Executive Report

The Risk Perspective

Risk Management and Internal Audit:

Forging a Collaborative Alliance

RIMS™ the risk management society

The Institute of Internal Auditors

Contributors

Ryan Egerdahl
Enterprise Risk Manager, Bonneville Power Administration

Carol Fox
Director of Strategic and Enterprise Risk Practice, RIMS

Hal Garyn
Vice President, North American Services, The IIA

Paul Hinds
Managing Director, PricewaterhouseCoopers LLP

Albert G. Holzinger
President, Words to Deeds

George Lewis
Director, Enterprise Risk Management, Best Buy Company, Inc.

Karen Livingstone
Director of Advocacy, The IIA

The contributing organizations would like to thank ***Alan Siegfried, Director of Internal Audit, Bank-Fund Staff Federal Credit Union*** *for his support of this project.*

Morgan O'Rourke
Editor

Tricia McGoey
Designer

Published by RIMS

About the Contributing Organizations

RIMS (Risk & Insurance Management Society, Inc.) is a global not-for-profit organization representing more than 3,500 industrial, service, nonprofit, charitable and government entities throughout the world. Dedicated to advancing risk management for organizational success, RIMS brings networking, professional development and education opportunities to its membership of more than 10,000 risk management professionals who operate in more than 120 countries.

RIMS' Mission: To advance risk management for your organization's success.

For more information, visit **www.RIMS.org**

Established in 1941, **The Institute of Internal Auditors** (The IIA) is an international professional association with global headquarters in Altamonte Springs, Fla., USA and provides services to over 170,000 members in 165 countries worldwide. The IIA is the internal audit profession's global voice, recognized authority, acknowledged leader, chief advocate, and principal educator. Members work in internal auditing, risk management, governance, internal control, information technology audit, education, and security.

The IIA's Mission: The IIA will be the global voice of the internal audit profession: Advocating its value, promoting best practice, and providing exceptional service to its members.

For more information, visit **www.theiia.org**

Acknowledgement of Case Study Organizations

The IIA and RIMS are grateful to the following individuals for sharing their approaches and expressing their commitment to advancing collaboration among the internal audit and risk management practices through their words and actions.

Cisco Systems
Philip Roush, Vice President of Governance, Risk and Controls

Hospital Corporation of America
Joe Steakley, Senior Vice President, Internal Audit and Risk Management Services
David Hughes, Assistant Vice President, ERM and Business Continuity Planning

TD Ameritrade
Michael Head, Vice President and Managing Director of Corporate Audit
Joseph Iraci, Managing Director of Corporate Risk Management

Whirlpool Corporation
Irene Corbe, Vice President of Internal Audit
Scot Schwarting, Director of Risk Management

Disclaimer: *Please note that the material presented is informational and is not based on research by either The IIA or RIMS, unless specifically noted. While the collaboration activities work for the organizations highlighted—given the organizational cultures, structures and the people involved—the authors recognize that these practices may not be appropriate for every organization.*

PART I:
THE ROLES OF RISK MANAGEMENT AND INTERNAL AUDIT

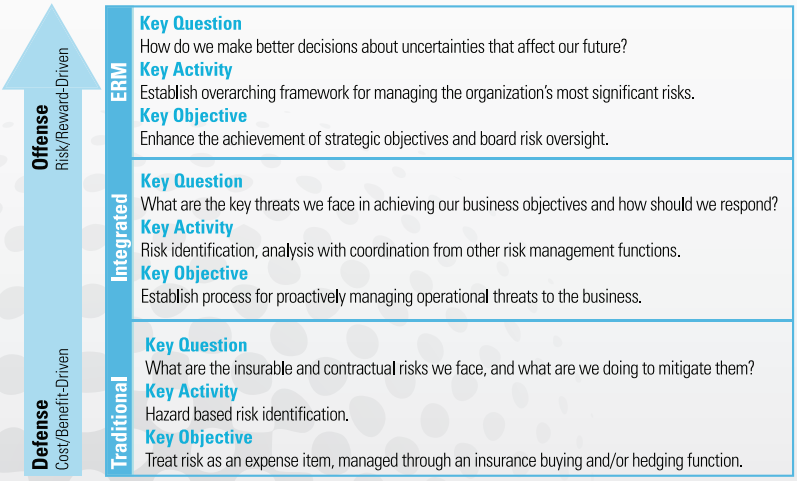
Much has been written about the need for organizations to improve their risk management capability. The collapse of Enron, the WorldCom scandal, the 2008 financial crisis, BP's Deepwater Horizon disaster and the European debt crisis have all been examples called out by regulators and news media evidencing the need for more inclusive, effective risk management practices and oversight. The IIA and RIMS believe that collaboration between the disciplines of internal audit and risk management, can lead to stronger risk practices in meeting stakeholder expectations. The two functions make a powerful team when they collaborate and leverage one another's resources, skill sets and experiences to build risk capabilities within their organizations. The adage, "the sum is greater than the parts," certainly applies. And, it is clear that leading organizations have discovered efficiencies, better decision-making and improved results by forming strong alliances between the risk management and internal audit functions.

Traditionally, risk managers have approached their duties with an eye towards protecting the organization's assets and balance sheet, while internal auditors have been concerned with reviewing the efficiencies and effectiveness of internal controls. But before we explore how these two groups can form an effective collaboration, it will be helpful to take a more in-depth look at their specific roles and responsibilities within an organization.

The Roles and Responsibilities of Risk Management

Over time, the risk management function has evolved in line with changing business needs, in order to deliver recognized additional value to organizations (Figure 1). The risk management function was originally formed primarily to deal with risk transfer, whether through hedging, insurance or some other instruments and is characterized as ***traditional/defensive risk management***. This approach focuses on insurance, contractual and transaction risks.

Figure 1 **Evolution of Risk Management**



The next major evolution was a movement to combine a few risk functions into an ***integrated/advanced risk management function***, focusing primarily on managing insurable hazard losses through prevention and severity decline, such as public liability, automobile accidents, worker injuries, property and other asset losses, where control programs such as safety, claims and physical security contribute. This approach concentrates on threats the organization faces.

The more contemporary risk management function, which is referenced as an ***enterprise risk management*** approach, deals with risks from a much broader scope, depth and response perspective, including strategic, operational and financial risks, among others, as an interrelated portfolio. In some cases, the scope of the risk management function's responsibility has been expanded to include business continuity planning. This approach focuses on how to make informed decisions about uncertainties that affect the organization's future.

Using the risk management function to play offense as well as defense, organizations can begin to assess risks in an interconnected portfolio. Risk-based business decisions across the organization may be guided by risk appetite statements on both corporate and operational levels. Rather than measuring losses and managing operational threats only, the enterprise risk management function provides the process and methods to manage unwanted variations from expectations, which are linked directly to the overall corporate strategy.

That said, taking an enterprise risk management approach does not in any way lessen the importance of traditional and integrated responsibilities, such as managing an insurance portfolio or effectively resolving claims to protect an organization's value.

Regardless of where enterprise risk management is initiated within an organization or its strategic purpose, the risk management function's role and responsibilities have been altered to reflect greater visibility with a broader span of focus and value. The broader span demands that risk management practitioners view risk in an entirely different way: a way that crosses silos, builds internal alliances, exhibits flexibility, expands to include emerging risks and enhances the strategic decision-making capability of the individual organization.

Critical to that end are building alliances with internal risk-related functions that also have the unique responsibility of understanding all that makes up the enterprise. Key among those is the internal audit function.

The Roles and Responsibilities of Internal Audit Related to Risk Management

In 1999, The IIA approved the contemporary definition of internal auditing as a component of the *International Standards for the Professional Practice of Internal Auditing (Standards)* to reflect the profession's global reach. More specifically, this updated definition explains internal auditing as, "an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes."

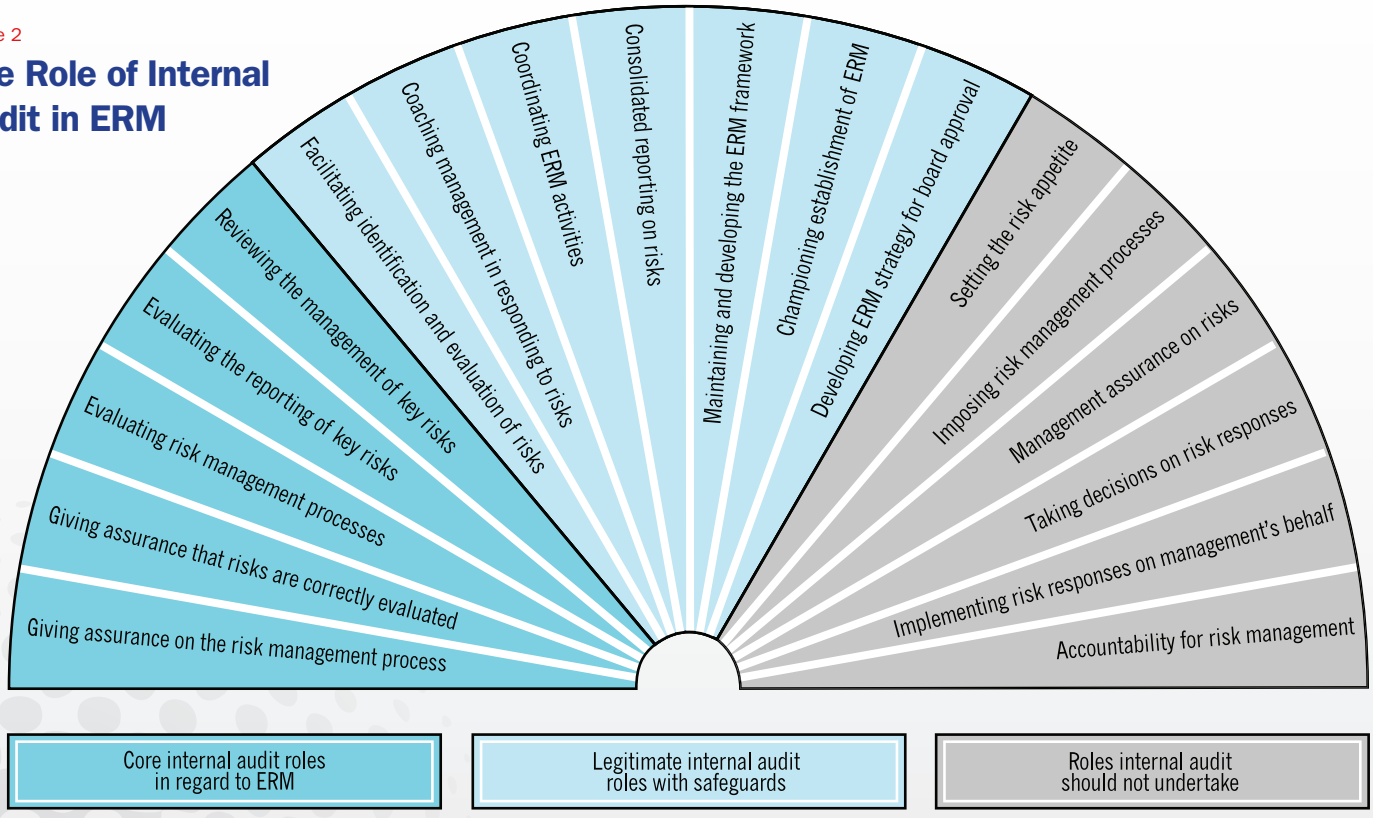
Specific to risk management, a position paper developed by The IIA's UK and Ireland affiliate in 2003, "The Role of Internal Auditing in Enterprise-wide Risk Management," defines the assurance and consulting roles an internal audit activity should and, as importantly, should not undertake to best protect internal audit's needed independence. At the heart of the position paper—whose adoption is "strongly recommended" as guidance by The IIA—is an 18-element "fan" graphic depicting the "core roles" of internal audit vis-à-vis enterprise risk management (Figure 2). The graphic also depicts "legitimate" roles for internal audit, provided appropriate independence safeguards are present. And finally the fan depicts roles that should not be undertaken except under extraordinary circumstances. "The key factors to take into account when determining [the appropriateness of] internal auditing's role are whether the activity raises any threats to the internal audit activity's independence and objectivity and whether it is likely to improve the organization's risk management, control, and governance processes," the paper explains.

The core roles of internal audit, the left third of the fan, are assurance activities; practicing in accordance with the *Standards* requires performing at least some of them. The most overarching of these five roles are evaluating and then providing stakeholders with assurance on the adequacy of the organization's overall risk management processes. Other important high-level roles are reviewing and subsequently evaluating the reporting on the organization's management of key risks.

The paper notes that, under the *Standards*, internal audit "should perform at least some" of the seven risk consulting services depicted in the center section of the fan,

Figure 2

The Role of Internal Audit in ERM



possibly including championing the establishment of ERM and developing and maintaining an ERM framework. "The internal auditor's expertise in considering risks, in understanding the connections between risks and governance, and in facilitation means the internal audit activity is well qualified to act as champion and even project manager for ERM, especially in the early stages of its introduction," the paper says. "As the organization's risk maturity increases and risk management becomes more embedded in the operations of the business, internal auditing's role in championing ERM may reduce. Similarly, if an organization employs the services of a risk management specialist or function, internal auditing is more likely to give value by concentrating on its assurance role than by undertaking consulting activities."

The paper stipulates that there are six roles internal audit should not undertake except in highly unusual circumstances —in a very small business, for example—because they are board and/or management responsibilities. These six roles, depicted in the right third of the fan, notably include setting the organization's risk appetite and making decisions on appropriate risk responses.

PART 2: WHY COLLABORATE?

Given the different historic roles and perspectives on risk management it should come as no surprise there could easily be confusion about the roles of the respective functions when it comes to enterprise risk management (ERM). What does ERM mean? Who should lead it? How do both functions fit into the equation? How can internal audit both assist and independently evaluate risk management activities? The fact that these questions continue to be asked highlights an apparent role confusion which, in some organizations, has hindered the collaboration between these two functions. Differing perspectives and terminology create challenges that can become problematic. For example, each discipline may choose different ways to express the concepts of inherent and residual risk.

The good news is that many organizations are overcoming these issues and realize that well-coordinated risk management and internal audit functions are required to support management and the board in effectively managing risk to achieve business objectives. To further illustrate how these two functions have been continually converging on a common view of risk and risk management, enterprise risk management definitions offered by RIMS and The IIA both describe a comprehensive approach in using ERM to achieve organizational objectives:

RIMS: *Enterprise risk management is a strategic business discipline that supports the achievement of an organization's objectives by addressing the full spectrum of its risks and managing the combined impact of those risks as an interrelated risk portfolio.*
www.rims.org/resources/ERM/Pages/WhatisERM.aspx

The IIA: *Enterprise risk management is a structured, consistent and continuous process across the whole organization for identifying, assessing, deciding on responses to and reporting on opportunities and threats that affect the achievement of its objectives.*
www.theiia.org/guidance/standards-and-guidance/ippf/position-papers/

Appropriately, RIMS defines ERM as a discipline while The IIA defines it as a process, since risk practitioners guide ERM practices for their organizations and internal auditors typically assess the ERM process. However, these two definitions reveal how similarly risk managers and internal auditors are thinking about enterprise risk management today. It does not stop there, either. Both risk management and internal audit professionals are using specific risk management standards, such as ISO 31000:2009, and guidance documents, such as The IIA's International Professional Practices Framework (IPPF), the Committee of Sponsoring Organizations of the Treadway Commission (COSO) ERM framework, the Open Compliance and Ethics Group's Red Book and others to help their organizations manage risk as well as audit those activities. Using a risk management standard or guidance documents and adapting the respective principles into the organization's culture and processes is one key to effective risk management. In RIMS' 2011 executive report, "An Overview of Widely Used Risk Management Standards and Guidelines," the reviewers found that the primary challenge is in harmonizing approaches and blending the "siloed" strategies through common elements, such as ERM adoption, process management, risk appetite management, root cause discipline, uncovering risks, performance management and business resiliency as found in the RIMS Risk Maturity Model (RIMS RMM).

In issuing this joint report, RIMS and The IIA demonstrate that the two disciplines are more effective working together than separately, especially when there is a common understanding of each other's roles. In Part 4, the report provides practical case studies highlighting four organizations in which these two functions are collaborating well together, albeit in different ways. Since there is still a lot of good work yet to come from many organizations on this front, this joint report should serve as a vehicle to learn from those who are leveraging the benefits of effective collaboration and in turn have elevated their organization's risk management capability.

The case studies spotlight Cisco Systems, Hospital Corporation of America (HCA), TD Ameritrade and Whirlpool Corporation. Although each of the case study organizations has structured its internal audit and risk management functions differently, certain common and effective collaborative practices emerged, resulting in recognizable value. These practices are illustrated in a number of the four case studies explored later.

- **Link the audit plan and the enterprise risk assessment, and share other work products.** Provides assurance that critical risks are being identified effectively.
- **Share available resources wherever and whenever possible.** Allows for efficient use of scarce resources, such as financial, staff and time.
- **Cross-leverage each function's respective competencies, roles and responsibilities.** Provides communication depth and consistency, especially at the board and management levels.
- **Assess and monitor strategic risks.** Allows for deeper understanding and focused action on the most significant risks.

PART 3: THE VALUE OF COLLABORATION

Risk practitioners and internal auditors are being asked by their organization's stakeholders to collaborate in order to increase the value they collectively bring to the organization. Although some organizations are well down this path, many are just starting. When the internal audit and risk management functions think of themselves as being complementary, they will work more effectively together to increase the overall value they bring to the organization. The following analysis illustrates how each company's program addressed each of the key collaborative practices.

Link the Audit Plan and the Enterprise Risk Assessment, and Share Other Work Products

Perhaps the two most notable products of internal audit and risk management functions are the risk-based audit plan and enterprise risk assessment, respectively. The audit plan defines the scope of work for the internal audit function over a given time period while the risk management function's enterprise risk assessment, is designed to get a sense of the risks facing the organization and call attention to the most severe risks that require management's focus. Very often, these two products are refreshed formally on an annual cycle, and informally more frequently, to keep up with the changing business environment.

While only one of our case studies, HCA, conducted a single, joint enterprise risk assessment, all linked their respective risk-based audit plans with the findings of the enterprise risk assessment.

On linking the audit plan and the enterprise risk assessment:

"In addition to integrating ERM risk considerations into our annual risk assessment process, an improvement we've introduced over the last few years is to show the linkage between the audits on our audit plan to the related primary ERM category. This linkage highlights in a tangible way the integration between the audit and risk management functions."

-Irene Corbe, Whirlpool

Cisco uses its consolidated enterprise risk assessment and internal audit's annual risk assessment to drive its 18-month audit plan. HCA includes a slide in its annual audit plan presentation to the audit committee that maps the top 10 risks surfaced through the ERM process to the audit plan. TD Ameritrade leverages what it learns from the risk management framework in building its annual audit plan. Whirlpool's internal audit team uses the enterprise risk assessment to inform both its annual risk assessment process, as well as the linkage contained in its audit plan.

There is tremendous value in sharing ERM results with internal audit so that these considerations can be factored into the audit plan. In addition, discussing the risk-based audit plan with the risk management team provides insights garnered from different perspectives on organizational governance and enterprise oversight. Over time, this approach adds value by eliminating redundancies in identifying critical risks to the organization, produces a common and aligned view of the organization's risk profile, and helps to instill a consistent risk management vocabulary.

Furthermore, sharing the work products of the internal audit and risk management teams at the planning, in-progress, and final-product stage, such as audit reports or risk modeling, can highlight areas of mutual interest, increase awareness and lead to action. For example, Whirlpool's practice of sharing audit reports has enabled its risk management team to "go back and influence risk mitigation activities."

Share Available Resources Wherever and Whenever Possible

Nearly all the case study organizations cited an efficiency value gained by leveraging the capabilities of their respective risk management and audit teams. At HCA, the ERM function, which has a staff of three, utilizes the company's 140 internal auditors and access to other governance participants for ERM purposes as needed. By using a single straightforward annual risk assessment process, HCA benefits from a consistent and aligned risk profile across a diverse and geographically dispersed environment. Internal audit provides resources and absorbs costs whenever risk management needs to draw on them.

> **On sharing available resources wherever and whenever possible:**
>
> "Working closely together multiplies the capabilities."
>
> -Philip Roush, Cisco Systems

Scot Schwarting, Whirlpool's director of risk management says, "My first year, I was able to get out to maybe 50 people. Now it's 150 because we are working jointly" by tapping into the reach of the approximately 60 internal auditors Whirlpool has around the globe. Irene Corbe, Whirlpool's vice president of internal audit, periodically is called upon to assist risk management's efforts, "Leveraging my global internal audit team is a very cost effective way to validate risk mitigation activities and helps Scot get a more realistic picture of the status, much more than he would be able to glean through e-mail or phone calls."

Philip Roush, Cisco Systems' vice president of governance, risk and controls, sees "a lot of synergy" rather than conflict as he "multiplies capabilities" among his 55-member internal audit and four-person ERM staff.

Although not specifically cited, a by-product of such resource sharing is that the approach calls for both functions to bring their specific areas of expertise to the table. This fosters a common understanding of risk management as both a discipline and a process that focuses on the achievement of an organization's objectives.

Cross-Leverage Each Function's Respective Competencies, Roles and Responsibilities

While efficiencies can be gained as noted above, all four organizations were unanimous in the value gained in increased communication when each function leverages the other's role. Cisco's Roush counsels collaboration "in a very significant way because there are so many points of intersection." Through the ERM process and collaborative discussions of its risk and resiliency operating committee, Cisco gets a broad view of the strategic-level thinking around risks. With business owners assigned for each risk, ERM and internal audit work together to track, monitor and report progress. Risk-related activity by management is included in the briefing material for all board meetings.

> **On cross-leveraging competencies, roles and responsibilities:**
>
> Now that [enterprise risk management] has assumed most of the "middle of the fan" responsibilities… internal audit … take[s] on an assurance and attestation, as opposed to consulting and partnering, role in risk management."
>
> -Michael Head, TD Ameritrade

At HCA, the ERM function facilitates the ERM process. The outcomes are reported jointly by ERM and internal audit to line management, interviewees, senior executives, the audit committee and the full board. HCA believes that the direct linkage with internal audit helps foster the perception that ERM is independent, objective and highly professional.

While many organizations have written charters or mandates for internal audit, TD Ameritrade has developed a formal risk management charter to define risk management roles and responsibilities. With this structure in place, the internal audit team at TD Ameritrade intends to provide assurance—for the first time—of risk management's effectiveness based on the ISO 31000 standard.

Whirlpool confirms that both internal audit and risk management learn new things and provide a wealth of risk- and control-related information that increases the effectiveness of both functions when they leverage each other's roles with open communications. Each reviews and learns from the other's reports. Together, they spend time with Whirlpool's executives and the executives' teams on risk-related issues.

An important outcome from this increased communication at the outset, whether formally as is done at TD Ameritrade or more informally, is developing a common risk language and framework. Truly leveraging not only the respective roles and

responsibilities but the skills and knowledge each discipline brings to the table, creates value that is more than just the sum of the two parts and provides consistent communication —especially at the board and executive levels.

Assess and Monitor Strategic Risks

RIMS and The IIA both have spent a considerable amount of time promoting how important it is for their members to help their organizations better manage strategic risks. Whether one defines strategic risk as significant risk that takes several years to develop, a threat to one or more of the organization's strategic objectives, a risk inherent in a strategy, or an event that can wipe an organization off the proverbial map, there is one critical commonality: organizations fear these types of risk the most (usually for good reason) and they typically are not sure how to manage them.

On assessing and monitoring strategic risks:

"Conducting monthly meetings with [enterprise risk management] has greatly enhanced our internal audit function's understanding of Whirlpool's overall macro risk profile."

-Irene Corbe, Whirlpool

Cisco uses its enterprise risk assessment to get a broad view of strategic-level thinking around risks that are not likely to change very often. Progress in managing the 20 most significant risks is tracked on a maturity model. At HCA, strategic risks also are surfaced in its enterprise risk assessment process. The leader of the ERM and business continuity functions reports to the CEO regarding strategic risks. TD Ameritrade's executive level risk committee, which is sponsored and chaired by the chief risk officer, meets quarterly to conduct strategic risk analyses, complemented by subsidiary subcommittees focusing on specific risks. A separate board risk committee provides oversight. Risks identified through Whirlpool's enterprise risk assessment interview process are rated, ranked and assigned one of five categories, including strategic. Whirlpool's key risks are owned by its executive committee.

Although each organization approaches strategic risks a little differently, these practices illustrate why it is important for both risk management and internal audit functions to stress the importance of proactively assessing and monitoring strategic risks, and recommend methodologies to manage them. As defined in RIMS 2011 whitepaper, "What is SRM?," strategic risks are those internal or external uncertainties, whether event or trend driven, which impact an organization's strategies and/or the implementation of its strategies. There is guidance available from RIMS, The IIA, and other sources, such as Dr. Mark Frigo and DePaul University's Strategic Risk Management Lab, on how to approach strategic risk management assessments.

In the 2011 IIA Research Foundation paper, "Internal Auditing's Role in Risk Management," author Paul Sobel encourages internal auditors to "evaluate strategic risks, such as whether management has comprehensively identified key strategic risks; developed prudent risk management techniques to address those risks; and established sufficient monitoring of strategic risk "signposts" to identify risk occurrences in time to take the appropriate actions." This position is complementary to the responsibilities of the risk management function for identifying key risk metrics and/or indicators to assist the responsible board committee and senior management in fulfilling their risk management responsibilities. As internal audit offers assurance as to management's effectiveness regarding strategic risks, the risk management function can provide the techniques and methods for management to be most effective.

Since the strategic risk management discipline is still evolving, risk management and internal audit should see each other as allies to bring attention to this topic and value the other's input on how to assess, respond to and monitor these types of risks.

The Value of Assessing Interrelated Risks

Not all risks are easily auditable, nor do they have just one owner. Cisco's Roush appreciates that "there are cross-functional issues that have risks associated with them, and such risks often do not have a particular sponsor or home." And, because certain risks are not easily or readily auditable, they sometimes do not populate internal audit plans, even when these plans are risk-based.

By working jointly with risk management, a much larger risk portfolio emerges. Risk areas may be uncovered in the "white spaces" that do not have a readily identifiable owner or associated control function. Risks that are categorized in one way, such as a compliance risk, over time may in fact become a strategic risk if not properly managed. Effective collaboration between risk management and internal audit can better identify these "white spaces," proactively fill them, and provide boards, audit committees and executive management better levels of assurance on the overall risk management program. Through collaboration, potential gaps are more effectively uncovered, assessed for interrelationships and managed to meet stakeholder expectations.

PART 4: COLLABORATION IN PRACTICE

The remainder of this report highlights four organizations that have benefited from coordination between their internal audit and risk management functions with respect to enterprise risk management. By telling their stories in their own words, the companies can serve as examples to consider when planning a constructive and mutually beneficial relationship between risk management and internal audit.

Cisco Systems

Networking equipment and services company Cisco Systems, Inc. is primarily aligned functionally rather than by business line or geography, as is typical of enterprises of its size, diversity of market offerings and extended global reach. Consequently, Cisco has become uncommonly adept at identifying and mitigating cross-functional risks, says Philip Roush, vice president of governance, risk and controls, who oversees the organization's internal audit, enterprise risk management (ERM), investigation, ethics and policy teams.

Take, for example, Cisco's innovative risk and resiliency operating committee (RROC). "Some people see a conflict between ERM and audit," says Roush. "I actually see a lot of synergy." Working closely together multiplies the capabilities of the 55-member internal audit and four-person ERM staff. Similarly, the highly collaborative RROC is made up of Roush and the vice presidents of the organization's treasury, security, operations, engineering and supply chain functions, as well as representatives of 17 activities that, Roush says, "have a high degree of focus on risk management." In Cisco's ERM governance hierarchy, the RROC is situated below the executive sponsors of ERM—the chief operating officer, the chief financial officer and the chief globalization officer—who, in turn, are positioned beneath the organization's board of directors, its audit committee and its CEO.

"What we found over time is there are cross-functional issues that have risks associated with them, and such risks often do not have a particular sponsor or home," says Roush. When such an issue is identified, the RROC constitutes a working group comprising staff with passion for and some involvement in it. The working group's mandate is to develop a plan to resolve the issue or, at least, appropriately manage related risks. The RROC then "challenges or blesses the proposal, figures out where any required funding needs to come from, and puts it into action," says Roush. Some issues that come before the RROC are long term, such as business resilience, for example, while others are "quick hits," such as pandemic or volcanic activity that may disrupt operations in a particular location.

RROC members do not "feel we can be prepared for every risk, and we don't try to go out and necessarily identify a lot of low-probability, high-impact, black swan issues," says Roush. What the RROC does try to do collectively is develop a series of playbooks so that when issues and risks of similar natures arise, the organization will know how to handle them effectively and promptly. The RROC and the ERM and audit staffs currently are developing a playbook for elevating and resolving compliance issues enterprise-wide. "Historically we've had a process for this, but it is not as repeatable and mature as we want it to be across the 100-plus countries where we operate," he says.

Other elements of Cisco's ERM governance process are consistent with leading practices. The organization conducts a top-down enterprise risk assessment (ERA) every two years. "We interview half a dozen board members, all of senior management starting with the CEO and his direct reports, and a cross-section of senior vice presidents and vice presidents," says Roush. Through this process, they get a broad view of the strategic-level thinking around risks, such as disruptive competition, for example, that are not likely to change very often. The risks surfaced by the ERA are assigned owners and risk management activities are monitored by Roush's staff. Progress in managing the 20 most significant risks is tracked on a maturity model ranging "from where we are today to where we want to be as an organization," says Roush. "If the responsible risk owner has not taken action on their risks that need addressing, the ERM and internal audit teams inquire why this is the case and highlight the status to senior management and the audit committee as appropriate.

The executive sponsors of the ERM process meet quarterly to review the process and discuss emerging risks and new initiatives. ERM updates are provided at each of Cisco's six yearly audit committee meetings and covered in depth at two of them. ERM activities are on the full board agenda on a periodic basis, but risk-related activity by management is included in the briefing material for all board meetings.

Internal audit conducts its own risk assessment (ARA) annually. It includes input not only from the strategic thinking of directors and senior executives consulted in the ERA but also the risk-related thinking of vice presidents, directors and managers of the day-to-day operations of the organization. It covers many of the tactical elements and changes occurring within the organization—for example, establishing a new commissions program or implementing an update to the enterprise resource planning (ERP) system. The consolidated ERA and ARA drive Roush's 18-month audit plan, which is refreshed annually, and the audit committee discusses the findings of the resulting audit work at each meeting.

Roush advises all chief audit executives (CAEs) "to care about risk because your board and audit committee care about it." CAEs who do not directly manage the ERM staff or others in the organization who are involved with risk "should be collaborating with them in a very significant way because there are so many points of intersection." Establish a formal collaboration process "because otherwise you can lose momentum as people rotate in and out" of their roles, he says.

Hospital Corporation of America

The ERM program of Hospital Corporation of America (HCA) is a logical and seamless extension of the organization's long-standing risk-based auditing process, observes Joe Steakley, senior vice president, internal audit and risk management services. More than a decade ago, Steakley and his internal audit staff began systematically documenting management's perception of the external and internal risks to HCA, which now comprises more than 160 hospitals and 100 free-standing surgery centers locally managed in 20 states and England. The leading risks that surfaced during this process became the principle focus of the annual internal audit plan. Steakley soon realized, however, that "some risks we really couldn't address from an audit standpoint still needed to be looked at by the board and the CEO and addressed by the risk owner." Steakley and his then-director David Hughes filled this gap with a relatively simple, cost-effective ERM program that largely remains in place to this day.

The program, initially imbedded within internal audit, is grounded in principles embraced by many leading organizations in recent years. The board establishes the risk appetite, and its various committees oversee management's efforts to identify and manage risks within that appetite. The ERM function facilitates the ERM process and reports on the outcomes to line management, senior executives, the audit committee and the full board. However, the day-to-day operation of HCA's ERM program is distinctive.

Hughes, whose current title is assistant vice president, ERM and business continuity planning, reports directly to Steakley, who in turn reports functionally to the audit committee and administratively to the CEO. This hierarchy enables Hughes, who has a staff of only three, to utilize Steakley's 140 internal auditors and his access to other governance participants for ERM purposes as needed. "We work very, very collaboratively together," says Hughes. Interestingly, Hughes also reports to the chief medical officer about physical risks, which are managed through HCA's business continuity function. The chief financial officer retains responsibility for risks arising from compliance with the U.S. Sarbanes-Oxley Act and other applicable laws and regulations and for financial reporting. "This is kind of an unusual organizational structure, but it works well here," says Hughes.

HCA's straightforward annual risk assessment process comprises telephone or in-person interviews of over 90 individuals including board members, the CEOs and CFOs of HCA's more than 16 divisions, and other high-level executives whose ongoing responsibilities or initiatives are closely linked to the company's strategies. The process also consists of surveying approximately 170 individuals including the CEOs, COOs, CFOs and chief nursing officers of a sampling of about 50 hospitals. All participants are asked the same questions, which Hughes notes are very high level. These questions include:

- What are the three business risks, in priority order, the company faces over the next two years that could have a significant adverse effect on the company's ability to achieve its strategic and/or financial objectives?
- What are some of the things the company is doing to help manage/mitigate each of these risks?
- In your opinion, are these risk mitigation strategies effective?

"We provide a risk universe of approximately 150 risks to everyone we interview or survey to give them a starting point in articulating their concerns," says Steakley. This risk universe, originally developed three years ago on the basis of data collected in previous surveys with input from risk-management experts at North Carolina State University, is updated periodically to reflect changes in the company and its business environment, he adds.

Interview participants also are told in advance that their responses will be awarded 10 points for enterprise-wide risk ranking purposes, assigned as follows: Five to the top risk they perceive, three to the second-highest, and two to the third-highest. Steakley says that a number of CAEs at other companies who he interacts with do not rank their risks by order of importance. "That's a big miss," he says. "All risks are not equal and if you don't rank your risks, how can you rationalize that you're spending the right amount of time on them?"

Steakley says that the first few years HCA conducted its risk-ranking exercise, "things weren't very well aligned. The people in the hospitals were saying things different from corporate management and the board." But a decade into this process, the same risks tend to surface in most interviews and the top four risks now account for about 80% of the total risk-ranking points. "The last several years the responses have been very well aligned," he says. "Last year, in fact, the board was even aligned with what the hospital staffs were saying. I believe this is a real testament to the maturity of our process."

After survey responses, which are not attributed to individual participants, are compiled and cross-tabulated by Hughes's staff, he and Steakley report the results to the board, the audit committee, senior management and interview participants. "We end up with an ERM briefing book with an executive summary. The farther back you read, the farther the information drills down," says Hughes. Steakley also has a slide in his annual audit plan presentation to the audit committee that maps the top 10 risks surfaced through the ERM process to the audit plan. Overall, Steakley notes, the principle underlying all reporting is to keep it at a strategic level. "Our approach is to try to keep it simple," he says. "If we go talk to people at HCA and get too granular, we will lose them quickly."

Hughes and Steakley agree that although the ERM function does not need to report to the CAE, this arrangement has many advantages. Hughes says, "The combined structure and approach allow ERM to remain lean. For example, internal audit provides resources and allocates costs whenever risk management needs to draw on them." More important in most organizations, Steakley says, is that a direct linkage to internal audit will help foster the perception that ERM is independent, objective and highly professional. "People know internal audit is the only department in the company that doesn't have a dog in any hunt and will be totally neutral to what people say," he says. "Also, people know internal audit reports directly at the board level without management pressure. They are confident they can talk freely because they trust we are going to keep it confidential and report it as we hear it. It's a way for them to get their voices heard without standing up at an executive meeting and saying we don't agree with all of this." Steakley admits, of course, that if internal audit is perceived poorly in the organization for whatever reason, "a negative perception of ERM may exist as well."

Steakley says in conclusion that structure and process are less important than action. "If you're a company that's struggling with risk management, do something," he says. Hughes adds, "When you're starting out, keep it simple." After all, HCA started simple, has kept it simple, and has achieved leading practice status as an outcome.

TD Ameritrade

TD Ameritrade's ERM program, though still maturing, already is sophisticated and capable. But this was far from the case in 1999, when founder and current board chairman J. Joseph Ricketts hired Michael Head to lead the internal audit activity of the online brokerage firm. "ERM as we know it today was nothing more than Joe's vision back then," says Head, whose current title is vice president and managing director of corporate audit. In fact, among Head's modest early objectives were establishing risk-based internal auditing and, beginning in 2001, evaluating the organization's quarterly efforts to self-assess, test and publicly disclose the effectiveness of key internal controls over financial reporting.

Prior to 2000, risk management was embedded in disconnected silos across the enterprise, and Ricketts wanted that changed, Head says. Senior management recognized that moving from this state to true ERM "is a journey and not something they could implement and have up and running effectively in six months," he recalls. Organizations that have attempted a quick-fix approach to ERM adoption, Head says, "have either failed altogether or wondered why ERM remains an add-on and not part of the fabric of how managers think and address risk on a day to day basis."

In 2001, Head teamed with the CFO to select TD Ameritrade's first chief risk officer. The new CRO, who reported administratively to the CFO's chief accounting officer, reported functionally to the audit committee. During the next several years, the organization methodically adopted tenets of the broad ERM framework developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). Meanwhile, administrative responsibility for internal audit was shifted from the chief administrative officer to the general counsel to safeguard internal audit's independence when evaluating the effectiveness of the organization's systems of internal control, including the evolving risk management activities. At this juncture, Head says, ERM had matured to a "repeatable process that functioned fairly well." However, he says, it still was widely perceived within the organization as a "necessary evil."

By 2008, the CRO and his team had established a common language and framework to identify and rank risks across the company. It was at that point, Head says, that the TD Ameritrade board said, "OK, we've made some good progress, but we can't continue to do the same thing and expect ERM to rise to the next level" of sophistication and effectiveness. One of the board's chief concerns at the time was that ERM activity was taking place too low in the governance structure to achieve the maturity that the directors, the CEO and the executive officers of the company desired. "The CRO was not sitting in the C-suite, and the audit committee was saying we fulfill our normal duties and focus on risk management as an add-on," says Head. "Directors said that was not how we thought it would be when we went in the direction" of ERM.

The board hired a consulting firm to evaluate the state of affairs, effectiveness and the actions needed to achieve leading-practice status, Head says. The consultant recommended, and the board approved, formation of a board-level risk committee, the elevation of the CRO position to the senior

executive level, the development of a formal risk management charter and a switch from the COSO to the ISO 31000 risk management framework. "The consultant saw no contradictions" in the two frameworks, Head says, but judged that "ISO 31000 provides the broadest possible view of risk management while COSO ERM is more narrowly tied to the evaluation of systems of internal control." Next year, Head notes, internal audit will provide assurance for the first time of risk management's effectiveness vis-à-vis the ISO 31000 standards.

David Kim was retained as the new C-level CRO and risk and assurance functions throughout the organization—including the old risk management organization and internal audit—began reporting to him administratively in matrix fashion. Joseph Iraci was hired as managing director of corporate risk management to play a lead role in growing and operating the ERM program. Prior to that time, Head says, internal audit had many "middle of the fan" (see Figure 2 on page 4) responsibilities for risk management. Now, he says, Iraci's staff has assumed most of these duties, "which has allowed internal audit to take on an assurance and attestation, as opposed to consulting and partnering, role in risk management." This arrangement, he says, "is working well from a working together and sharing perspective. Some of the power of having the same administrative report in the C-suite is you get consistent direction."

Iraci's corporate risk management group continued to grow, and the corporate risk, business continuity and corporate insurance teams currently total 17 people. "This growth reflects risk management's increasingly broader role and expanded day-to-day support of TD Ameritrade's varied business units," says Iraci. For example, Iraci's team got involved in emerging product reviews and helping business leaders develop key risk indicators and risk dashboards. "Joe already has taken our ERM program way beyond where it was before," says Head.

Although Head works in TD Ameritrade's Omaha, Nebraska headquarters facility and Iraci works in a corporate office in New York, they coordinate their work and collaborate closely. This includes meeting face-to-face about three times monthly. "I have more interaction with Mike and his team than I typically have had with internal audit functions elsewhere during my career," says Iraci, who previously worked in several global financial services organizations and a federal regulatory agency. For example, he says, although the risk management and internal audit teams perform risk assessments independently, they share results and discuss any inconsistencies. But what is more important, says Head, is that both operate within a common risk definition and framework. Across the top of this framework are eight risk categories and down the side are so-called risk assessable business units, starting with the C-suite and cascading downward. "We leverage what we learn from Joe's risk management framework in building our annual audit plan and he, in turn, considers our information" in determining the organization's top risks, Head says. "The degree of collaboration is great."

TD Ameritrade now has an executive-level risk committee, sponsored by the CEO and chaired by the CRO, that meets quarterly to conduct strategic risk analyses. There is a subsidiary subcommittee for each of the organization's eight risk categories, including regulatory, disclosure, technology, human capital and brokerage operations. These subcommittees meet at least quarterly. Iraci's team supports each of these groups, and a member of the internal audit team attends each meeting to facilitate a free flow of information between the groups.

The board's risk committee meets quarterly to review the work of the management committees. The audit committee also meets quarterly to review the organization's overall control structure; the work of internal audit, and any risk arising from TD Ameritrade's 10-K and 10-Q filings with the U.S. Securities and Exchange Commission. To ensure cohesion and identify potential responsibility overlaps, the chair of the board risk committee attends audit committee meetings and vice versa. Moreover, once yearly the two committees hold a joint meeting, during which annual reporting and planning takes place. Head says that "the full board also is very active in overseeing risk management because, after all, it drove the current changes to the structure."

"I think the governance structure now is where it needs to be and has the staff support it needs," says Head. "Now it's a matter of building out the tools and tweaking them to meet the risk information needs of the organization. We've clearly made a lot of progress, but we're not all the way there." However, Iraci adds, "What I do think clearly works well now is having very open communications between internal audit and risk management."

Whirlpool Corporation

The ERM and internal audit functions of global home-appliance manufacturer Whirlpool Corporation do not have the same organizational structure as some organizations where the top executive of the ERM function reports administratively to the internal audit activity or vice versa. Though both functions at Whirlpool report functionally to the audit committee of its board of directors, vice president of internal audit Irene Corbe reports administratively to the CFO while director of risk management Scot Schwarting reports to the vice president of the organization's treasury function. However, Corbe and Schwarting, both of whom joined the company about five

years ago, maintain a remarkable and enviably collaborative professional relationship that both agree adds substantial value to their respective activities.

"Conducting monthly meetings with Scot has greatly enhanced our internal audit function's understanding of Whirlpool's overall macro risk profile," says Corbe. "As we scope our audits, we specifically consider how those risks are impacting our internal control environment and are able to tailor the audit procedures accordingly. This approach results in driving more comprehensive risk coverage for Whirlpool and helps us to identify gaps earlier. I have found that by having a regular dialogue with Scot, we are able to share process and business knowledge to assess how risks are changing and have an open dialogue on how we can best optimize and leverage our efforts. With the complexity and volatility of today's business environment, staying on top of and identifying emerging risks is a real challenge. At the end of the day, collaborating with ERM has made our audits that much more meaningful for the business and for our senior leaders."

Schwarting adds that his recurring interactions with Corbe provide him with a wealth of risk- and control-related information that help increase the effectiveness of the overall ERM program. "I would tell risk managers that if they get the opportunity to work with internal audit, seize it," he says.

Meeting monthly is just one of many efforts by Schwarting and Corbe to ensure risk management and internal audit activities are complementary and supplementary in nature. Whirlpool's risk management team is comprised of Schwarting, four direct reports and a small number of risk management specialists embedded in the supply chain, procurement and other business functions. In addition to ERM, the risk management group is responsible for business continuity, claims and insurance portfolio management, as well as loss prevention. Each year, this team, in partnership with Corbe's staff of internal auditors around the globe, conducts an enterprise risk assessment comprised of written, telephonic and in-person interviews of selected executives. "My first year, I was able to get out to maybe 50 people," says Schwarting. "Now it's 150 because we are working together and sharing information" with internal audit.

Major ERM risks identified through the interview process are rated, ranked and assigned one of five categories: enterprise, strategic, operational, financial and compliance. An owner is identified for each risk commensurate with its potential impact on the organization, and risk mitigation strategies and goals are developed. This information is vetted during several meetings with members of the senior management team and then presented to the audit committee and the board of directors as needed.

The process does not end there, however. Whirlpool's key ERM risks are owned by its executive committee. Consequently, Schwarting says, "besides reporting to the board and the audit committee, Irene and I spend a significant amount of time with our executives discussing their respective risks and even more time working with their direct reports to identify projects and actions to achieve mitigation goals and objectives."

Since 2009, the risk identification and ranking processes as well as the monitoring of mitigation plans have been facilitated by a software application procured by internal audit two years earlier. "The tool itself is fantastic because we can slice, dice and run different risk scenarios and show how certain risks might impact different parts the organization," says Schwarting. Joint use of the software has enabled internal audit and risk management to develop and maintain a common risk vocabulary. "Our ERM program has matured a lot over the past four years in terms of what we gather, why we gather it and what we do with the information, and I anticipate that will continue," he says. "We want our ERM process to be something that's live and active and working well for Whirlpool."

"My team uses qualitative and quantitative information, including ERM data, and we run it through a very robust model that helps us identify the highest risk locations, processes and areas and this becomes the basis for our annual internal audit plan," adds Corbe. "In addition to integrating ERM risk considerations into our annual risk assessment process, an improvement we've introduced over the last few years is to show the linkage between the audits on our audit plan to the related primary ERM category. This linkage highlights in a tangible way the integration between the audit and risk management functions."

Schwarting says one practice he's "found particularly helpful" is receiving copies of every audit report. This has often helped his team better understand a business process, thereby giving ERM "the ability to go back and influence risk mitigation activities." Another practice that "has been extremely helpful and has produced very good results," he says, is Corbe's willingness to let him periodically leverage internal audit's global footprint of approximately 60 auditors for ERM purposes. Each geographic region has its own top risks, a microset of Whirlpool's overall risk universe. "If I learn at a monthly meeting that Irene has an audit going on in Asia, for example, then I might ask Irene's group to go in and validate that the work's been done, that it's functioning and that it is meeting designed expectations," says Schwarting.

"We don't change our internal audit scope or planned procedures related to our scheduled audits as a result of

requested consulting on behalf of ERM," Corbe says, "and such requests tend to be very targeted. However, leveraging my global team is a very cost effective way to validate risk mitigation activities and helps Scot get a more realistic picture of the status, much more than he would be able to glean through e-mail or phone calls."

"I think the collaboration between ERM and internal audit the last few years has been phenomenal," says Schwarting. "The level of communication between our two groups allows us to plan and reorganize ourselves when things come up that need to be tackled. "I don't think we've ever stepped on each other's toes. I think we just have a good working relationship in general, and if I have something on my mind, I will speak to Irene directly and vice versa." Corbe concurs that "the partnership between internal audit and ERM is definitely working well for our company. Perhaps it is due to our corporate culture, but Scot and I plan to continue to strive to find ways to improve our process and figure out additional ways that we can collaborate and make our alliance stronger to deliver even better results for Whirlpool and its investors."

CONCLUSION

RIMS and The IIA agree that how risks are assessed and managed can materially affect how an organization is positioned to achieve its objectives. Historically, the risk management and internal audit disciplines have approached risk considerations from their respective independent viewpoints. At times, this disconnected approach has created confusion at best and conflict at worst. The IIA and RIMS believe that collaboration between the risk-related disciplines of internal audit and risk management can lead to stronger risk practices in meeting stakeholder expectations. The two functions make a powerful team when they collaborate and leverage one another's resources, skill sets and experiences to build robust risk capabilities across their organizations.

Leading organizations have discovered efficiencies, better decision-making and improved results by forming strong alliances between the risk management and internal audit functions. In highlighting four case studies, this joint report identified four fairly common practices, although each organization approached them in different ways:

- Link the audit plan and the enterprise risk assessment, and share other work products
- Share available resources wherever and whenever possible
- Cross-leverage each function's respective competencies, roles and responsibilities
- Assess and monitor strategic risks

More importantly, from the descriptions provided, the authors recognized certain value that the organizations gained from the collaborative activity:

- Assurance that critical risks are being identified effectively
- Efficient use of scarce resources, such as financial, staff and time
- Communication depth and consistency, especially at the board and management levels
- Deeper understanding and focused action on the most significant risks

Additionally, we believe that effective collaboration and open dialogue results in a more robust view of the entire risk portfolio.

As a single starting point that can benefit any organization, RIMS and The IIA recommend that risk management and internal audit leaders and teams commit to frequent, open communications, using multiple methods, ranging from formal correspondence to ad hoc touch points. Open communication is a common thread in all of the case studies, even though the channels may vary. A number of the organizations mentioned that they conducted regularly scheduled in-person meetings, others that they corresponded in writing, while some communicated telephonically. Most mentioned multiple methods. What is evident is that the commitment to communication enabled the common practices and understanding described in the report.

We hope that this joint report serves as a vehicle to learn from those who have figured out how to collaborate effectively, consistent with their respective organization's unique situations, needs and cultures, and in turn helps you to enhance your organization's overall enterprise risk management capability and value.