# Internal Auditing Around the World

*Internal Audit's Role in Leading Enterprise Risk Management Initiatives*

VOLUME VII

protiviti®
Risk & Business Consulting.
Internal Audit.

*Powerful Insights. Proven Delivery.®*

# Introduction

> "Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."
>
> Committee of Sponsoring Organizations of the Treadway Commission (COSO), Enterprise Risk Management — Integrated Framework, 2004

Over the years, we have written extensively on enterprise risk management (ERM) and stressed the importance of organizations establishing the oversight, control and discipline to drive continuous improvement of their risk management capabilities in a changing operating environment.[1] These issues have always been on the minds of board members and management. However, at no time in recent memory has sound ERM guidance been more critical for business success. Amid perceived risk management failures in the wake of the recent global financial crisis and its lingering consequences, increasing regulatory scrutiny and growing technology risks, boards are mandating that ERM be a high priority in their organizations. As a result, the internal audit functions at the 10 companies profiled in this year's *Internal Auditing Around the World* are taking steps to integrate risk management into their processes for formulating and executing their audit plans.

The companies featured in this book – whether headquartered in Canada, China, France, Italy, Singapore or the United States – are truly international in the scope and size of their operations. They are among the industry leaders in e-commerce, financial services, hospitality, Internet, manufacturing and distribution, paper, retail, telecommunications, and utilities. As to be expected, the internal audit approach to ERM is often targeted to address the unique industry and geographical challenges each organization faces.

At Sequana, for instance, the need to be in compliance with French financial regulatory requirements caused the internal audit team to focus on updating and rebuilding its risk mapping strategies. Not surprisingly, given the ever-multiplying risks in the Internet industry, salesforce.com adopted ERM because it believes trust and security are paramount to its business. And at Visa, a global financial services company, product innovation must be on an accelerated timetable to stay competitive – but not at the expense of ERM, which needs to be effective and efficient to ensure risks are identified and managed.

A careful study of the profiles reveals certain common practices that these organizations employ to make ERM a strategic imperative. Above all, regular communication with senior management is considered pivotal to the success of any ERM initiative. Among the key risk management areas these internal audit functions are addressing: regulatory compliance, managing financial risks, establishing specific risk programs, coordinating ERM with corporate strategies and redefining risk methodologies.

[1] *Guide to Enterprise Risk Management*, *Enterprise Risk Management in Practice*, *Board Perspectives: Risk Oversight* and other publications discussing risk management are available at www.protiviti.com.

For the interviewees, their commitment to ERM in terms of time and resources is an investment that is already yielding dividends. One major benefit is being able to reassure both internal and external stakeholders that critical risk management concerns are being addressed. This, in turn, can help satisfy board mandates, possibly even allowing the pursuit of opportunities that come with substantial risk; enhance an organization's reputation, which may encourage analysts to recommend investing in the company; facilitate a favorable outcome to the rating process by financial agencies; and achieve greater customer satisfaction through increased confidence that key risks associated with the company's products and services are reduced to an acceptable level, among many other advantages.

Most important, though, we believe strongly that ERM has to "work" and not just be another "tick the box" exercise. This means fewer surprises and that when surprises do occur – as they certainly will – there is a plan or response already thought through for that particular event, increasing the company's preparedness for the unexpected. A working program also means that everyone in an organization understands the concepts of risk, shares a common vocabulary and sees risk assessment, management and mitigation as part of their job, which allows them to perform better and achieve better results. ERM should also provide for consistent and bigger bonuses, as plans will be achieved and exceeded more frequently because of better risk knowledge and more robust plans and actions taken around those things that can get in the way of meeting the organization's objectives. And finally, a working ERM program means that more "opportunities" are uncovered, discussed and acted on that will yield new products, markets, better profitability and a more satisfied workforce. Internal audit *can*, *should* and *must* play a role in getting ERM to work and evolve to higher levels of effectiveness over time.

The risk landscape has changed dramatically since 2005, when Protiviti published the first volume of *Internal Auditing Around the World*. Each volume in this series has been well received, and we are optimistic that these insightful profiles will assist boards of directors, C-level executives and internal audit professionals worldwide in improving risk management in their organizations. We believe the most successful companies will set the trends in integrating risk management into their core management processes and advancing risk metrics, measures and monitoring.

Protiviti Inc.
June 2011

## Acknowledgements

Protiviti is grateful to the interviewees and companies for generously sharing with us their ERM initiatives and other risk management best practices. Special thanks to Nancy Hala for conducting the interviews and writing the profiles featured in our book. We wish to acknowledge the leadership of The Institute of Internal Auditors (IIA) as the preeminent global authority for internal audit. As a longtime IIA Principal Partner, we know the value of this leadership and are proud of our affiliation with The IIA.

# Table of Contents


**Company Headquarters** — China
**Number of Countries Operates in** — 11
**Number of Employees** — 20,000+
**Industry** — E-commerce
**Annual Revenues** — RMB¥5.6 billion
**Annual IA Operating Costs/Budget** — US$1 million – US$5 million
**Number in IA Function** — 23
**Number of Years IA Function Has Been in Place** — 7
**IA Director/CAE Reports to** — Audit Committee

Note: All of the above information is accurate as of December 31, 2010.

*"Aligning risks with strategy is especially critical in enterprise risk management, so resources will not be wasted on unnecessary efforts."*

*– Kevin Au Yeung*

# Enterprise risk assessment and management at Alibaba.com

Alibaba.com is a global organization specializing in e-commerce for small businesses. Founded in 1999 in Hangzhou, China, Alibaba.com supports online business transactions for buyers and suppliers worldwide by providing a global trade platform for importers and exporters; a Chinese platform for domestic trade in China; and, through an associated company, a Japanese platform for facilitating trade to and from Japan. It also offers a transaction-based wholesale platform on a global site geared for smaller buyers seeking fast shipment of small quantities of goods.

More than 61 million registered users (as of December 31, 2010) in over 240 countries and regions leverage Alibaba.com, which also offers business management software and Internet infrastructure services for businesses across China, and educational services for enterprise management and e-commerce professionals. Additionally, Alibaba.com owns Vendio and Auctiva, providers of third-party e-commerce solutions for online merchants, and has offices in more than 70 cities across China, India, Japan, Korea, Europe and the United States.

Kevin Au Yeung is a senior director of the organization's Group Internal Audit function, which consists of 23 individuals divided into three teams: information technology (IT) audit; finance and operations audit; and integrity and compliance. The three teams report to Samuel Yen, a vice president in the finance function of Alibaba Group, parent company of Alibaba.com. Alibaba Group also owns Taobao, the largest online retail website in China, and Alipay, the leading third-party online payment platform in China.

The primary goal of the Group Internal Audit team at Alibaba.com is to secure assurance for financial statements and operational efficiencies. An equally important goal is to promote risk awareness and encourage an ethical working environment. "Alibaba Group companies operate in an ever-changing, dynamic environment, so our job is to provide a significant amount of audit and consulting services with the various business operations throughout our organization," Yen says.

## Enterprise risk assessment

The Group Internal Audit function at Alibaba.com takes a risk-based approach to audit plans, examining the organization's business strategy and financial statements and conducting operational audits based on what they find. "We began implementing enterprise risk assessment for Alibaba.com, following

the COSO model, in 2007," Au Yeung says. "We used the Protiviti Risk Assessment model, which contains 80 subsections within its modules. With this as our platform, we asked management to help determine the organization's top 10 risks over a 12-month period, as well as the likelihood and impact of those risks."

Between 60 and 80 senior managers filled out a questionnaire that focused on company strategy and risks with the potential to undermine the organization's goals. "Aligning risks with strategy is especially critical in enterprise risk management (ERM), so resources will not be wasted on unnecessary efforts," says Au Yeung. "Training sessions with small groups were conducted to clarify the purpose of the risk assessment and nature of the survey questions. This encouraged our managers to bring up concerns and ask questions about the risk assessment process. Conducting this training was a great opportunity to raise risk awareness of our company's operations."

Au Yeung continues, "With our understanding of the COSO model and the Protiviti tool, we felt we had the requisite expertise and knowledge to conduct our risk assessment. We began in 2007, and continued in 2008, conducting the risk assessment for the second time. We used the same methodology and questionnaire, but the results startled us: The top 10 risks were the same. We realized we had to change our approach; we could not merely repeat our efforts and end up with the same risks identified every year. We needed to help management solve the existing issues and move on. We needed an evolving road map."

Alibaba.com's CEO suggested that Group Internal Audit introduce the top 10 risks to the management team at a monthly meeting, asking the managers to vote on the top three risks from that list. The top three risks identified were:

- **Human resources** – accessing optimal talents
- **Customer needs** – identifying what Internet users want and need
- **Technology** – identifying risks associated with technological innovation

After the top three risks were targeted, a vice president with relevant knowledge and expertise was delegated as an "owner" for each risk area. "This was our jumping-off point in 2008," says Au Yeung. "We tried to figure out how to achieve a level of comfort with these risks. We had to understand how to measure them, and how to train employees to monitor and mitigate them."

## ERM: The next step

Group Internal Audit followed up this effort by allocating a percentage of its resources to ERM in 2009 and 2010. "Developing measurable and practical actions to address risks is a huge challenge in our fast-changing industry and market," says Au Yeung. "Identifying the top three risks meant involving three different groups of operational management. The role of the internal audit team was transformed to keep management focused on developing the necessary actions to address these risks, so we can ensure management actions are being properly measured and followed."

According to Yen, "The Chinese market, especially the e-commerce sector, evolves quickly. We need to revisit our work plan frequently to update the key risks and challenges ahead, as well as our corresponding actions, in order to help management to capture market opportunities and address the risks at the same time. With ERM, we are in constant communication with management with regard to the right approach and plan for monitoring and mitigating risks."

Yen points out that with any enterprise risk initiative, it could take as long as two to three years to make progress in China's environment. "In 2010, for example, we managed to invite the vice president responsible for customer needs to talk to the audit committee about the inherent risks in that area, as well as the company's related actions. The whole concept behind enterprise risk assessment and management is that we want Alibaba.com's leadership team to be aware of risks and how the company reacts to them."

The Group Internal Audit team helps Alibaba.com's audit committee monitor ERM progress on a continuous basis through corporate governance meetings. As a result, the respective risk owners are able to update the audit committee members periodically on the status of identified and evolving risks.

## Benefits of ERM

The primary benefits of Alibaba.com's overall ERM strategy include:

- **Increased risk awareness:** Encouraging employees throughout the organization to think about risk in their day-to-day operations, and ensuring all levels of management are more aware of the risks that can impede strategic goals.
- **Capturing opportunities:** In a fast-evolving industry, the "flip side" of risks assessed and identified by ERM often represent opportunities. Group Internal Audit's program welcomes all input from the organization, which helps senior management identify opportunities it had not previously considered.
- **Risk education:** Increasing education throughout Alibaba.com and its parent company, Alibaba Group.

"ERM is sponsored by senior management, which emphasizes the importance of the program and sets the right tone at the top," says Au Yeung. "With proper training from Group Internal Audit on the program and the process for voting on top risks, we believe we can continue to develop managers' risk awareness. Through subsequent internal audit projects in different functions, we leverage this established platform to communicate to other key staff about risks and controls. We are still in the infant stage, but we hope ERM will become a common language throughout the organization one day."

Yen and Au Yeung agree that ERM provides the Group Internal Audit function with a systematic approach for evaluating and improving the effectiveness of risk management, control and governance. "The risk assessment aspect of ERM connects the company's challenges with overall corporate strategies," says Yen.

He adds, "For example, our recent project on how we handle customer complaints resulted from the enterprise risk assessment. Traditional financial statement risk assessment could hardly identify such an area, but enterprise risk assessment can point the Group Internal Audit team in this direction. Being an independent team, we can evaluate the effectiveness of cross-department and cross-function processes and provide impartial recommendations on ownership, program structures and resource allocations. Senior management welcomed the results because it helped them to address how efficiently they handle core customer needs. This type of project demonstrates how the value of an internal audit function can go beyond evaluating internal control effectiveness in typical business cycles."

Having ERM does not mean companies are "bulletproof" – and there are many other management endeavors to address risks. For example, it is important to build integrity and ethical behaviors with the right tone from the top to enable employees to align their efforts with the company's mission and vision.

ERM is still evolving at Alibaba Group and throughout China as well. Although Au Yeung and Yen believe they are among the earliest participants in ERM for "homegrown, startup companies" in China, they recognize that they are not yet truly able to evaluate their success. However, they say they do believe the process represents an excellent platform for education about risk awareness and for providing a sense of ownership for employees.

**Company Headquarters** — Singapore
**Number of Countries Operates in** — 15
**Number of Employees** — 15,800
**Industry** — Financial Services
**Annual Revenues** — S$7.1 billion
**Annual IA Operating Costs/Budget** — › US$15 million
**Number in IA Function** — 130
**Number of Years IA Function Has Been in Place** — At least 40
**IA Director/CAE Reports to** — Audit Committee Chairman

Note: All of the above information is accurate as of December 31, 2010.

*"We span boundaries to promote risk and control learning throughout our organization ... Ours is not a culture where we avoid sharing information."*

*– Lim Him Chuan*

# DBS applies holistic view of risk to its Group Audit approach

DBS Group Holdings (DBS) is one of the largest financial services groups in Asia. Established in 1968 as the Development Bank of Singapore, it was a catalyst for economic development during that nation's early years of independence. Today, DBS is one of the largest financial services groups in Asia, providing a full range of services in consumer, SME (small and medium enterprise), and corporate banking activities across Asia and the Middle East. With one of the highest credit ratings in the region, DBS serves customers in 15 markets and six key geographic areas – Singapore, Hong Kong, China, India, Indonesia and Taiwan – and has a regional network spanning more than 200 branches and over 1,000 ATMs across 50 cities. Among the various accolades received, the bank was named by *Global Finance* as the "Safest bank in Asia" for both 2009 and 2010.

Lim Him Chuan is the head of Group Audit for DBS, and Yik Yeng Yee leads the Audit Management and Practices team, which is part of the overall Group Audit function for DBS. Based in Singapore, she reports to Him Chuan, who in turn reports functionally to the audit committee.

"From 1968, when DBS was founded, until 2000, the bank had a very conventional audit function," explains Him Chuan. "DBS was a development bank, and only existed in Singapore, so our business was not complex. As the bank expanded into Hong Kong and the Southeast Asia region, it became more complex in its products and business lines; for example, we overhauled our trading business. Because of the change in the bank's risk profile, the Group Audit function had to respond. From 2000 onward, there was a significant effort to transform the Group Audit function into one that is more risk-based. This transformation did not happen overnight. It took a sustained, concerted effort by a group of dedicated audit staff working with key stakeholders to change the direction, strategy, methodology, operating and engagement model, as well as resourcing in the department."

The primary role of Group Audit is to help both the bank's board of directors and its executive management team meet the strategic and operational objectives of DBS. Group Audit provides an independent appraisal of the adequacy and effectiveness of risk management, control and governance processes.

As the last line of defense within DBS' risk control framework, Group Audit assists the bank in meeting its objectives by:

- Performing effective and efficient audits to foster a robust control culture within DBS
- Promoting cross-unit, cross-location operating effectiveness, also known as "boundary spanning"
- Being a source of talent and future leaders for DBS
- Making DBS a great place to work

## Boundary spanning

"Mission and vision drive what we do, and are fundamental to our culture," says Him Chuan. "Everyone in the bank who works at or above the assistant vice president level must attend a course on how to manage people effectively and to be emotionally engaged to contribute to DBS' ambition to become the Asian Bank of Choice for the New Asia. The term 'boundary spanning' is borrowed from that course. We span boundaries to promote risk and control learning throughout our organization. For instance, when I see problems in Singapore, I will share the issues and lessons learned at least monthly with all of the bank's teams and countries. This standard practice helps promote risk awareness on critical issues and supports our growing bank. Ours is not a culture where we avoid sharing information."

Cross-unit risk control learning means that one business unit, such as corporate banking, can and should share experiences and best practices on risks and controls with other business units – for example, consumer banking – where appropriate. Group Audit engages all of the bank's business and support units, framing the audits it conducts as case studies, looking for root causes and ways to standardize audit practices, and using the cases as opportunities for risk and control education. Group Audit distributes a monthly *Audit Watch* bulletin to bank management and the audit committee, which outlines emerging issues as well as lessons learned.

"We use our *Audit Watch* bulletins as talking points when meeting with stakeholders," says Yeng Yee. "We also provide training for staff members throughout the bank, to promote boundary spanning. In a way, Group Audit consists of not only 130 auditors, but also many 'volunteers' who help spread risk awareness throughout the bank. As we train staff and new managers, we educate them about the risks and controls in the bank and share lessons learned from control gaps and failures previously highlighted."

Group Audit is also a source of talent and future leaders for DBS. "We invite employees to join us for formal job rotation," Him Chuan says. "We also host guest auditors who are assistant vice presidents and above and can work with us for two weeks at a time. This program is driven from the top, so it is highly recognized and appreciated throughout DBS. Both the job rotation and guest auditor programs are win-win solutions to enable Group Audit to not only become scalable and be equipped with certain industry and functional expertise, but also to transfer high-performing individuals back into the business and contribute to a more control-conscious organization."

## Health checks and credit risk review

Since 2005, Group Audit has helped the consumer banking business unit form its own health check teams. These teams conduct detailed examinations of each branch's compliance with established sales and service procedures, which in turn helps management reinforce supervisory monitoring over the branches.

With the consumer banking health check teams firmly established in the bank's major locations, Group Audit was able to revamp its approach to auditing branches. Instead of the conventional branch audits on a rotational basis, Group Audit now focuses on auditing the health check teams, augmenting that work with some routine audits of control units in consumer banking, as well as continuous monitoring of the branches. "This has worked so well that we have extended continuous monitoring," Him Chuan

explains. "While it was once only executed by the consumer audit team, continuous monitoring is now an integral part of our audit methodology."

Group Audit also performs credit risk reviews. "We visit the business units in multiple locations to challenge the credit quality of our loan portfolios," says Him Chuan. "This had previously been under the purview of the bank's Risk Management group, but by 2009 we brought credit risk review teams into Group Audit. Today, we have derived synergies with the credit risk review teams. Now, when we conduct audits, we are able to perform more integrated reviews on an end-to-end basis on our loan portfolios. So, on top of credit processes, we also cover business risk and credit quality to provide the audit committee and management a more complete picture of the risks."

## Audit Risk Assessment (ARA)

"Group Audit has a comprehensive view of the risks in each business and support unit within DBS," says Him Chuan. "We have a good, independent view of the key areas of concern and developments within the bank."

Group Audit's efforts have enabled the audit teams to evaluate the risks for all the auditable entities in DBS; each auditable entity is assigned a color rating that determines the audit frequency. It uses its Audit Risk Assessment (ARA) methodology to assess auditable entities on an annual basis. Developed in-house in 2004, and recently refreshed, ARA was designed specifically to meet Group Audit's needs. It is supported by a proprietary system application known as Audit Exchange (AX), which automates the entire audit risk assessment, planning, resourcing and execution activities.

"The whole ARA process involves the auditors having to review nine identified risk types," says Him Chuan. "The definitions of these nine risk types are identical to what the bank's Risk Management team uses – it is the same risk language. The unique aspect of ARA is the way we assess each auditable entity. We spoke to many people in the bank, as well as studied regulatory requirements and practices of other institutions about the types of risk we should explore."

Each of the nine risk types in ARA carries equal weight, and for each auditable entity, an assessment of the level of risk (between one and six) against each of the nine risk types is placed on the Y-axis. On the X-axis, control effectiveness is scored (between one and five). The control effectiveness score is based on previous audit ratings, continuous monitoring and engagement with stakeholders. Group Audit plots that score of the risk level and control effectiveness onto a heat map, which in turn determines the frequency of the audit.

"We find this methodology to be quite rigorous," Yeng Yee says. "We have a system (AX) that needs to capture an explanation for each score given. Out of a few hundred auditable entities, each is scored this way. It is a granular and detailed exercise, and it drives our annual audit plan. We also produce a write-up for each business unit that outlines the details of what we plan to do for the year and why. Getting to this level of granularity means we can more efficiently manage our time."

According to Him Chuan, "Our audit methodology and approach gives Group Audit a holistic view of the bank's risks so that our audit projects can be conducted in the most effective and logical manner possible. We hope to be one of the change agents to help the bank mold and propagate the risk and control culture through our boundary-spanning activities. For all of this to happen, we are fortunate that we have a clear tone from the top, with a strong mandate for what we are doing. And that drives us to aim to become the most respected and admired internal audit function in Asia."

**Company Headquarters** — United States
**Number of Countries Operates in** — 45
**Number of Associates** — 85,000
**Industry** — Hospitality
**Annual Revenues** — US$3.5 billion
**Annual IA Operating Costs/Budget** — Prefer not to disclose
**Number in IA Function** — 16
**Number of Years IA Function Has Been in Place** — 4
**IA Director/CAE Reports to** — Audit Committee and CFO

Note: All of the above information is accurate as of December 31, 2010.

*"The support we get from the CFO, CEO and business unit leaders drives the success of our eRM process."*

*– Jim Werner*

# 'eRM' at Hyatt

Hyatt is a global hospitality company, headquartered in Chicago, with 453 properties in more than 45 countries (as of December 31, 2010). For the past 50 years, Hyatt has managed, franchised, owned and developed Hyatt-branded hotels, resorts, and residential and vacation ownership properties around the world. The company's business units are segmented into three sectors: North American properties, international properties, and real estate and development interests. Hyatt is a US$3.5 billion company with more than 85,000 associates.

Jim Werner has been the vice president of internal audit at Hyatt for three years. He oversees 16 auditors and functionally reports to the audit committee of the board of directors with an administrative in-company reporting responsibility to the company's chief financial officer (CFO). The internal audit function provides independent and objective audit services for Hyatt, engaging management to add value by improving the company's overall effectiveness.

## The Risk Council

In November 2007, Werner was hired to create the internal audit function as part of the preparation for Hyatt becoming a public company in November 2009. Prior to this time, Hyatt's audit and compliance responsibilities were dispersed among hotel, internal control, and IT auditors throughout the company. Werner's role was to coordinate those efforts and build an internal audit function able to meet the demands of a public company. In July 2009, the Risk Council was formed – a coordinated group of senior leaders who manage people throughout Hyatt and evaluate risk. "We viewed the Risk Council as an effective governance tool for bringing together all the assessment efforts we needed to develop a robust internal audit plan," Werner says.

Hyatt's enterprise risk management program is denoted with a lowercase "e" – eRM – to signify the company's approach to risk management is not meant to layer on an additional oversight function. "We do not have a chief risk officer," Werner says. "Both the Risk Council and eRM were piloted in early 2009; the Risk Council formulates eRM itself and drives the process."

The Risk Council coordinates the assessment of Hyatt's risks and helps identify and evaluate the controls and other mechanisms that should be in place to mitigate those risks. The team is comprised of 20 representatives from operational business units, as well as corporate functions such as the corporate controller, treasurer, vice president of risk management (the corporate insurance function), vice president of public relations, the chief information officer, and representatives from legal and marketing.

"Our creation of the Risk Council and eRM stemmed from a need to develop a robust risk assessment to support an internal audit plan," Werner says. "Based on my past experience, I knew I needed the right information to achieve the most accurate and comprehensive risk assessment possible. I presented our CFO, who is the sponsor of the Risk Council, with a proposal to create a risk governance program for the company that would also fulfill my requirements to establish a risk assessment for my internal audit plan."

The Risk Council begins with a hospitality risk universe, a template of 61 risks for the hospitality industry, tailored specifically for Hyatt. "This Hyatt Risk Universe gives us the outline we need to conduct a formal, annual, bottom-up assessment of risk. We vote on the impact and likelihood of the risks, ranking them one through five, and document our findings so that we can give them to the executive team. After we vote and reach a consensus, we ask the outliers to explain their viewpoint. After the discussion, we ask the group if it changed their point of view. We occasionally revote some of the risks."

Werner and his internal audit team focus their risk management efforts primarily on those risks with the highest impact and likelihood. They develop a matrix that distinctly outlines the risks to Hyatt and the controls that mitigate them. They also produce a risk deck for the executive team, which is a summary of what the Risk Council sees as the key risks of the company and how well they are managed, as well as the actions that should be taken to further mitigate emerging risks, such as changing business factors or the economic downturn.

"This is our annual approach," Werner says. "We do not perform bottom-up voting every quarter, but we do go through the same process in which we ask for environmental changes or new business initiatives and update our priority risks accordingly. Everything is documented for the executive team's review. This is our eRM process."

Werner serves as the coordinator on Hyatt's Risk Council. Working with tools provided by Protiviti, he completes the documentation, disperses it, and then gathers feedback from members to make sure all aspects of the business are well represented. "I am one of several spokespeople to the executive team," he says. "I am also responsible for sharing internal audit's view of the risks."

Hyatt's CFO is the sponsor of eRM. "The support we get from the CFO, CEO and business unit leaders drives the success of our eRM process," Werner says.

## eRM benefits

The Risk Council also plays an important role in evaluating whether Hyatt's publicly disclosed risk factors require adjustments on a quarterly basis. According to Werner, the Risk Council is an excellent forum for discussing and communicating information about risks. "We have designed eRM to be a robust function of assessment that provides management with the mechanism it needs to ensure the most significant risks are covered," he says.

Before the advent of the Risk Council, risks were identified; however, the Risk Council gives Hyatt the structure it needs for management to say that the organization has robustly considered risks, identified the critical ones, and acted on them. Additionally, eRM helps the board of directors execute its oversight role, providing a focused and coordinated view that enables the board to confirm that its actions are facilitating adequate risk coverage.

"When you are talking about the biggest risks to the organization, it is unlikely you are talking about things you have never noticed before," Werner says. "However, our Risk Council and eRM approach have given us a much-needed framework for bringing greater attention and more efficiency to managing and understanding Hyatt's risks."

## Communication and feedback

Werner likens the Risk Council to the United Nations, where representatives come with their concerns about their respective countries and leave with pertinent information that they communicate to their groups. "Everyone feels our approach is very helpful," he says. "This has been both a learning and teaching experience. Our challenges are that we're trying to educate people, while at the same time keeping them focused on our most significant areas of risk."

According to Werner, the small "e" in Hyatt's eRM effort is all about significance. "We robustly assess our risks on an annual basis, and update quarterly on our most key risks. Some risks are not as significant as others, or they are just very well managed," he says. "But the point is that we do not have an additional layer of risk documentation and reporting on these lesser risks." This commonsense approach has helped make eRM at Hyatt a companywide success.

**Company Headquarters** — Canada
**Number of Countries Operates in** — 1
**Number of Employees** — 5,717
**Industry** — Utilities
**Annual Revenues** — CAD$5.1 billion
**Annual IA Operating Costs/Budget** — US$1 million – US$5 million
**Number in IA Function** — 12
**Number of Years IA Function Has Been in Place** — 12
**IA Director/CAE Reports to** — President and CEO

Note: All of the above information is accurate as of December 31, 2010.

*"Our management genuinely believes that you cannot manage well without ERM; it pervades everything we do."*

*– John Fraser*

## Complementary roles: Audit and ERM at Hydro One

Hydro One Inc., owned by the province of Ontario, Canada, is strongly influenced by government policy. Yet it is operated like a public company with substantial bonds rated by rating agencies and requirements to file public documents. Even though its operations are limited to the province of Ontario, Hydro One is one of the largest electricity transmission and distribution companies in North America, with about 29,000 circuit-kilometers of transmission lines, about 1.2 million electricity distribution customers, CAD$15.8 billion in assets, CAD$5.1 billion in revenue, and 5,717 employees. It also transmits electricity from generating stations to remote rural communities in northern Ontario that are not connected to the transmission grid.

Hydro One's corporate structure consists of a holding company with four key subsidiaries, one being a major operating subsidiary: Hydro One Networks Inc., which plans, builds, operates and maintains the company's transmission and distribution network; Hydro Telecom Inc., which is focused on fiber-optic capacity and telecommunications; Hydro One Remote Communities Inc., which operates and maintains the company's generation and distribution assets in Northern Ontario for remote communities that are not on the electricity grid; and Hydro One Brampton Networks Inc., which distributes electricity within an urban center outside of Toronto.

John Fraser is the Senior Vice President of internal audit for Hydro One, as well as its Chief Risk Officer (CRO). "I wear two hats," he says. "In 2000, I was assigned the dual roles of audit and enterprise risk management (ERM). When I address the company's board of directors and management teams, I explain which hat I am wearing at that time. Whenever I wear my 'risk hat,' I am purely a facilitator to management."

Fraser reports administratively to Laura Formusa, the President and CEO of Hydro One Inc., and reports functionally to the Audit and Finance Committee. His internal audit staff consists of 10 veteran internal auditors with experience in finance, operations, information technology, safety, environment and electricity operations. Internal audit and ERM are executed as separate functions. "There is full cooperation, but separate staff," Fraser says.

## High-risk environment

The internal audit team's mandate is to audit the high-risk areas of Hydro One's group of companies. "We are a mature internal audit group whose strategy is to be a best practice function," explains Fraser. "Every member of our staff is a professional internal auditor and as a team, we strive for continuity. Hydro One is a dynamic organization that experiences significant change, so our risks are high and our challenges can be dramatic. We have one of the most modern operating centers in the world for controlling electricity and we are a leader in smart meter technology implementation. We also just implemented a major computer system (SAP) that revolutionized how we process data. Employing cutting-edge technologies like these is necessary to seize new opportunities and stay competitive, but they come with substantial risk."

Fraser and his team have implemented ERM practices into their operating structure only partially. "We implemented these practices to the extent we felt was appropriate," he says. "We have been considered leaders in ERM for about 10 years. Today, we are re-examining our ERM status and plan to move forward even more strongly by adding a full-time staff member dedicated to this process."

## ERM – getting started

In 1999, the Hydro One management team regarded ERM as a desirable best practice. However, while it was assigned to the strategic planning function, there was no real forward movement with the initiative. That year, the company was set up to issue an initial public share offering; from a governance point of view, a well-defined ERM function became an imperative. Later that year, after Fraser had been leading the internal audit function for about six months, he agreed to take on ERM as part of his job. To avoid potential conflicts, he decided to run ERM as a separate product line. He inherited two staff members who managed the ERM process for Hydro One until 2003.

"During that time, we immersed management in ERM by conducting risk workshops focused either on a specific type of risk, such as environmental or human resources risk, or on a major project or business unit," Fraser says. "In these workshops, we educated and engaged management about the levels of risk criteria, risk ratings, action plans required, and more. They became excited and engaged by the initiative. They understood the value ERM brought to line management and we started receiving many requests for additional risk workshops."

When Fraser's first ERM manager retired, he promoted an internal audit manager to that role. "He had the charisma and skills to do the job," Fraser says. "Now, internal audit uses risk profiles for audit planning and the ERM staff interviews the audit staff to help identify risks and control quality." However, to ensure the units are complementary but still independent, internal auditors cannot view risk workshop results without the permission of line management – and ERM team members do not conduct audits.

## ERM timeline and ownership

In the beginning, Fraser and his team drafted a policy to obtain senior management's buy-in to ERM. They conducted a pilot risk workshop to demonstrate that they could quickly deliver value and clearly stated the corporation's strategic objectives as they related to ERM's mission. "We drafted and validated risk criteria as a basis for identifying and prioritizing risks," he explains. "We set a goal of conducting five workshops in 2000 and then ended up doing about 10. Over the next three years, we conducted between 40 and 50 workshops annually. This was a major success, as almost all of the workshops were requested by line managers."

One challenge they faced was redefining risk methodologies, since some existing theories were not appropriate, such as terms like "inherent risks." "Instead of inherent risk, we now use the term 'largest credible risk' to describe the impact of an event or incident in practical terms in the event that key controls fail," Fraser says. "This differs from inherent risk because we believe that inherent risk is too

theoretical and seldom experienced in reality – in other words, a situation where there is zero control. Also, ERM ensures that managers must be forthright and declare the risks they face, otherwise they will not be funded – 'no risks' equals 'no funds needed' to meet business objectives. This solves the problem faced by many ERM implementers who have managers reluctant to admit to having any significant risks in their functions."

By the end of 2003, Fraser and his staff felt they had achieved their objectives and decided to enter maintenance mode. Fraser says, "I decided we would do nothing further with ERM, but rather just keep going with what we had in place, allowing our ERM staff to move on to other roles within the company. Thankfully, they returned to help me with risk workshops and profiles whenever practical, despite having other full-time accountabilities."

Ultimately responsible for ERM is Hydro One's board of directors, which receives and reviews the risk criteria, ERM policy and framework, and risk profiles, and participates in risk workshops. Senior management owns the accountability for risk management and related processes, and is responsible, along with line management, for the achievement of strategic objectives. Fraser's ERM role is to help ensure alignment and prioritization of identified risks and resources required to address the risks. Strong support from Hydro One's President and CEO is critical, according to Fraser, who says that without it, ERM success would not be achievable. "It is our current President and CEO who encouraged the full board to allow me to run risk workshops with them to demonstrate our methodology," Fraser says. "This is now a standing annual event on the board's agenda. We have come a long way since 2000, when the then-chair of the Audit and Finance Committee asked why I was bringing risk matters to the committee. In those days, he considered risk to be a management responsibility only."

## Benefits: A tale of two companies

One of the most important benefits of implementing ERM at Hydro One is that the company has adopted a common understanding of risk criteria and priorities. The allocation of resources to tackle the most significant risks is clearly communicated. Another benefit is that the company has gained respect and credibility from rating agencies and investment bankers, who recognize that Hydro One keeps abreast of its risks and avoids surprises. "Good ERM allows internal audit to focus on the priorities and not waste resources on the small stuff," Fraser says.

He continues, "Let me compare two companies. In one company, there is no discussion among the board of directors, senior management and line management with regard to the company's risk levels. There is also no discussion about major problems or obstacles to strategic objectives. So, no one is talking about risks, action plans or prioritization of resources. As a result, one of the company's divisions might get a large amount of money and resources, but another with equal or bigger risks may not.

"Compare this to another company – Hydro One – where we have agreed-upon priorities of risks, conduct risk workshops to generate structured conversations about risk, and allocate resources based on the riskiest items that we face. All of this helps us to avoid surprises and reach our critical business goals."

## Tools and communication

Fraser and his teams use Resolver voting software for facilitating risk workshops and Methodware software to roll up workshop data for the risk profile. "There are several different models for ERM; my model is that I'm the facilitator. I do not make decisions or get in the way of line management," Fraser says. "For some organizations, the CRO may have a different function, such as setting corporate policy. I am an enabler rather than a doer. I help vice presidents manage, but I do not carry a big stick – only persuasion."

He continues, "The same is true with software – some software solutions claim to do everything. We use the voting software because we think structured conversations in workshops are vital. We use tools that roll up all the workshop data for corporate viewing."

The importance of the ERM effort has been communicated throughout Hydro One mainly by engaging all levels of staff in risk workshops so they have the opportunity to have a hands-on experience with the concepts, terminology and practical aspects of ERM. The message of ERM at Hydro One has also been communicated externally. In 2005, Morgan Stanley's Journal of Applied Corporate Finance featured an article, co-authored by Fraser, on the rise of the CRO and the evolution of ERM. In 2008, Harvard Business School produced a case study featuring ERM at Hydro One.

For internal audit and ERM, performance is measured against the expectations of the President and CEO and the board, what Hydro One's peers are doing, and how external experts view the company's methods. "The response has been overwhelming," Fraser says. "Our management genuinely believes that you cannot manage well without ERM; it pervades everything we do. No project manager would run a project today without using the ERM principles and conducting risk workshops. As for the internal audit team, ERM provides the framework we use to identify the areas of risk that will be factored into the risk profile and to plan annual audits to validate key controls."

The question often comes up as to whether the roles of ERM and internal audit should report to the same executive. Fraser points out that The Institute of Internal Auditors is clear about incompatible roles in its September 29, 2004, paper, *The Role of Internal Auditing in Enterprise-wide Risk Management*, and these guidelines are all in place at Hydro One. Because of the ERM implementation, and the support of a highly qualified internal audit function, Fraser believes he has achieved optimal capability for delivering excellent risk and assurance services to the board and management team at Hydro One.

**Company Headquarters** — Italy
**Number of Countries Operates in** — 40
**Number of Employees** — 60,800
**Industry** — Manufacturing and Distribution
**Annual Revenues** — €5.8 billion
**Annual IA Operating Costs/Budget** — US$1 million – US$5 million
**Number in IA Function** — 20
**Number of Years IA Function Has Been in Place** — 7
**IA Director/CAE Reports to** — Chairman and CEO of Luxottica Group

Note: All of the above information is accurate as of December 31, 2010.

*"This exercise can be seen as somewhat bureaucratic, but we feel confident that once the ERM process is fully implemented, the benefits will become clear."*

*– Luca Fadda*

## Luxottica Group – on the road to ERM

Luxottica Group is a global leader in the design, manufacture and distribution of premium eyewear, selling such well-known brands as Ray-Ban®, Oakley®, Persol and more through wholesale and retail channels. Founded in 1961 by Leonardo Del Vecchio, Luxottica, based in Milan, Italy, today has net sales of €5.8 billion, more than 60,000 employees and more than 6,000 retail locations in the Asia-Pacific region, China, Europe, North America and South Africa. In North America, Luxottica also operates in the managed vision care business through its EyeMed Vision Care division.

Luca Fadda has been the vice president of internal audit for Luxottica since May 2009. Previously, he served as an audit director for three years in the company's U.S. offices, returning to Milan in August 2008. The internal audit function at Luxottica consists of 20 professionals, with one team based in Milan, another in Sydney, Australia, and two in the United States. Fadda leads the four teams and sends a dual report to the CEO and the chairman of Luxottica Group.

The primary goals of the internal audit function at Luxottica are to help the organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes. This also helps senior management guarantee accurate financial reporting and improve the efficiency and effectiveness of company processes from both a financial and operational perspective. The four internal audit teams address more than just compliance – they must also align within the company's key strategies.

To help meet these goals, Fadda and his team have begun implementing enterprise risk management (ERM) in the organization. In 2007, they initiated a formal risk assessment process, an exercise that led to a more accurate and comprehensive audit plan. This process began with interviews of Luxottica's senior managers to identify the organization's most significant risks, the risks' owners and the mitigating activities in place.

"Last year, we decided to improve the risk management process, enhancing governance of the process and ensuring our management was more embedded in the daily activities of the senior staff," Fadda says. "We identified a chief risk and compliance officer, Valerio Giacobbi, and began building the risk management and compliance function." Like Fadda, the chief risk and compliance officer reports to the CEO, giving the relatively new ERM initiative strong sponsorship from Luxottica leadership.

In May 2010, the corporate office distributed formal communication regarding the establishment of the improved ERM approach. "Overall, the reaction was positive," Fadda says. "Individuals accustomed to these types of exercises were highly positive because they were already aware of the value ERM would bring to their work. In certain cases, this exercise can be seen as somewhat bureaucratic, but we feel confident that once the ERM process is fully implemented, the benefits will become clear."

## On the road to ERM

Luxottica decided to pursue a structured ERM approach as the company's CEO, chief financial officer (CFO) and board of directors recognized the value of having a more defined approach to risk analysis, as well as a list of the most significant and likely risks facing the company and a detailed plan for addressing them. "It is becoming ever more critical for companies to have a well-defined ERM approach," Fadda says. "For example, financial ratings agencies, such as Standard & Poor's and Fitch, frequently ask questions relating to the risk management function. Luxottica needed someone to collect all the necessary risk and control information and ensure that all risks are efficiently and effectively accounted for and addressed."

Overall, the internal audit function has been the main driver toward implementing ERM at Luxottica. "In our mind, we took the first step in 2007 with the risk assessment," Fadda says. "We worked with Protiviti to develop the methodology and risk model, which we tailored to our business, and then passed that knowledge to Giacobbi's risk and compliance team." Fadda and Giacobbi are partners in the ERM process.

According to Fadda, the plan is to roll out the new ERM approach fully in late 2011. The main challenge for implementation is that currently there is no consistent level of risk management maturity across the organization. Certain factions already fully embrace the value of ERM, while other locations are not as far down the road.

"One of our challenges is to make sure all senior management throughout our organization understand the value of this exercise," says Fadda. "We interviewed our professionals in Australia, China, Italy and North America and consolidated that information in order to maintain consistency and be positioned to report accurately and comprehensively on what we were told."

He adds, "We have found a common language with which to communicate to everyone. We rate risks based on likelihood and impact. This is always a challenge, especially if not all participants are in the same room at the same time. We also have worked hard to reach consensus. It is important to ensure that what you are doing is doable – results must be achieved in a reasonable span of time. This is the balance to find – goals and time span – while always keeping an eye on the strategic plan and linking ERM to that strategy."

Key players in the ERM process are senior managers at Luxottica's various locations, including the U.S. corporate CFO and CEO, as well as executives in the Australia and China regions. These individuals work with Fadda and Giacobbi on Luxottica's risk committee, a group that is steadily evolving.

## ERM benefits

From an audit perspective, ERM helps Fadda and his teams build more effective, risk-based, value-adding audit plans. From a companywide point of view, ERM can be a tool to further support the senior management team through its strategic decision process, helping the organization to reach its goals and create sustainable value for all the stakeholders. This process also motivates employees and leadership teams to understand the primary or perceived risks to the organization. "When you can finally have all the key players in the same room, the discussion is interesting," Fadda says. "Everyone has different viewpoints and information with regard to business processes."

ERM resonates with financial risks as well. "From a practical perspective, we have certain risks with easy-to-understand money attached," Fadda says. "For example, when you work for a company with revenues in dollars, interest rates and exchange rates are very relevant risks. Being able to manage these risks properly has a tremendous impact on the organization. When you go to the capital markets, you will obtain money at a lower cost if you can demonstrate the company uses an effective ERM process."

Activities related to ERM are communicated to Luxottica through periodic senior management meetings in the corporate office, where details are discussed and the status of the ERM initiative and goals are updated. ERM results are reported consistently to the company's board of directors, which is comprised of several committees, including the internal control committee. "We have already presented the particulars of the ERM project to the internal control committee and to the audit committee," Fadda says. "Once we have fully implemented ERM later this year, we will report everything to them."

Performance of audit work and ERM initiatives are measured comprehensively at Luxottica. The performance of the internal audit function is measured in the following ways:

- Audit plan completion – The plan is presented to the CEO and the internal control committee, who monitor the progress of the audit plan and receive updates on projects.
- Closing of findings – There is an action plan for each finding, and the closing of issues is closely monitored.
- Customer satisfaction – This is a qualitative measure; each audit client is surveyed to determine satisfaction with the audit process.
- Sarbanes-Oxley Act compliance – Fadda is the project manager and responsible for ensuring the organization is in full compliance.

ERM is evaluated on an ongoing basis in terms of its impact on certain risks – specifically, those that can be quantified (for example, the already mentioned exchange rate or interest rate fluctuation risk).

According to Fadda, Luxottica is currently exploring software tools to use in its ERM efforts. "We are still working on the software direction," he says. "We need to manage a significant amount of information. Our first step will be to finalize the organizational structure and then decide on the system and tools we will use to support it."

The expectation for a more sound ERM process at Luxottica is high. Fadda and his team are embracing the goals of better supporting senior management through the strategic planning process and providing assurance to stakeholders both inside and outside the company. Fadda adds, "We want to facilitate the growth sustainability path designed and reflected in the key milestones of the ERM plan itself."


**Company Headquarters** — United States
**Number of Countries Operates in** — Prefer not to disclose
**Number of Employees** — 5,306
**Industry** — Internet
**Annual Revenues** — US$1.7 billion
**Annual IA Operating Costs/Budget** — US$1 million – US$5 million
**Number in IA Function** — 11
**Number of Years IA Function Has Been in Place** — 7
**IA Director/CAE Reports to** — Audit Committee solid line reporting and to EVP, Legal administratively

Note: All of the above information is accurate as of January 31, 2011.

*"We face multiple priorities across the company, but ERM is a top priority."*

*– John Beeler*

## Salesforce.com uses ERM to support 'V2MOM': Vision, Values, Methods, Obstacles and Metrics

Salesforce.com is an enterprise cloud computing company that provides comprehensive customer management and collaboration applications and an application development platform to businesses of all sizes and industries worldwide. The company was founded in February 1999 and began offering its customer relationship management (CRM) application service in February 2000. In its fiscal year 2011, salesforce.com reported net revenues of US$1.657 billion, and about 92,300 net paying customers.

John Beeler has been salesforce.com's senior vice president of internal audit for more than three years. He is responsible for the company's global internal audit program and risk management process.

"Our team's performance is measured by meeting the objectives outlined each year in the company's goal-setting process, which we refer to as the 'V2MOM' process," Beeler says. "This stands for Vision – what we want; Values – what is important about it; Methods – how we achieve it; Obstacles – what prevents us from achieving it; and Metrics – how we know when we have it."

The Vision of the internal audit function is to protect salesforce.com by delivering trusted, independent assurance and consultative services to its internal customers, while also providing development opportunities for the internal audit team. The internal audit function's Values include ensuring customer success and facilitating talent development. The Methods that support the Vision and Values are:

- **Protect the company:** This is accomplished through a comprehensive global risk assessment process. Based on identified risks, salesforce.com's internal audit team develops an audit plan and executes global audits – as approved by the audit committee of its board of directors – through a deep level of engagement with the business partners during the planning, fieldwork, reporting and follow-up processes. The internal audit function partners with the business units to identify and address risks continually; in addition, it conducts investigations and other relevant projects with a similar focus on delivering effective, objective work products. Additionally, the internal audit organization partners with the company's senior management and audit committee in executing its risk management program.
- **Scale risk and compliance activities:** To scale salesforce.com's risk and compliance activities, internal audit coordinates the activities of applicable internal organizations to maximize the effectiveness and efficiency of the risk and compliance teams.

- **Enhance visibility, processes and tools:** The internal audit team evaluates whether the function is in compliance with the standards of The Institute of Internal Auditors and examines its tools and processes to ensure it supports and even augments the existing internal audit model. Beeler and his team also benchmark other internal audit organizations and leverage lessons learned.
- **Be the best place to work:** The internal audit function at salesforce.com creates an optimal workplace by providing a fast-paced learning environment for internal auditors through challenging assignments, an effective development and training program, and opportunities to move into new roles within the company.
- **Measure performance:** The internal audit team enhances their balanced scorecard and related measurements throughout the fiscal year with a focus on continuous process improvement. They incorporate other relevant metrics as necessary based on their participation in peer benchmarking forums and input from internal customers.
- **Protect leadership position:** To protect and enhance salesforce.com's leadership position in the market, the internal audit team partners and collaborates with internal clients to help them scale the company's operations. Additionally, they focus on scaling the internal processes and systems within the internal audit function.
- **Ensure customer success:** Internal audit partners and collaborates with internal clients to improve the effectiveness and efficiency of salesforce.com's processes and controls.
- **Facilitate talent development:** A key focus of the internal audit function is its ability to develop talented people who understand salesforce.com's business model, processes and systems. It works to provide opportunities for team members to grow professionally both within internal audit and other areas of the company.

The internal audit function at salesforce.com consists of 11 professionals globally, including team members who are based in international markets; all team members work together to execute audits of the company's global processes and systems. Beeler and his team report functionally to the audit committee and administratively to the executive vice president of legal.

"Over the long term, we are charged with providing assurance and recommendations to our global audit clients through financial, information technology (IT), and other operational audits and projects," Beeler says. "We also lead a comprehensive risk assessment process across the global enterprise and provide an avenue to feed internal audit talent into business process streams. We are also focused on further building upon our risk management program in our fiscal year 2012, with the support and input of our audit committee and senior management team."

## Risk management plays integral role

Given that the internal audit function provides assurance and consulting services to the organization, the company's risk management process is embedded within the fabric of its goal-setting process. "We also track the completion of audit recommendations by our client groups, those recommendations that are past due, and overall audit client feedback. These and other key measures are captured in a one-page scorecard we use to monitor our performance and the value of our audit and risk programs. ERM and internal audit have a clear linkage at salesforce.com," Beeler says.

To assist with refining ERM and the internal audit process, Beeler and his team are using an internally developed application called AuditForce – a repository and tracking system built on the company's application development platform.

The factors that led salesforce.com to adopt ERM stemmed from the nature of the business itself. "Given the type of business we are in, trust and security are paramount to our existence," Beeler says. "As part of that, internal audit performs a risk assessment process. Three years ago, the internal audit function facilitated an effort to integrate its risk assessment process, engaging many other groups, including legal, technology compliance, the Sarbanes-Oxley team and other key compliance organizations."

The internal audit function executes a global risk assessment across the worldwide enterprise, engaging in a series of interviews with senior management and focus groups with middle management. Internal audit also meets regularly to review the identified key risks, which are included in its public filings, and incorporates them into its audit plans.

## ERM encompasses a continuous improvement framework

"ERM is an ongoing process for us," Beeler explains. "Risk management has been a focus at the company prior to our public offering in 2004. Since then, ERM continues to improve each year. We face multiple priorities across the company, but ERM is a top priority."

According to Beeler, many of salesforce.com's executives are involved in ERM efforts. So far, the benefits realized from ERM include:

- Overall enhanced definition and measurement of risks within the company
- Focused execution on mitigating risks
- An internal audit plan designed to ensure that business processes and systems are managing risk effectively

"The internal audit function applies a series of risk management processes in various ways across the company," Beeler says. "Our team is always re-evaluating and pursuing additional avenues to enhance our risk management approach. We continue to learn and grow our enterprise risk management (ERM) processes. So, whether an initiative is led by internal audit, treasury, legal, IT security or other compliance teams, we are all working toward improving our risk management processes."

The internal audit team continually reassesses the ERM program, with a focus on enhancing and improving it each year. Beeler adds, "We are looking forward to a great fiscal year 2012 as we continue to evolve our risk programs. At salesforce.com, we are focused on continuous process improvement."

# SEQUANA

**Company Headquarters** — France
**Number of Countries Operates in** — 55
**Number of Employees** — 12,900
**Industry** — Paper
**Annual Revenues** — €4.3 billion
**Annual IA Operating Costs/Budget** — ‹ US$1 million
**Number in IA Function** — 5
**Number of Years IA Function Has Been in Place** — 6
**IA Director/CAE Reports to** — CEO

Note: All of the above information is accurate as of December 31, 2010.

*"Our operations must be smooth, efficient and fast. At the same time, they must be framed by proper monitoring and risk management."*

*– Alexander Danjou*

## Risk management and mapping at Sequana

Sequana Group is a leader in the paper industry with two primary business units – Antalis, a worldwide business-to-business distributor of paper and packaging materials, and Arjowiggins, a global producer of creative and technical paper.

Alexander Danjou is the group internal audit director of Paris-based Sequana and reports directly to the organization's CEO. In addition to overseeing individuals in the internal audit department, Danjou taps several outsourced resources for local language, tax and fiscal knowledge.

In 2010, Sequana realized it needed to reinforce its compliance with French financial regulations related to internal control and risk management procedures. The risk assessment and risk mapping exercise performed in 2004 for Antalis and in 2006 for Arjowiggins had to be updated and used as a framework to produce consolidated risk mapping at a group level.

To meet this requirement, Danjou and his team began focusing on updating and rebuilding their risk mapping strategies, using two key approaches:

**Fieldwork approach** – This involves extensive travel, with two teams covering two different locations within the same week. "For us to cover two entities within the same time frame, we have implemented a new tool – TeamMate – which eases the process by helping us to efficiently gather input from all relevant risk professionals, clearly communicate rationale and scope of audit, and issue the final audit report, including management's comments (remediation plans and associated timetable) within one month after the visit, at the latest," says Danjou. "TeamMate also facilitates ongoing follow-up."

**Yearly approach** – Another tool, the Protiviti Portal, was implemented in 2005 and now covers 88 percent of the organization. It includes a questionnaire that addresses 12 processes and features 302 questions that help illuminate segregation of duties and delegation of responsibilities on topics such as compliance and group control processes. "This year, we added a new questionnaire linked to corporate governance to satisfy French regulators," Danjou says.

Sourcing for Arjowiggins' manufacturing facilities is an important and potentially high-risk area of the business. "We met with the purchasing director at Arjowiggins to design a working program to make sure we put the right controls in place to mitigate risks related to sourcing and manufacturing," Danjou explains. "We also met with their human resources function for the same reason; as a result, we have a working program that ensures local job appraisal and facilitates and monitors the flow of information."

## A common view of risk

Risk management at Sequana, performed by executive managers, is driven mainly by internal data and supported by top management and risk mapping. Risk mapping provides an independent view of the company's internal control approach, which is why the internal audit function was chosen to oversee it.

"We were the natural choice, but we conducted many meetings with business leaders to get their input," says Danjou. "Some of the challenges we encountered along the way were administrative in nature, establishing all the controls necessary to mitigate risks, but ensuring that they do not get in the way of business. Our operations must be smooth, efficient and fast; at the same time, they must be framed by proper monitoring and risk management. At this point in the evolution of our risk management approach, I am certain Sequana is ready to face risk."

Risk mapping at Sequana was established in three phases:

1. **Interviewing** – gathering input about risks from more than 50 executive managers worldwide
2. **Brainstorming** – taking the 200 identified risks and reducing them to a "Top 20" list
3. **Risk mapping** – assessing the risk and drawing the chart

The risk mapping initiative at Sequana began in December 2009 and ended in June 2010. Among the Top 20 risks identified through this exercise: competition, drop in paper demand, margin deterioration, environmental disaster, loss of key people, and supply disruption.

"This risk mapping exercise provides us with a common view of our risks," Danjou says. "It also gave us a valuable gift: the time to really think about our risks. Often, in any business, managers and executives are caught up in daily operations. It is important, at regular intervals, to take the time to think about existing and emerging risks and how to manage them. In this respect, risk mapping has been a very important exercise for us."

To make sure the Top 20 risks are always accurate and current, Danjou and his team meet to discuss the list at least twice every year, prior to the biannual audit committee meeting. "The audit committee has challenged us to present an updated list of risks and related mitigation strategies," says Danjou. "Our last meeting was in March 2011. It is important for our shareholders that we ensure we are implementing proper remediation plans."

## Risk profile analysis

Part of the risk mapping approach at Sequana is to create a profile for each identified risk. Strategies for addressing the risks are differentiated according to the risk profile. Depending on the position of the risks on the risk profile, the following types of actions can be followed:

- **Address:** Risks are considered important but not well controlled. These risks need to be addressed as a priority, as they are viewed as a potential threat for Sequana.
- **Monitor:** Risks are considered important and relatively well controlled. They should be considered for further analysis to validate that the perception regarding mitigation effectiveness is accurate, and could be included in the scope for internal audit reviews.
- **Optimize:** Risks are considered less important and perceived as under control. They can be a potential source of resource optimization.
- **Follow:** Risks are considered less important and not well controlled. While focusing on these risks should not be a key priority, they still need to be followed to make sure their significance does not increase.

## Communication and reporting

The risk mapping initiative has been communicated to targeted groups at Sequana. As an example, for one of the company's main risks – antitrust noncompliance – specific exercises were conducted in management meetings to illustrate activities that would keep Sequana in compliance, and to learn what actions to avoid. "We conducted a two-hour workshop, and everyone liked it," says Danjou. "Top managers for each location around the world – about 200 people – attended. Even the smallest or most remote areas had representatives who carried the information back to those regions. We plan to conduct these workshops for the other top risks, as well."

One of the key performance indicators (KPIs) used to monitor the efficacy of the internal audit team is the issuance of the audit report. "We have a compulsory set of KPIs for the issuance of the report," says Danjou. "On the first day our internal auditors are in the field, they hold a kick-off meeting. During the fieldwork, they hold daily debriefs with management. On the last day, they conduct an exit meeting where they present their recommendations, making all points and rationale transparent to the auditees. Five days later, the draft report must be submitted."

Danjou explains that because the internal auditors work in such small groups and have a rigorous traveling schedule, they must be extremely efficient. With an enhanced risk mapping strategy, better communication and a well-defined common language for risk, Sequana has increased efficiency and improved its risk management efforts across the enterprise.

**Company Headquarters** — United States
**Number of Countries Operates in** — 165
**Number of Employees** — 40,000
**Industry** — Telecommunications
**Annual Revenues** — US$32.6 billion
**Annual IA Operating Costs/Budget** — US$1 million – US$5 million
**Number in IA Function** — 46
**Number of Years IA Function Has Been in Place** — Unknown
**IA Director/CAE Reports to** — Audit Committee

Note: All of the above information is accurate as of December 31, 2010.

*"Certain catastrophic events, and the economic downturn over the past two years, have really pushed us to enhance ERM at our company."*

*– Suzanne Williams*

## ERM triggers risk awareness, communication at Sprint Nextel

Sprint Nextel offers wireless and wireline communications services to more than 49.9 million private consumers, businesses and government users. The company is widely recognized for developing, engineering and deploying innovative technologies, including wireless 4G service, industry-leading mobile data services, and prepaid brands such as Assurance Wireless, Boost Mobile, and Virgin Mobile USA. While Sprint Nextel has some presence globally, its operations and clientele are primarily U.S.-based.

All business units within the company – including the business markets group, consumer markets group, the 4G group, network operations and wholesale, and customer management – report to Sprint Nextel's CEO. Corporate staff functions within the organization include human resources, legal, finance, marketing, corporate communications, corporate social responsibility, and corporate strategy. Sprint Nextel employs about 40,000 professionals.

Suzanne Williams, who oversees a team of 46, has been the vice president and chief audit executive for Sprint Nextel since September 2008. She reports to the audit committee of Sprint Nextel's board of directors, with a dotted line to the company's chief financial officer. Six internal audit managers report directly to Williams: one focuses entirely on enterprise risk management (ERM), one is devoted to retail operations, and the remaining four managers have responsibility for the rest of the company.

"In 2005, when Sprint merged with Nextel, the company's leadership wanted to implement ERM," Williams says. "Previously, ERM resided in the treasury organization; however, due to a realignment of resources within the finance organization, ERM was moved to the internal audit organization for enhancement and improvement, based on our risk knowledge and expertise. I have had responsibility for ERM for almost two years."

The internal audit function at Sprint Nextel is responsible for facilitating ERM, but management owns the process of determining mitigation plans for each key risk, with the board of directors providing oversight and governance. In 2010, the company's ERM process was truly revamped. The internal audit team developed the chart below, which outlines the team's objectives for audit and ERM. "It was our role to communicate these risks to the audit committee and ensure management enacted mitigation plans for each one," says Williams. "Now, we plan to take ERM a step further in 2011."

## Sprint Nextel: Internal audit objectives for 2011

| | |
|---|---|
| Identify areas of potential savings or cost avoidance | Identify savings to the enterprise through cost reduction/cost avoidance/increased revenue. |
| Facilitate the ERM process and develop timely audit plans | Facilitate the prioritization and assessment of key risks at the enterprise level and develop timely audit plans based on risk assessments and business needs. |
| Perform quality audits | Perform two semi-annual self-assessments from a sample of 2011 completed audits and pass both assessments. |
| Enhance and improve fraud identification efforts | Use the *Fraud Risk Assessment* process (developed internally) to identify fraudulent activities through our audits. |
| Staff development | Continue to develop the expertise of staff by increasing the percentage of staff members with certifications. |
| Recruit, develop and retain highly effective people | Maintain an appropriate number of resources to complete the audit plan. |

In 2010, Sprint Nextel's internal audit team used a classic "bottom-up, top-down" approach toward risk. "We performed a significant amount of benchmarking with companies to set the baseline with ERM," Williams explains. "We conducted an enterprisewide risk assessment and an audit risk assessment, and took the results of each to the CEO and the company's lead teams, such as human resources and consumer markets. We visited each staff meeting and presented our results, whittling down our top risks based on management's input to about 10 focused on strategy, finance and operations. An owner responsible for creating a mitigation plan and measurements was assigned to each risk."

In 2011, Williams and her team intend to improve their ERM process even further by incorporating five key enhancements:

- Building a better risk framework by adding compliance to strategic, financial and operational risks
- Dedicating a full-time resource to ERM
- Establishing a risk steering committee, with a vice president representative from all major operational units in the company
- Identifying "black swans" or unforeseen events, such as environmental disasters, that can have a catastrophic impact on the company
- Creating a heat map to illustrate comparability between risks, as well as risk impact, likelihood and overall risk appetite

## Educating the company about risk

"If I look back to 2010, one of the biggest challenges I see that we faced was making sure everyone understood what a risk is," Williams says. "There are different categories of risk, and it was a complex undertaking to develop a language around those risk categories. Today, everyone is more educated." Williams also cites well-publicized incidents with other companies that brought the critical nature of business risks to the forefront, such as the BP oil spill in the Gulf of Mexico in 2010.

"Certain external catastrophic events, combined with the economic downturn over the past two years, have really pushed us to enhance ERM at our company," she says. "Having audit committee support, as well as support from our leadership team, has been very helpful. As we move through the process of adopting and enhancing ERM, we hope to further educate everyone throughout Sprint Nextel about the nature and importance of risk management, and gain even more buy-in."

ERM manager Steve Kerns and the internal audit team are the primary players in ERM implementation at Sprint Nextel; however, according to Williams, it all starts with the survey process, where every company executive has an opportunity to voice his or her opinion on ERM. "When it comes down to it, the internal audit group facilitates ERM, senior management owns it, and the audit committee is responsible for oversight," Williams says.

## Getting everyone on the same page

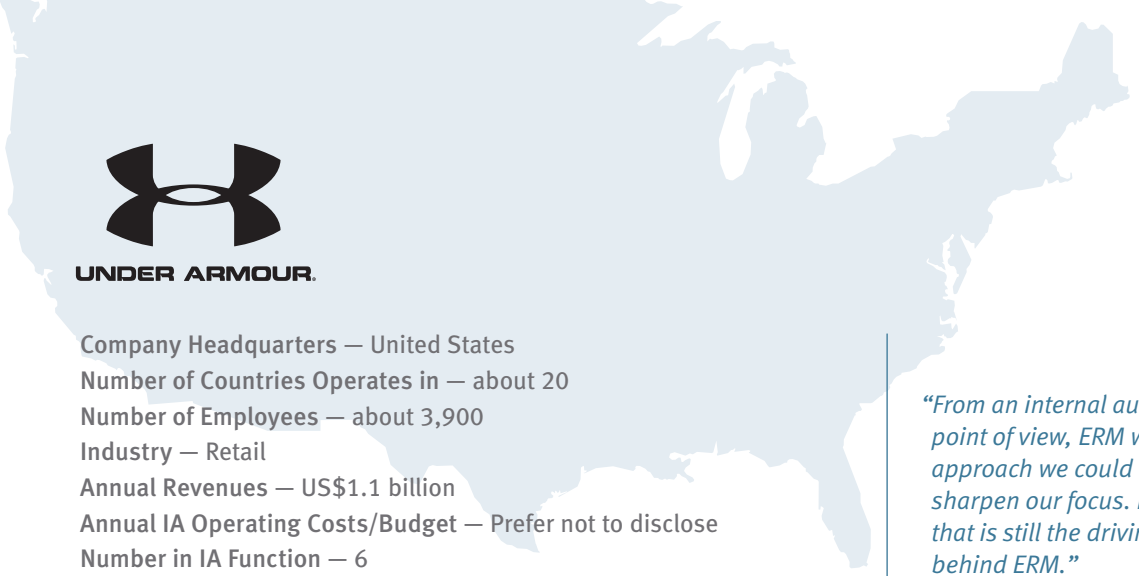
ERM helps the internal audit team ensure its audit plan is risk-based, covering the primary risks of the company. "ERM gets the team on the same page and helps everyone focus on what can actually go wrong with the plan so that we can all be more proactive than reactive," says Williams.

The survey provides the definition of each of the four risk categories and asks participants to rate their key risks in terms of likelihood and magnitude. "The survey is our way of gathering input on key risks," Williams explains. "Directors and leaders in the company are positive about ERM. They are starting to understand risk and ask more questions. The response to the survey has been great."

Key risk results, as well as each mitigation plan and related measurement, are reported to Sprint Nextel's audit committee. The CEO's direct reports provide the audit team with their mitigation plans and results each quarter. To measure internal audit performance, including ERM, the internal audit team is required by The Institute of Internal Auditors to undergo an external independent assessment every five years. "The best way to determine the effectiveness of the internal audit function is to audit it," Williams says.

Currently, Williams and her internal audit organization do not use specific tools to aid them in their ERM efforts. "That is something we will explore in 2011," she says. "Right now, this process is really about more fully integrating the risk processes we have out there. I have learned you cannot implement ERM overnight. It is a gradual process."

Williams adds, "I had an interesting discussion recently about the ways in which ERM supports the mission of the internal audit function. In a good audit department with limited resources, you have to focus on the highest risk elements of the company. ERM brings this together for us in a formalized way. We can map our internal audit plan to our key risks. That is the biggest benefit of all."



**Company Headquarters** — United States
**Number of Countries Operates in** — about 20
**Number of Employees** — about 3,900
**Industry** — Retail
**Annual Revenues** — US$1.1 billion
**Annual IA Operating Costs/Budget** — Prefer not to disclose
**Number in IA Function** — 6
**Number of Years IA Function Has Been in Place** — 5
**IA Director/CAE Reports to** — VP Corporate Governance and Compliance

Note: All of the above information is accurate as of December 31, 2010.

*"From an internal audit point of view, ERM was an approach we could use to sharpen our focus. For us, that is still the driving force behind ERM."*

*– Elysa Lipsky*

## High performance at Under Armour

Under Armour is a brand synonymous with performance. Founded by former University of Maryland football player Kevin Plank and incorporated in 1996, Under Armour is the original creator of high-performance apparel designed for athletes.

Jonathan Schwartz, senior director risk management, leads the risk management function at Under Armour. Schwartz reports functionally to the chairman of the audit committee and administratively to the vice president of governance and compliance. The internal audit function sits under the umbrella of risk management along with asset protection, insurance, ethics, enterprise risk management (ERM), and other compliance activities. Elysa Lipsky, senior manager internal audit, leads the daily internal audit and Sarbanes-Oxley activities and partners with Schwartz on the ERM initiative.

Risk management activities are focused on identifying, documenting and prioritizing the strategic risks of the company. Working closely with the executive team, Schwartz and Lipsky analyze management's mitigating activities and develop transparent reporting on risk status for management and the board of directors. "It is our objective to understand the pulse of the business and partner with the executive team to develop effective means of mitigating strategic risk," Schwartz says.

In their quest to implement ERM more fully throughout the organization, Schwartz and Lipsky meet regularly with executive management, at least quarterly with the company's CEO and audit committee, and at least monthly with the chief operating officer (COO). Apart from these meetings, which are currently the key touch points on Under Armour's journey to ERM, Schwartz and Lipsky utilize documentation from the quarterly VP certification process, completed by all executives of the company, and results from the internal audit reports and Sarbanes-Oxley compliance documentation.

The quarterly interview process yields an inventory of enterprise risks and related mitigating actions that Schwartz and Lipsky consolidate to prioritize and rate risks. "It helps us understand how our risks impact our strategic objectives," says Schwartz. "On the back end of the process, we follow up on specific mitigation efforts conducted by management that help us determine and report on risk status."

The ongoing dialogue with leadership at Under Armour helps illuminate the challenges around achieving strategic objectives. "We like to put that information into what we call 'risk areas,'" Schwartz adds. "If we learn five things that are related, we consolidate them into one risk area. This allows us to talk to the audit committee, board of directors or our leadership team more intelligently about significant risk areas."

## The push to ERM

Many factors drove Under Armour to adopt an ERM process. Members of the audit committee and board of directors – most of whom sit on boards at other companies – were experienced with ERM and saw the trend toward embracing this approach as a strategic initiative. "They believe that companies must get better at risk management because it is critical to long-term success and creates competitive advantage," Schwartz says. "Our board of directors recognized that part of their responsibility is to oversee risk and provide guidance on how the company is managing risk. To accomplish this, they wanted a tool – something that would correlate strategic objectives to risks and provide a level of accountability for the management of those risks."

External factors such as rating agencies, analysts, and external auditors also played a role in moving Under Armour toward formalized ERM. "It became important for us to assure these external entities that our management team is focused on the most significant strategic risks and that as a company, we are driving toward understanding our risk environment," Schwartz says. "We needed a more formalized risk management process."

Lipsky adds, "From an internal audit point of view, ERM was an approach we could use to sharpen our focus. For us, that is still the driving force behind ERM."

The risk management and internal audit functions have been involved jointly in the implementation and execution of ERM in the organization. "When Under Armour went public in 2005, the internal audit function was keenly focused on Sarbanes-Oxley compliance. Then, in 2007, we formed the risk management function and performed the organization's first comprehensive business risk assessment," says Schwartz. "At that point, we started educating the organization about the strategic value of risk management, and in 2008, Elysa and I gave a presentation to the board about formalizing a risk management process."

Schwartz recalls the time, in November 2009, when Under Armour's CEO said during a risk update presentation that, going forward, he wanted to be more involved in the preparation of the quarterly risk update prior to the audit committee meeting. "That was a big 'aha' moment," says Schwartz. "We knew we had reached a milestone when our CEO implied that ERM is critical to the success of the organization and will receive the highest levels of management support."

The road to ERM at Under Armour has not been without obstacles, however. "We went through fits and starts," Schwartz says. "We began by developing a 'Risk Council.' It was difficult at first – an administrative quagmire of scheduling, since it was not a top priority for executives. Everyone had different thoughts and agendas. We quickly saw we needed a process – a methodology for ERM."

"The most significant challenge was coming up with the right reporting methods," says Lipsky. "We needed to find a way to report the right information to the right people. We decided that letting leadership prioritize its own risks makes the process more relevant to them and results in strategically focused reporting on risks and mitigating actions."

Another critical ERM success factor for Under Armour is to make sure the information is as practical as possible. "It is tough to drive accountability without a clear link of risk to strategic objectives," she says. "When writing reports, we ask ourselves, 'Is this just an inherent business risk or is there a clear relationship between the risk and achievement of objectives?' This is the art of what we are doing."

## Reaping the benefits of ERM

For Under Armour as a whole, Schwartz and Lipsky believe that ERM will ultimately create a greater likelihood of achieving strategic business objectives. "Overall, ERM gives us the benefit of reducing surprises," Schwartz says. "The internal audit function conducts risk-focused audits that are linked to strategic objectives. Moreover, the consensus that comes out of our ERM processes is unique. It is a powerful tool for managing the business and understanding risk from the viewpoint of the 'big thinkers' in the company."

ERM is communicated throughout Under Armour by risk management in partnership with the company's COO, who is the project's executive sponsor. "Before we set out to conduct ERM interviews, the participants receive communication from the COO promoting active participation in the ERM process," Lipsky says.

## Measuring performance

The internal audit function strives to have a risk-based internal audit plan, which is predicated on its understanding of Under Armour's risk profile. "The internal audit plan is derived from the results of ERM. This ensures that our resources are aligned with the company's strategic direction," Lipsky says. "Where mitigating actions are established, internal audit may audit the processes and controls. Where gaps in mitigating actions are identified, internal audit may partner with risk management to consult with the business in the development and implementation of processes and controls," she adds.

Schwartz says, "2011 will be a big year for us. There is much momentum toward governance, risk and compliance at Under Armour. We aim to become increasingly strategic in the organization by partnering with management in the ongoing effort to understand and manage strategic risks."

**Company Headquarters** — United States
**Number of Countries Operates in** — 200
**Number of Employees** — 6,800
**Industry** — Financial Services
**Annual Revenues** — US$8.1 billion
**Annual IA Operating Costs/Budget** — US$6 million – US$10 million
**Number in IA Function** — 45
**Number of Years IA Function Has Been in Place** — 3
**IA Director/CAE Reports to** — Chief Risk Officer

Note: All of the above information is accurate as of September 30, 2010.

*"The ERM program is tightly coordinated with the strategy of the company and helps Visa's managers execute their objectives with confidence."*

*– Tim Arnold*

# All ACES at Visa

Visa Inc. is a global payments technology company that connects consumers, businesses, financial institutions and governments in more than 200 countries and territories, enabling them to use digital currency instead of cash and checks. Visa operates the world's largest retail electronic payments network but does not issue cards, lend money or set rates or fees for consumers. Visa's innovations enable its financial institution customers to offer consumers more choices: pay now with debit, ahead of time with prepaid products, or pay later with credit.

Tim Arnold has been chief auditor at Visa since February 2008, one month before the company went public. "Prior to the IPO, we were working hard to become a more coordinated global company," he says. "While the progress since that time has been remarkable, the work of implementing and refining best-in-class audit, compliance and enterprise risk management (ERM) programs for a public company of significant scale continues today."

## Internal audit's journey

Before Visa became a public company, it had a mostly outsourced audit function that was divided into two groups with separate focus areas. Merging these groups into one department with a common mandate and audit approach was one of the first challenges Arnold tackled. Today, he oversees a global team of Visa internal auditors and forensic specialists. Arnold reports directly to the audit and risk committee of the board of directors, and administratively to the chief risk officer (CRO). Most members of Arnold's team are familiar with risk programs and enterprisewide risk management functions.

"Much of what we have put together in the risk organization is new for Visa, and this allows for more seamless coordination," Arnold says. "Our CRO was hired in late 2007, followed by the head of global ERM and the chief compliance officer later in 2008. The fact that we started within a year of each other has allowed the risk organization to be more conscious of the potential for overlap and inefficiency as new programs are developed and rolled out. It helps that we have a lot of fun with each other and respect for each other's opinions," adds Arnold.

Rather than divide and conquer – or worse, compete – the three agreed to work together to ensure the entire governance, risk and compliance (GRC) process at Visa is well designed. They are so committed to smooth coordination that they code-named their efforts "ACE," which serves as a constant reminder that audit, compliance and ERM programs work best when they are fully aligned, mutually supportive and thoughtfully deployed.

Common reporting lines to the company's CRO are another plus: The group meets several times a month and constantly assesses whether the programs are customer-friendly and as coordinated as possible. "On a philosophical basis, we all agree," Arnold says. "That does not mean we don't constantly challenge what we are doing and evaluate whether we are adding value to Visa as an enterprise. We do that every day."

## Enterprise risk management programs

Over the past several years, ERM has further evolved several important initiatives at Visa:

- **Risk Identification and Assessment Program (RIAP)** – This bottom-up analysis facilitated by the ERM team focuses on the primary risks facing the company. "This is not just an intellectual exercise," Arnold says. "ERM spends time with key executives in meaningful, risk-focused conversations. As a result of analyzing this feedback, RIAP helps the executive team to agree on the big picture risks that confront Visa." Internal audit uses the RIAP data as a key input when developing the annual audit plan and when planning individual audit engagements.
- **Risk Advisory Services** – This capability is similar to a Basel II scenario analysis and addresses complex, hard-to-solve problems that typically span the enterprise. The ERM team leads the exercise by hosting a one-day workshop with key managers, which is aimed at both quantifying exposures and identifying actions that directly address the risk being targeted. Arnold thinks so highly of this program that he has recommended the ERM team conduct workshops on issues that the audit team feels have not yet been solved effectively.

  According to Arnold, "The risk advisory program has been tremendously valuable in engaging a cross-section of experts in very structured settings to focus on solving what were once thought to be unsolvable issues. This capability provides us with yet another tool to remove current or anticipated obstacles from Visa's success."
- **Risk Assessments** – Visa uses many different variations of risk assessments across the company. For example, product risk assessments help frontline managers think through and mitigate potentially significant risks when introducing a new product. ERM's current focus is to bring a more common framework and vernacular to the multitude of risk assessments currently in use across the company and ensure they are deployed in a way that allows for better alignment and leverage by other stakeholders. ERM also wants to provide a quality control mechanism to ensure that risk assessments are well executed and actually used to drive management actions rather than simply to "check the box."
- **Corporate Risk Committee (CRC)** – Chaired by the CRO and attended by the heads of ERM, compliance and audit, as well as a cross-section of senior leaders, this committee meets monthly and oversees the management of key enterprise-level strategic and operational risks, both individually and in aggregate. The CRC operates under a formal charter and oversees the work of two subcommittees – the ethics and compliance steering committee and the business controls working committee. According to Arnold, "A current initiative of the CRC is to supplement already robust reporting with more clearly defined risk appetites and associated metrics to facilitate earlier action on emerging risks. The real goal of ERM and the CRC is to make sure we are *risk intelligent* as an organization – that key risk decisions are based on good data and are well articulated and transparent."

## Benefits of a coordinated approach

One major area of coordination among the ACE team involves assurance activities. "Neither ERM nor compliance goes in before an audit to clean up," says Arnold. "In fact, we coordinate schedules so that their visits occur sometime *after* our audit to help make sure recommendations are effectively implemented and training is delivered where needed. When management control groups need to clean up before an audit, it generally means that compliance and control are not baked into the day-to-day operation of the function under review. That is not the case here."

While reporting is somewhat coordinated, a key objective this year is to design a way to give Visa's executives a more consolidated view of what the various risk programs are indicating, and to help them more proactively address issues that are known or can be reasonably anticipated.

Enterprise risk programs have helped Visa coordinate its responses to various risk trends, such as emerging competition and disruptive technologies. "More of that coordinated dialogue is happening naturally now," says Arnold. "As a result, we are better informed when we make decisions about how to mitigate risk. As we coordinate these programs, we make them easier to operate, understand and use from a line management standpoint."

Governance throughout Visa is also sharper three years into being a public company. "We have rationalized and streamlined our policies and processes," Arnold explains. "We were in a build mode until this year; we are now in a continuous improvement mode. While feedback has been very good, executives and managers want even more coordination and communication from us."

One example of improved communication is a monthly report to the CEO, in which each discipline provides a brief summary of key issues for the executive team. The CRO acts as the consolidated voice of Visa's risk organization and presents the report at regular executive sessions with the CEO. "Having a persuasive and articulate CRO as an advocate is a key to our success – she paves the road for us," Arnold says. "She also challenges us to rethink conventional approaches, and couldn't be a more committed believer that effective audit, compliance and risk management programs help companies win in the marketplace."

ERM was implemented at Visa because the external environment in which the company operates is dynamic and radically different from what it was three years ago. "Product innovation needs to happen rapidly – you simply cannot be slow to market in this business," Arnold says. "So while we are all focused on growth, no one at Visa wants to disrupt that growth with costly and distracting mistakes or preventable miscalculations. Hence, there is broad agreement on the need for effective and efficient ERM, compliance and audit programs to supplement the management decision-making and controls improvement process."

ERM has come a long way at Visa since early 2008 when it was a decentralized activity with few links to strategy. "Today, the ERM program is tightly coordinated with the strategy of the company and helps Visa's managers execute their objectives with confidence," Arnold says. "The risk program is alive and well at Visa. It is a vital part of how we grow our business every day – prudently – around the globe."

# About Protiviti

Protiviti (**www.protiviti.com**) is a global business consulting and internal audit firm composed of experts specializing in risk, advisory and transaction services. We help solve problems in finance and transactions, operations, technology, litigation, governance, risk, and compliance. Our highly trained, results-oriented professionals provide a unique perspective on a wide range of critical business issues for our clients in the Americas, Asia-Pacific, Europe and the Middle East.

Protiviti is proud to be a Principal Partner of The IIA. More than 700 Protiviti professionals are members of The IIA and are actively involved with local, national and international IIA leaders to provide thought leadership, speakers, best practices, training and other resources that develop and promote the internal audit profession.

Protiviti has more than 60 locations worldwide and is a wholly owned subsidiary of Robert Half International Inc. (NYSE symbol: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

## Internal Audit and Financial Controls Solutions

We work with audit executives, management and audit committees at companies of virtually any size, public or private, to assist them with their internal audit activities. This can include starting and running the activity for them on a fully outsourced basis or working with an existing internal audit function to supplement their team when they lack adequate staff or skills. Protiviti professionals have assisted hundreds of companies in establishing first-year Sarbanes-Oxley compliance programs, as well as ongoing compliance. We help organizations transition to a process-based approach for financial control compliance, identifying effective ways to appropriately reduce effort through better risk assessment, scoping and use of technology, thus reducing the cost of compliance. Reporting directly to the board, audit committee or management, as desired, we have completed hundreds of discrete, focused financial and internal control reviews and control investigations, either as part of a formal internal audit activity or apart from it.

One of Protiviti's key features is that we are not an audit/accounting firm; thus, there is never an independence issue in the work we do for clients. Protiviti is able to use all of our consultants to work on internal audit projects – this allows us at any time to bring in our best experts in various functional and process areas. In addition, Protiviti can conduct an independent review of a company's internal audit function – such a review is called for every five years under standards from The Institute of Internal Auditors.

Among the services we provide are:

- Internal Audit Outsourcing and Co-Sourcing
- Financial Control and Sarbanes-Oxley Compliance
- Internal Audit Quality Assurance Reviews and Transformation
- Audit Committee Advisory

For more information about Protiviti's Internal Audit and Financial Controls solutions, please contact:

Robert B. Hirth Jr.
Executive Vice President – Global Internal Audit
+1.415.402.3621 (direct)
robert.hirth@protiviti.com

## Enterprise Risk Management Services

Protiviti's ERM professionals partner with management to ensure that risk is appropriately considered in the strategy-setting process and is integrated with performance management.

Over the years, studies and experience continue to indicate that risk is too often not aligned with the corporate strategy and performance management. The financial crisis has reminded management and directors that a comprehensive view of their risks is no longer a luxury, but a requirement. With the speed of business today, companies must provide the appropriate incentives, metrics, controls and culture to counter the potential for individuals to discount or ignore risks that are significant to their organizations.

Our consultants assist companies with implementing a practical approach to ERM that is integrated with existing management processes and aligned with the company's culture, with the goal of providing an enterprisewide view of risk, improving information for decision-making, reducing the risk of costly surprises and positioning risk management as a differentiating skill and source of competitive advantage. We work with companies to assess, design, implement and maintain effective capabilities to manage their most critical risks and address cultural and other organizational issues that can compromise those capabilities. We help them evaluate technology solutions for reliable monitoring and reporting, and implement new processes successfully over time. Most important, we help companies integrate risk with strategy-setting and business planning and risk management with performance management.

For more information about Protiviti's enterprise risk management services, please contact:

Jim DeLoach
Managing Director
+1.713.314.4981 (direct)
jim.deloach@protiviti.com

Cory Gunderson
Managing Director
+1.212.708.6313 (direct)
cory.gunderson@protiviti.com

## Protiviti's Governance Portal for Internal Audit

Protiviti's Internal Audit Portal is a web-based audit management system designed to improve the efficiency and effectiveness of your audit department. The Internal Audit Portal is an electronic work paper package that facilitates the audit process from risk assessment through issue tracking. Our advanced reporting engine will provide transparency, real-time status updates and a streamlined audit reporting experience.

Our clients are able to configure the solution to fit their approach and methodology, positioning both small and large internal audit functions to meet their objectives. When combined with our professionals and content, Protiviti will help you create a personalized response to your audit tool needs.

The Internal Audit Portal is an integrated module within the Protiviti Governance Portal that can be used independently or in conjunction with other modules to create a true governance, risk and compliance (GRC) platform. This enterprise solution allows you to leverage frameworks and build a common language and repository that brings internal audit information into a GRC context. Additional modules of the Governance Portal include:

- **Controls Management** – A framework that supports control documentation (e.g., Sarbanes-Oxley), evaluation, documentation and testing.
- **Risk Management** – A framework for assessing inherent, tolerable, and residual risk across defined enterprise categories.
- **Assessment Management** – An integrated survey engine that supports a sustainable self-assessment process across multiple GRC programs and modules of the Governance Portal.
- **Incident Management** – A system that captures actual, near-miss and potential events that can result in operational and financial losses.
- **Regulatory Enabler** – A highly structured and automated regulatory alert feed that allows the business to understand what has changed, where it impacts the business and what action plan is required.

For more information about Protiviti's Governance Portal for Internal Audit, please contact:

Scott Gracyalny
Managing Director – Risk Technology Solutions
+1.312.476.6381 (direct)
scott.gracyalny@protiviti.com

## Relevant Publications from Protiviti

Visit **www.protiviti.com** to obtain copies of the following publications and other thought leadership materials from Protiviti.

- **Guide to Internal Audit: Frequently Asked Questions About Developing and Maintaining an Effective Internal Audit Function** (Second Edition)
- **Enterprise Risk Management in Practice**
- **2011 Sarbanes-Oxley Compliance Survey – Where U.S.-Listed Companies Stand: Reviewing Cost, Time, Effort and Processes**
- **2011 Internal Audit Plan Considerations**
- **Board Risk Oversight – A Progress Report (from COSO and Protiviti): Where Boards of Directors Currently Stand in Executing Their Risk Oversight Responsibilities**
- **Guide to Enterprise Risk Management**
- **Changes to The IIA Standards: What Board Members and Executive Management Need to Know**
- **Guide to International Financial Reporting Standards: Frequently Asked Questions** (Second Edition)
- **Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirements** (Fourth Edition)
- **Internal Audit Capabilities and Needs Survey** (2006-2011)
- **Internal Auditing Around the World** (Volumes I-VI)
- **Powerful Insights** (Protiviti's podcast series)
  - – Enterprise Risk Management and Board Risk Oversight – A Tale of Two Surveys from COSO
  - – Internal Audit Quality Assessment Reviews – Required as well as Beneficial
  - – IT Audit – Assessing and Managing Risks Effectively Within the IT Environment
  - – Sarbanes-Oxley Compliance: Where U.S.-listed Companies Stand Today
  - – The Benefits of Outsourcing the Internal Audit Function
- **The Bulletin** (Volume 4, Issue 6) – "Risk Management: A Look Back and a Look Forward"
- **Performance/Risk Integration Management Model – PRIM²: The Convergence of Enterprise Performance Management and Risk Management**

## Protiviti Internal Audit and Financial Controls Practice – Contact Information


Robert B. Hirth Jr.
Executive Vice President – Global Internal Audit
+1.415.402.3621
robert.hirth@protiviti.com

### AUSTRALIA
Garran Duncan
+61.3.9948.1205
garran.duncan@protiviti.com.au

### BELGIUM
Jaap Gerkes
+31.6.1131.0156
jaap.gerkes@protiviti.nl

### BRAZIL
Ricardo Lemos
+55.11.5503.2020
ricardo.lemos@protivitiglobal.com.br

### CANADA
Carmen Rossiter
+1.647.288.4917
carmen.rossiter@protiviti.com

### CHINA (Hong Kong and Mainland China)
Philip Yau
+86.755.2598.2086
philip.yau@protiviti.com

### FRANCE
Francis Miard
+33.1.42.96.22.77
f.miard@protiviti.fr

### GERMANY
Michael Klinger
+49.69.963.768.155
michael.klinger@protiviti.de

### INDIA
Adithya Bhat
+91.22.6626.3310
adithya.bhat@protiviti.co.in

### ITALY
Alberto Carnevale
+39.02.6550.6301
alberto.carnevale@protiviti.it

### JAPAN
Yasumi Taniguchi
+81.3.5219.6600
yasumi.taniguchi@protiviti.jp

### MEXICO
Roberto Abad
+52.55.5342.9100
roberto.abad@protiviti.com.mx

### MIDDLE EAST
Manoj Kabra
+965.2295.7700
manoj.kabra@protivitiglobal.com.kw

### THE NETHERLANDS
Jaap Gerkes
+31.6.1131.0156
jaap.gerkes@protiviti.nl

### SINGAPORE
Philip Moulton
+65.6220.6066
philip.moulton@protiviti.com

### SOUTH KOREA
Sang Wook Chun
+82.2.3483.8200
sangwook.chun@protiviti.co.kr

### SPAIN
Angel Munoz Martin
+34.91.206.2000
angel.munozmartin@protiviti.es

### UNITED KINGDOM
Tim Brooke
+44.020.7024.7525
tim.brooke@protiviti.co.uk

### UNITED STATES
Robert B. Hirth Jr.
+1.415.402.3621
robert.hirth@protiviti.com

## KnowledgeLeader℠ provided by protiviti®

KnowledgeLeader℠ is a subscription-based website that provides information, tools, templates and resources to help internal auditors, risk managers and compliance professionals save time, stay up-to-date and manage business risk more effectively. The content is focused on business risk, technology risk and internal audit. The tools and resources available on KnowledgeLeader include:

- **Audit Programs** – A wide variety of sample internal audit and IT function audit work programs are available on KnowledgeLeader. These work programs, along with the other tools listed below, are all provided in downloadable versions so they can be repurposed for use in your organization.
- **Checklists, Guides and Other Tools** – More than 800 checklists, guides and other tools are available on KnowledgeLeader. They include questionnaires, best practices, templates, charters and more for managing risk, conducting internal audits and leading an internal audit department.
- **Policies and Procedures** – KnowledgeLeader provides more than 300 sample policies to help in reviewing, updating or creating company policies and procedures.
- **Articles and Other Publications** – Informative articles, survey reports, newsletters and booklets produced by Protiviti and other parties (including *Compliance Week* and Auerbach) about business and technology risks, internal audit and finance.
- **Performer Profiles** – Interviews with internal audit executives who share their tips, techniques and best practices for managing risk and running the internal audit function.

Key topics covered by KnowledgeLeader:

- Audit Committee and Board
- Business Continuity Management
- Control Self-Assessment
- Corporate Governance
- COSO
- Enterprise Risk Management
- Financial and Credit Risk
- Fraud and Ethics
- IFRS
- Internal Audit
- IT Audit
- Sarbanes-Oxley

KnowledgeLeader also has an expanding library of methodologies and models – including the robust Protiviti Risk Model℠, a process-oriented version of the Capability Maturity Model, the Six Elements of Infrastructure Model, and the Sarbanes-Oxley 404 Service Delivery Model.

Furthermore, with a KnowledgeLeader membership, you will have access to AuditNet Premium Content; discounted certification exam preparation material from ExamMatrix; discounted MicroMash CPE Courses to maintain professional certification requirements; audit, accounting and technology standards and organizations; and certification and training organizations, among other information.

To learn more, sign up for a complimentary 30-day trial by visiting **www.knowledgeleader.com**. Protiviti clients and alumni, and members of The IIA, ISACA and AHIA, are eligible for a subscription discount. Additional discounts are provided to groups of five or more.

KnowledgeLeader members have the option of upgrading to KLplus℠. KLplus is the combined offering of KnowledgeLeader's standard subscription service plus online CPE courses and risk briefs. The courses are a collection of interactive, Internet-based training courses offering a rich source of knowledge on internal audit and business and technology risk management topics that are current and relevant to your business needs.

## THE AMERICAS

### UNITED STATES

Alexandria
Atlanta
Baltimore
Boston
Charlotte
Chicago
Cincinnati
Cleveland
Dallas
Denver
Fort Lauderdale
Houston
Kansas City
Los Angeles
Milwaukee
Minneapolis
New York
Orlando
Philadelphia
Phoenix
Pittsburgh
Portland
Richmond
Sacramento
Salt Lake City
San Francisco
San Jose
Seattle
Stamford
St. Louis
Tampa
Washington, D.C.
Woodbridge

### ARGENTINA

Buenos Aires*

### BRAZIL

São Paulo*

### CANADA

Kitchener-Waterloo
Toronto

### MEXICO

Mexico City

### PERU

Lima*

### VENEZUELA

Caracas*

## ASIA-PACIFIC

### AUSTRALIA

Brisbane
Canberra
Melbourne
Perth
Sydney

### CHINA

Beijing
Hong Kong
Shanghai
Shenzhen

### INDIA

Mumbai
New Delhi

### INDONESIA

Jakarta**

### JAPAN

Osaka
Tokyo

### SINGAPORE

Singapore

### SOUTH KOREA

Seoul

* Protiviti Member Firm
** Protiviti Alliance Member

## EUROPE

### FRANCE

Paris

### GERMANY

Frankfurt
Munich

### ITALY

Milan
Rome
Turin

### SPAIN

Madrid

### THE NETHERLANDS

Amsterdam

### UNITED KINGDOM

London

## MIDDLE EAST

### BAHRAIN

Manama*

### KUWAIT

Kuwait City*

### OMAN

Muscat*

### UNITED ARAB EMIRATES

Abu Dhabi*
Dubai*

protiviti®
Risk & Business Consulting.
Internal Audit.