ENTERPRISE RISK MANAGEMENT: WHY THE ETHICS AND COMPLIANCE FUNCTION ADDS VALUE

The Ethics Resource Center and The ERC Fellows Risk Assessment Working Group

John Dienhart, Ph.D.
Frank Shrontz Chair for Business Ethics
Seattle University

ERC
ETHICS
RESOURCE
CENTER

THE ERC FELLOWS RESEARCH SERIES 2010

CONTRIBUTING AUTHORS/EDITORS:

JACLYN KUPCHA, Researcher
ALLISON PENDELL JONES, Former ERC Fellows Program Director
Ethics Resource Center

RYAN HICKS, Graduate Assistant
Seattle University

ERC FELLOWS RISK ASSESSMENT WORKING GROUP
of the Ethics Resource Center

Working Group Chair: **JOHN DIENHART**, Frank Shrontz Chair for Business Ethics
Seattle University

THE ERC FELLOWS are a select group of corporate, government, non-profit and educational senior-level leaders who share an expertise and strong practical interest in the field of organizational ethics. The purpose of the ERC Fellows Program is to identify, examine and further understand the critical organizational ethics questions challenging organizations today. The ERC Fellows pledge to accomplish their mission through open dialogue around cutting edge ethics issues, collaborative research, communications, and work products with practical applications.

Founded in 1922, the **ETHICS RESOURCE CENTER (ERC)** is America's oldest non-profit organization devoted to the advancement of high ethical standards and practices in public and private institutions. For more than 85 years, ERC has been a resource for public and private institutions committed to a strong ethical culture. ERC's expertise also informs the public dialogue on ethics and ethical behavior. ERC researchers analyze current and emerging issues and produce new ideas and benchmarks that matter – for the public trust.

For more information about ERC, please visit **WWW.ETHICS.ORG**.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The aftermath of the frauds and bankruptcies at Enron and WorldCom led to a rapid increase in regulatory requirements for businesses. The Sarbanes-Oxley Act (SOX), the revised 2004 Federal Sentencing Guidelines for Organizations (FSGO), and the SEC and other regulatory agencies all require risk management in a variety of areas. In response, companies began to embrace an approach called enterprise risk management (ERM), which assesses risk in a comprehensive, company-wide manner. ERM gathers information on risk together to create a larger picture, which allows organizations to uncover risks that affect multiple departments and address them together. Furthermore, consolidating risk reporting enables companies to create standards and more efficient processes for recognizing and mitigating risk. This is a departure from the less cost-effective "silo" approach used by businesses, which leaves separate departments and business segments to deal individually with their own specific risks. The report argues that ERM is not only effective in reducing risks and preventing loss, but it can also discover new business opportunities and promote efficiency and growth.

Effective Enterprise Risk Management:

- Provides – through its emphasis on overall risk appetite – a more objective basis for resource allocation, therefore improving capital efficiency and return on equity.
- Stabilizes earnings and reduces stock-price volatility.
- Offers the tools to make more profitable, risk-adjusted investment decisions.
- Improves transparency to stakeholders, therefore reducing regulatory scrutiny, litigation expenses, costs of access to equity capital, and the rate of return on incurred debt.

According to the report, the involvement of Ethics and Compliance in ERM is essential to its success. There are several reasons why E&C can add value to an organization's ERM process, and thus add value to the organization. First, E&C has extensive cross-functional experience from years of helping their organizations implement FSGO requirements, as well as regulations from SOX and the SEC. This skill set transfers seamlessly to dealing with new requirements and puts E&C in a good position to ensure that these regulations are accounted for by the ERM. Secondly, E&C has been doing risk management as part of their regular duties for quite some time. This experience will prove valuable in guiding management to make wise decisions regarding risk cases going forward. Lastly, E&C has a keen understanding of how culture influences individual behavior in businesses. This knowledge will be valuable as the focus on culture has intensified since the 2004 FSGO emphasized the need for organizations to promote a culture of ethics and compliance.

The paper then explores nine case studies of companies or organizations that have either successfully implemented ERM or are in the process of doing so. The specific details of each case are not that significant, but there are some important commonalities worth mentioning. In all cases, the company decided to undertake ERM either in response to their own internal

experience with fraud or as a reaction to the increase in regulatory requirements. Generally, these companies would create a committee consisting of management, E&C, and other relevant staff to oversee ERM. These committees would then create standardized procedures for employees to report risk and to consolidate data. Through regular meetings, the committees discuss current risk concerns and look for solutions. They also look for patterns in risk issues so they can set up structures to prevent problems before they occur instead of reacting once something happens. These companies all took slightly different approaches based on their unique culture, values, and business objectives, but in all the cases, E&C played an integral role in the success of ERM.

The report concludes that ERM is an effective way for organizations to both prevent loss and promote growth. Also, for the reasons mentioned above, E&C needs to work closely with a company's leadership for ERM to be successful. If implemented properly, E&C will add value to ERM, and ERM will add value to the organization.

INTRODUCTION

The 2002 Sarbanes–Oxley Act (SOX), the 2004 Federal Sentencing Guidelines for Organizations (FSGO), the SEC and other regulatory agencies require risk management in a variety of functional areas. Faced with these multiple requirements, many organizations have embraced enterprise risk management as more effective than the siloed risk management that focused solely on specific regulatory areas. For example, a survey by Protiviti Inc., showed that "three out of four companies... are taking steps to better balance SOX compliance with broader risk management [ERM] activities and priorities."[1]

As we will show, ERM is not only effective in reducing and mitigating risks, but can also reveal new ways to gain efficiencies, discover business opportunities, and deliver on strategy. In other words, ERM not only prevents loss but can also promote growth. The Conference Board (2007), for example, notes that effective ERM:

- Provides—through its emphasis on overall risk appetite—a more objective basis for resource allocation, therefore improving capital efficiency and return on equity.
- Stabilizes earnings and reduces stock-price volatility.
- Offers the tools to make more profitable, risk-adjusted investment decisions.
- Improves transparency to stakeholders, therefore reducing regulatory scrutiny, litigation expenses, costs of access to equity capital, and the rate of return on incurred debt.[2]

---

[1] http://www.protiviti.com/portal/site/pro-us/menuitem.38e6cf4feb72f275266d4110f5ffbfa0.

[2] Newswise "Emerging Corporate Governance Practices in Enterprise Risk Management" http://www.newswise.com/articles/view/527382/ retrieved June 3, 2007.

Knight and Pretty argue that effective ERM can also help companies protect their stock price in case of scandals or other reputational problems.[3] Enterprise risk management gives senior management information and resources for managing crises quickly and efficiently.[4] This is no small point. Reputation and other "intangibles" now make up more than half of a companies stock value.[5] With the rise of globalization, the shifting domestic and international political landscapes, and the ability of the media and special-interest groups to spread information instantaneously, reputational risks abound. Understanding and managing these risks well is crucial to the success of a company, its owners, and other stakeholders.

While enterprise risk management can be a powerful tool, fewer than 40% of CEOs trust their current enterprise risk management.[6] Further, a significant number of CFOs who participate in ERM believe the process needs to be improved.[7] In this white paper, we discuss how Ethics and Compliance can help increase the trustworthiness and coherence of enterprise risk management, reducing the need for outside consultants.

In Part I, we discuss the scope of risk and the advantages and disadvantages of Ethics and Compliance leading or participating in enterprise risk management. In Part II, we look at several examples of how Ethics and Compliance departments and officers have participated in risk management programs, from leadership of the program to executing smaller parallel activities. In Part III, we show that this new role moves Ethics and Compliance from a cost center that prevents harm to a functional area that adds value. Our concluding message is that Ethics and Compliance is an undervalued asset. Companies that fully utilize the Ethics and Compliance function in risk assessment and management can gain a competitive advantage.

---

[3] Rick Funston, Principal, Enterprise Risk Management Leader, Deloitte & Touche LLP.

[4] Reputation & Value - the case of corporate catastrophes © Rory F Knight and Deborah J Pretty, Oxford Metrica, 2001.

[5] Rick Funston, Principal, Enterprise Risk Management Leader, Deloitte & Touche LLP.

[6] IBID; also see: Financial Executive Survey Shows Enterprise Risk Plagues Corporate America, Despite Confidence in Risk Preparation: "Companies are embracing the concept of enterprise risk management but continue to struggle with implementation according to the findings in the 2006 Oversight Systems Report on Risk Management. The national survey of financial executives released today also found room for improvement in the way companies assess, manage and prevent risk." http://www.oversightsystems.com/news_events/release_Risk_Plagues_Corporate_America.php retrieved June 3, 2007. Also see Protiviti U.S. Risk Barometer (survey conducted by Protiviti 2005) http://www.protiviti.com/content/PRO/pro-us/request/index.html?id=us- retrieved June 3, 2007 pub19&doc=http%3A%2F%2fwww.protiviti.com%2Fdownloads%2FPRO%2Fpro-us%2FProtivitiUSRiskBarometer.pdf.

[7] Internal Audit Capabilities and Needs Survey (survey conducted by Protiviti third and fourth quarters of 2006) http://www.protiviti.com/portal/site/pro-us/menuitem.21d938e1a3e99f7bd5332a10f5ffbfa0/ (accessed June 3, 2007).

PART I: ETHICS AND COMPLIANCE: A VALUABLE ADDITION TO THE ERM TEAM

Prior to the corporate frauds and bankruptcies that began this century, senior managers devoted their attention to increasing the value of the company—stock price, market share, and other metrics. Protecting current assets was the job of functional areas such as Ethics and Compliance.[89] Enron and WorldCom changed this mindset, but not as much as was warranted. On the one hand, senior managers realized that if functional areas devoted to protecting corporate assets did not do their job, the entire enterprise could be lost. Fear of these spectacular losses gave Ethics and Compliance more attention from the C-suite and boards of directors. On the other hand, Ethics and Compliance was still seen as a cost center preventing loss. In this white paper, we will see that Ethics and Compliance can add significant value to an organization's ERM process, and therefore to organizational value.

There are several reasons why Ethics and Compliance is well-suited to play a role in the enterprise risk management team. First, Ethics and Compliance has extensive cross-functional experience. This experience stems from helping their organizations to implement the Federal Sentencing Guidelines for Organizations[10]. These guidelines were open-ended with no history of how to apply them.[11] ERM is also a new effort, with many open-ended guidelines and little history of application. The skills Ethics and Compliance has acquired in the more than 15 years of working with the FSGO prepare them well for adding value to ERM.

Second, Ethics and Compliance has often played a role in applying the regulations that have come out of SOX, the Public Company Accounting Oversight Board, and the SEC. As a member of a cross-functional team, Ethics and Compliance is in a good position to make sure that these regulations and their nuances—as well as any business opportunities they may generate—are captured by ERM.

---

[8] Rick Funston, Principal, Enterprise Risk Management Leader, Deloitte & Touche LLP. Also see "Improving Risk Quality to Drive Value" p. 4 ©Oxford Metrica 2003.

[9] Internal audit and security are other functional areas devoted to protecting assets.

[10] In this way, it is similar to internal audit. However, Ethics and Compliance has a skill set that internal audit does not. Internal audit guidelines are relatively specific, and where they are not specific there is a history of application. This is not to say that issues in internal audit are always clear. Far from it. The point we are making is one of relative clarity.

[11] For example, Ethics and Compliance have to satisfy criteria enumerated in the Federal Sentencing Guidelines for Organizations, first established in 1991 and revised in 2004. The Guidelines list seven criteria for an effective Ethics and Compliance program. These criteria were written so that they could be used by organizations of different sizes and structures. The wide applicability of these criteria comes with a price. Organizations need to figure out how to satisfy these criteria in their particular circumstances. In short, there was no cookie-cutter, one size fits all framework that Ethics and Compliance officers could simply install in their organizations. Nor could they rely on past practices.

Third, Ethics and Compliance has been doing risk management as part of their regular duties for quite some time. The 1991 FSGO did not explicitly require risk management, but it did require companies to note recurring problems and address the root causes of these problems. These recurring problems signaled risks that needed to be mitigated. In 2004, the FSGO explicitly required risk assessment. This requirement is worded in a general way so that companies of different size and structure can satisfy it: "the organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement set forth in subsection (b) to reduce the risk of criminal conduct identified through this process" (§8B2.1.(c)). How often the risk assessment is conducted will differ from organization to organization as will what counts as adequate assessment and "appropriate steps" to mitigate. The good judgment of ethics and compliance officers is crucial to make appropriate decisions in these areas. This experience is important as the ERM team supports management to make effective decisions in ambiguous areas.

Fourth, Ethics and Compliance has experience in understanding how culture influences individual behavior in organizations. This focus on culture has intensified since the 2004 FSGO stating that organizations should promote a culture of ethics and compliance. Organizational culture includes "tone at the top" which has been identified as a risk factor by COSO and other documents addressing the prevention of organizational misconduct. The Ethics Resource Center's 2007 National Business Ethics Survey® (NBES) identifies ethical leadership—defined as tone at the top and the belief that leaders can be trusted to do the right thing—as one of the four components of a strong enterprise-wide culture. According to NBES, a strong enterprise-wide culture dramatically decreases misconduct, increases the likelihood of reporting, and reduces retaliation against employees who report.[12] As we will see in the cases in Part II, several ERM processes focus on culture.

It is also important to note the disadvantages when Ethics and Compliance participates in ERM. First, while many ethics and compliance office personnel have the skills noted above, not all do. Another problem is allocation of resources; ethics and compliance departments are not likely to be staffed to handle this extra role. There are a variety of ways to handle this depending on the structure and goals of the organization. Finally, Ethics and Compliance is often seen as an obstacle to business success rather than a vehicle for promoting it. This may be the most difficult problem to overcome.

In the next section, we discuss several cases in which Ethics and Compliance has played significant roles in the success of ERM, and therefore in the success of the organization itself.

---

[12] Ethics Resource Center (2007). *National Business Ethics Survey*, Washington, DC; ERC.

PART II: CASES

A. Large Perishable Goods Manufacturer and Distributor

Large Perishable Goods (LPG) manufactures and distributes standard and specialized perishable products throughout the United States. In the past, LPG had experienced fraud at a high level of the company. In helping to build a new culture at LPG, Ethics and Compliance wanted to make sure they were satisfying the requirements of risk assessment in the revised Federal Sentencing Guidelines and other regulations. A benchmarking process led them to believe that the best way to proceed was to integrate enterprise risk management tailored to its business requirements and the recovery process the company was following. This benchmarking also revealed that ERM could help the business identify new opportunities and better implement strategy, rather than merely dealing with legal and compliance issues.

Ethics and Compliance presented their benchmarking data to the senior executive group. The senior executive group approved a cross-functional, high-level Business Risk Committee (BRC) to oversee an ERM program. The BRC included corporate leaders, field leaders, and functional experts. By consensus, the BRC established a charter that included supporting the organization's business objectives, promoting compliance, and adhering to the highest standards of ethics, integrity, and prevention.

Using this charter as a guideline, the BRC established processes for gathering information about risks and opportunities throughout the enterprise. This process was informed by materials developed by an external party, the Compliance and Ethics Leadership Council (CELC – part of the Corporate Executive Board organization): "Toward Better Risk Detection and Prevention" (September 2005) and "Step by Step Implementation Guide for Performing a Legal and Compliance Risk Assessment" (2005).[13] These materials provided a practical process for applying elements of COSO, FSGO, and other pertinent regulatory requirements. As the project progressed, LPG found more and more ways to customize the process in a manner that fit the company. The BRC charged the office of ethics and compliance to facilitate the implementation of the ERM process. Ethics and Compliance would work with the BRC to compile a report to be submitted to the CEO.

In the first year, Ethics and Compliance convened two all-day meetings with the BRC occurring within two months of each other. Ethics and Compliance got buy-in for meeting dates and pushed the process around those dates relentlessly. Using the CELC materials, as well as information gathered from subject matter experts and senior management, Ethics and Compliance developed a list of broad risk areas for review by business leaders. Prior to each meeting, expert presenters were provided with a brief template to describe and classify their top three to five risks as

---

[13] These materials are proprietary and cannot be reproduced here.

reputational, financial, or operational. Additionally, each expert was required to rate the risks by likelihood and severity according to a provided template. Working with the expert presenters in advance was key. The experts, most of whom were members of the BRC, presented the top three to five risks they identified in their area. Ethics and Compliance was included as a risk area as well. The experts were allowed to bring very brief slides to the meeting to further explain the risks identified.

Preparation for the meeting was carried out through phone calls and e-mail. Confidentiality was emphasized throughout. For example, BRC members were not allowed to retain hardcopies of the documents used in the meetings. Further, disclaimers were put on all the documentation used, including the final report for senior managers.

During the meeting, which was sponsored by business leaders and facilitated by Ethics and Compliance, BRC members asked questions about the risks and the current state of mitigation of the risks. Business opportunities and risks related to strategy were also noted during the meeting. A heat map was used to represent the overall rating of risk combining the likelihood and impact scores. For each risk identified, the BRC would reach consensus on whether the risk was low, medium, medium high, high, or very high. Facilitators pushed to keep the process moving by focusing on points of agreement versus those about which there was disagreement. If there was substantial disagreement or lack of clarity over an area, Ethics and Compliance would record possible solutions to the problem for further discussion with the BRC.

As the workshops progressed, the prioritized risks were further grouped by overall area, such as Operations, Safety, Food Safety, etc. Especially noteworthy was the addition of a separate category for strategic risks that included such areas as Market/External Environment, Human Resources, Operations, and Systems. These categories were created to bring in matters that were not specifically legal or compliance-related, but that were perceived to be critical to business success. Inclusion of these strategic areas led to excellent results, with an ultimate report of prioritized risks identified in each area together with risk owners responsible for mitigation plans.

After the initial risk assessment meetings, the BRC convened several times by telecon to consider written mitigation plans submitted by risk owners for each risk. The BRC reached a consensus on whether each plan was satisfactory or needed improvement. This assessment of the risk mitigation plans would be part of the annual work done by the BRC following an update of prioritized risks.

The BRC submitted a draft report to senior management; after final approval, the report was provided to senior leaders in the company with a briefing. Additionally, the next level of management was briefed on the results of the report. Finally, a summary of the key priority risks and attendant mitigation plans in the form of a daily calendar marker were provided to key managers at all divisions in order to provide a handy reminder of risk management priorities.

A recent development in the company's ERM process has been the completion of a regulatory compliance certification process that provides line level self-assessment data to the company's BRC. After the first report out of that data, it seems clear that it will provide needed input from the "front lines" of the company into the risk assessment process. Additionally, as the second year of the process has unfolded, it is clear that it is beginning to gain momentum as some risks were resolved and dropped from the process while new and emerging risks were brought to the process for discussion and follow-up. The next steps at LPG are: 1) To review how risks are sorted into reputational, financial, and operational categories in order to better prioritize those risks; 2) To continue to review the year implementation process for gaps and opportunities for improvement; and 3) To continue a very rigorous follow-up on mitigation activity to ensure the process continues to add value to the company.

Key Learnings:

- While ERM was initiated in response to prior problems and regulatory requirements, Ethics and Compliance turned ERM into a process that created a forum to discuss and resolve strategic issues, and thus, add value to the company.
- Having business leaders sponsor and lead the ERM discussions of potential risks gave the process credibility.
- Rigorous follow-up and analysis of the effectiveness of mitigation activity is essential for the process to be valuable. Without action and follow-up, the process is an empty exercise.
- Facilitators had to work relentlessly to keep the process on track. Two of the most important actions were: 1) thorough preparation before the meeting (an educated facilitator with experts who understood the process which they would present); and 2) suggesting and recording for further discussions possible solutions to substantial issues about which there was disagreement or lack of clarity.
- Secure document management was important to ensure that ERM did not generate risks by producing information that could have been taken out of context.
- Material from the Compliance and Ethics Leadership Council was helpful in the design of the ERM process. COSO and FSGO were not as easily applied, though they provided a baseline for ensuring that the ERM process was sufficiently complete.

Value-Added ERM Contributions:

- New business opportunities were identified.
- Better ways of implementing strategy were discovered.
- Overall understanding of the risk position of the company was improved, as well as the quality of mitigation of risk.
- ERM workshops helped strengthen the understanding and pursuit of business objectives and strategy throughout LPG by providing a forum for discussion of barriers to those objectives and mitigation actions.
- Improved communication among and between teams and functional areas.

- The effectiveness of activities and mitigation plans were analyzed in an open forum, and improvements were discovered and implemented.

B. Very Large Chemical Company

Very Large Chemical Company (VLC) is an international company that produces chemicals for industrial and retail products. VLC was prompted to do ERM because of the frauds that had occurred at other companies and because of new regulatory requirements, specifically the 2004 revisions of the Federal Sentencing Guidelines.

VLC, like Large Perishable Goods, used materials from the Compliance and Ethics Leadership Council. These materials provided a practical process for applying elements of COSO, FSGO, and other pertinent regulatory requirements. However, it was the revised FSGO that formed the core of their process, with a focus on culture, the seven steps, and periodic risk assessment.

A new committee was formed to oversee ERM. This ERM Committee was headed by the chief ethics and compliance officer and included much of the staff of the ethics and compliance office. Personnel were added to the ethics and compliance office to make up for this resource loss. VLC has over 28 business units, several of them quite large. The ERM Committee worked with the senior managers of each business unit to conduct a risk assessment. This team usually included the CEO/President of the business unit, senior VPs, and representatives of support areas relevant to the risks being considered. Before the teams met, the ERM Committee staff worked with members to complete worksheets that identified risks and gave these risks an initial prioritization. The advanced preparation allowed for a relatively short meeting, two hours, in which risks were identified and prioritized. The ERM Committee initially tried to assign risks using numbers one through ten, with one being the lowest. This proved difficult, as there was often quite a bit of discrepancy over whether a risk was, for example, a five or six. The ERM Committee then instituted a simple priority system, which worked much better. The next step was to assign risks of the highest priority to specific people or groups so they could propose mitigation plans. The last step in the process, which occurred in a separate meeting, was finalizing a control plan for the risks identified. Documents created throughout the process were carefully managed and protected. The ERM Committee paid close attention to the culture of the company. For example, there was a widely used business process for measuring and obtaining business and production excellence that was adopted by the ERM Committee.

As a result of the attention given to risks in all business units, they were able to identify common risks in the enterprise and address them together; this resulted in considerable cost savings. An unexpected benefit was the amount of learning that occurred during the business unit risk assessment meetings. New business opportunities and more effective ways of dealing with recognized issues were discovered on a regular basis.

Key Learnings:

- While ERM began focusing on traditional risks, the process quickly revealed business and strategic opportunities.
- Benefit of using materials from the Compliance and Ethics Leadership Council and FSGO.
- Benefit of using business tools and processes already embedded in the corporate culture.
- Useful to work closely with participants before the meeting.
- Document management and protection was key.

Value-Added ERM Contributions:

- Better ways to organize operations were discovered.
- New business opportunities were identified.
- An overall corporate view of risk, allowing similar risks to be handled more effectively with lower cost.
- The promotion of consistent risk management across the corporation.

C. Another Very Large Chemical Company

Another Very Large Chemical Company (AVLC) is based in the United States and has a large international presence. Enterprise risk management is just beginning to integrate risk management that was occurring in isolation throughout the organization. One of the goals of ERM is to anticipate risks rather than reacting to them. At AVLC, risk appetite is different for different categories, i.e. the company's appetite for risk is fairly aggressive in business strategies but conservative for financial, ethical, and reputational elements.

Executive management worked with the audit committee to design an ERM process along the lines of COSO I. Ethics and Compliance had continuous discussions with the audit committee and executive leadership responsible for ERM about the process and about the place of Ethics and Compliance within the process.

As a result of these discussions, Ethics and Compliance, with support from the audit committee, devised a risk assessment protocol and tools for ethics and compliance that could be applied across its businesses, functions, and geographies. This protocol would satisfy the revised Federal Sentencing Guidelines for Organizations, which requires periodic risk assessment and management of the Ethics and Compliance function. Each of the business directors is currently reviewing the protocol. The next step is a series of pilots whereby a company lawyer and other appropriate functional representatives will lead teams of business unit leaders through a risk assessment and management questionnaire.

Although many of the steps in ERM will focus on loss prevention, the company believes that through better anticipation, coordination, resource allocation, and efficiency in addressing risks,

they can create value and improve their competitive position. For example, by studying transportation and supply chain risks comprehensively, the company anticipates realizing operational efficiencies. Second, the area of "reputational risk" is one that people tends to view in silos. As a result, almost every business, function, and geography has a narrow view of reputation tied to their own organization (e.g. Public Affairs "owning" reputation as a function of corporate branding activities). The result is a variety of overlaps and white spaces, with reputation risks not well-coordinated overall. It is expected that ERM will resolve the problem.

Ethics and Compliance wants to add three elements to ERM. First, it wants to increase managerial awareness of the complexity of risks. Second, it wants to emphasize the need for close coordination among those managing risks. Third, it wants to increase managerial awareness of how leadership tone, culture, and consistency affect risk. Promoting this awareness is a major initiative of the Ethics and Compliance personnel involved in ERM, since Ethics and Compliance believes that leadership tone will have a disproportionate impact (positive or negative) on all the other risks.

Key Learnings:

- Appetite for risk is fairly aggressive in business strategies but conservative for financial, ethical, and reputational elements.
- The most important objective is imparting an awareness of how leadership and culture can reduce, exacerbate, and create risk.

Value-Added ERM Contributions:

- The process is just beginning.

D. Large Technology and Manufacturing Corporation

Wanting to be best in class, Large Technology and Manufacturing Corp (LTM) mainly serves domestic and international government markets. LTM has several large business units. What follows is a description of a risk management program for one of those units.

The risk assessment tool used by Ethics and Compliance divides the world of compliance into 17 areas. Some of these areas include Employee Relations, Government Contracts, HSE, and Intellectual Property, with questions for each area. Ethics and Compliance puts these questions into a web-based instrument so that VPs can input the data directly into a database. When functional areas are supported by other business areas, the question set may also be sent to this supporting area; the functional VP can request further information and interaction. Each VP only has access to the compliance functions for which they are responsible.

Respondents were asked to do two things. First, write a narrative evaluation of the risks: this could be one sentence or three pages, depending on need. Second, they were asked to rate the

controls appropriate to the area using a five-point scale according to two dimensions: effectiveness and maturity. Effectiveness was rated from one to five: not effective at all to extremely effective. Maturity was also rated from one to five: no controls in place to well-developed policies and practices in place. Any assessment below three for either variable required corrective action, typically the identification and implementation of proper controls. Ethics and Compliance uses data to increase efficiencies and reduce risks by looking for commonalities, significant differences, and gaps. A yearly report is given to the business unit CEO that summarizes the conclusions from the data and its analysis.

Using an electronic database to gather and coordinate information fits well with the company's engineering and technical culture. It also addresses the reality of a small Ethics and Compliance office.

Key Learnings:

- Risk management was triggered by an awareness of regulatory requirements, an understanding of how other companies failed to manage risks well, and the revised FSGO.
- The process and the tools for risk management were devised by the Ethics and Compliance office and were well suited to the culture.
- The web-based instrument provided a way for an ethics and compliance office with few resources to gather a great deal of data in a short amount of time in a way that allowed for comparison and contrast.

Value-Added ERM Contributions:

- Ethics and Compliance gathered information quickly and with minimal cost.
- Business unit CEO received a coherent and integrated account of risks across the functional areas of the business unit.
- Accountability was clearly identified for each risk element.
- VPs got a holistic look at their own areas of risk.
- The ethics and compliance office was able to get a holistic understanding of risks throughout the business units.

E. Large Healthcare System

Large Healthcare System (LHS) is a faith-based, not-for-profit entity with acute-care hospitals, nursing care facilities, ambulatory sites, assisted living facilities, and home health and hospice services in over eight communities throughout the United States. LHS revamped its governance and management structures after a substantial fraud—sustained over several years—was discovered in one of its operating units. The fraud prompted investigations by enforcement and regulatory agencies.

Prior to the fraud, LHS subscribed to an organizational philosophy of “corporate minimums.” Similar to a holding company model, with this philosophy the requirements from corporate headquarters were kept to a minimum so that field based operating units would have maximum flexibility and autonomy. This was consistent with the common wisdom of the times: Ethics and Compliance was one of several jobs of a senior executive. Growth in LHS was robust, primarily through acquisitions.

The fraud was a blow to the leadership of LHS, who saw it as deeply inconsistent with the mission and values they wanted to guide decision-making in LHS. Instead of limiting themselves to removing the perpetrators of the fraud, they insisted on taking a therapeutic approach by focusing on their culture. Why didn't individuals within the operating unit who had questions and concerns about certain business practices speak up? This question and others led to a root cause analysis of the culture that unwittingly enabled the fraud.

Working with external consultants, the root cause analysis identified more than 200 recommendations at the system level. These recommendations were reorganized into less than 20 broader categories. One of the recommendations was to have a corporate officer responsible for ensuring that a culture of corporate responsibility was adopted at every level of the organization. LHS hired a person for this position from outside the organization who had extensive experience in operations, as well as a background in theology, philosophy, and ethics. The corporate responsibility officer reports to the chair of the board with a dotted line to the CEO, and serves on the executive leadership group for the corporation. The focus of effort in Ethics and Compliance utilizes various metrics, but always in the context of organizational culture.

As one way to measure culture, LHS focused first on employee satisfaction. However, they soon realized that one could be satisfied at a very low level. LHS now focuses on employee engagement as one measure of culture. Employee engagement is defined as: "commitment, loyalty, and focus," which, in turn, is measured by a variety of individual questions. Improving employee engagement across the company is a key metric by which LHS measures organizational performance. Other performance metrics focus on such things as finance, quality of care, community commitment, and community health. Another metric rolls up key Ethics and Compliance activities (e.g. education, background checks, conflict of interest disclosures) into an index. LHS tracks these metrics on a monthly basis, and shares them with the board of directors.

The organization supports the focus on culture in several different ways. For example, the leadership team announced an initiative to pay workers a “just living wage” that is tied to the cost of living at the healthcare sites. This initiative is consistent with respect for human dignity, one of their core values. Previously, a focus on respecting human dignity was directed primarily at patients and their care. Management has extended this concept to all stakeholders.

As it relates to ERM, LHS is currently following two tracks. In the near-term track, they have identified five risk clusters. An example of one of these clusters would be physician relationships,

which generate a variety of risks regarding billing and referrals. The focus of effort in this arena is to clarify risk impact, risk likelihood, and risk mitigation efforts in each of the five areas; thus, it focuses primarily on current issues and challenges. In the long-term, LHS is creating an organizational infrastructure that utilizes expertise and resources from both headquarters and from operating units in the field. The focus here is to build reliable systems and processes that will better enable LHS to anticipate emerging risks.

Key Learnings:

- While fraud triggered awareness of problems, regulatory issues did not dictate the approach to rectify the fraud. Instead, a system-wide approach was instituted that resulted in a more coherent and integrated understanding of the entire entity.
- The ethics and compliance leader was hired to maximize fit with the culture they were working to create.
- The corporate responsibility officer reports to the chair of the board with a dotted line to the CEO. The ethics and compliance effort is strongly linked to governance, and is guided by governance best practices.
- Even though many people in LHS were on board with its mission and values, this did not result in peer enforcement of these values or reports of violations.
- While LHS did not want to increase bureaucracy to manage acquisitions, they recognized the importance of corporate support of the mission, values, and culture throughout the healthcare units.
- Meaningful and visible acts by senior management—such as the new living wage policy—were used to support an emphasis on an ethical culture.
- The focus on culture identified new ways to apply the organization's mission and values.

Value-Added ERM Contributions:

- LHS is moving away from a holding company model seeking alignment through a shared partnership model that influences both operations and governance.
- Hypothesis: enterprise risk management will further solidify LHS into an entity that has one mission and set of values that guides its different activities.
- Hypothesis: enterprise risk management will identify new opportunities for acquisitions in the future.

F. Incredibly Large Health System

Incredibly Large Health System (ILHS) is a government-based healthcare system with over 160 healthcare facilities. The Ethics and Compliance Group in ILHS is currently planning for ERM. No particular problem prompted ERM; however, the size of ILHS made ERM a likely candidate for helping to efficiently mitigate common risks and to standardize assessment and reporting.

The Ethics and Compliance Group is responsible for planning and coordinating ERM. Ethics and Compliance wants a process that will blend local risk identification with national rollout strategies resulting in a sharing of successful approaches to risk mitigation and reporting. They used COSO I and II and the revised FSGO to make sure they were covering the right areas. However, the ERM process itself has been customized to the practices and cultures of ILHS.

Ethics and Compliance is accountable to ILHS leadership, oversight bodies, and the individual healthcare sites. Each constituency focuses on different expectations. Local health care facilities want ERM to be transparent and helpful to business operations. ILHS leadership and oversight bodies want consolidated risk reporting and analysis across the healthcare sites, demonstrating a national commitment to thoughtfully and critically managing local and national risks.

Ethics and Compliance began the process by convening a task group that included senior and technical leaders within Ethics and Compliance and invited input from business process owners, national performance measurement experts, local process owners, local program leaders, and operational staff. They also reviewed reports from internal and external oversight reporting bodies and requested more information when appropriate, especially regarding risk trends.

When implemented, ERM will add value to ILHS. Not only will common risks be managed more efficiently and less expensively, but relationships between the central office of ILHS and health care units should improve. For example, ERM will not be pushed down as a completed entity that each facility must follow. Instead, there will be room for input and customization. Existing resources at local facilities will be used as much as possible. Technology will be introduced to reduce the time and effort to make accurate reports. Finally, leadership of local healthcare facilities will be rewarded for progress and effort, as well as outcomes, as they assess and mitigate risks and pursue better business solutions. The last point is important– there is no expectation that all knowledge flows from the center. Specific healthcare facilities may be tapped for their expertise to educate others in the system.

Risk appetite is defined externally as well as internally. ILHS will examine what risks the public, legislature, and other oversight bodies are willing to tolerate. Internally, as ILHS is in the healthcare business, they have no appetite for risking the health and well-being of patients. Still, given the reality of limited resources, they have to make choices about policies that will favor some groups of patients over others.

The major problems ILHS need to address not only include methods, techniques, and tools, but also determining the sequence and priority of risks to address and the timelines to manage risk assessment rollout and reporting.

The overarching goal is to integrate risk assessment and management with strategic planning and normal business practices and processes. One way to do this is to put risk assessment and management into performance reviews.

What surprised ILHS was the difficulty of creating linkage between existing internal control measures and enterprise risk management. Additionally, using IT in ERM was more challenging than originally anticipated.

Key Learnings:

- ERM was triggered by a need to coordinate risk assessment and management in a large number of healthcare facilities.
- COSO I and II, as well as FSGO, were used to develop the ERM process.
- ERM for this organization is carried out in the context of legislative and public scrutiny.
- ERM will be a part of performance reviews.

Value-Added ERM Contributions:

- The process is just beginning.

G. Large Manufacturer of Wood Products

Ethics and Business Conduct, which takes more of a values-based than a compliance-based approach, has been asked to support a companywide risk assessment. The decision-making process that led Large Manufacturer of Wood Products (LMW) to ERM began with new regulations, such as the revised FSGO and SOX that require risk assessment and management. These risk assessments begged the question of what other risks are present, and how best to address them. The ethics office of LMW turned to ERM as a way to address the risks holistically, but also to increase communications and coordination between areas already doing risk assessment, such as safety, security, internal audit, information technology, and environmental.

LMW has done preliminary work to ensure that the right people are at the table, e.g., internal audit director, security director, ethics director, environmental health & safety, information technology security, and human resources. Ethics and Compliance anticipates they will probably take a broader view of risk than these functional areas. This is because they will not limit themselves to laws and regulations, but will include risks to the reputation and values of the company. No particular frameworks have been chosen for implementing ERM. Due to the number of consultants who have contacted the law department requesting to provide their (expensive) services to do a COSO risk assessment, there is a resistance to using COSO.

Key Learnings:

- The approach to mission, values, and compliance by those leading ERM, in this case Ethics and Legal, is likely to shape the way ERM is handled.

Value-Added ERM Contributions:

- The process is just beginning.

H. International Distributor of Commodities Company

International Distributor of Commodities (IDC) had problems with compliance and ethics several years ago. As part of the recovery plan, IDC instituted an ethics and compliance office. When the office was first created, it focused on compliance. As it grew, ethics and values came into focus. At this point, the office sees itself as focusing equally on both. Compliance is absolutely necessary, but there are many risks to the organization that are not legal or regulatory; this is where ethics and values come into play. According to IDC, "Paying attention to ethics will help us avoid an overly technical and legal approach to risks."

The past five years have seen Ethics and Compliance grow in stature and scope at IDC. For example, training that included compliance and values was controlled by many different areas. Ethics and Compliance now oversees all training that includes ethics and compliance topics.

When the revised Federal Sentencing Guidelines for Organizations came out in 2004, Ethics and Compliance began to assess and manage risk in their own area. Not wanting to reinvent the wheel, the head of Ethics and Compliance wanted to find out how other areas were assessing and managing risk at IDC. Discussions with the controller led to Ethics and Compliance working with the controller to devise an ERM framework.

Ethics and Compliance is considering COSO II and the revised FSGO for developing the ERM framework. However, as these can be difficult to apply, the company may rely on guidelines from the Open Compliance and Ethics Group (OCEG). OCEG presents a framework for applying COSO II and the FSGO in a way that integrates best practices, appropriate technology, simple forms, etc.

Ethics and Compliance is working toward a centralized, unified method for assessing risks. However, the culture is not accustomed to surveying on a systematic basis; this means they are looking at face-to-face interviews and meetings. They will focus initially at higher levels and roll it out and down throughout the corporation.

Compliance, ethics, and reputational risks are viewed both internally and externally. Goals of the ERM include aligning it with strategy, understanding the extent to which there is agreement throughout the entity about what risks are important, and heightening an awareness of the risks that may be just developing.

Key Learnings:

- The Federal Sentencing Guidelines for Organizations played a key role in initiating ERM.

- Ethics and Compliance can take the initiative in ERM by joining with other functional areas.
- ERM needs to fit with the culture, but also can be used to change the culture.

Value–Added ERM Contributions:

- The process is just beginning.

I. Financial Services Company

In the Financial Services Company (FSC), the ethics officer conducts risk assessment and management training as the second hour of a two-hour ethics training. There are four steps to the process:

STEP A: Distinguish ethical lapses from legal lapses. Use well-known cases, such as AIG, Citibank, and Andersen to initiate discussion about the effects of ethical failures on achieving a company's strategic objectives. Note: Participants initially differentiate ethical lapses from legal ones, but come to realize that the general public does not see a difference between the two in terms of a company's reputation.

STEP B: Examine a recent ethical lapse outside FSC in more detail. This examination is guided by the following four-step "Ethics and Value Risk Assessment/Mitigation Cycle" developed in-house.

- If we could look into the past, before the failure, what were the ethical risks for the company that likely led to the ethical lapse? A good way to define this is what actually happened, but at a little higher level than the details of who, what, where, etc. (for example, the risk of high-level officers of a company misallocating funds as opposed to noting specifics, such as names, dollars misallocated, etc.).
- When risk became reality, what were the effects on the company's assets, values, and reputation? This helps answer the question, "So what?"
- What were the external and internal conditions, including corporate culture, which may have contributed to the ethical lapses?
- What steps could the company have taken to mitigate the conditions, thereby preventing the ethical failure?

STEP C: Just as we have analyzed ethical lapses in retrospect, now we use the Ethics and Value Risk Assessment/Mitigation Cycle to anticipate and define risks to ethics and values at FSC (A worksheet is provided for this exercise).

- Identify one possible ethics or values risk in your area/unit/department.
- List effects on our assets, values, and reputation if the risk were to materialize.
- What external and internal conditions, including corporate culture, expose us to this risk?
- What should we do to mitigate this risk?

This exercise helps individuals think in terms of risks to ethics and values as opposed to just regulatory issues. It also gives them an opportunity to engage in an ethics/business dialogue with peers that can be replicated outside of training. More formally, it provides a structure to proactively anticipate risks to ethics and values and to develop mitigating strategies. Many ethics issues seem to catch companies off guard—a blind spot, so to speak. In most cases, the risk factors were already there—people just were not acknowledging them or controlling for them. Finally, this training reinforces the ethics and compliance office as a proactive and strategic resource as opposed to a crisis center. According to FSC, "If people view us as a crisis center, then we'll have more crises. When we are viewed as an advisory partner, we are able to get in front of problems."

The overall goal is to uphold FSC's strong reputation of trust and to emphasize that they, as a company, lead proactively in ethics just as they do in every other area of their business. In the absence of leadership in any particular area, people tend to define and seek out their own level of performance—in some cases high, in others, low—but not consistently. This type of approach helps FSC ensure both quality and consistency in ethical business practices and conduct.

In addition, conducting this exercise with different groups helps to identify common risk factors across the enterprise. In other words, the frequency with which the same or similar risks are independently identified in separate groups provides important clues both to the probability of risks materializing, as well as the severity of the related consequences to the company.

Key Learnings:

- Ethics and Compliance can find innovative ways to encourage ERM.
- An ERM mindset can be promoted in the absence of ERM.
- This approach to ERM supports the mission values and reputation of FSC.

Value-Added ERM Contributions:

- Waiting for metrics.

PART III: SUMMARY

We began our discussion of enterprise risk management with regulatory requirements. Next, we saw how ERM can bind these risks together into a larger picture. Finally, we saw that ERM, when integrated with the mission, values, strategy, and business objectives, develops a picture of the organization poised for development. We gave several reasons why Ethics and Compliance should play a principal role in this most mature form of ERM: cross-functional experience, deals regularly with regulatory requirements, has a history of risk assessment and management, and has a role in aligning the actions of the company with its mission and values.

We discussed nine cases where Ethics and Compliance played unique roles in enterprise risk management. These roles went from leading ERM in a complex multi-organizational entity, to running parallel activities that were intended to raise awareness of risks throughout the enterprise. While these companies were different, many similarities arose. First, while ERM was often developed in a defensive posture, the ERM led to business opportunities and greater efficiences, growing the value of the organization. Second, Ethics and Compliance needed to work closely with business unit leadership for ERM to be effective. These relationships needed to be established early.

Another theme that arose in the highlighted cases was the importance of culture. One point was the necessity of conducting ERM in a way that is consistent with the organizational culture. Another point was the importance of guiding—and changing—culture in a way that integrates enterprise risk management, the mission, values, business objectives, and strategy. In the case of most organizations discussed, the focus was on leadership carrying this integrative message.

In all of these cases, Ethics and Compliance added value to ERM and ERM added value to the organization.