensure the appropriate focus is put on those mitigation plans.

Communication & Monitoring





The ERM team provides a risk report to the risk council quarterly. To the extent that a particular risk involves sensitive information, that information will only be provided to the risk owner of that particular risk. In addition to this, there is a transparent risk register that displays non-sensitive KRIs throughout the organization so that employees are aware of risk information relevant to their work.

Risk Culture & Leadership

Company B has a strong culture of accountability at all levels, and accountability for appropriate risk management is an integral part of that. In addition, there are numerous avenues for employees to escalate risk concerns: a risk mailer that goes directly to the global risk manager, an ethics hotline, and an escalation tool for employees to report potential control deficiencies to Internal Audit. There is a strong tone at the top within Company B that supports the continued maturation of the ERM process.

Development of KRIs

Company B began to design and implement its KRIs 3 years ago. As many of their risks were financial with measurable quantitative data, it made it easier to implement KRIs to further the understanding of risk within the firm. Additionally, KRIs create a clear expectation of where risks are targeted to be. The KRIs were initially designed by the risk owners (senior leaders within the organization) which aligns accountability for the implementation and success. The global risk manager compiles all of the KRIs for each risk theme and reports them through a risk dashboard as illustrated below:

Inherent Impact	Inherent Likelihood	Risk Score	Sized Annual Impact	Control Value	Residual Risk	
4	4	16	\$250M	\$187.5M	\$62.5M 	
Key Risk/Key Performance Indicators			Target	Actual	Q/Q Change	Directionality
GRC / Internal Audit Finding			0 Findings	 1 in FY18	None	Stable
Significant External/Market Events			None noted	 Several	Inc.	Increasing
DPP Incidents Reported			0 Mod / High / ≤2 Low	 1 Laptop Loss	+1	Increasing
DPP Implementation Status			On Track	 On track	None	Increasing
Current Risk Level						Increasing

Mitigation & Response Assessment	Residual Impact	Residual Likelihood	Residual Risk Score	% Mitigated	Risk Response Capability
	4	2	8	75%	Significant

Figure 5: Dashboard

The top portion describes the risk assessment for the high-level risk that was set on the basis of impact and likelihood. An overall risk score is calculated by multiplying impact and likelihood and the potential annual impact is estimated. Then the ability of Company B to mitigate the risk is assessed to find a control value that is netted against the annual impact to calculate the residual risk level. The KRIs used to track recent activity within the risk area are shown in the middle portion of the dashboard. The targets, which are set on an annual basis, describe the necessary performance needed to get a “green” assessment. The next column describes the actual performance which can be put into three different categories. “Green” indicated the KRI is being well managed, “yellow” is an in between point for the KRI and “red” triggers further action and escalation within the organization. The next two columns describe the change quarter over quarter and the directionality of the change in the KRI over the period.

The KRIs were developed by risk owners with the objective of tracking changes in the risk over time and predicting future risk events. Currently, around 25% of Company B’s KRI portfolio is made up of leading KRI indicators with the other 75% made up of lagging indicators. Within the financial industry there is a large amount of external data available to be tracked and Company B has used this information to set its KRIs where appropriate. Some more company specific risks such as talent risk are better tracked internally. The thresholds for the KRIs mentioned previously (green, yellow,

red) were developed by the risk owners as well. It is notable that there are typically at least three KRIs used to track each risk theme which allows for an evaluation of the KRIs at more of a portfolio level. Instead of a single KRI's movement triggering a response, typically it would take a couple within the same category to move in the same direction. As an example, if one KRI within counterparty risk moved from green to yellow it would not garner the same amount of attention as if two or three of the related KRIs moved in an adverse direction.

KRIs at Company B have provided an effective tracking and control mechanism. The participation of the risk owners in the development and reporting of the data making up the KRIs has been instrumental in ensuring buy in to the process. The ERM team continues to update the KRI reporting, using feedback from the risk owners to further improve the quality of risk information provided and to ensure the KRIs provide relevant information on the status of risks and response plans.

APPENDIX C

Company Overview

Company C is a business holding company whose subsidiaries provide supplemental health and life insurance in the United States and overseas. This insurance company offers provide a layer of financial protection against income and asset loss. Company C has revenue of almost \$22 billion in the most recent fiscal year.

ERM Overview

ERM Function

At Company C, there is an ERM team for each of its three subsidiaries. Overseeing each risk team is a risk committee, and all risk activities are aggregated with the global risk committee which acts as a governing body for the three subsidiaries. The CRO leads the ERM function and is also the chair of the global risk committee. The CRO reports to the Chief Financial Officer (CFO) and the Audit Committee (AC). Below the CRO, is the Global Risk Officer (GRO) who oversees eight personnel in the United States subsidiary. The GRO is responsible for corporate level activities that support each of the local functions such as Finance, Treasury and HR. The risk team in the US focuses on operational risks, as well as governance activities, such as developing policies and reporting risk information.

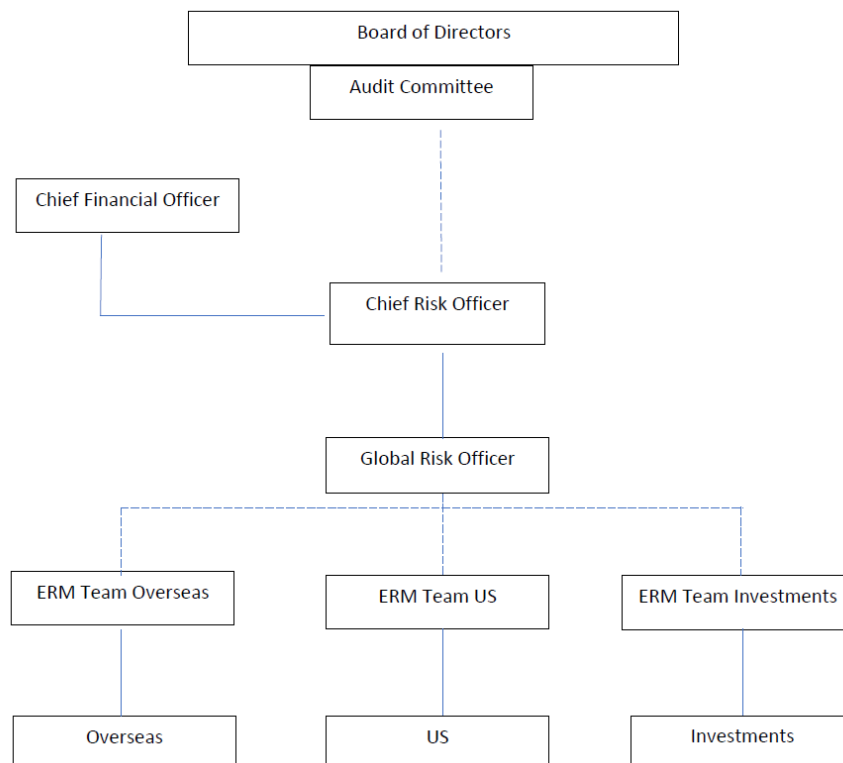


Figure 6: ERM Reporting Chart

Strategy & Objective Setting

At the Company, the objectives of the ERM team are closely linked to the strategy of the overall organization. Six months prior to the annual business planning meeting, senior management informs the ERM team of the Company's objectives and new initiatives for the upcoming fiscal year. When preparing for the business meeting, the Risk Management team conducts a risk assessment, looking at individual strategic initiatives of the organization. The risk assessment seeks to answer the following questions for each strategy:

- What risk does this mitigate?
- What risk is created? and
- What are the risks to effectively executing the strategy?

For example, automation is a new strategic initiative that creates opportunities and risks. Therefore, the ERM team would guide a discussion around how the risks related to automation may affect the company overall.

From the top down, the CRO is heavily involved with prioritizing the risks to be addressed. Company C recently changed its organization structure, breaking down their ERM departments into more local teams using risk liaisons, instead of being strictly, US and-overseas teams. Some of the risk team’s top ERM initiatives for the upcoming fiscal year include building and expanding their risk liaisons through the organization and creating more first line ownership of risks in their areas of responsibility. These are all efforts to build upon the foundation of promoting risk culture awareness.

Risk Identification & Risk Assessment

Company C’s risk identification process involves both top-down and bottom-up approaches. This process is conducted mostly through surveys and interviews beginning at the top of the organization. These interviews include 54 employees at the Senior VP level and above, along with 5 members of the Board of Directors. The questions are very strategic focused, specifically on the risks affecting corporate objectives. The goal is to gain a high-level view of the risks that could jeopardize the achievement of business objectives. The bottom-up approach uses Risk and Control self-Assessments (RCSA) to different process owners across the subsidiary with quarterly surveys to keep them updated. The objective of the frequent surveys is to track as much data as possible, including economic data. Economic and financial data are used to develop key risk indicators and key performance indicators

The ERM team assesses the identified risks by likelihood and impact, using a five-point scale for each. For likelihood, a one would be rare and a five would be frequent, which they consider happening ten or more times a year. Impact is also on the five-point scale with one being minor and five being extreme. These are both then displayed on a heat map and captured into the risk register which is shared more broadly within the organization.

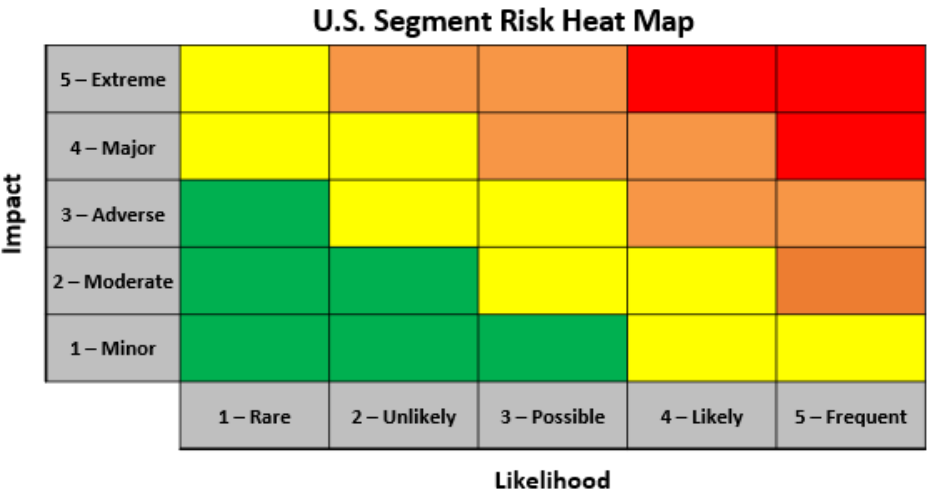


Figure 7: The five-point scale of Impact and Likelihood is used to create a risk heat map.

The process owners who participated in the survey are responsible for identifying any changes in controls, organization, or regulation. In addition, vulnerability and the speed of onset are also considered. Further follow-up and reassessment of risks are conducted on a quarterly basis, or when trigger events occur. Specific trigger events are identified using the following methods:

- Issues reported in internal or external audits and exams
- Breaches in Key Risk/Performance Indicators limits
- The introduction of new strategies or initiatives
- Material system changes
- Sox updates

When any of these events occur, a follow-up interview will be scheduled, and the risk management team will reassess the risk exposure and gather related information. Ultimately, it is the risk owner's responsibility to perform a sufficient review to determine whether a trigger event would require changes to the risk and control register.

Risk Response

The risk register lists risks and risk statements as well as the risk owners that have primary responsibility for each risk. Risk owners are those who own the process that creates the risk, and their responsibility includes executing mitigation plans. The risk owner's responsibilities include developing the risk responses and executing the mitigation plan. The top-level ERM team's role in risk response is to decide if the proposed mitigation plan is appropriate based on the Company's risk appetite. For significant exposures beyond the scope of the business unit, the ERM team is brought in to consult about how to respond and mitigate the risk event. The ERM team would also be responsible for issuing a standard statement regarding the event. Generally, the ERM's function is to review and challenge responses of the business units. Risk owners report risk updates monthly to the ERM team, and they are accountable for communicating to higher level ERM employees. In each subsidiary, department risk owners are assigned for specific duties, and are held responsible for risks affecting their vertical.

Communication & Monitoring

The U.S. segment of Company C uses a dashboard to connect risks to specific owners and to monitor the results of risk management activities. The updated dashboard is communicated to senior management and management committees monthly and to the board quarterly. The granularity of information increases as the individual's involvement in the design and implementation of risk mitigation processes increases. Risk owners report to the ERM team regarding the specific business unit-related risks and the risk management process monthly.

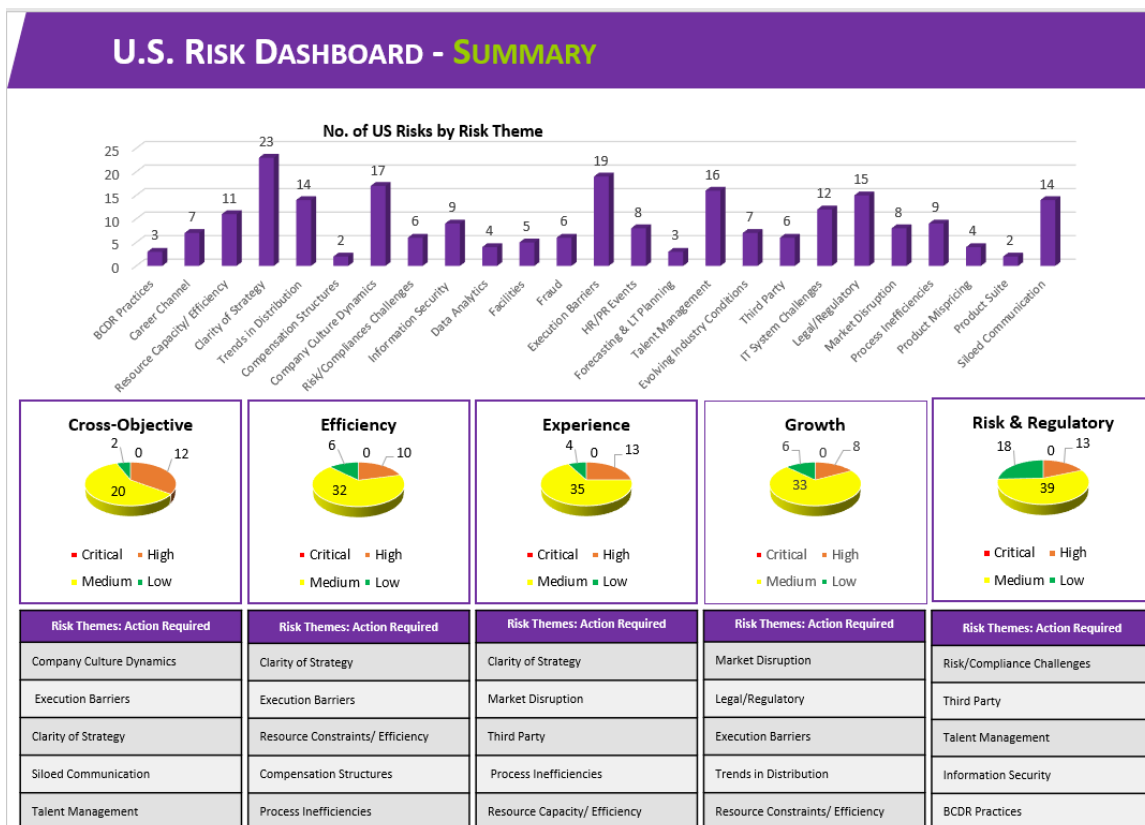


Figure 8: Dashboard

Risk Culture & Leadership

Senior management has been very supportive of the ERM process and this is demonstrated by welcoming the ERM team in the business planning process. There are channels in place for the reporting of risk concerns, including the use of department leaders as risk liaisons to be the “eyes” and “ears” of the ERM team. The Department leaders report risk information to the ERM team in order to provide for an enterprise view of risk. To further the risk culture and leadership, the ERM team is working to design and implement risk management training that would teach the risk owners how to develop their own risk controls and risk management plans independent of the ERM team. Currently, training is available for management on the risks, controls, and mitigation plans of the company. The new employee orientation also includes a segment on risk management.

The next step in promoting more effective risk management is linking incentives to risk ownership, such as including risk management in an employee’s performance evaluation and incentive plans. The goal for the risk culture is to have everyone consider themselves a risk manager within the organization, not just those with the “ERM” title.

Development of KRIs

Company C began developing KRIs 3-4 years ago as a monitoring tool to identify areas that need attention and focus for the mitigation of risks. Since the organization’s KRIs are developed using mostly external data, such as unemployment rates, the ERM team leads the KRI process. However, if a risk applies to a specific business unit and the KRIs can be measured using internal data, then the risk owners within the business unit are also involved in developing, implementing, and monitoring the KRIs.

During business planning, management determines Company C goals and objectives and the ERM team takes each goal and objective and determines the risk events that could prevent the achievement of these goals and objectives. The first step in developing the KRIs for trigger events is to determine how macroeconomic trends can impact results. For example, if Company C’s goal is to grow sales and sales are derived from employment relationships, then the labor population is used as a macroeconomic measure.

To determine how the macroeconomic trend may impact the company goal, the ERM team works with the Data Analytics team, which is part of the Finance Department, to look at trends against the business goal and to determine what can be measured. The Data Analytics team filters through thousands of macroeconomic metrics and data points per month to find external data that correlates with the business goal. Then the team would apply different conditions to see how macroeconomic trend impacts the goal. For the sales growth example, the Data Analytics team may create a large increase or decrease in the unemployment rate and determine the impact that has on sales growth. Then the team may look at a small increase or decrease in unemployment rate and how that impacts sales growth.

The second step is to identify the critical success factors for attaining the goal and the key assumptions related to the goal. To determine the answers, the ERM team will review historic internal data. For example, in order to grow sales, not only must the sales team continue to make a certain number of phone calls per day, but the number of sales agents making sales calls must also grow. By considering what is key to success and what assumptions are being made, the ERM team identifies that the recruiting function in Human Resources is one of the keys to the achievement of the sales goal. The ERM team uses historic data to forecast the number of recruits required to sustain the growth strategy, and the accuracy of the forecast is monitored using performance metrics.

Company C uses approximately the same number of external and internal metrics to design its KRIs. The ERM team found that internal data is easier to obtain and measure than external data. Risk owners of the relevant business units can also help to design and develop KRIs. As a result of using more performance metrics, there are currently more lagging than leading KRIs. The leading KRIs versus lagging KRIs as a percentage of total KRIs is thirty and seventy percent, respectively.

The third step is to define the approximate levels for each metric that would indicate the relative level of risk to achieving the goals. The risk levels are indicated by four colors: green, yellow, orange, and red. Green denotes no risk

events preventing the achievement of the company goal, and each color subsequent to green indicates an increased risk of not achieving the company goal.

Risk Level	Description for Business Risks	Description for Project Execution Risks
Critical Risk	Escalate Mitigation: Immediately enhance and/or implement controls to prevent, detect, correct, and/or escalate the risk to Executive/Board Attention	Escalate Mitigation: Immediately enhance and/or implement controls to prevent, detect, correct, and/or escalate the risk to Senior Management / Committee Attention
High Risk	Enhance Mitigation: Enhance current control environment and execute mitigation plan to prevent, detect, correct, and/or escalate risk to Senior Management / Committee Attention	Enhance Mitigation: Enhance current control environment and execute mitigation plan to prevent, detect, correct, and/or escalate risk to Program or Business Unit Sponsor
Medium Risk	Monitor and Mitigate as Needed: Monitor controls on frequent basis and strengthen them as needed and escalate risk to Management Attention	Monitor and Mitigate as Needed: Monitor controls on frequent basis and strengthen them as needed and escalate risk to the Project Management Team
Low Risk	Monitor and Improve Control Efficiency: Monitor controls on an infrequent basis – Redeploy dedicated resources to more critical risks	Monitor and Improve Control Efficiency: Monitor controls on an infrequent basis – Redeploy dedicated resources to more critical risks

Figure 9: The four colors used to indicate risk levels.

Company C uses KRIs to indicate trends of how well the company is doing at meeting its goals instead of setting specific numbers as thresholds. Therefore, the thresholds are set through discussions with the risk owners. To develop the thresholds, the ERM team member and the risk owner look at what is “good”, “bad”, or “in the middle” and design mitigation plans based on the impact and likelihood of the risk event. For example, if recruiting is not at a rate that can sustain sales growth, this risk event would be indicated by an orange or red color to express the urgency of picking up the recruiting rate.

Monitoring & Reporting KRIs

The last step in the KRI process is to communicate the KRIs which will involve compiling the data from an internal Excel spreadsheet, and presenting it on a dashboard that links the identified risks to broad goals. Risk owners and business leaders are able to view more detailed dashboard information. This means a risk owner in a business unit would have all the information regarding the identified risks, the key risk indicators, the mitigation plan, and the trend. Senior management will receive a higher-level view with less detailed KRI information. Currently, the KRIs are monitored and updated annually at the end of Company C’s business planning cycle.

US Risk Dashboard: Growth Summary




Risk Theme	Key Drivers	Key Mitigations	Trend
Trends in Distribution	<ul style="list-style-type: none"> Missed growth opportunities due to a culture focused on products instead of distribution Ineffective go-to-market approach in the US business due to a shifting distribution model industry-wide towards the broker and direct-to-consumer channels 	<ul style="list-style-type: none"> US Distribution is focused on shaping the marketplace with a variety of products and services while leveraging our strong brand to remain competitive in the changing external environment. Strengthening the value of existing products by adding Value Added Services Expanding use of Alternative Distribution Channels (Partnerships & Direct to Consumer) 	
Resource Capacity/ Efficiency	<ul style="list-style-type: none"> Not executing BAU activities and/or other strategic projects due to resource constraints & resource dependency issues Poor adoption of change from the sales force 	<ul style="list-style-type: none"> GRM provides monthly Resource Capacity Risk Assessment updates to proactively assess potential impacts of resource capacity constraints to the execution of key initiatives and BAU activities. The recent Transformation Assessment in response to resource capacity constraints resulted in pausing some planned activities. Further, the US Organizational Readiness and US Operation Risk Committees serve to identify and mitigate initiative execution risks and resource conflicts 	
Execution Barriers	<ul style="list-style-type: none"> Lack of organizational swiftness regarding innovative efforts due to excessive governance and slow approval decisions Inadequate IT infrastructure for future state needs 	<ul style="list-style-type: none"> Currently reevaluating the US IT Roadmap to deliver replacement capabilities that effectively move us from old systems onto new platforms Executing the Vision 2020 roadmap and replacing the old systems with updated modern systems 	

Figure 10: The trend of the arrows reflects an increased or decreased risk of achieving the company’s objectives.

Challenges & Improvements

The ERM team recognizes that an effective ERM process is “part art, part science.” To facilitate increasing the “part science,” the ERM team is introducing more quantitative data in designing the KRIs. The challenge to obtaining quantitative data is that the data is open to individual interpretation. To overcome these challenges and to increase “buy-in,” the ERM team continuously updates the KRIs instead of waiting to perform an annual evaluation of KRI accuracy. This continuous effort helps to ensure that KRIs are a relevant focal point of risk management discussions.

APPENDIX D

Company Overview

Company D is a holding company whose subsidiaries are in the regulated utility industry. Company D has a market capitalization of \$24 billion and reported revenue of approximately \$12 billion.

ERM Overview

ERM Function

The ERM process at Company D is maintained through interplay between the Board, the ERM department, the ERM Steering Committee, and the ERM Corporate Risk Committee. The ERM process at Company D is overseen by the Audit Committee of the Board of Directors. The ERM Steering Committee also assists with ERM program oversight and risk oversight. The ERM function at Company D is facilitated by an ERM department that includes the ERM director, who reports to the CFO and a four member team, who jointly facilitate the ERM program. The ERM director is responsible for the deployment of the ERM process throughout the organization. The ERM department receives assistance and input from employees throughout the organization such as Oversight Officers at the Corporate Senior VP Level, Risk Officers at the Organizational VP level and Responsible Team Members (RTMs) at the director level who act as risk owners. The ERM process at Company D includes the ERM Corporate Risk Committee that consists of general managers and directors (RTMs) that are generally closer to the operations. This committee meets quarterly to receive updates on Corporate risks from RTMs and to evaluate risks that may be elevated to the corporate level. 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 quarterly to discuss current trends, ERM process changes, and fluctuations in risks. The entire ERM process at Company D directly involves about 300 employees out of 14,000 total employees at COM Company D.

Strategy & Objective Setting

While the ERM process at Company D has limited involvement with strategy setting for the entity, risk considerations play an important role in the annual budgeting process. There is explicit consideration of the resources needed to adequately mitigate to the most material risks the organization faces. In addition, the department with responsibility for strategic planning considers the key risks that shape this highly regulated industry.

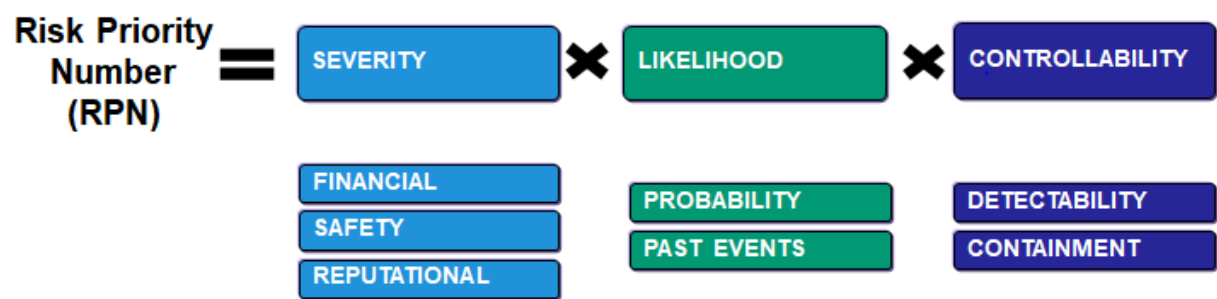
Risk Identification & Assessment

Risk identification at Company D uses both a top down approach as well as a bottom up approach. Risks are identified from the top down by the ERM Steering Committee, which scans the landscape for higher-level emerging risks, benchmarking with industry peers along the way. From the bottom Company D sources risks from surveys, brainstorming meetings, research, publications, and media. Company D issues surveys to its employees to identify new risks and Company D conducts brainstorming sessions with tailored questions to identify risks. Once a risk is identified it can go into one of two categories or both categories if applicable: Tier 1 Corporate risks and Tier 2 Departmental risks. Corporate risks are risks that are significantly material to the Company. Departmental risks are deemed material to the individual department. It is important to note that this ERM Overview is only covering the ERM process as it relates to Corporate risks. This was done because the case study above covers the KRIs for Company D at the corporate level and to keep the process as easy to understand as possible. The company maintains approximately 14 Corporate risks whose nature is not limited to operational but also includes strategic, financial, safety and compliance risks. Once a risk has been identified it is assigned to a Risk Officer who delegates the risk to RTMs that are responsible for performing detailed risk assessments and implementing mitigation strategies. Corporate risks receive multiple RTMs due to the high level of materiality the risks present and the multiple areas that it could affect.

Identified and assigned risks are assessed and prioritized by the RTMs. Information is collected from RTMs throughout the year and documented to keep current information on the risk which also serves as a baseline of information on the risk for the entire process. While the assessment process provides insights on the risks it is not a quantitative process. Quantitative amounts are assigned to risks based upon the risk's severity, likelihood and controllability factors. 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 factor is scored on a scale of 2, 4, 6, 8, or 10. Then, the severity, likelihood and controllability scores are multiplied together to generate a Risk Priority Number (RPN), as shown in the figure below. In order to qualify as a Corporate risk a risk must be assessed to have a severity score ≥ 8, likelihood score ≥ 4, and controllability score ≥ 6. The risk’s RPN determines how it is managed and reported to the Board with a higher RPN indicating a higher risk.

Figure 11



Risk Response

Company D focuses their mitigation strategies to prevent, detect, respond, and/or transfer risks. Appropriate mitigation strategies are developed based on the risk assessment process that yields a RPN. Root cause analyses are fundamental to eliciting a proper risk response, as the identification of the sources of risks leads to more effective mitigation strategy. 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. In this case the Company can develop a bow tie analysis that begins with focusing on consequences to ensure that an effective mitigation strategy is still being used. Accordingly, an informed decision can be made as to whether risk responses will center on causes or consequences.

Communication & Monitoring

The bow-tie has facilitated creation of key risk indicators (KRIs) based on identified risk root causes and consequences. A KRI dashboard has also been formed to monitor risk trends and risk exposure. The Company thinks of KRIs as a stoplight, with the colors of the light signaling whether when the risk exposure is at an unacceptable, escalating or acceptable level. A risk’s causes, consequences, mitigation strategy, and KRIs are linked, allowing for senior management to monitor the risk exposure and if necessary implement 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 that could include prevention, detection, response, and/or transfer. KRIs and bow-tie analyses indicate whether additional mitigation efforts are necessary. KRIs and bow-tie analyses also provide quantitative, data-driven monitoring over risks. This quantitative data is combined with qualitative input solicited from SMEs to determine a proper risk assessment, mitigation strategy, and, if appropriate, corrective action. Together, these data-driven and subjective perspectives merge as part of monitoring practices.

Corporate risks are given a quarterly review of their risk assessments and mitigation strategies; this process also produces a KRI performance report. Annually, the ERM director prepares a standard single page report for each Corporate risk that is combined into an ERM Report to the Board to keep them informed of Company D’s most material risks. The standard reports on each risk go through various layers of approvals beginning with the RTMs, up to the VP, and through the Senior VP before being finalized for the CEO’s review. The ERM Report to the Board is uploaded to a SharePoint and made accessible to ERM’s key stakeholders. Additionally, at least once every three years the RTMs for each Corporate risk is presented to the Board providing a deep dive into their assigned risk.

Figure 12 shows the risk assessment guidance document to walk risk owners through their annual or quarterly assessment.

2019 Corporate Risk Assessment Factors

The following is a guide to assess risk scores (A, B, C), velocity (D), and outlook (E). Consider the most probable worst-case scenario.

A) Severity Factor							
Estimate the severity of the event using the point scale and use the highest score of the three perspectives.							
Factor		Reputation		Public/Employee Safety		Financial	
Insignificant	2	No Effect	Media: No known media attention Compliance: Not reportable to regulator Corporate Image: No impact to image with key stakeholders ¹	No Injury	No injury	up to \$3M	Cost of event resulting from fines, penalties, lost revenues, and/or other expenditures, net insurance.
Minor	4	Minor	Media: Local media attention, quickly remedied Compliance: Reportable to regulator, no follow-up required Corporate Image: Short-term, strains relationships, but does not impact trust with key stakeholders ¹	Minor	Minor injuries, not requiring medical treatment (excluding first aid)	\$3 to \$15M	
Moderate	6	Moderate	Media: Local long-term media attention Compliance: Reportable to regulator with immediate correction to be implemented Corporate Image: Short-term, strains relationships and diminishes trust with key stakeholders ¹	Moderate	Out-patient medical treatment required	\$15 to \$50M	
Severe	8	Severe	Media: National short-term media coverage Compliance: Reportable to regulator requiring major project for corrective action Corporate Image: Short-term, significantly strains relationships and strongly diminishes trust with key stakeholders ¹	Severe	Hospitalization required	\$50 to \$250M	
Catastrophic	10	Catastrophic	Media: National long-term media coverage Compliance: Significant prosecution, fines, litigation, etc. Corporate Image: Long term, severed relationships and loss of trust with key stakeholders ¹	Fatality	Fatality	>\$250M	

B) Likelihood Factor			C) Controllability Factor		
Estimate the probability of the event occurring based on past experience, industry experience and current conditions.			Determine the likelihood that existing detections and response mechanisms would predict or mitigate the consequences of the event.		
Factor		Description	Factor		Description
Rarely	2	One incident in 10 or more years	Almost Certain	2	Excellent detection and very high degree of influence over the consequences of the event
Unlikely	4	One incident between 5 and 10 years	High Probability	4	Highly predictable detection and high degree of influence over the consequences of the event
Likely	6	One incident between 3 and 5 years	Moderate	6	Limited detection and some influence over the consequences of the risk
Very Likely	8	One incident between 1 and 2 years	Low	8	Very limited detection and low degree of influence over the consequences of the risk
Certain	10	Greater than one incident per year	Impossible	10	No ability to detect or influence the consequences of the event

D) Risk Outlook		E) Risk Velocity	
Based on internal and external factors, determine the direction of the risk in the next three to five years.		Time that elapses between the occurrence of the event, as defined, and the point at which the Company first feels its effects.	
Increasing	Threat is expected to increase or the overall environment is becoming more risky	High	Rapid onset, instantaneous
Decreasing	Threat is expected to decrease or the overall environment is becoming less risky	Medium	Slow onset, occurs in a matter of several months
Stable	Threat expected to stay static or overall environment will remain stable	Low	Very slow onset, occurs in a year or more

Notes

¹ - Key stakeholders include regulators, customers, political officials, investors, etc.

Figure 12

Figure 13 is single page report framework for the Corporate Risks.

Example Regulation		
Definition:		
Management Discussion:		
Risk Outlook: Increasing/Decreasing Description	Financial Resources Addressing Risk:	
	Mitigation Strategy: Description	Prevent <input type="checkbox"/>
Risk Consequences: Description		Detect <input type="checkbox"/>
		Respond <input type="checkbox"/>
		Transfer <input type="checkbox"/>

Figure 13

Risk Culture & Leadership

ERM is integrated within many facets of Company D, one of which being the budgeting process. A risk factor is considered by Company D when determining funds to be allocated to various projects and departments, speaking to ERM's involvement. Additionally, ERM engages in annual meetings attended by top officers and company departments to review ERM processes at Company D. After these meetings, departments make presentations before the CEO and President, reviewing the major points from their previous meetings and requesting funding for projects. The ERM department is also intertwined with Strategic Planning, Auditing, Emergency Preparedness, Compliance and Corporate Affairs to help ensure the business leverages ERM's information to help drive and inform business decisions, priorities, and allocation of resources.

Development of KRIs

The Company began developing KRIs over 5 years ago as the ERM function matured and became more integrated with the operations of the Company. The goal was to develop metrics that would provide signals to alert management to increasing risk exposures or trends that could either present opportunities or threaten the achievement of corporate goals. Company relied on data driven analysis to support its conclusions throughout this process, and organized its thinking by using a technique referred to as a "bowtie analysis" to identify the metrics that would be most helpful in predicting risk events.

The bowtie analysis (see illustration below) starts with the risk at the "knot" of the tie which represents the risk event itself. The analysis can then be created through describing the events or circumstances that may cause the risk event to occur or the consequences or effects of the risk event occurring. If the bowtie is developed using causes, once they have been identified the analysis then identifies preventive measures that could be implemented. At this point there could be an evaluation of the actual preventive measures that the organization has in place to determine whether additional measures should be put in place. The analysis then moves to the right to look at the potential consequences that would result after the risk event happens, and the plans the organization either has or should have in place to minimize the negative effects of the risk. The root causes that have been identified in the box on the upper left of the

bowtie analysis become the focus of the development of the KRI with the goal being to identify metrics that track those root causes. If the bowtie is developed using consequences of the risk event, the process is mirrored to identify what plans the Company has in place to minimize the damage from the risk event. The analysis then moves to the left to look at what could cause the risk event to occur and what the Company is doing to prevent it from occurring. The consequences that have been identified in the box on the upper right of the bowtie analysis become the focus of the development of the KRI with the goal being to identify metrics that track those consequences. By being able to develop a bowtie analysis based upon causes or consequences the Company has more flexibility into how the risks can be thought of in the risk assessment stage.

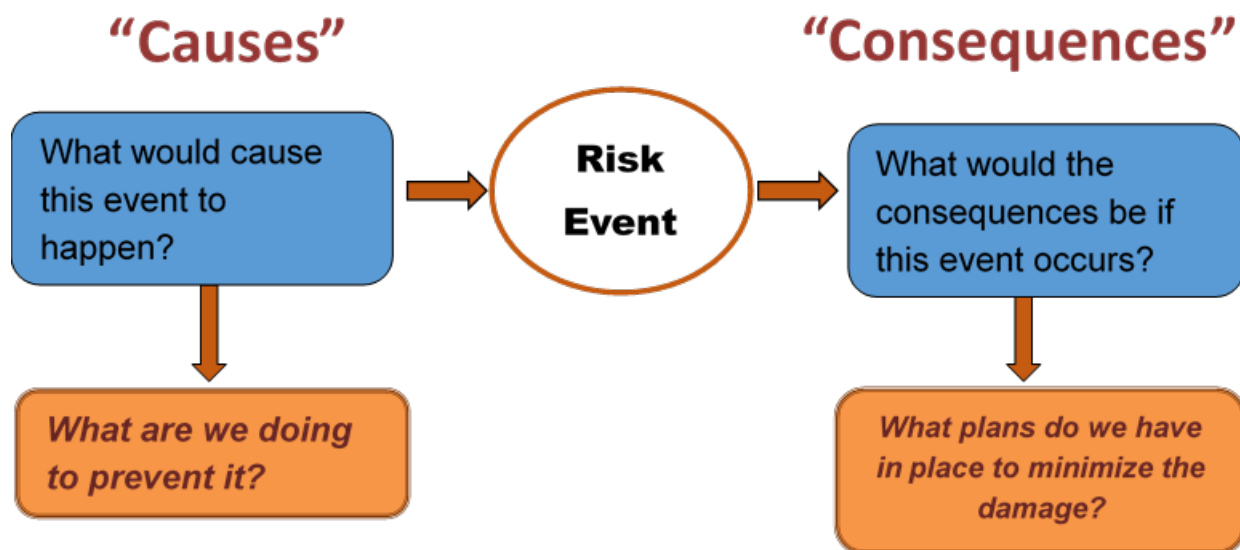


Figure 14: Bowtie Analysis

After the bowtie has been completed the appropriate responses can be developed that address the consequence or cause. The driving force behind this initiative for the Company is the desire to proactively address both root causes and consequences of a risk event. While a singular KRI cannot apply to both causes and consequences, the Company would like to have KRIs of both types for a singular risk rather than focusing solely on causes or consequences.

At the Company, the bowtie analysis is completed through a series of workshops organized by the ERM director. Each workshop included the RTM as well as subject matter experts from each department. These subject matter experts usually worked within the organization at the department level, but also had experience dealing with issues affecting the Company at the enterprise level. The ERM director included subject matter experts to help create a setting which encouraged debate, but limited the number of subject matter experts to between 6 and 8 in order to keep the discussion focused. The ERM director believed that with the right combination of people and the appropriate level of preparation he could create the kind of atmosphere that would drive the creativity needed to identify the relevant root causes of the major corporate risks of the organization. Each workshop would last two to four hours, and depending upon the complexity of the risk the number of workshops needed to vet each risk could range from two to four. The ERM director found that these workshops had to be broken down into a series of meetings in order to be more effective due to the exhaustive nature of the approach.

Each RTM is asked to pull together information on their risk in advance of the meeting in order to optimize time in the workshop. Once the causes or consequences are identified, subject matter experts help the group by providing relevant information. With that information in hand, the group can look more closely at potential causes or consequences and discuss differences of, all of which sharpens the group's focus. The members then work together to decode the indicators of the identified risks by discussing what combination of events would lead to the occurrence of each risk. Then, they seek to understand the issues which cause the event to occur or the consequences from the event. This

requires the involvement of subject matter experts who are well versed in the fields relating to each identified risk. Then the Company reviews mitigation strategies that are either in place or need to be developed for each cause.

The following chart illustrates the analysis of regulatory risk at the Company. The risk is defined as a regulatory body issues rate or other orders or new or modified regulations that have a material operational or other impact. The bowtie analysis begins by identifying any causes for this risk. The causes identified are the price of energy commodities rising, poor economic conditions, the typical customers bill increasing, safety thresholds that are breached, or a poor relationship with the particular regulatory body. Then, the potential consequences of the risk are identified. These consequences are rate disallowances or reductions, measures for austerity, a negative financial impact on the organization, and significant reputational damage.

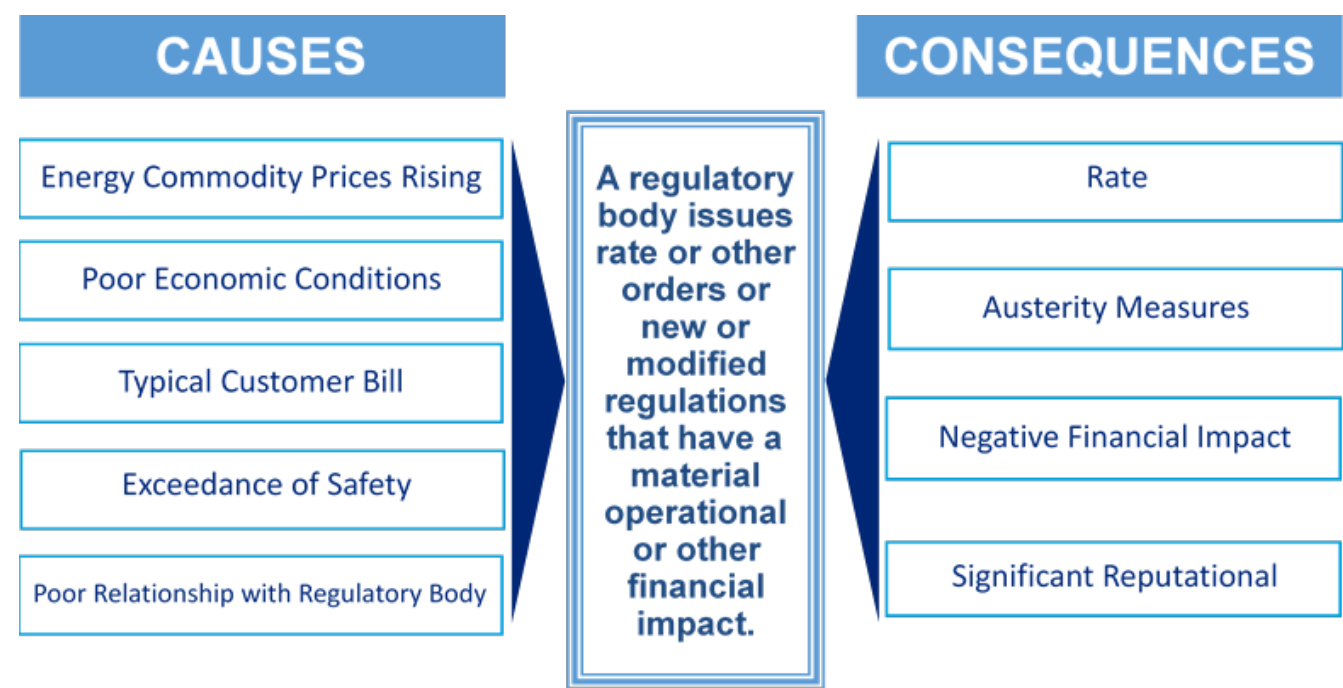


Figure 15

The causes identified in the bowtie analysis are then evaluated to identify predictive metrics that could be used as KRIs. The RTMs were asked to define one key data point which could be linked to each of the identified causes, and then gather three years of historical data on that data point. Data can be sourced both internally and externally; however internal data is heavily relied upon given the mature nature of the Company’s monitoring activities. The ERM director at the Company found that the key component of this process is to develop KRIs that look at metrics in different ways. There should be at least one or two KRIs for each risk that go beyond pure numbers. The reasoning behind this strategy is that some KRIs are effective predictors but are not easily measured by numbers. These KRIs must be utilized in some way in order to effectively monitor the risk. The subject matter experts help to develop metrics which are then used to monitor each KRI. The process was made easier because the data for most risks was already being monitored either within the Company or externally. In the example given, “state economic conditions” is a metric that is measured externally by many independent sources, and this allows the RTM a means to gather metrics for this KRI.

The ERM director then worked with the RTMs to set thresholds for each KRI. This often involved the finance department as their knowledge of risk management was critical. After viewing the historical information, thresholds were determined by the RTMs by selecting the data points where the KRI had moved into an area of more or less influence upon the risk. The KRI thresholds are formally reviewed annually by the RTMs. Going forward the Company is implementing a formal escalation and review process for KRI activities. Included within the review process is oversight officer approval of KRI thresholds set by RTMs. This approval action is being put into place to increase transparency in

the process and ensure updated information is being used. The thresholds are represented by three colors: red, yellow, and green. The green threshold represents an area where the KRI being measured is at an acceptable level, and no action is necessary in regard to the risk it represents. In the example given, the green threshold for “energy commodity prices” would be anytime the monthly ratio is below 0.9. When the KRI’s data point moves into the yellow threshold, it has moved into a cautionary area. This means that the KRI is communicating to the RTM to look closer into the risk that the KRI represents. In the example “energy commodity prices”, this would be when the monthly ratio moves in between 0.9 and 1. When the KRI’s data point moves into the red threshold, RTM must consider action in regard to the mitigation strategies in place for that particular risk. For “energy commodity prices”, the red threshold represents when the monthly ratio moves above 1.

Next, the subject matter experts determine a weight for each KRI, and this is a scale of high, medium, or low. The process of determining the weighting is subjective based on the subject matter experts’ opinion of the influence of that factor on the likelihood of the risk occurring. The weighting of KRIs brings a more specific approach to monitoring the risk associated with them. Each KRI represents a trigger event which has a proportional impact on the likelihood of the identified risk occurring. For example, if a KRI like “energy commodity prices” with a high weighting, moves above the red threshold, it would make regulatory risk more likely to occur than if a KRI like “state regulatory success rate for prior 12 months” with a low weighting moved above the red threshold.

The result of this process for regulatory risk at the Company is illustrated in the Figure 16 below:

Description	Measure	Goal	Thresholds	Weighting
Energy commodity prices	# - Ratio / monthly	N/A	Red: $x \geq 1$ Yellow: $0.9 < x < 1$ Green: $x \leq 0.9$	High
Typical customer bill	Ratio of 12 -month average to 5 yr. average / monthly	N/A	R: $x \geq 1$ Y: $0.9 < x < 1$ G: $x \leq 0.9$	High
State economic conditions	Unemployment % rate / monthly	N/A	R: $x \geq 9$ Y: $7 < x < 9$ G: $x \leq 7$	Medium
Exceedance of performance thresholds	# per every 3 years / monthly	N/A	R: $x \geq 4$ Y: $1 \leq x \leq 3$ G: $x = 0$	Medium
State regulatory success rate for prior 12 months	% of success rate / monthly	70%	R: $< 25\%$ Y: $25-70\%$ G: $\geq 70\%$	Low

Figure 16

Figure 17 shows the graphs of the metrics for three of the KRIs used for regulatory risk:

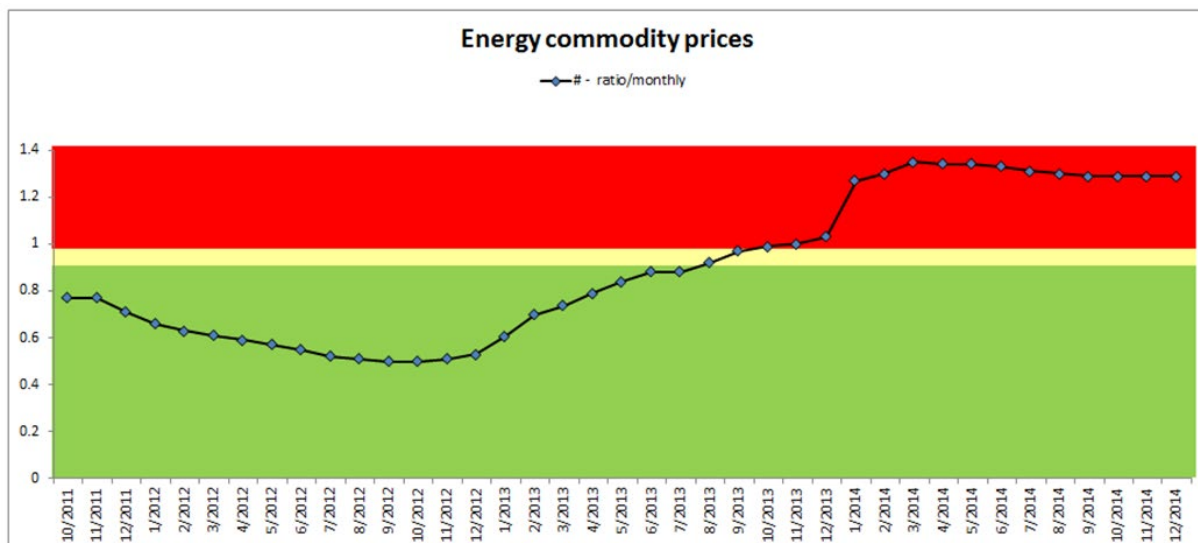


Figure 17

For energy commodity prices, a ratio showing the percentage change from the previous month is used and thresholds are set. Red is set at greater than 1, yellow between 0.9 and 1, and green at anything below 0.9 and the weight given is high. For example, a change in energy commodity prices above 1% would be reflected in the red area.

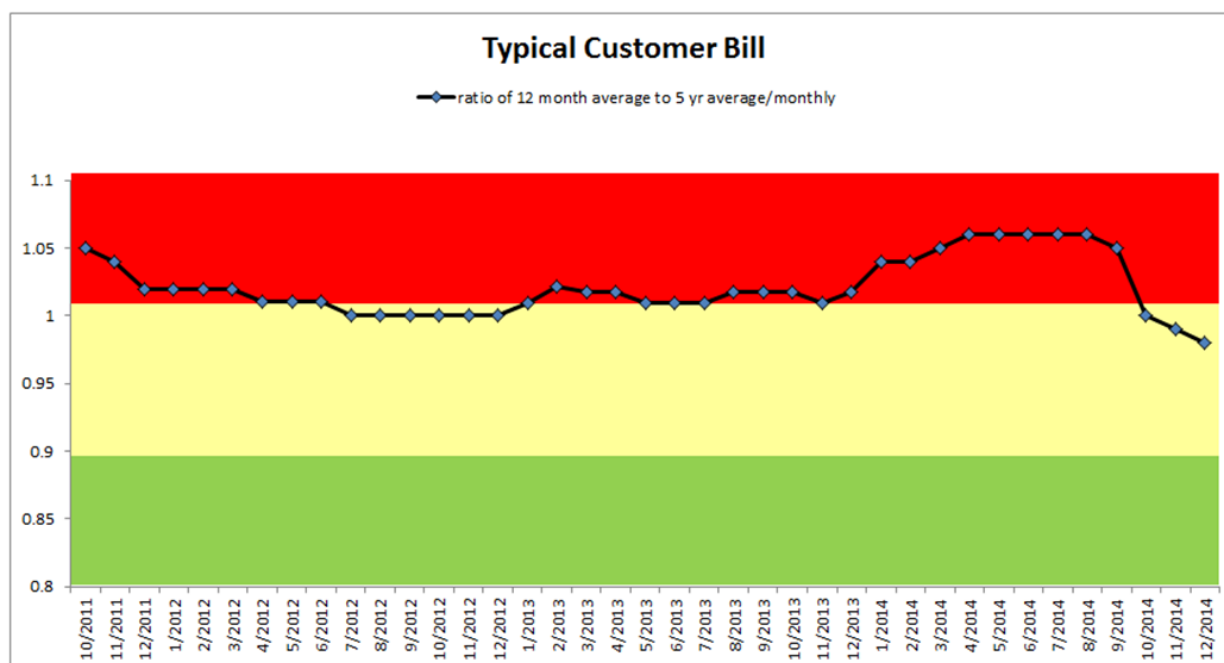


Figure 18

The typical customer bill is tracked using a ratio of the average customer bill for the last 12 months compared to the average customer bill over the last 5 years. Thresholds are set for red at greater than 1 (12 month average has exceeded the 5 year average), yellow between 0.9 and 1 (12 month average is 90-100% of the 5 year average, and green at anything below 0.9 (12 month average is below the 5 year average by 10% or more). When compiling the overall status of Regulatory risk, the weight given to customer bills is high. The example shows that the 12 month average for the

typical customer bill is between 95 and 100% of the 5 year average at December 2014. While this is still in the yellow or caution area, the trend is positive.

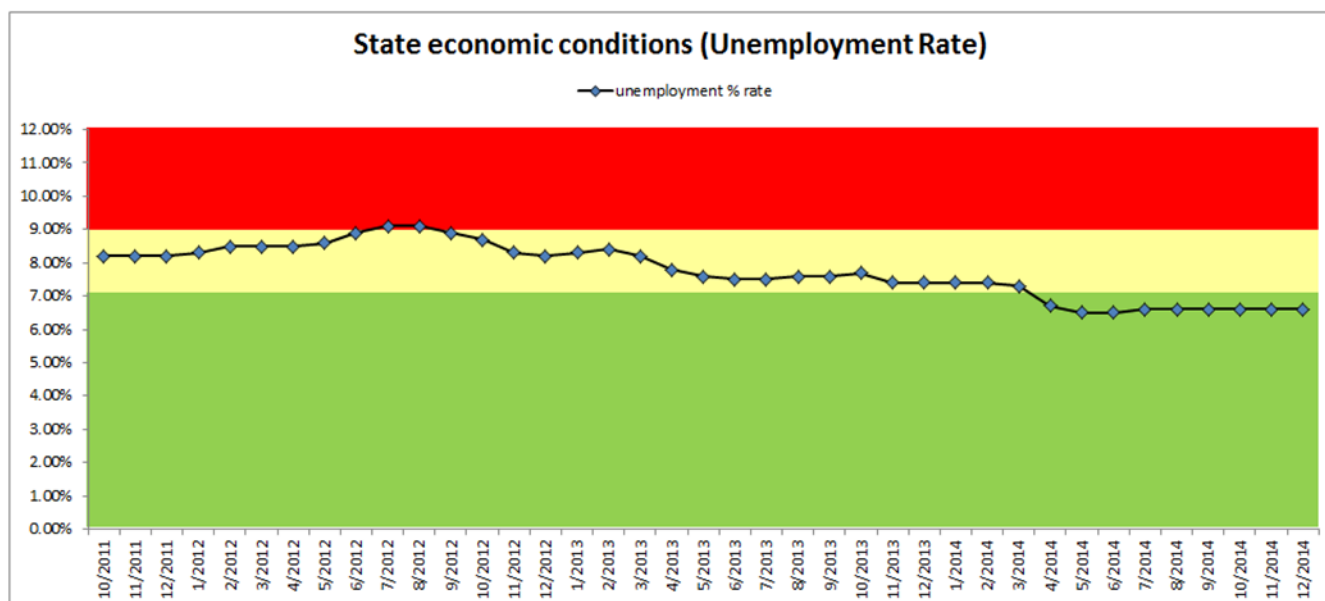


Figure 19

State economic conditions are measured using the unemployment rate data taken from independent sources which monitor the economy of state. The red threshold is set at 9% which represents the unemployment rate, and when the KRI metric exceeds this threshold the RTM is now aware that the likelihood of the occurrence of this risk has increased. The yellow threshold is set between 7% and 9%, and this communicates to the RTM to monitor this risk closely because it is inside the cautionary area. The threshold for green is set for below 7%, and this communicates to the RTM that the unemployment rate for the state is less than 7% and the KRI data point is within the acceptable range. When compiling the overall risk assessment, unemployment is assigned a medium weight in determining overall regulatory risk.

The final two KRIs that are used for regulatory risk are performance threshold exceedance which relates to reliability metrics and the regulatory success rates which relates to regulatory decisions. These KRIs are measured and monitored like the three KRIs discussed above.

Monitoring & Reporting KRIs

After the development process has been completed, each RTM has the responsibility of monitoring the risks belonging to the department in which he or she works. The monitoring process involves a continuous gathering of metrics relating to each KRI. While gathering these metrics, the RTM must keep an open line of communication with the senior officer of the department in regards to how the risk is being managed. This dialogue includes mitigation strategies that are being implemented, the status of the mitigation strategies, and any plans for developing new mitigation strategies. Going forward the Company is implementing an annual review of the KRI's that will require a sign off from the responsible team member and oversight officers on the KRI process. The purpose of implementing this authorization agreement is to provide more oversight of the KRI process, increase accountability for KRI activities, and to further ensure that mitigation activities continue to be correct and accurate.

At the end of each quarter, the ERM director works with each RTM individually and compiles a KRI summary dashboard for the risk in that RTM's department. A comprehensive KRI report is prepared by compiling the KRI summary dashboards for all the 14 Corporate risks facing the Company. This report is uploaded to a SharePoint that is accessible to ERM key stakeholders, and provides a high level overview of each risk and the current status of the KRIs in relation to the risk. The report includes a summary dashboard that communicates the risk assessment, definition of the risk,

KRI mitigation activities, as well as the current trend and a key headline. Each Corporate risk has its own scorecard to display the information.

The KRI summary dashboard contains metrics comparing the current quarter measurements against the previous quarter as well as the previous years' matching quarter. The metrics show the changes between the current quarter and the other two quarters in order to give the senior officers an idea of the direction in which the KRI is heading. The dashboard is organized as a chart that lists the RTM, the risk, and each KRI along the top portion. Measurements for the three quarters are listed underneath each KRI for easy reference. The dashboard also includes a KRI overall color assessment, which is taken from the RTM's KRI graph for that particular KRI. Underneath each KRI summary dashboard, a short narrative is provided that describes any changes in the colors of the KRIs. This summary describes the change, what specifically occurred to cause the change, and whether this change was an improvement or a setback. This narrative gives the senior officer enough information to be able to have a discussion with the RTM in regards to any actions which may need to be taken to address the status of the KRI. These discussions occur regularly between the RTM and the senior officer, so if there is any unexpected change the narrative will be descriptive enough to inform the senior officer of why it occurred.

The most significant initiative the Company has for the future of its KRI process is the internal publication of its KRI "playbook". This playbook will cover the entire KRI process from start to finish and contain all of the information that pertains to the risk each KRI tracks including risk description, assessment, and mitigation actions. This is being implemented to assist the Company in making the KRI process as continuous as possible so the most up to date and accurate data is being used.

The ERM director at the Company understands that some KRIs are within the organization's control and some are not. The reason for employing KRIs is to help determine whether the mitigation strategies being employed by each department for managing risks are effective. The ERM director does not own the risks being managed, but they do own the process of managing the risk. This is essential to the success of the process, and the team continuously monitors the effectiveness of KRIs. They do this by meeting quarterly with the corporate risk committee and challenging the data being presented to them by the RTMs from each department.

Summary

The Company effectively uses Key Risk Indicators to monitor the major 14 Corporate risks that face the organization. The process started by identifying the causes or consequences to these major risks by using a bowtie analysis. The ERM director then employed an efficient process that enables the RTMs from each department to apply measurable metrics to each of these KRIs. Each KRI was then monitored quarterly using graphs to display those metrics in an easy to follow way. The role of the ERM function with regards to KRIs at the Company is that they are facilitators of this process, while it is the responsibility of the RTMs to manage the risks in their respective departments. The reporting process actively engages senior executives by providing key information on KRIs which trigger a review and may lead to potential change to current mitigation strategies. The Company has a robust ERM function in place, and the development, monitoring, and reporting of KRIs has given them a valuable tool in managing their key corporate risks. Nonetheless, the Company will continue to seek ways to improve its ERM program and the KRI process. The recent implementation of an annual formal review of trigger points to increase KRI transparency and the current development of "playbooks" for each KRI are two examples of continuous improvement efforts.

APPENDIX E

Company Overview

Company E is in the highly competitive hospitality market but has seen major success in the past decade and is now seen as an industry leader. Company E is a global brand, with over 5000 properties in 109 countries. Their goal in 2019 is to continue to expand into new markets, with 2,500 properties in the pipeline. The majority of Company E's revenue is earned in the US and Europe.

ERM Overview

ERM Function



Figure 20

Company E, along with a few others, has moved away from the standard ERM process and moved towards an advisory process. They believe the risk function is not charged with managing risk but rather is a facilitator of the process. The idea was to change the standard perspective of managing risk, and instead act as more of a consulting group, whereby the function serves to facilitate and advise on risk management practices that risk owners can use in their specific department. The ERA function is made up of the Head of Enterprise Risk Advisory. There are three lines between the Head of ERA and the CEO. The process involves the Head of ERA reporting to the Chief Risk Officer then the CFO and then CEO. Company E's aim for 2019 is to expand this team and bring in individuals who understand the ERM function as well as Company E's business model. While it can be helpful to hire from within the company, Company E believed it was even more important to have someone who understood the importance of having a well-structured risk management process and the opportunities this can bring to an organization.

The CFO is very involved with the ERA process. He is briefed every six- eight weeks to keep him updated. He attends Executive committee meetings one to two times per year. He will also meet with the audit committee four times and the board once per year. The meeting with the board will discuss the risk at a high level.

Typically, the CEO will receive the risk reports at the closure of the risk assessment phase, which occurs once a year during the second quarter. The closure of the risk assessment phase typically ends with the CRO and Head of Enterprise Risk Advisory meeting with the full Executive Committee and the CEO to discuss the details of each risk and how they are intertwined. This meeting involves the final risk determination presented to the Audit committee of the board in

Q2 (Note: Company E's Board decided to delegate responsibilities for risk oversight to the Audit Committee, they have not established a distinct Risk Committee at the board level). The risk assessment results are also communicated to the Board of Directors during the third quarter. General updates on risk office activities are provided each quarter to the Audit Committee.

Strategy & Objective Setting

In recent years, Company E's top risks have moved from being more execution and compliance related to strategic. This change has allowed the activities of the ERA function to be more in line with the business and its strategic objectives. This in turn has improved the shareholders outlook as they are invested in the value of the company. This has enabled the risk assessment process to be more efficient and accurate.

Company E has linked Enterprise Risk Analysis to their strategy through the use of multiple functional strategy teams. The strategic teams meet every 90 days to remain connected to the initiatives and objectives. The strategic plans are updated every three years and the company is in the process of establishing sophisticated ERA materials to use throughout the planning process.

Company E has adopted an annual MBO (Management by Objectives) process based upon the objectives that are part of a long-term strategic plan. The Human Resources team is responsible for developing the MBO alongside the business functions and leaders. This team includes the Executive Vice Presidents, Senior Vice Presidents, Vice Presidents, all corporate team members and General Managers. In 2019 the ERA team partnered with HR to ensure all of the risks identified by the ERA process are covered by the leadership MBO's. During 2019 the HR and ERA teams are evolving the process of MBO development with the aim of gaining further engagement from executive staff. They look to accomplish this by providing them with more real time knowledge on the organization's top risks, through Key Risk and Performance Indicator analysis which will further demonstrate the importance of the ERA function and the opportunities effective risk management can present.

Risk Identification & Assessment

Throughout the risk identification and assessment process, Company E relies heavily on surveys. This allows them to reach more people and gain a greater understanding of the risks in the first phase of the process. The survey breaks the risks up into thirteen versions by function. The six different categories applied to risk in the universe include: strategic, external, financial, people, process and technology. These surveys are distributed to 200-250 employees, with a separate survey on each risk category being distributed to the subject matter experts. The survey process begins with the Head of Enterprise Risk Advisory and is distributed throughout the organization. The employees who receive the surveys are part of the Company E leadership group. This means they are at a management level within their specific department, with 88% being Vice Presidents and above. The other 12% include the SME's, Managers of Departments, and Senior Directors. At the end of the survey, each respondent is able to rate those risks that have not been identified in the survey. The survey rates the risks on impact, likelihood and capability using a 5-point scale.

An example of this is the IT department would receive the survey focused on those risks related to information technology including cyber security and system downtime. In addition to the surveys, the ERA team will gather additional risk information to understand area's with potential blind spots. This risk identification process occurs on an annual basis. Prior to the move towards ERA, they used to give all 200 employees the same survey. However, they realized this was problematic as throughout the initial stage everyone was identifying different key risks and many risks suffered from collapsing to the mean due to lack of knowledge of survey respondents (i.e. everything was a 3).

Once the surveys have been collected, the Chief Risk Officer and ERA team will go through a deep dive process with 60 employees who are subject matter experts. The top risks are identified and discussed with the experts in the appropriate field. The risks are then rated again based on the three dimensions, with impact and likelihood averaged. They then measure these averages against capability in order to develop the "GAP" scale, which is the area between capability and exposure. If the "GAP" shows capability is lower than exposure, it becomes a top risk.

The third phase of the risk identification process involves a discussion between the Enterprise Risk Committee. This is a non-executive meeting that meets and reviews the results. From there the ERA team will determine whether the risk should be elevated or demoted. All of this occurs prior to the Executive Committee meeting discussed above.

The risks are rated individually, as previous attempts to measure as a group were overly complicated. They were heavily reliant on the ERA team to define connections. They realized this was not a good determination of how the business side of the company connected risk. This is something leadership is hoping to implement in the long run as they see value in it. The mechanics of the process have been the stumbling block. While Company E uses spider diagrams to show how risks are connected, the ERA function has found conversation with management to be the best approach to connect risks with other areas of the business.



Figure 21

The survey process has been helpful for Company E as it allows them to identify risks proactively and monitor those risks that could evolve over the next three years. The Chief Risk Officer travels to various regions around the world to discuss the risks with the management team located in those regions.

In 2019 Company E is implementing a new model. This model looks to give more risk ownership at the executive level. The ERA team will develop the KRIs to assist those leaders in their evaluation of exposure. Currently most evaluations are based on qualitative information from their teams and then the survey. Company E have Executives who debate the accuracy of the survey results in evaluating the risk. The ERA team hopes the approved KRIs provide a more objective venue to look at how risk is moving. A leader whose team is conveying positive movement qualitatively, might see something different in these KRIs and be able to challenge their teams accordingly. The hope with this new model is that the natural behavior of thinking we assign resources to the risk and then “think” exposure is reduced will be mitigated.

We can use the risk of cyber security to present this. By employing a CISO (Chief Information Security Officer) we have not automatically mitigated the risk. The officer must do something to make the risk exposure change. It is noted that Company E survey, and qualitative process often attempts to give credit to hiring and or allocation of funds. However, the process should not end here.

This new model will look to increase communication and transparency in Company E. It will set up a two-way street so risk information by the way of KRIs flows both up and down within the organizational hierarchy. This will ultimately drive greater alignment.

Risk Response

Company E assigns responsibility for developing risk response to risk owners and leaders throughout the business but assigns articulating risk responses to risk experts / liaisons and Enterprise Risk Committee members. This group includes 60 people, with 25 being on the audit committee, who is actively involved in discussion throughout the first quarter of the year. This approach allows them to determine any events that could lead to a risk in the future. While documenting the risk the ERA team challenges the liaisons, Risk Owners and Committee members to identify how the risk could hurt the company. The ERA team notices that as a company we should not only focus on what “are” we doing but also what we “should” be doing to mitigate risk in the future. This will further increase forward visibility and help respond to the risk. This group may change from year to year in order to bring in fresh ideas and minimize the potential for blind spots. This group of experts includes management level experts in particular fields as well as certain executives, including the CFO, who would have the enterprise view. The company promotes the discussion of risks at all levels of the company and believes this has created a healthy culture.

The role of the ERA function is to challenge management to develop responses to risks that are not overly generic at the enterprise level. The CRO oversees enterprise and operational risk and must evaluate new risks to determine their impact, and whether the risk is significant enough to involve senior management. This is based on the CRO assessment of the residual effects of the risk. For some risks the risk function has established partnerships e.g. with legal compliance, to perform ad hoc risk assessments. An example of these type of risk assessments is country-based risk assessment given some of the company’s prospective business growth is forecast to be taking place in less politically stable environments as well as in areas where there is a heightened risk of terrorism or conflict. The Risk Officers are looked to by leadership to perform objectives throughout the risk assessment process. Throughout the risk response they will challenge leaderships articulated responses. The ERA team is better equipped to assess whether risks have been mitigated or not.

Communication & Monitoring

Company E uses dashboards, workshops and memorandums to communicate risk information throughout the organization. At the business level they determine the dimensions of the risk by answering three questions: what it is, why do we care, and what are we going to do about it. These three questions are answered in a written document, which is then published to executives. This distribution is very limited and may not be given to all executives. At higher levels of management, Company E is focusing on trends and grouping those trends into distinct categories based on the risk. This categorization was preferred by the executive leadership as it gives them a broad view to assess the impact the risk trend may have on the company. Company E has begun using workshops to identify new risks because the workshops allow the ERA function to reach more employees across various departments.

Due to confidentiality concerns, Company E limits distribution of its risk reports with most of the information being delivered up the chain of command. The Executives of each department are the only ones who get the report containing their department’s gap analysis. Communication begins with the risk expert and continues up the ladder to the Executive and C-Suite members. Twice a year the Enterprise Risk Committee meets to discuss whether the risk assessment and response is satisfactory and how to combat any residual effects, following that the Chief Risk Officer, Head of Risk Advisory and the CFO brief the Executive team on risk.

Company E noticed over several years of conducting survey-based risk assessment that the responses are prone to sentiment influences that don’t correlate to actual risk movements. As a result, in 2018, a decision was made to reconsider Key Risk Indicators. KRI adoption was attempted for some risks earlier in the ERM program’s evolution with limited success. In late 2018, the ERA team started to develop a methodology and approach for KRIs. Thus far they have identified a somewhat significant overlap with 1KPIs and are evaluating the best approach to adopt.

Risk Culture & Leadership

“Making [Company E] different and innovative in the ERM space is what will make [Company E] successful in the future.” (CEO)

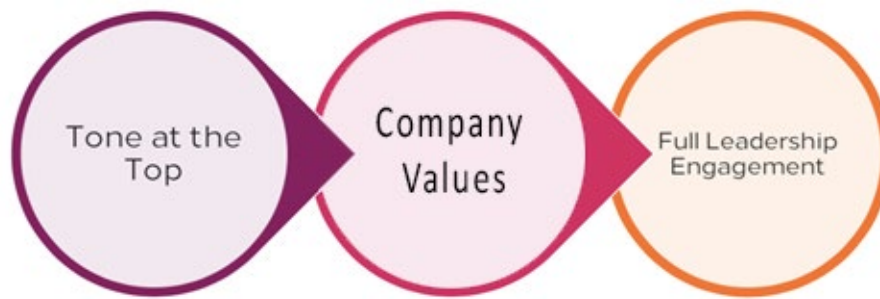


Figure 22

Company E has a great risk culture, which starts with a strong tone at the top. This is shown by their implementation of an ERM process back in 2010, and then the establishment of the Risk Office in 2014. This saw them become a leader with regards to risk management in the hospitality industry. They attribute much of their success to their ability to foresee risk events and have the correct controls in place to mitigate risks. They have consistently challenged management to be involved with the process, and the results have allowed them to be an industry leader.

Development of KRIs

The company began designing KRIs in 2015, with the goal to develop metrics and provide signals to alert management to increasing risk exposure or trends that could negatively impact the strategic objectives. Company E began to develop KRIs, while the Enterprise Risk Analysis process was in the early phases of development. In this initial attempt, KRIs were not seen as a feasible option. The business side was more focused on the growth and profitability of Company E and wanted to see a greater implementation of KPIs, instead.

However, in 2018, they began to see a need for both leading and lagging KRIs given the volatility of survey results in order to help with risk quantification.

The ERA team developed KRIs, by collaborating with senior leadership and management. This was seen as a three-step process:

- Initial metrics determined based on the information given by the business leaders and management
- Interviews between the ERA team and business leaders to determine the effectiveness of the metric's previously determined by the ERA team
- ERA team establish the measurements for the KRIs

Department leaders and management would be asked to provide KRI suggestions on top risks that had the greatest impact on their area of expertise. They were then asked the reasons behind why they felt these risks appeared and some of the challenges they had to monitoring the specific risks. The ERA team, based on the information that had been provided to them, would begin to develop their first metrics that will represent the challenges to these risks. These metrics include both qualitative and quantitative values. Once this had been accomplished, the ERA team would meet with the department leaders and management who had provided them with the initial risk information. They would meet to discuss their thoughts and reactions to the metric provided. The ERA team would tend to have three to five sets of conversations before they moved onto the next step. Throughout these conversations, the ERA team made it a priority to make sure the department leaders understood the metrics and the reasons behind why they had been used. The tracking of the metrics was also discussed to determine any changes that had to be made and whether a more efficient and effective value could be used. In the initial meetings it was normal that three to five key business leaders would meet as a group. However, as they got further through the process, they would turn to one on one interviews.

Once these initial meetings were concluded and the potential metrics had been agreed upon, thresholds of the KRIs needed to be determined. Company E intends to implement thresholds through the use of brainstorming activities between the ERA team and leaders of the departments.

Company E uses spreadsheets to help facilitate their KRI process. They begin with the initial risk and the reasons why this is a risk. From there, the ERA team will discuss the various options with upper level management. The ERA team will provide potential metrics that will be used to measure the risk.

After the initial KRI process has been completed pending on their upcoming threshold implementation, Company E will determine the risk mitigation direction.

Risk Mitigation Direction

The Risk Mitigation direction (increasing or decreasing) will be produced after conversations by the ERA team with the risk owners and department managers. If this data is quantifiable, the ERA team will produce a report. This report is then analyzed further by the ERA team to pick up on themes mentioned by individual risk owners. If this isn't possible, the ERA team will spend more time interviewing and obtaining an understanding of the current risk environment as well as looking at external data.

Thresholds

	Lower Threshold (%)	Target Threshold (%)	Upper Threshold (%)
KRI (1)	50%	95%	100%

Above is an example of what the threshold would look like in the spreadsheet. These thresholds will be determined by the ERA team based off numerous discussions with upper- management and executives. The lower thresholds are based on what Company E's risk appetite would be, without it affecting the strategy. The upper threshold is what "utopia" looks like. This is the number or percentage Company E is aiming for and would be a "best case scenario" situation. From there they will determine the target number. This is what the risk owners should be striving for. If the number goes below the target, further discussions will be had with the head of that department and the ERA team, who will determine how to reach these targets. The risk is not seen as unacceptable until it falls below the lower threshold.

Monitoring & Reporting of KRIs

Once the KRI's have been developed, they will be distributed to Risk Owners and Enterprise Risk Committee members. The department leadership team is comprised of risk owners with the primary responsibility of monitoring risks. The risk owners will in turn distribute the findings to employees within their respective departments as appropriate. Throughout the quarter, there will be a direct line of communication between the risk owners (department leaders) and the ERA team.

The ERA team continues to update their spreadsheet, including new metrics and the amount of residual risk at the end of each quarter. Once calculated, the trend of risk movement quarter over quarter is analyzed. This trend will then be placed into three categories, increasing, stay the same and decreasing. Based on these metrics, the ERA team will go onto update their "effective exposure." The "effective exposure" is measured by likelihood and impact of the risk at its current level. From this, the ERA team will determine their risk exposure in comparison to where it was at the beginning of the year.

The monitoring process is ongoing and continues throughout the year. The thresholds function as appetite statements by each metric used as triggers are constantly evaluated and updated throughout the year. If a new piece of information could affect a KRI, the threshold will be changed to account for this. The ERA team expects that as mitigations against a risk get better, the area of exposure will be easier to track. The parameter by which Company E determines exposure and manages the risk will get more precise and hopefully narrow.

The ERA team communicates their KRIs using excel documents to those at the risk owner level. As they begin to present their findings to upper management, the ERA team will begin to introduce dashboards. The ERA team decided to use this style of spreadsheet as it is simplistic and easy to understand. They noted that to have an effective KRI program, the risks and controls must be easily understood by the key risk owners (department leaders).

Company E is hopeful as the ERM system matures it will become more digitized. They are looking to establish a risk analysis portal that would allow each department to log in and see their risk trend on a quarterly basis. This will make it easier for department leaders to track their risk in comparison with the metrics and thresholds set forth by the ERA team.

Challenges & Improvements

Company E found that despite the culture being very risk based, the topic of KRIs often created tension in the organization. The difficulties were due to misunderstandings between the ERA team and risk owners about their roles and difficulties with buy-in. Based off of feedback from upper management, Company E decided to adopt a mix of KRI's and KPIs in the coming year. Management believes KPIs are less subjective and will be better accepted throughout the organization. KPIs will allow the business leaders to focus on the growth of the company.

The business side of Company E consistently identifies lagging KRIs to use within models. For an effective KRI process, it is important to see a mixture of both leading and lagging KRIs. The business unit leaders deferred to the ERA team to develop leading KRIs. The development of the leading indicators has proved to be problematic for some risks as the ERA team lacks an appropriate level of knowledge compared to the risk owners in managing the risk. The development of thresholds can be contentious within Company E and attempting to assign monetary values with the risks identified was difficult. The ERA team saw this as necessary so that the business leaders could efficiently manage the capital assigned to risk mitigation.

Conversely, the ERA team at Company E sees the importance of using KRIs within their risk management process. The use of KPIs is a great tool but they are typically focused on past events. KRIs on the other hand help an organization by providing leading information to mitigate future exposure. Company E's ERA team is continuously attempting to find new ways to implement KRIs into their business strategy. The CEO and much of his core leadership team realize the importance of effective risk management as a long term strategic tool that Company E can use to their advantage, however some leaders remain more reticent on the potential value of a systematic, process and metric based approach, versus the more informal processes they use today. The ERA team believe this level of focus on risk will eventually be present at all levels of the company. The ERA team will continue to work hard finding new quantitative data that can be used effectively by upper level management.

ABOUT THE AUTHORS

NC State ERM Practicum Team Biographies



Truth Chou is a graduate student in the Master of Accounting program at NC State University with a concentration in Enterprise Risk Management. She is originally from Vancouver, Canada and earned her Bachelor of Arts degree in Linguistics. Her love for languages, culture, and people have led her to travel all over the world as a volunteer with not-for-profit organizations. Upon graduation, Truth will begin her career in Risk Advisory Services.



Jordan Fulbright completed a BS in Accounting from UNC Asheville. While attending, Jordan also played varsity baseball and was the spokesperson for the team on the Student Athlete Advisory Committee. Jordan enjoys being outdoors and exploring new adventures. Jordan will be working for Johnson Lambert on the audit side after completing the Masters of Accounting program and earning his CPA licensure.



Campbell Irwin completed a BS in Accounting with a concentration in Financial Analysis at NC State and continued his education in NC State's MAC program. As part of the ERM concentration, he plans to further develop professional presentation skills and to better understand risk assessment within firms. After graduation, Campbell intends to work as an auditor.



Michael Patch is an international graduate student from London, England in the Master of Accounting program at NC State. He completed his undergraduate degree at Catawba College, with a BS in Economics and Finance, and a minor in Accounting and French. While at Catawba, Michael played on the tennis team, competing in the NCAA Southern Atlantic Conference. Upon graduation, Michael will begin his career in audit while earning his CPA license.

