Closing the Gap

Between Traditional & Enterprise Risk Management Systems

By Jack Ogutu, Mark R. Bennett and Richard Olawoyin

IN BRIEF
- This article aims to help readers differentiate between traditional risk management (TRM) and enterprise risk management (ERM).
- It identifies gaps that exist between TRM and ERM.
- Finally, readers will learn to apply practical steps to a more comprehensive approach to risk management that are transferable to global ERM needs.

This article is part of an ongoing collaborative effort to promote learning and innovative engagement in the risk space. The initiative includes ongoing research, bringing industry's perspective to the classroom as well as educational publications and student mentoring initiatives.

The study presented aims to deconstruct the challenges and opportunities in the risk and insurance industry from the perspective of the large employer. The large employer space has been selected as a focus of study due to the collective baseline of knowledge and resources that this sector of industry offers. Large employers attract some of the best and most forward-thinking professionals who are continuously making advancements through working in larger, more complex environments that allow for accelerated industry learning and evolution of trial and error.

The study focuses on what large employers do best-in-class and where they struggle. Best-in-class practices provide industry learning that is transferable at all levels and sizes of organizations. Struggles are transitioned into development to explore better, more efficient and innovative ways for risk teams to operate. To this end, the article explores the differences, connections and opportunities between traditional risk management and enterprise risk management.

TRM & ERM

Risk management breaks down into traditional risk management (TRM) and enterprise risk management (ERM), which are two different methods used to achieve some of the same goals. Dionne (2013) defines TRM as a system that focuses on pure risks and views each risk separately.

Currently, the evolution of risk management provides effective techniques for employee protection. Organizations have become aware of the importance of employee well-being and have focused attention on employee safety rather than just finances. TRM assesses pure risk and speculative risks to protect employees. Pure risk is defined as a risk that has a loss or no loss. Examples of pure risk are a building fire or a building break-in incident. Pure risks can be insured by organizations. Whereas, speculative risk is defined as a risk where outcomes are loss, profit or status quo (i.e., no gain, no loss or a break-even situation). An example of a speculative risk is potential loss from stock market fluctuation. TRM is broken down into five main components (Figure 1): Risk identification; risk analysis; risk control; risk financing; and risk administration.

Risk identification is a classification system that investigates operational, property and liability risks. Risk assessments use identification tools such as surveys, inspections and checklists to derive information from gathered data (Pagura, 2016). Risk analysis is the process of examining potential losses and severity. Once losses are analyzed, actions and

Jack Ogutu, Ph.D., CSP, AEP, is assistant professor and program coordinator of the occupational safety and environmental health program in the Department of Applied Engineering Safety and Technology at Millersville (PA) University. He also oversees the NIOSH Training Program Grant for the university. He earned a Ph.D. and M.S. in Industrial and Systems Engineering with a concentration in Occupational Safety and Ergonomics from Auburn University, and a B.S. in Mechanical Engineering from University of Nairobi. Ogutu is a member of the Society's Academics Practice Specialty and Blacks in Safety Engineering Common Interest Group.

Mark R. Bennett is founder and president of Risk Innovation Group. He specializes in consulting and technology to promote strategic, efficient and effective risk systems. Prior to this, he was vice president, claims services, for Murray Securus, where he worked for 27 years in various roles including multiline adjuster, claims supervisor, claims manager, vice president of claims operation and vice president of risk management solutions. Bennett holds a B.S. in Personnel Management with a minor in Economics from Indiana University of Pennsylvania.

Richard Olawoyin, Ph.D., CSP, CEP, ASP, is assistant professor of environmental health and safety at Oakland University. He has worked in the petroleum industry as a geologist, geophysicist, petroleum engineer, safety and environmental health scientist, both in the upstream and downstream oil and gas sectors. He has presented at several international and national conferences on petroleum technology, environmental-health, safety and geoscience. He is a professional member of ASSE's Greater Detroit Chapter and a member of the Society's Blacks in Safety Engineering Common Interest Group.

FIGURE 1
Traditional Risk Management Components

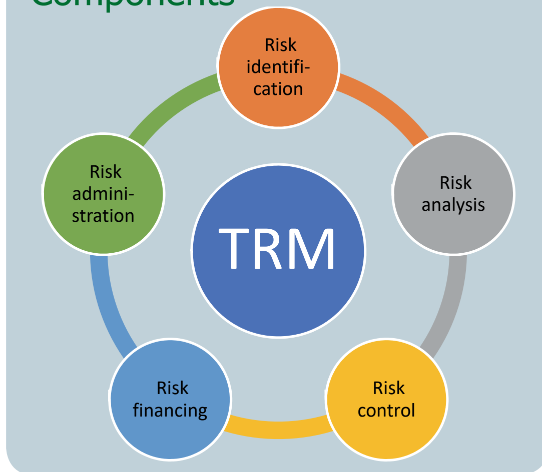
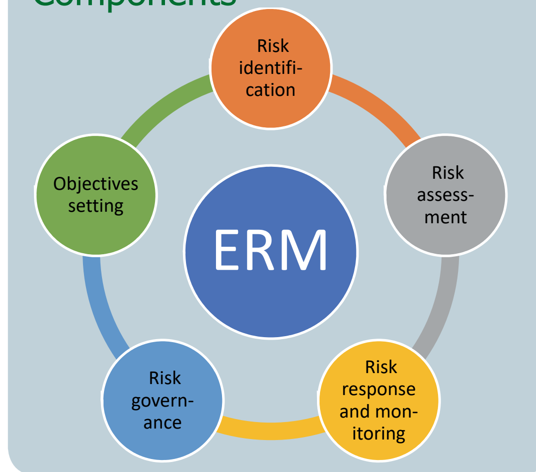


FIGURE 2
Enterprise Risk Management Components



alternatives are then proposed through the process of risk control. Risk control is used for pre-loss assessments and the preventive actions introduced to reduce the frequency and severity of workplace incidents. The actions are to avoid, prevent, reduce, segregate, combine and redesign processes. Small to medium risks usually involve risk financing, which may include purchasing insurance, use of support personnel and use of loss investigation.

The final component of TRM is the management of risk activities through the process of risk administration. These management solutions include risk information systems, safety records for facilities, use of incident reports and analyzing risk assessment data. TRM integrates these five components with the goal of mitigating risks and for proper planning.

ERM is a system with focus on all potential risks, whether pure or speculative (Lundqvist, 2015). ERM has been known to benefit organizations by decreasing earnings and price stock volatility, reducing external capital costs, increasing capital efficiency and creating partnerships between different risk management activities (Hoyt & Liebenberg, 2011). Organizations have shown increased interest in ERM and growing numbers of organizations have implemented or are considering ERM programs. In addition, consulting firms have established specialized ERM units (Hoyt & Liebenberg, 2011).

Compared to TRM, ERM offers companies a more comprehensive approach to effective risk management, with action plans involving stakeholders, shareholders and investors. Like TRM, ERM includes five modified components (Figure 2): Risk identification; risk assessment; risk response and monitoring; risk governance and objectives setting. A major goal of ERM is to incorporate risk considerations into the organization's agenda and decision-making processes (DeLoach, 2014).

The major identifying component of ERM is risk governance, which is a combination of corporate governance and risk management. Risk governance provides the structure of the risk management system and specifies responsibilities, authority and accountability in the risk management system, as well as the rules and procedures for making decisions in risk management (Lundqvist, 2015). ERM addresses all risks faced by an organization including environmental, compliance, financial, strategic and operational.

With ERM, risks are comprehensively addressed instead of managing them individually (Schroeder & Jackson, 2007). Risks cannot be individualized because they interact and affect each other (Baranoff, Brockett & Kahane, 2009; Kusserow, 2007).

The ERM framework identifies and analyzes risks, which then provide the ability to facilitate the following actions (Dafikpaku, 2011):

- avoidance of risk by stopping actions that contribute to risk;
- reduction of risk by reducing the likelihood or impact of risk;
- share or insure risk by transferring or sharing a portion of the risk;
- acceptance of risk by taking no action because of a cost/benefit decision.

The benefits of ERM consist of strategic implications, which are the effects of the ERM process on setting strategic objectives. The mechanisms of ERM must be built into the infrastructure with the goal of ensuring that the company's objectives (strategic, operation, reporting, compliance) are achieved. Strong valuation implications regarding ERM include explicit risk ownership by business units, formalized measures of risk, the collection of knowledge from employee expertise and electronic databases, and documentation of risks and opportunities (Farrell & Gallagher, 2015). These implications allow a firm to uncover and track risk to prevent future mishaps. The goal of uncovering and tracking risk information is to enhance the organization's ability to uncover correlations and dependencies across the entire enterprise (Lo, 1999). Therefore, it is important for risk managers to remember that these risk correlations may change drastically in times of dramatic changes in market conditions (Bookstaber, 2010).

FIGURE 3
Enterprise Risk/Governance Indicators

•No structure for connecting strategic and operational risk: All areas of an organization hold risk that affects the mission. Companies that do not have a process to capture and address risk in a systematic, structured format miss opportunities.

•Struggle with transparency and collaboration: This area speaks to the heart of governance. The ability for a company to be effective, efficient and accountable is directly related to how well it communicates and works together. Consistent and defined processes to quantify and qualify risk speaks to the ability to cut through politics, silos and other areas that distract organizations from making timely and well-informed decisions.

•Poor communication among business process areas: In organizations, everything is connected. This feedback speaks to lost opportunities due to silos, including redundancies and best practices that are not shared and commonalities that go undiscovered.

•Risk appetite is not defined: Without the boundaries that are defined by a risk appetite statement, organizations are taking on more than they can handle or being too cautious and not taking advantage of right fit opportunities.

•Find silos challenging: Redundancies and missed opportunities due to walls that prevent effective organizational communication and collaboration.

FIGURE 4
Traditional Risk Indicators

•Missed opportunities with service partners: This speaks to the ability of organizations to concisely define where they are, what they are good at and where they struggle. In short, being able to define where stakeholders can best support them.

•Lack of innovation in the risk space: Innovation speaks to a company's ability to recognize risk opportunities and to shift time and resources to what is most important. It also speaks to the ability to capture risk that is emerging and putting controls in place to avoid or minimize any potential negative outcomes.

•Ineffective monitoring: This speaks to an organization's ability to make sure what is most important happens. Testing, metrics and incident management all come into play to support accountability and compliance.

•Lack of a risk identification process: If organizational risk is not identified, assessed, evaluated and transitioned into action, the organization is subject to random activity and missed opportunity.

•Board/senior management not aware/engaged: This speaks to the ability of an organization to capture risk that ultimately allows it to quantify risk, deal with it and appropriately aggregate the information up so that effective and timely decisions can be made.

Current Study: Survey Methods & Results

The authors designed and distributed a survey to participants through a survey link to assess the role that risk plays in organizations, obstacles that exist and what best-performing employers are doing. The survey questions addressed areas of traditional risk, global enterprise risk and organizational governance. The study was mainly targeted at large employers, brokers who service large employers and carriers who service large employers. The researchers selected the large employer space as a focus of this study because of the collective baseline knowledge and resources that this sector of industry offers. Large employers provide environments that allow for accelerated industry learning through an evolution of trial and error. Large employer personnel involved in the study included executives, corporate risk managers, claims managers and human resources managers.

The Results: Overview

The study suggests that gaps exist between traditional risk management (hazard risk) practices and the enterprise of risk (all other risk) that an organization must address. The survey results confirmed the existence of these gaps and suggest that risk managers are in the right position to take on this expanded responsibility in closing these gaps.

Additionally, the study shows that plenty of opportunities exist for large employers struggling in the risk space. Figures 3 and 4 highlight key survey results. Notable results are divided into two main clusters: 1) enterprise risk/governance indicators (Figure 3) and 2) traditional risk indicators (Figure 4).

In the enterprise risk/governance area (Figure 3), comments surrounding company silos are the leading response to struggles in the risk space. This is a natural outgrowth of not having a commitment to a structured risk assessment framework that can be consistently applied throughout the organization.

The next group of struggles with similar importance is the inability to effectively communicate between core business process areas, which speak to the need for a common language. This area of communication finds additional obstacles when it comes to an organization's ability to simply operate with a level of transparency and collaboration. Lastly, not having a defined risk appetite speaks to the lack of boundaries in place that guide what organizations pursue.

In the traditional risk area (Figure 4), the study shows that risk managers struggle getting executive attention and buy in. The board is not aware of the risk or at least cannot make comparisons with traditional risk and the other business risk it must face and address daily. Both the survey questions and comments pertaining to service partners show that risk managers have not positioned themselves to take full advantage of their available services. The survey suggests TRMs are primarily missing opportunities because they do not have a well-defined baseline that outlines their risk system, one that allows stakeholders to capture what the employer does well and where it struggles.

The survey identified the need for a foundational risk identification process. Next in importance is monitoring, which relates to accountability for making sure that what is most important actually happens. Lastly, the lack of innovation hit the top indicators. The responders found it challenging to break into more strategic approaches. The results of the survey highlight the main obstacles large employers face in the risk space. Two main obstacles identified are 1) governance obstacles and 2) strategic challenges. These are summarized in Table 1. Nonetheless, the survey results also pointed to the many good things happening (Table 2).

Discussion: Who Should Take Responsibility?

The survey suggests the existence of gaps: areas of inefficiency and missed opportunities due to the lack of a centralized framework and processes to address all risk consistently. Gaps are challenging areas because many of those identified by the survey are not areas that organizations are accustomed to dealing with. They fall into a middle ground, where most may know issues exist, but it is difficult to get momentum behind addressing them. In part, this is because the issues are challenging, and it is unlikely that they are discussed other than in backroom conversations out of frustration.

Who should take on issues such as redundancies due to silos, misappropriation of resources due to politics, poor cross-functional communication, inconsistent processes, poor reporting, random activity and limited accountability?

The analysis from this study suggests that the risk manager is the right person to take on a broader role to tackle these challenges. These individuals understand how to manage risk based on their experience dealing with risk frameworks, which is foundational to this process.

TABLE 1

Overview of Obstacles Identified

Is there value to dedicate time and resources in these areas? Can risk managers play a more active role in these areas?

Governance	
Siloed environments	Different process areas not sharing resources and ideas
Lack of standardized frameworks	Lack of standardization to address risk creates costly redundancies
Cultural struggles	Management buy-in and support to risk focus inconsistent
Ineffective controls	Resources and efforts applied to high-risk areas not working
Ineffective monitoring	No structure to make sure what is most important happens
Addressing risk at a process level	Process owners not identifying and addressing risk day-to-day
Need for simplification	Identifying and addressing risk is complex and slow
Matching resources with highest risk	Difficulties quantifying and qualifying risk
Struggles addressing regulations	Compliance with numerous and changing regulations is challenging
Inability to identify emerging risk	Technology and changing environments create new challenges
Strategic	
Lack of a risk identification process	No structured process to capture, organize and prioritize risk
Consistent platform for addressing risk	Lack of structure to transition identified risk into actionable plans
Risk appetite not defined	Boundaries for risk taking not defined
Inability to quantify and qualify risk	Challenging to make apples-to-apples comparisons
Executive team's buy-in	Inconsistent messages from the top on risk
Reporting on risk	Reporting of top risk and emerging risk ineffective
Lack of continuous improvement structures	Lacking time, resources and focus to enhance ineffective processes
Collaboration	
Available resources not realized	Risk systems that are not defined do not capture stakeholders' best efforts
Poor communication between offices	Similar risk in different process areas are handled differently
Gaps between strategic and operational risk	Risk buy-in between executive and operations is not consistent
Redundancies and inefficiencies	Lack of centralized processes to identify and address risk
Inefficiencies due to politics	Competing agenda distracting from centralized focus on the mission
Missed opportunities	Lost time and resources due to not taking advantage of global efficiencies

TABLE 2

Large Employers Best-in-Class Practices

The survey results show that many good things are happening:
- focused attention on cross-functional communication;
- organization-wide gap analysis;
- structured peer reviews;
- integrating risk management into critical areas;
- dedicated resources to support the frontline;
- leadership audits and accountability;
- executive team receiving quality metrics and reporting;
- risk and compliance managers effectively communicating risk across the organization;
- increased focus on transparency;
- scales in place to rank risk;
- training and attention to risk at all levels;
- structured focus and attention to reducing redundancies;
- enterprise-wide risk reviews;
- use of risk registers;
- use of heat maps and dashboards;
- client outreach to minimize exposure to risk;
- structure to risk identification;
- risk managers engaging in expanded roles;
- budgeting to support a broader risk-based approach to business needs;
- structured focus in integrating business risk with traditional risk management;
- more focus to enterprise solutions;
- embracing technology;
- empowering process owners at all levels to identify, assess and deal with risk;
- structured monitoring processes;
- business continuity plans within all aspects of the business.

The survey shows that some risk managers are getting out of their traditional comfort zones and allocating time toward a framework that can have a broader effect on the organization.

Definitions

Company silos: A silo mentality occurs when a team or department shares common tasks but derives its power and status from its group or area. People find it difficult to share resources or ideas with other groups or welcome suggestions as to how they might improve.

Risk space: This speaks to the collection of all risk a company faces to include pure risk (possibility of loss or no loss) or speculative risk (possibility of loss, no loss or gain).

Risk appetite: What risk a company is willing to take to support its business model.

Transparency: The lack of hidden agendas. Communication that supports collaboration in the decision-making process.

Collaboration: The ability for those in business settings/different process areas to work together to the common good of the company.

Closing the Gap

The data gathering and analysis procedures in this study explored efficient measures that can effectively be implemented to close the gaps and enable organizations to prioritize time and resources. The data and analysis suggest that immediate impact can be realized by taking the following three actions:

1) Make the connection that risk resides throughout all business processes.

2) Be committed to a framework/logic to capture organizational risk.

3) Embrace a consistent process to address organizational risk.

1) Make the Connection That Risk Resides Throughout All Business Processes

As organizations evolve, they become more complex and risk resides in all facets of the business. The make-up of an organization typically involves operations, shared services and many other dimensions that are put in place to serve the company's mission. Operations include important functions such as sales, service, production and distribution. Shared services include functions such as human resources, IT and finance. Other dimensions of an organization include strategic initiatives, geographic regions and compliance areas. All of these areas have risks that are connected to the company's mission and compete for allocation of time and resources.

TRMs can make this connection by simply asking stakeholders what risks employees are facing daily. Often, safety-hazard risk takes a backseat to other risk types that organizational process areas face. By asking about other types of risk that might be on someone's plate, it sets the stage to identify root causes or connections that otherwise may not have been considered.

2) Be Committed to a Framework/Logic to Capture Organizational Risk

The framework must be clear and concise so that all risks can be accommodated, pure and speculative. A best practice is to accomplish this through a structured risk register. The register must have the capability of taking the overwhelming amount of risk information and compartmentalize it through a logical process. The structured process guides how the risk is registered and effectively processed for exit into actionable plans.

Overall, the register houses risk, organizes it into categories and promotes strategic thinking to classify each risk into indicators that define the root cause. Identifying the root cause enables organizations to then systematically pull these root causes into plans.

A perfect landing spot to show the value of a risk register is to start with TRM risks. Risk managers already know and deal with various risks, therefore it is intuitive for them to put their risk in the register to be a pilot for a broader risk collection initiative.

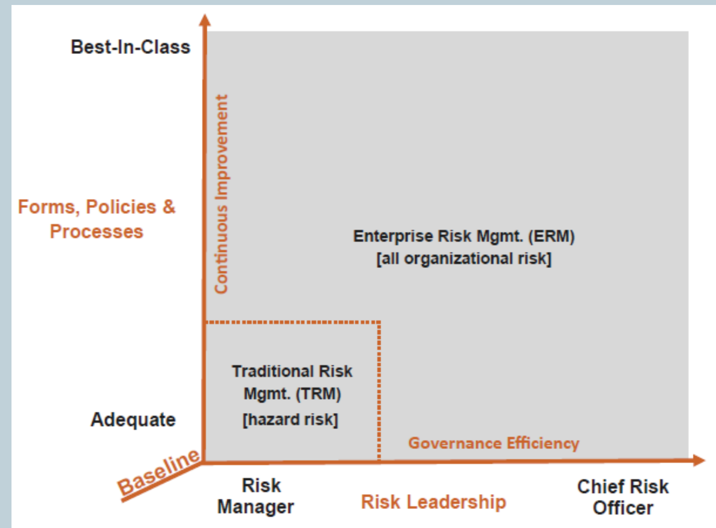
3) Embrace a Consistent Process to Address Organizational Risk

Embracing a consistent process to address organizational risk involves ERM plans, which are defined as structured and consistent ways of dealing with risk. Plans pull select root-cause risk so that the risk can be effectively mitigated and managed with focus and accountability. Enterprise risk assessment software can provide a consistent platform. Generally, those getting started will use spreadsheets to house and add consistency to the process.

Root-Cause Risk to Plans to Action

Once root-cause risk is integrated into action plans, this makes the risk management plans more actionable. As organizations have numerous plans, it is important for these plans to be consistent in

FIGURE 5
Closing the Gap: A Consistent Framework



language used and how they are assessed, mitigated and monitored. Once root-cause risk is put in a plan, a best practice is to:

1) Identify, assess and evaluate. This stage includes a) identifying the root-cause risk to go into the plan; b) selecting and implementing controls/mitigation activity for each root cause risk; c) attaching owners to each control; d) assessing each root-cause risk and the controls that are applied with a selected rating criteria; e) evaluating whether immediate action is required; and f) looking at the root-cause risk/controls to determine what could go wrong.

2) Mitigate. Mitigation puts assessment results into action. Targeted mitigation needs to happen within every risk plan an organization has in place. Indexes are the end product of an effective rating system and are what create the logic to where time and resources will be allocated to drive effective mitigation.

3) Monitor. For a successful risk program, monitoring must be simplified and made a regular part of the process. Three key factors must come into play: testing, metrics and incident management. Testing speaks to making sure what is important is happening: yes or no. Metrics are in place to make sure controls are operating effectively and incident management speaks to learning from controls that broke down, then either building into training or adding new or changing existing controls.

Conclusion

From a traditional risk perspective, it is essential to maximize resources to eliminate risk. From an enterprise risk perspective, looking for the right combination of risk for profitability is key. The gap between the two perspectives is challenging and can lead to inactivity. It is a middle ground where much can be left on the table. Often the gap leaves TRMs frustrated that they are not getting the needed attention and resources. At the same time, this gap does not provide management justification to allow for the additional resources requested. Ultimately, it does not allow for timely and accurate decisions for all organizational risk.

Efficiencies can be realized by looking at and addressing risk from a more holistic perspective. It all starts with implementing risk frameworks that apply consistent logic to both areas, allowing for informed decisions. It is the risk manager's job to embrace a framework that is robust enough to handle the broader risk that organizations face. After embracing a foundational framework, it is recommended that they use their area of pure risk to demonstrate processes that can be transitioned to the broader speculative risk the organization faces.

The survey data supports that the risk framework is the connection that allows risk managers to develop solid TRM practices that are transferable to more global ERM needs (Figure 5). Companies that cut through the challenges embrace continuous improvement processes to move from adequate forms, policies and processes to best-in-class, and shift to a role more associated with a chief risk officer to capture governance efficiency in dealing with all organizational risk. **PS**

References

Baranoff, E., Brockett, P. & Kahane, Y. (2009). The risk management function. In E. Baranoff, P. Brockett & Y. Kahane (Eds.), *Risk Management for Enterprises and Individuals: Vol. 1.* (pp. 147-150). Retrieved from https://open.umn.edu/opentextbooks/BookDetail.aspx?bookId=37

Bookstaber, R.M. (2010). A framework for understanding market crisis. In W.V. Haslett Jr. (Ed.), *Risk management: Foundations for a changing financial world* (pp. 7-24).

Dafikpaku, E. (2011, March). The strategic implications of enterprise risk management: A framework. Paper presented at the 2011 ERM Symposium, Chicago, IL. Retrieved from www.ermsymposium.org/2011/pdf/dafikpaku.pdf

DeLoach, J. (2014, Aug. 13). The role of executive management in ERM. Corporate Compliance Insights. Retrieved from www.corporatecomplianceinsights.com/the-role-of-executive-management-in-erm

Dionne, G. (2013). Risk management: History, definition and critique. *Risk Management and Insurance Review, 16*(2), 147-166.

Farrell, M. & Gallagher, R. (2015). The valuation implications of enterprise risk management maturity. *Journal of Risk and Insurance, 82*(3), 625-657. doi:10.1111/jori.12035

Hoyt, R.E. & Liebenberg, A.P. (2011). The value of enterprise risk management. *Journal of Risk and Insurance, 78*(4), 795-822. doi:10.1111/j.1539-6975.2011.01413.x

Kusserow, R. (2007). Enterprise risk management: The next evolutionary step in compliance. *Journal of Health Care Compliance, 9*(4), 53-54.

Lo, A.W. (1999). The three Ps of total risk management. *Financial Analysts Journal, 55*(1), 13-26. doi:10.2469/faj.v55.n1.2238

Lundqvist, S. (2015). Why firms implement risk governance: Stepping beyond traditional risk management to enterprise risk management. *Journal of Accounting and Public Policy, 34*(5), 441-466. doi:10.1016/j.jaccpubpol.2015.05.002

Pagura, I. (2016). Work health and safety: Risk management. *Journal of the Australian Traditional-Medicine Society, 22*(3), 164-166.

Schroeder, B. & Jackson, J.A. (2007). Why traditional risk management fails in the oil and gas sector: Empirical frontline evidence and effective solutions. *AACE International Transactions*, RI011-RI016.