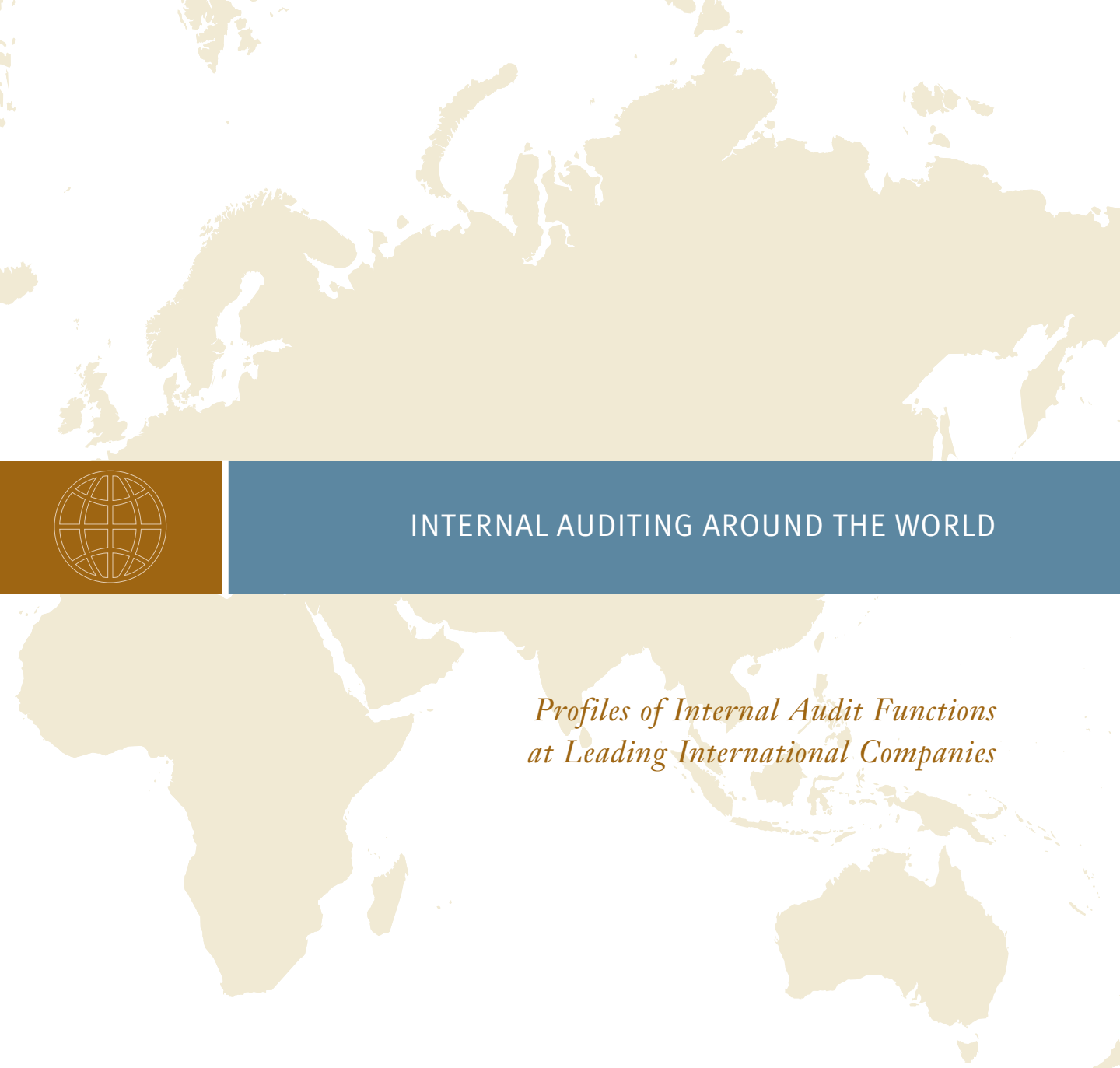

INTERNAL AUDITING AROUND THE WORLD

Profiles of Internal Audit Functions at Leading International Companies

protiviti®
Independent Risk Consulting

Business Risk | Technology Risk | Internal Audit

TABLE OF CONTENTS

INTRODUCTION

Internal Auditing: The Global Profession Thrives

Look at any genuine business profession and it likely is characterized by a dedication to craft, a sponsorship organization, a set of standards and ethical guidelines, a member certification program that includes continuing professional education requirements, and a forum for ongoing discussion and continuing professional education.

What differentiates internal auditing from most other professions, though, is the single, global nature of its standards. Our worldwide profession is shaped and guided by the International Standards for the Professional Practice of Internal Auditing. These standards, from The Institute of Internal Auditors (IIA), engender quality and consistency for internal audit organizations throughout the world. Yet flexibility and adaptability underscore the standards; as the internal audit profession continues to evolve, so does our understanding of its parameters.

Globalization is a key initiative under the leadership of The IIA's current president, Dave Richards, and one that was endorsed enthusiastically by The IIA's former president, the late Bill Bishop, a uniquely talented individual who is wholeheartedly missed throughout the profession. With more than 100,000 official current members, The IIA is a highly respected and influential worldwide organization, one that eagerly embraces the challenges and opportunities to implement critical initiatives so that our profession can continue to improve, expand and evolve.

We are proud to release this book – a collection of 13 Performer Profiles that highlight the internal audit and risk management strategies of leading multinational organizations – at a time when effective internal auditing is more essential to the international business community than at any time in history.

Corporate governance, ethics, fraud, risks, controls, regulations, communication, adding value – these issues are at the core of our profession as we stand on the threshold of the next generation of change. The organizations featured in this book are truly outstanding, yet there are many more companies that have insights and viewpoints to share. As we update this publication in the coming years, we will reach out to more organizations so that we can learn their stories of growth and progress and share them with you.

We hope this book will be a helpful and informative guide to all members of the internal audit profession as well as to those who have not yet joined. We also believe this publication can benefit other stakeholders and constituencies: audit committees, boards of directors, CEOs, CFOs, and other company executives and professionals. These profiles illustrate one essential truth – our profession has an enduring responsibility to the people and the businesses we have the privilege to lead.

Protiviti Inc.
June 2005

BARCLAYS' INTERNAL AUDIT FUNCTION RAISES THE BAR ON INTERNATIONAL PERFORMANCE

Barclays is one of the largest financial services organizations in the United Kingdom and a leading provider of coordinated global services to multinational corporations and financial institutions worldwide. With about 80,000 employees in 70 countries, Barclays' mission is to be an innovative, customer-focused company that delivers high-quality products and services and contributes positively to the communities it serves.

Mark Carawan began his tenure as director of Barclays' internal audit (IA) group a little more than one year ago. In that time, he has supervised a number of strategic initiatives designed to help the organization reach its mission and ensure that Barclays identifies and mitigates risk through effective communication, consistent methodologies and an enhanced awareness of IA's role and responsibilities across the organization.

Barclays' primary business units, or clusters, include Barclaycard, Barclays Capital, Private Clients and International, Barclays Global Investors and UK Banking. Each business unit is assigned a senior member of the audit team. This allows Carawan and his group to achieve constant communication at the highest levels of each business to help ensure that risks and controls are well managed throughout the worldwide organization.

"The audit function responds to Barclays' organization structure and to these individual business clusters," Carawan says. "Our audit teams are aligned to each of these business areas and are geographically dispersed around the world. We have 222 auditors, with teams deployed in Singapore, Hong Kong, Madrid, San Francisco, Geneva, Johannesburg and New York."

Three key forums for communicating risk strategies

All IA professionals within Barclays report to Carawan, who in turn reports to the CEO, the group chairman and the Board Audit Committee chairman. To ensure that communication channels are always open, three different Internal Audit forums meet monthly. These sessions help guarantee that effective communication is taking place and that risk management and control objectives and strategies are properly aligned.

The Board Governance Standard Forum consists of risk professionals within the audit function and reports to Carawan, who in turn reports to the board audit committee and the board risk committee on Barclays' compliance with risk governance standards and adequacy of controls. Risk areas under this forum's jurisdiction include credit, market, liquidity, capital planning, human resources, legal, regulatory, brand and reputation, strategic planning, strategic change, operational and nonfinancial risk, technology, finance and budgeting. The forum is chaired by the quality assurance director, Paul Marshall.

"The Board Governance Standard Forum is responsible for making certain that our audit work gives assurance to the Board and to Barclays' leadership that the Board's risk standards are complied with and maintained," says Carawan.

With the audit team reviewing the group according to Board Governance Standards, auditors are looking across each business area. "For example, if we want to give assurance to the Board about the quality of

market risk management and the adequacy of controls, we must identify all those components within the organization where there is market risk and how it is captured, evaluated, measured, monitored, controlled and reported, and be able to respond with an appropriate opinion to the Board with regard to the adequacy and effectiveness of management's governance, risk management and the system of internal controls.

"This means that instead of engaging in silo behavior and examining everything vertically within a particular business unit, we have to ensure that we adopt common policies and procedures across the group. Whether we are auditing credit in Africa or in the UK – and those are very different environments – we want to ensure that we have consistent standards and methods. This poses a significant challenge to the business and for the audit team."

The second forum is the Group Internal Audit Operating Committee, which includes a representative from each GIA business unit. The representative in the individual location is responsible for ensuring the operational efficiency and effectiveness of IA for that team or location. This includes financial and operational reporting, premises, head count, budgets and salaries, compliance with health and safety regulations, maintenance of business continuity plans, and other requirements for the division. This committee is chaired by Barclays' internal audit COO, Louise Fleming.

The third forum is the Executive Committee, which is comprised of the heads of audit for each of the business units. "This forum gathers and assesses information and IA's judgment on the adequacy and efficacy of policies, procedures, methodologies and toolkits," Carawan explains. "It proposes adjustments we should make in how we approach our work. For example, it may make recommendations of how we should audit third-party suppliers." This committee is chaired by Carawan.

All three of these forums refer matters for ratification to the Board, which consists of GIA's four most senior executives. Carawan takes whatever is decided at the GIA board level to the Group Board's Audit Committee (BAC) for decisions on changes in GIA's operating policies or mandates. The BAC is ultimately responsible for GIA's policies and mandate.

An ongoing improvement process

Performance improvement is a central motivating theme for Carawan and his team. In the first year as director, he identified a few key areas for improvement, which included the careful evaluation of the audit work itself. "We looked at our audit work in terms of what approach we were using and what we were doing in the field in order to determine if we needed new methodologies and tools or new strategies for continuous improvement."

The result is that the internal audit team has adopted a new approach to auditing. "We have introduced enterprisewide auditing to Barclays, so we audit across the organization according to board governance standards and key themes," Carawan says. "We have moved away from what I call high-altitude auditing, which means we no longer simply assess whether management has the right governance framework to manage controls. Instead, we are conducting substantive testing, auditing controls and sampling. In a sense, we've become auditors again, rather than high-level governance process consultants."

There are now three components to the IA mission: To audit the governance around the risk management and system of internal controls, to audit the system of internal controls itself and to audit the risk management of the organization. "We had only been doing the first of those three components. Now we are committed to addressing all three," says Carawan.

Carawan is careful to note that the job is not yet completed; these changes represent an ongoing improvement process.

"In changing what we audit and how we audit, we also have had to change the staff because the former skill sets were not as well suited to doing substantive audit or risk management assurance, which requires more technical skills in the business areas," Carawan says. "I am in the process of hiring a new team and assessing the training needs of remaining staff with the goal of enhancing skill levels. I have drafted 222 specific role profiles to make sure that we achieve the right skills and experience in each area."

"We have also introduced a quality assurance team and a quality assurance director, responsible for ensuring that we in internal audit, as an organization, apply policies and procedures consistently to the same high standard around the world and across the various business units."

Practice reviews conducted by the quality assurance team represent one way to ensure standards across the organization. In practice review, an audit team visits a certain location, for example, San Francisco, and determines whether the location is adhering to the IA standards that operate globally, rather than using its own tools and templates. "This not only drives changes in behavior, it ensures that we get better, more comparable documentation standards and approaches to reporting data across the group."

Regulations, strategies and challenges

Foreign corporations subject to Sarbanes-Oxley regulations do not have to report for Sarbanes-Oxley section 404 until 2005, and for Barclays this means the year ended December 31, 2005. "We are using 2004 as the period to prepare for that deadline by gearing up and running 'dry run' tests on controls," says Carawan.

He adds, "Within Barclays, the role of internal audit includes the testing of the operational effectiveness of controls on behalf of management. Management is responsible for identification of which processes and controls are key and will present documentation and attest themselves to the design effectiveness of controls." Having added headcount to supplement business-as-usual audit work, Carawan is confident that he will not deviate from his audit plan for 2004 and 2005.

One of the major challenges for large, global organizations is dealing with multiple jurisdictions and regulations. Barclays has other regulations besides Sarbanes-Oxley to stay abreast of, including the UK's financial services regulator, the FSA, as well as "Turnbull," a corporate governance regime much broader than Sarbanes-Oxley, although not as detailed on financial controls or financial reporting.

"We have over 200 regulations to be in compliance with the various jurisdictions. Our audit team conducts a wide range of regulatory compliance auditing, social responsibility auditing, brand and reputation auditing as well as testing the adequacy and effectiveness of governance, risk management and the system of internal controls. Best practice institutions will increasingly have to take on those broader responsibilities. This will mean that I will have a wide range of audit specialists on my team, including experts on human resources, brand management and ethics."

Carawan sites additional potential upcoming exposures, such as complications arising from outsourcing to offshore entities and the establishment of call centers and payment centers abroad. "There are enormous challenges inherent in strategic initiatives impacting business activities as well as infrastructure, such as telecommunication links, business continuity planning and security. How we audit and staff up for the next wave of business change will be an interesting challenge."

Interview with Mark Carawan, director of internal audit, March 2004.

BP: A SPIRIT OF CHANGE

Imagine combining five companies from the S&P top 50 and requiring them to develop a common culture, with shared values and purpose. Imagine asking the leadership of this new entity to effectively articulate those messages and help build a single, inclusive, consistent organization, with one spirit.

From 1999 to 2002, BP undertook about $140 billion of mergers and acquisitions that combined six large corporations, including many of the world's most significant gasoline and oil producers. BP, now one of the world's largest publicly held energy companies with more than 100,000 employees and locations in more than 100 countries, had $200 billion in market capitalization and $285 billion in revenues in 2004. The company is segmented into three main groups:

- Exploration and production, which locates, develops and produces oil and gas.
- Refining and marketing, which refines crude oil and sells oil products, including consumer and petrochemical products, through the group's 28,000 retail outlets.
- Gas renewables supply and trading, which adds value to the other businesses by integrated marketing and trading of energy and energy solutions.

Ian Rushby has been BP's group vice president and group general auditor since July 2001. Rushby, who has a broad, international business background, joined BP in 1977. "During the three years leading up to 2002, we experienced corporate change on a mega scale," he says. "We increased the company size two and a half fold, and brought disparate organizations together to create a new entity. The articulation of a management framework and the creation of a centralized internal audit function were critical to our evolution. We had to rethink how the new company would operate."

As a first step, BP revised the audit function's orientation, from a distributed and dispersed entity, strictly aligned to BP's business segments, to a function that was more centralized and holistic in nature. These changes took place not only due to the expanded BP organization and the need to unite its diverse operating structures, but also in response to the surge of rules and regulations reshaping corporate governance in the United States, the UK and the EU.

The purpose of internal audit

The purpose of the IA function, according to Rushby, centers on governance and examining how the company operates in the broadest sense. Rushby's IA team, which comprises 150 auditors with diverse professional and cultural backgrounds, helped implement key operational and strategic decisions in 2002 and 2003 that enabled BP to cope with the significant changes it faced.

"After we completed the mergers and acquisitions, I was involved in deciding how the management processes and executive governance would work and how resources would be distributed between the business segments," Rushby says. "To make these determinations, we looked back to how the old BP worked and identified what was and was not successful. We created a management framework to include language that would engage the group leadership. We taught that framework to more than 600 leaders in a six-month period, and we are currently rolling out the framework to 6,000 leaders in the firm."

The management framework was a key element in BP's change management effort. "We were trying to create a single culture," Rushby says. "We wanted to ensure that each part of the organization could operate together seamlessly, which is difficult to do in an entrepreneurial environment. It's about engaging leadership and creating the right processes to underpin the desired behavior. The framework describes an holistic system of internal control and provides a clear expectation against which we can plan and carry out our audit work."

To help communicate the goals of the framework, the IA team maintains two web-based portals, one that stores best practice business solutions and one that houses information on the company's management framework and system of internal control.

The centralized IA function comprises five domains. Each domain is led by a director who reports to Rushby. The domains are supply and trading; manufacturing and production; marketing; financial control, accounting and treasury; and additional functional activities of the group, such as HR, health and safety, and group compliance and ethics. To further centralize the function, Rushby oversees all IA budgetary issues.

The corporate governance challenge

As a foreign, SEC-registered company, BP must comply with Sarbanes-Oxley regulations as well as the Combined Codes in the UK and the governance codes of the EU. So during a time of change, when the IA team had to help develop a common culture for the organization, there were many new compliance activities taking place.

"Much of the Sarbanes-Oxley compliance work is done within the group controller's department, which is where I believe it should be," says Rushby. "In my opinion, the audit function is not the right place for this type of activity. It is fundamentally a financial control activity, and the financial controllers should ensure that their processes and documentation are compliant. My role is to test the documentation and ensure that the processes are working as intended, and I can only do that independently if I am not involved in creating the documentation in the first place. There are divergent views on this, I know, and it underscores one of the dilemmas of internal auditing today. In one sense, people want us to be objective, retain separate opinions and take an alternative view, but they also want us to participate in improving the executive processes and internal controls, and those are slightly contradictory roles."

Performance measurement

"Are we doing the right things, and are we doing them right?" These are the two questions that matter to Rushby with regard to IA performance, leading him to focus primarily on audit coverage and audit impact.

The process for selecting audit work, which is an annual planning exercise, centers on three components of the BP audit universe: the operating units of the organization, the major enterprisewide processes and key enterprisewide risks. "We select our audit program using those three lenses," Rushby says. "The audit committee and the ethics committee examine whether the IA function is well positioned and well resourced and whether it is aligned with management objectives."

Tone at the top

Rushby looks for auditors with broad and diverse business backgrounds. On his team, approximately 25 percent of the auditors have a CPA or equivalent and some have banking or trading experience. But the majority have general business backgrounds. "We look as much for the type of people as for their skills and experience," he says. "I seek people who act with integrity, impartiality and independence, and who can base opinion on fact, and are actively searching for better ways to do things to add insight for the organization."

The goal for the audit function is to create a single, inclusive group. From the UK to Singapore to Houston, all of BP's auditors should feel that they belong to one family. To further integrate the company's diverse audit professionals, Rushby blends his teams.

"Because many of our audit teams are global, we try to blend them, combining varied business expertise, as well as origins and cultures," he says. "I think that has created an extraordinary energy. I am a great believer in the wisdom of diversity. We want to create a single team out of 150 people and give it a global feel, which reflects what we are trying to do with the company as a whole.

"Part of our role at BP is to reflect the tone at the top. It is a phrase that is used often when talking about Sarbanes-Oxley and control environments. People ask what was wrong with Enron. The tone at the top was wrong. At BP, we internal auditors are challenged to be exemplars. If you can't rely on IA to have integrity, then who can you rely on?"

The question of risk management

"Risk management is part of doing business and is not separate from that," Rushby says. "I actually find the culture of trying to create enterprise risk management separate from the business almost defeating its own purpose. I do understand that those outside the organization want to be aware of the articulation of risk and that some areas, such as financial services, must manage risk in a consistent way. Risk management, however, underpins everything we do. You want to take it out and measure it, but taking it out and measuring it changes it."

The role of the IA team in risk management is to make sure risks are appropriately defined and managed, but also to ensure that everyone involved truly understands their risks and can take effective actions to mitigate and manage them.

"I have done many enterprise risk management conferences and speeches, and I always come back to believing that risk management is part of doing business. If you are not thinking about risks when you're thinking about business, then you are probably not thinking about business the right way."

The spirit of the organization

We live in a dynamic world, one beset by a complex array of change. To face challenges ahead, Rushby says, "you have to create a balance between testing if things are working as intended against an existing standard, and making a judgment about when it is time for that standard to be moved."

BP created the management framework in 2003, and at this time it may be necessary to coach people on how to meet its intended goals more effectively. As the organization gets better, however, there is a question of understanding the dynamic of evolution.

"The challenge may be to stay with organic change and make sure that the processes are evolving in an organic way," says Rushby. "I don't think it's possible to lock internal controls into a static framework. The controls are good for a period of time, but then they have to change. I wonder if the burden of continuous reevaluation and documentation is understood."

According to Rushby, it is far better for an organization to be based on principles and values rather than on rules and regulations, because being based on the former is more organic and a better position for evolution.

"It is the spirit of the framework rather than the mechanics of it," he says. "It comes back to the question of whether it is possible to create an organization in which 100,000 people (with different cultures and in different external environments) have the same spirit. And if you do have the same spirit, you don't have to keep going back to the manual."

Interview with Ian Rushby, vice president and group internal auditor, January 2005.

EDISON PREPARES FOR THE OPEN MARKET

Edison is the oldest Italian company in the country's energy sector. From constructing the first European thermoelectric power plant for the commercial production of energy in 1883, the history of Edison is said to be representative of Italy's industrial history.

In the 1960s, an era of nationalization for the energy market in Italy, Edison sold its assets to the government and merged with Montecatini, the country's largest chemicals group. The company changed its name to Montecatini Edison S.p.A., which was later shortened to Montedison, an organization that soon became a powerful conglomerate of agribusiness, chemicals and energy capabilities.

Edison remained the energy branch of the organization, and in 2001 the move was made to focus entirely on energy and sell all non-energy business for a sum of 9 million Euros. As a result, Edison is now the second largest energy company in Italy, producing electricity and gas, with sales revenues of 5.6 billion Euros and a 14 percent market share.

The latter part of the 1990s was the beginning of the liberalization of Italy's energy market. Before liberalization started, Edison could only sell to ENEL (Italy's state-owned power company) and to subsidiaries and sister companies. After its onset in 1999, Edison began selling to other companies. In 2008, the market will be completely open, which means that Edison will be able to sell to residential clients. In this new business environment, Edison faces challenges and opportunities. According to Gian Michele Mirabelli, senior audit executive of Edison's internal audit (IA) function since June 2003, "Over the next three years, we must take advantage of this tremendous opportunity by developing the capacity to market and sell to private customers. This will cause our organization to become more market-oriented. In this new business arena there will be many new risks for audit to identify and manage."

Risk-based auditing

Edison has four primary business units, two dedicated to the production of electricity and gas, one focused on marketing and one dedicated to energy management and trading. The marketing and energy management units have been established as an answer to the challenges of the liberalization movement in the marketplace. The company also has a business unit focused on corporate functions, such as general counsel, personnel, finance and internal audit.

The IA function is comprised of 15 professionals, all based in the Milan headquarters, and charged with auditing Edison and its subsidiaries operating in the company's core businesses of electricity and gas production and sales. The audit team reports to Edison's chairman and CEO, with an informal reporting relationship to the audit committee.

"Our mission is to help management evaluate internal controls," says Mirabelli. "We are part of the company's governance system, and according to the Italian Code of Corporate Governance, we are in charge of supervising internal control activities. Our goal is to focus mainly on risk-based audits related to operations and compliance. While our external auditors are responsible for financial audits, we actively exchange information with them in an effort of collaboration and partnership."

In 2003, the IA team completely changed its audit activities to align with the shift in Edison's business. "This new business brings new opportunities and risks in marketing and energy management," he says. "Prior to this, our activity was focused on production, but now production is not as risky as the other areas, so our audit plan is focused mainly on energy management and marketing."

To identify and assess these new risks, Mirabelli and his team created a system of evaluation based on extensive information gathering and scoring. The auditors interviewed all the directors and managers in the company and shared information with colleagues both inside and outside the IA function about the particular risks and problems in the various business areas. "We also analyzed previous audits and spoke to the chairman and the CEO about risks and controls. We categorized this information, and, in 2003, developed a scoring system, which rates every business unit and every corporate function based on risk." Mirabelli explains that every audit produces two ratings: one that rates the audit facts, findings and recommendations, and one that provides a general overview or evaluation of the strength and efficacy of internal controls.

"Our mission is to help management evaluate internal controls. We are part of the company's governance system, and according to the Italian Code of Corporate Governance, we are in charge of supervising internal control activities. Our goal is to focus mainly on risk-based audits related to operations and compliance. While our external auditors are responsible for financial audits, we actively exchange information with them in an effort of collaboration and partnership."

– Gian Michele Mirabelli, senior audit executive of Edison's internal audit function

To continue to improve this risk-based process, the IA team collaborates with business unit managers. "We are part of the Management Committee and hold half-day meetings in which we exchange information about the business," Mirabelli says. "Our relationship with business unit managers is positive and proactive, and we are striving to develop consulting services for risk-related matters in both governance and information technology."

The IA team also works closely with Edison's risk management function, which is responsible for helping the company set policies, conduct risk mapping and coordinate the process to identify and control risk. However, the ultimate responsibility for risk rests with each business unit and its operating manager.

Corporate governance

The Italian Stock Exchange has established a Code of Governance based on COSO, and it requires that a certain percentage of a company's directors be independent. For example, at Edison, 30 percent of the directors are independent. In addition, the audit committee must be largely independent and assume an advisory role in the evaluation of internal controls. In this role, the IA function supports audit committee activity. "This year we doubled the meetings from three to six, which has resulted in hard work but also in improved governance."

The IA team also helps the audit committee and the company to adopt Italy's new accounting standards, the International Financial Reporting Standards, to be implemented in 2005. The auditors present an audit plan, audit results and special projects to the audit committee and invite the CFO to discuss financial statements, financial reporting and management control. Edison's external auditors also are asked to join these meetings to facilitate information and knowledge sharing within the organization.

"Regarding governance, most Italian companies implemented compliance programs according to a law issued in 2001 ("legislative decree 231") to adopt an OECD agreement on fraud similar to federal sentencing guidelines systems," Mirabelli says. "According to this law, companies are liable if certain types of illegal actions are committed by employees on behalf of the organization, unless the organization can demonstrate that it has adopted effective compliance programs. Therefore Edison – and most companies – have implemented comprehensive compliance programs."

This program included an evaluation of the adequacy of the current organizational structure and of internal controls, the analysis and evaluation of related risks, the implementation of a control model based on a code of conduct, and specific procedures dedicated to preventing the crimes set forth in the decree, as well as the institution of a compliance committee formed by independent directors.

These compliance-related activities have resulted in significant work and a drain on internal resources for the company. In response, Mirabelli now outsources 20 to 40 percent of its compliance work. "We have a compliance committee, the same way as we have an audit committee, and we report to this body. It is a lot of work for us, similar to Sarbanes-Oxley-related work for other organizations."

Challenges ahead

The primary challenge for Mirabelli and his team is to improve the effectiveness of their risk-based auditing approach and to adequately support the compliance efforts stemming from the "legislative decree 231" compliance program. "In addition, we want to fully understand the new world of risks our company will face as a result of market liberalization. Our company is going to evolve during the next two or three years as we sell to the customers and not to the state. To do this, we must change everything, including audit."

Interview with Gian Michele Mirabelli, senior audit executive of Edison's internal audit function, December 2004.

FIAT REVI: FIAT GROUP'S INTERNAL AUDIT AND COMPLIANCE EXPERTS

Fiat Group, with more than 100 years of experience in the automotive industry and annual revenues of up to 47 billion Euros, designs, manufactures and markets high-quality cars, trucks, tractors, agricultural machinery, construction equipment, motor vehicle engines and components and production systems.

Some 160,000 Fiat Group employees around the world, working in the company's various operating sectors, perform its manufacturing and service activities. The three primary sectors are Fiat Auto, the automobile division; CNH Global, the agricultural and construction machinery group; and Iveco, the commercial vehicles sector. In addition, the following groups comprise the organization:

- Ferrari and Maserati – luxury sports cars
- Magneti Marelli – components
- Comau – production systems
- Teksid – metallurgical products
- Business Solutions – services
- Itedi – publishing and communication

Since January 2004, Mauro Di Gennaro has been Fiat's chief audit executive and compliance officer. His team, Fiat REVI, is Fiat's internal audit function. Headquartered in Italy, it consists of 170 professionals in a variety of countries, including Poland, France, Spain, the United Kingdom and Brazil.

Fiat REVI is organized in consortiums, in which all the sectors participate. Costs are allocated according to which sector spends the most time involved in audit activities. Fiat REVI's mission is to provide independent objective assurance and consulting services designed to add value and improve the organization's operations and help Fiat Group accomplish its objectives by bringing a systematic disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.

"To accomplish this mission, we help the organization maintain the validity of its internal control systems by assessing their effectiveness and efficiency, and by promoting continuous improvement," says Di Gennaro. "We also help Fiat Group identify and assess the greatest exposures to risk and contribute to improvements in the risk identification and reduction in management systems. Fiat REVI is responsible for implementing the oversight activities that verify any weaknesses of the internal control systems and identify any failings or needs for improvement in the internal control systems. We also verify that the rules and procedures constituting the terms of reference of the control processes are actually applied and that all those involved operate in compliance with the stated objectives."

Primary goals: transforming the audit function

During the past year, Di Gennaro adopted short- and long-term goals for Fiat REVI. The first was a process of change management in the audit function, shifting the function from an "inspection" to a "consulting" approach.

His longer-term goals included adopting as flat an organizational structure as possible to empower foreign officers to become autonomous, in order to reduce travel costs from headquarters, create local knowledge centers and begin to cast Fiat REVI as an internal repository of new management candidates. "Ultimately, my employees can take on management positions in the rest of the company, not only because of their professional knowledge, but because of their experience in different countries and various Fiat Group sectors."

Di Gennaro began his tenure as chief audit executive and compliance officer by implementing a new organizational scheme. In July 2004, he developed an audit structure based on the type of audit performed. "I have teams that focus on the auto sector, the financial sector and the services sector. These teams are not created based on specific experience in compliance or operational management audit, but rather on the knowledge that they have of each sector."

The second step in this new organizational scheme will be to structure Fiat REVI based on geographical areas to be covered. "We need empowerment, not only in terms of responsibility, but also in terms of the human resources assigned to the different offices, where these professionals will be autonomous as they perform different types of audits," says Di Gennaro. "I plan to have a geographic area designated for Italy, another for Europe and the third for the rest of the world."

"We need empowerment, not only in terms of responsibility, but also in terms of the human resources assigned to the different offices, where these professionals will be autonomous as they perform different types of audits."

– Mauro Di Gennaro, chief audit executive and compliance officer, Fiat.

Fiat REVI also has designed internal software to help conduct risk assessments in the audit universe. This software was designed with the help of experts from the information technology group. "The software evaluates and helps manage Fiat's risk exposures, not only from the audit point of view but also from management's perspective," Di Gennaro says. "It's called ERMSW, which stands for Enterprise Risk Management Software, and we piloted the first version in June 2004. We have used it on an ongoing basis since January 2005."

ERMSW allows Fiat REVI to map and manage more than 100 risk factors, as well as to monitor the evolution of the factors, and assess them per business process, according to fixed periods of time.

All of this change has been well received, but it remains a challenge. "Fiat REVI has a history of 40 years, so to change the approach, methodologies, standards and goals of the group is not so easy," says Di Gennaro. "However, in the second half of 2004, progress improved."

The internal audit process

Fiat REVI prepares its audit plan based on a comprehensive risk assessment process. The process leverages ERMSW in that the software helps the auditors identify and evaluate significant exposures to risk. ERMSW also explores the reliability and integrity of financial and operational information, the effectiveness and efficiency of operations, the safeguarding of assets and the compliance with law, regulations and contracts.

"In the course of our audit process, we also consider the input of senior management and the board of directors," Di Gennaro says. "When I prepare the draft of the audit report, I discuss it with the CEO of the sector we are auditing and then with the CEO of Fiat Spa. I then propose the report to the audit committee for review and approval."

The Fiat REVI audit process is based on three steps:

1. Audit scope, which is determined by the audit team during the project's kick-off meeting.

2. Fieldwork, which is conducted with regard to internal controls systems evaluation.

3. Audit results, the step that takes place before leaving the fieldwork, and during which the audit information is shared, discussed and agreed upon.

"For each audit, we provide an audit opinion that is based on a scale from 1 (the best) to 5 (the worst)," says Di Gennaro. "If we find significant weaknesses involving the effectiveness and efficiency of the internal controls systems, we develop an interim letter, in which we outline fast recommendations to take place immediately."

The group's audit report is called Audit Flash, and it contains the name of the business sector under audit, the time period, the audit scope, the value of the risk assessment, a summary of primary findings, proposed action steps to remedy any problems, and the actual audit plan that outlines the issues, actions, responsibilities and timing.

"For the top management of the sector and Fiat, we prepare a one-page management report that summarizes this information," says Di Gennaro.

Corporate governance: challenges and solutions

Like many Italian companies, Fiat Group has two pillars of corporate governance rules with which it must comply – Italian and American.

"For Italian corporate governance rules, which came into effect in January 2003 and are based on the code of the Italian Stock Exchange, we have to establish guidelines for the internal control systems," says Di Gennaro. "Each listed company has to name an internal control compliance officer, which is why my title includes the name 'compliance officer.' These professionals are appointed by the board of directors, and they report solely to the CEO, the audit committee and the Board of Statutory Auditors."

Within the Italian corporate governance rules, Di Gennaro and his team have to facilitate the effectiveness and efficiency of company operations and ensure that all financial information is in compliance with laws and regulations. The same must be done with Sarbanes-Oxley compliance.

Fiat REVI's obligations related to Sarbanes-Oxley include implementing a fraud prevention program and a code of conduct. "When an employee in Italy wants to make an anonymous declaration about possible fraud, he or she can use a telephone hotline. In addition, we have established a code of

conduct and business ethics that is shared within the group and with managers and employees," Di Gennaro says. "Also, Sarbanes-Oxley outlines specific corporate governance rules, such as having a well-defined relationship with external auditors, in which we meet with them and share the results of our work. We are also responsible for the pre-approval of audit fees and audit services."

Di Gennaro must report in a timely manner to the audit committee about all the audit activity in his department, including primary findings, the audit plan and any other subject that is important to the internal control systems of Fiat.

"To meet our governance obligations, I have put together a small team called Forensic Audit," Di Gennaro says. "This team is composed of three professionals, all with law degrees, and two with external auditing experience. The team helps us remain compliant with new regulations, and it also helps direct the audit team in its interpretation of laws and guidelines."

Talent search: internal auditor skills

"When I begin a search for auditors who recently graduated from university, I try to understand their level of commitment to auditing," says Di Gennaro. "I look at curiosity, knowledge of accounting and controlling, basic IT knowledge and risk matrix understanding. For professional auditors, I try to find individuals with a maximum of four years experience. I also look at external auditors who can change their focus. I need people who can assess the internal control environment of the company, not just the figures of a financial statement."

Di Gennaro says that he wants individuals on his team who can help verify whether the organization is prepared to reach its objectives and identify whether the organizational structure and operational methodology of managerial systems is effective and efficient. "These are the main characteristics that I look for in the professionals I try to hire," he says.

In the future, Di Gennaro expects to have a team of auditors who each have a minimum of three years' experience and a maximum of five years, depending on their professional profile. He conducts periodic monitoring and professional development sessions to assess auditor performance, strengths, weaknesses, and learning and development needs. Leadership is also assessed. "All of this is based on one concept," he says, "and that is, in order to create a good auditor, a company must spend a great deal of money, both in formal development and in on-the-job training. Our goal is to keep talented people within the Fiat Group so that we can recover our investment of resources."

Interview with Mauro Di Gennaro, chief audit executive and compliance officer, November 2004.

FRANCE TELECOM: AUDIT COMPETENCIES AND COMMUNICATION ARE KEY

France Telecom, a global telecommunications company, operates in a wide range of telecom activities, including wire line, wireless, business solutions and Internet. The company, which has annual revenues of 47 billion Euros, employs approximately 200,000 individuals throughout the five continents and serves 130 million customers worldwide.

As a leader in telecommunications innovation and research and development, France Telecom has established its own research centers and has forged alliances with high-tech centers in the United States and Asia.

Marc Chambault, director of France Telecom's internal audit and risk management department (DACR), has overseen the growth and development of the internal audit function at France Telecom for more than four years. His management style is hands-on and he guides the function closely with his management team.

Regardless of geographic location, all the internal audit teams report directly to Chambault. With a scope that includes a large range of internal audit and risk management activities, the DACR is organized by geography and competency.

"A small centralized team is responsible for internal audit methodology and tools, as well as compliance with IIA standards," says Chambault. "This team is also responsible for managing the internal control self-assessment approach implemented in the operational and commercial units of the group and its subsidiaries."

"Additionally, a dedicated risk management team manages and develops the group risk policies and practices," he says. "We work on group risk assessment and risk mapping, following up closely with the company's key managers and risks owners in order to assist them in risk assessment and action plans."

At the corporate level, an audit team of 60 professionals performs audits that focus on corporate functions and global group projects, such as human resources, legal, finance, accounting and information systems. Among this team, 20 internal auditors are specialized in information technology (IT) audit, focusing on technology-related risks.

Finally, five internal audit teams are dedicated to each of the company's major geographic areas: France, Poland, Europe, Africa and the United States. "These five teams work on all specific audit programs for these business units," says Chambault. "The audit programs include regular audits of the various entities as well as specific subjects within the subsidiaries. They also include full audits and internal control reviews."

In total, the internal audit headcount is 180 auditors. The DACR performs approximately 250 audit assignments every year.

Independence: A key value for the DACR

Chambault reports directly to the Internal Risk and Audit Committee, a management committee led by France Telecom's Vice CEO. Additionally, the DACR meets three times a year with the Group Audit Committee to present audit results and risk assessment updates, as well as the annual audit program, with results and major trends for the following year.

DACR's vision is to help management better understand and manage risks and related internal controls, while it shares risk management and controls best practices with leadership and the organization as a whole. This vision is supported by several key components, including:

- Quality audits, executed according to professional and IIA standards. "The DACR has initiated a quality certification project," says Chambault. "After having reached the ISO certification for France, the team will carry on this ISO quality process. We will also embark on a certification program with the IFACI, which is the French branch of The Institute of Internal Auditors. This is conducted through a quality review currently in process."
- Sharing of best practices between internal audit and risk management teams through the implementation of a technological platform which is used as a bridge between teams.
- The development of the company's risk culture and risk management strategies. "This is accomplished through the ongoing implementation of a risk management network that will exist in the business units," says Chambault. "This network will be leveraged by the DACR to monitor current and emerging risks."
- Quality deliverables, including audit reports and executive summaries. "Quality of communication is a key element to building a successful relationship with management," he says.

A multidisciplinary team

Differentiating the DACR from other corporate audit teams of its size is its large range of competencies, which enables the auditors to play key roles in all areas related to risks, such as internal audit, internal control, risk management and IT risks. The DACR has five core strengths:

1. A small central function is predicated on standards, methodology, training and tools. It is responsible for the consistency of the audit practices.
2. Teams with multiple competencies are able to work on main functional and operational processes.
3. The DACR leads the company's internal control self-assessment process, establishing a specific self-assessment guide for each business unit, as well as monitoring the process overall.
4. Direct involvement in the risk assessment and mapping approach and on the implementation of a risk management program enables DACR to provide technical and knowledge support to key managers and risks owners. DACR performs the follow up of the risk action plans managed by the risk owners. Finally, DACR consolidates feedback of the risk management network to identify and monitor emergent risks.
5. Corporate governance has become an important new project for DACR, with regard to Sarbanes-Oxley compliance. A biannual corporate governance review is now performed by Chambault in conjunction with the company's top 12 chief executives and their management teams. Using the COSO Framework, interviews are conducted with each chief executive regarding the primary actions they have taken on each COSO component: control environment, risk assessment and control activities. This review helps generate a report and update action plans every six months.

IT tools and performance measurement

The DACR is currently customizing an IT platform for the audit, communicating best practices in order to obtain a shared system of reference by the end of 2005. This will increase efficiency of knowledge sharing and help implement a consistent audit methodology, regardless of geographic location.

Audit performance measurement is achieved internally through an independent appraisal at the completion of each audit assignment, and externally in connection with the quality review and French IIA certification.

The Risk and Audit Committee submits a performance measurement of the DACR, which includes an annual interview with Chambault. The 12 members of the Group Executive Committee also conduct their own assessment.

"One significant way we add value for the company is through our knowledge of France Telecom's risks and internal controls," says Chambault. "Based on this knowledge, the DACR is considered as an important business partner of top management. We gather information and provide feedback on key risk management issues. Also, we are in a good position, through our assignments, to provide managers with a comprehensive vision of these risks, which allows them to develop and implement more efficient action plans. Finally, the DACR plays a key role in global corporate governance."

Critical upcoming goals for the DACR

Chambault and his team have several objectives for the coming year. First, it is important for them to follow through with the quality certification for auditors, and extend that approach to all the geographies of DACR so that all of its services fall under the ISO and French IIA quality certification.

The team also plans to finalize implementation of its IT platform in order to optimize access and exchange of key information, and to ensure the consistency of practices and methods across the enterprise.

"Finally we will start thinking beyond Sarbanes-Oxley first-year management testing, which is partly done by the DACR team, and move toward helping each business unit take charge of this oversight work," says Chambault.

In order to retain its talented audit staff and maintain its broad scope of competencies, the DACR will focus on the following challenges:

- Manage a progressive transition to reduced Sarbanes-Oxley involvement by adopting a long-term perspective. The testing phases of the Sarbanes-Oxley project will be performed by local dedicated people within the finance departments of each business unit.
- Strike a balance with regard to audit scheduling, and develop competencies needed to perform audits in the future. One such target is to reinforce legal competencies in connection with corporate governance and entity-level control.

"The ultimate goal of the DACR is the continuous improvement of corporate governance practices," says Chambault. "This will be achieved through our global vision on risks and internal controls; our integrated approach to management of these issues; effective communication and knowledge sharing between internal audit teams with regard to risk management projects; and finally, a comprehensive corporate governance review, conducted with top management, which will facilitate continuous monitoring and improvement of our current business practices."

Interview with Marc Chambault, director of internal audit and risk management, March 2005.

DRIVING CHANGE AT GM AUDIT SERVICES

General Motors Corporation, the world's largest automaker, has led global industry sales since 1931. Founded in 1908, GM employs approximately 321,000 people around the world, with manufacturing operations in 32 countries and vehicles sold in 200 countries. In 2004, GM sold nearly nine million cars and trucks globally. General Motors Acceptance Corp. (GMAC), a wholly owned subsidiary of GM, is a growing financial services company with 10 consecutive years of increased earnings. Since 1919, GMAC has provided more than $1.3 trillion in credit to finance more than 158 million vehicles in 41 countries. GM's global headquarters is at the GM Renaissance Center in Detroit.

General Auditor Chet Watson and his direct reports formed the Audit Leadership Board (ALB) to assist GM's Audit Committee in fulfilling its governance and oversight responsibilities, and assist management in the effective discharge of its responsibilities by providing relevant analyses, assessments, advice, recommendations and information concerning the activities examined. The ALB is comprised of the general auditor and Global Audit Service Line executives – T. Mapson, Automotive Audit; Chuck Gravener, Financial Services Audit; Jay Taylor, Information Technology Audit; Dave Aldorfer, Environmental and Capital Projects Audit; and Angie Chin, Business Risk Management, Sarbanes-Oxley 404 Support and Special Investigation.

The vision for GMAS is to be a recognized leader in providing independent appraisal and advisory services promoting global, enterprise-wide management of risks. The group's stated mission is to provide a balanced perspective to management and the Audit Committee between the risks to achieving the company's business objectives, and the condition of the supporting control environment.

"When I joined GMAS in 2003, one of my specific mandates was to reexamine our stakeholders' expectations, especially those of the Audit Committee and senior management, and align our priorities and resources with their expectations and the changing business needs," says Watson. "The Sarbanes-Oxley Act of 2002 has had a profound impact on the regulatory environment, corporate governance, and the internal and external audit profession."

GMAS is committed to providing high quality, value-added services. It recently received IIA's Recognition of Commitment Award for Professional Excellence, Quality and Outreach. In 2004, GMAS engaged an external quality assurance review team to meet the new IIA Standards. The review team highlighted a number of best practice examples at GMAS.

Achieving results

Watson has a few firmly held beliefs about how to achieve his goal:

- People are the first priority. "We operate in a complex, dynamic business environment. In order to deliver the types of services that our business units and our Audit Committee expect of us, we need the right staff size, the right people and the right skill sets. My first priority is to bring effective resources on board. That is priority number one," he says.

- Future leadership must continue to be developed. "When you look at leadership throughout GM, many of our top leaders have rotated into key positions in both the automotive and financial services side of the business. GMAS has the opportunity to work on global automotive and financial services assignments. Similarly, we work with business units to rotate their management experience into GMAS. Candidates who had completed the rotation found their internal audit experience invaluable," he says.
- Audit plan execution should be risk-based, comprehensive and effective, and include Sarbanes-Oxley (SOX) 404 coverage.
- Support risk management on an enterprise-wide basis. GMAS led the implementation of Process Risk Management (PRM), GM's control self-assessment (CSA) methodology. GMAS developed the infrastructure for PRM and is the owner of the PRM methodology and system. GMAS works with Process Owners and Operators to develop control frameworks and execution strategies, and trains business units to conduct the assessment and validation. GMAS also provides input to GM's Enterprise Risk Management (ERM) Committee.
- Effective communication is key. "We must communicate with our constituents in business language rather than in technical auditing or accounting terms," he says. "We focus on connecting with the business through effective communications."

"Given the diverse roles we play, from providing assurance services to consulting and coordinating the global implementation of SOX 404 compliance, effective communication is critical," says Chin. "We have devoted tremendous effort on improving communication to ensure that business unit management, as well as senior management, the Audit Committee and our own audit staff, are well informed of key initiatives."

"We hired a communication specialist to focus on internal communication in terms of compiling relevant information and disseminating it globally, enhancing leadership messages, publishing newsletters, and organizing global audit management, All-People, and focus group meetings. We make sure that we maintain a consistent flow of information exchange," she says.

"Given the diverse roles we play, from providing assurance services to consulting and coordinating the global implementation of SOX 404 compliance, effective communication is critical. We have devoted tremendous effort on improving communication to ensure that business unit management, as well as senior management, the Audit Committee and our own audit staff, are well informed of key initiatives."

– Angie Chin, GM's Audit Leadership Board executive for Business Risk Management, Sarbanes-Oxley 404 Support and Special Investigation.

Watson stays in constant touch with his direct reports, and also communicates on a regular basis with stakeholders and the Audit Committee. "We have revamped how we communicate with the Audit Committee," Watson says. "Since it is our primary constituent, we listen closely to what the members think is relevant. We have increased the frequency of communication and face-to-face meetings, revised the agenda topics and time allocation, enhanced the content and changed the format of the Audit Committee Report." Additionally, he benchmarks with other organizations to examine audit committee best practices, audit trends and emerging issues.

The overall performance of GMAS is measured through a balanced scorecard approach, which includes several measurement components, such as managing headcount and budget within targets, completing the approved audit plan by year-end, issuing audit reports within a 10-day turnaround period, and meeting targets set in the communication plan. "Essentially we start with the goals and objectives of my boss, John Devine, GM's vice chairman and chief financial officer, to see how we can best align my objectives to support the overall direction of the corporation," Watson says. "The ALB then sets GMAS' objectives and develops performance objective templates to cascade down to the entire team."

Developing the annual audit plan

GMAS uses a Risk Model to develop the annual audit plan. The auditable entities are evaluated against six risk factors: criticality to GM's and GMAC's strategic objectives; impact on the COSO components; degree of changes in business, systems and processes; key risks inherent in the business; time since last audit; and prior audit rating. The company's audit universe includes business units, joint ventures, strategic alliance partners and outsourced service providers.

GMAS coordinates audit work with 404 assessments to enhance the degree of reliance by external auditors and avoid redundant work at the business units. Where the scope of 404 overlaps with the audits, the audit team performs the assessment and validation to support management's assertion. In 2005, 15 percent of the 404 work is being performed in conjunction with audit projects.

Providing coverage

GM is divided into two distinct business segments: automotive and financial services, which includes financing, mortgage and insurance operations. GMAS is organized along the same lines and geographical regions. On the financial services side, GMAS services international and U.S. operations. On the automotive side, GMAS services:

- North America, including Canada and Mexico
- Latin America, Africa and the Middle East
- Asia Pacific
- Europe

With a full-time equivalent staff of approximately 250, GMAS is comprised of professionals with pertinent industry and audit experience. The team places a significant emphasis on education and professional certifications, with a majority of the auditors holding one or more of these designations: Certified Public Accountant (CPA), Chartered Accountant (CA), Certified Internal Auditor (CIA), Certified Information Systems Auditor (CISA) or Certified Fraud Examiner (CFE). We also partner with co-sourced service providers to meet our business needs. The management team is active on the IIA International Board of Directors and Committees, and the local IIA Chapter Board of Governors.

In order to serve customers effectively, the audit work is divided into five service lines. The first is the automotive operation. "T. Mapson's team assesses controls, risk management and governance practices for our automotive operations, joint ventures and alliance partners worldwide," says Watson.

The second is financial services. Chuck Gravener's team evaluates controls, risk management and governance practices at GMAC commercial and consumer lending, insurance, mortgage services and GM treasury operations worldwide.

The third area is information technology. "Jay Taylor's team evaluates risks, controls and governance for computer infrastructure, communication networks, applications, major new systems under development and related outsourced global IT services," Watson says.

The fourth is environmental and capital projects. Dave Aldorfer's team evaluates the effectiveness of the environmental compliance program and internal controls over execution of large engineering-based capital projects.

The fifth area, led by Angie Chin, focuses on risk management and special investigation. The PRM team coordinates the global implementation of processes, system and methodologies that enable business units to perform CSA and SOX 404 compliance. The Special Investigation team works jointly with Legal and Global Security to investigate allegations on potential wrongdoings.

Each year the ALB determines key areas of audit focus, for example in 2004 we included:

- Disclosure Controls and Procedures – an evaluation of financial disclosure controls and procedures to determine if they are adequate and consistent with requirements of Section 302 of the Sarbanes-Oxley Act.
- Revenue and Expense Recognition – an assessment of revenue and expense recognition procedures and controls to determine if they are consistent and adequate to ensure the integrity of financial and performance reporting.
- Account Reconciliations – an examination of accounts to determine whether they have been properly reconciled, whether exceptions are resolved, reviewed and approved by management and monitored for timely resolution.
- Management Assertion on Internal Control – an evaluation as to whether effective plans and processes are in place, consistent with requirements of SOX 404.

Sarbanes-Oxley 404 compliance

Compliance with SOX 404 is an important initiative, and GMAS plays a key role supporting management. Watson serves on the 404 Steering Committee while Chin chairs the Compliance Methodology Work Group. The PRM infrastructure serves as the foundation for the 404 compliance program. The group performs a number of key tasks, such as:

- Work with management to determine scope of coverage, develop control frameworks, identify cost-effective approaches to assess internal controls executed by outsourced service providers, incorporate compliance provisions in contracts and agreements, and recommend changes to GM's Due Diligence Review program.
- Make appropriate enhancements to the PRM system, methodology and training program.
- Coordinate the global 404 assessment schedule with the business units, the internal auditors and external auditors.
- Conduct additional agreed upon assessment work for management.
- Serve on a Quality Assurance team to ensure consistent control deficiency classification worldwide.
- Compile status reports and performance metrics for management and the Audit Committee.

Using GoFast! to drive continuous improvement

In 2000, GM embarked on an initiative named GoFast! to improve efficiency, reduce costs and expedite decision making. GoFast! workshops are high-impact sessions that gather Process Owners, Process Operators, subject matter experts, stakeholders and decision makers together to make quick, informed decisions that are implemented in a timely manner. "GoFast! expedites decision making," says Watson. "When we have a specific problem to solve, we define the issues, assemble the appropriate group of people, and come up with action plans. The decision makers approve action plans on the spot at the conclusion of the workshop."

Chin adds, "We are not just practitioners of GoFast!, GMAS also play a major role in GoFast! sessions sponsored by other business units. GMAS is invited to participate for a variety of reasons – our expertise on risk management, internal controls, information technology and business processes, or because we are a key stakeholder. Some of our staff members who are trained GoFast! facilitators are often tapped to facilitate the more complex workshops."

Watson can attest to the power of GoFast! He has sponsored a number of GoFast! workshops that range from enhancing GM's whistleblower process, improving the Integrated Process Audit Approach, revising the internal control rating definition, developing GMAS performance objective templates, to enhancing the concurrence process on internal control ratings.

Challenges overall

"In the view from my perch, retaining people is the number one challenge," Watson says. "It's very competitive out there. With the advent of SOX, auditors are in demand, especially highly qualified individuals. Retention is critical."

"Another challenge is to make sure we don't cross the line between helping management and our role as the independent, objective audit function," he says. "This is a constant challenge, because the more management perceives us as adding value, the more they call on us to participate in the process. When that involves decision making, we must be careful to maintain our independence and objectivity."

"Finally, as a global company, we have to be sensitive and aware that we are not living in one culture, but a multicultural world. What is good for the United States is not always good for the rest of the world, from both a business and an audit perspective."

Interviews with Chet Watson, general auditor, and Angie Chin, GM's Audit Leadership Board executive for Business Risk Management, Sarbanes-Oxley 404 Support and Special Investigation, April 2005.

HARLEY-DAVIDSON AND INTERNAL AUDIT: "WE RIDE WITH YOU"

Harley-Davidson has always had a mission: To fulfill dreams through the experience of motorcycling. For more than 100 years (the iconic company celebrated its centennial in 2003), Harley-Davidson has achieved its mission.

Made famous by the movie "Easy Rider," and the growth of factory custom motorcycles, the company enjoyed great popularity before experiencing a decline in sales, brought on at least in part by a merger with American Machine and Foundry Company (AMF), an organization that did not invest in Harley-Davidson. Then, in the early 1980s, with a well-timed management buyout, Harley-Davidson experienced a dramatic turnaround through implementing a new quality management system and modern manufacturing methods. Visible improvements in product quality and strong customer loyalty drove resurgence in popularity that revitalized the company and enabled the company to capture its industry's No. 1 position in U.S. market share for heavyweight motorcycles. Today, the company reports $5 billion in revenues, about 20 percent international and 80 percent domestic.

Culturally, it is an unusual fit for Harley-Davidson to have an internal audit (IA) function. Guided by its informal motto of Freedom with Fences, Harley-Davidson is a place with little bureaucracy, a relatively flat management structure, a relaxed atmosphere and casual style. All employees are empowered. The president of the Motor Company is rarely seen wearing a suit, only jeans. And the corporate philosophy is to be as collaborative as possible.

According to Rob Gould, who has been the director of internal audit at Harley-Davidson since August 2003, there is an upside and a challenge with the culture. "The upside is that there is a strong spirit of collaboration, a high level of trust and open communication at all levels. The challenge for audit is that controls, policies and procedures are sometimes not readily accepted within this culture."

As for the term "Freedom with Fences," Gould says, "When I came on board, I wondered if we knew where these fences were. In some cases, we didn't. The fences needed to become more visible. In other words, we needed to define the operating scope and those things that people were accountable for. To effectively fold audit into this environment, I have to be continually aware of the cultural landscape here."

Creating an audit function

In fact, Harley's corporate culture matched Gould's audit philosophy: An independent partnership with a focus on the end result, which is to have an effective audit process, in which recommendations are accepted and implemented. "We truly want to be viewed by those we interact with as 'riding partners' along the journey to a stronger control environment."

Particularly in a business environment sensitive to Sarbanes-Oxley compliance, it is critical that employees and management become owners of their internal controls and business processes. An increasing number of companies are complying with the new requirement to create IA departments; Harley-Davidson was no exception. "Harley-Davidson's audit committee and senior management became more concerned about the need for a strong internal control environment as the company

continued to grow," Gould says. "The company has grown rapidly in recent years, business processes are more complex, and the control environment had not kept pace. A large, international company needs more sophisticated controls and regular monitoring."

Gould's primary mandate when he was hired was to form the department. His first major task was to develop a risk assessment methodology and create an audit plan. Within a few months, he had met this goal. "I was hired in August and by December I had a plan and a strategy to present to the Audit Committee," he says. "During those few months, I met with senior management, explained the role of the audit function, and, importantly, developed an IA brochure to market the new function. The brochure was an important aspect of my communication strategy. It outlined how the audit team would interact with management, as well as our goals and objectives."

The brochure, "Gearing up for Internal Audit," describes:

1. What is Internal Audit;
2. Reasons for Establishing an Internal Audit Department;
3. Internal Audit Responsibilities;
4. The Audit Scheduling Process;
5. Internal Audit Procedures;
6. The Audit Team Backgrounds;
7. How Management Can Prepare for the Audit;
8. Reporting to Senior Management and the Audit Committee;
9. Other audit services such as SOX Compliance, Internal Control Consultation, Business Process Evaluation and Best Practices Information.

The three circles

Harley-Davidson is divided into two main business units. The Motor Company comprises 90 percent of the business and is responsible for the manufacturing and sales of the motorcycles. The Financial Services group is in charge of financing consumer purchases of the bikes. The Motor Company is segmented into three circles, with a team of auditors assigned to each circle:

Create Demand. This circle focuses on creating demand for the motorcycles, including marketing, sales, motorcycle styling, demand planning, forecasting, market presence and brand reputation.

Produce Products. This segment comprises the manufacturing and engineering portion of the business.

Provide Support. The administrative functions, including legal, HR and finance.

Gould's Motor Company internal audit team consists of seven process auditors, along with an administrative professional and Gould, who reports directly to the Audit Committee and administratively to the CFO. The teams assigned to each circle report directly to him, as well as two IT auditors who oversee all three circles. "Harley-Davidson is structured this way because it reflects the viewpoint of management, from an accountability standpoint," Gould says. "For this reason, we have our audit teams organized in the same fashion." The Financial Services group already had an existing internal audit function of five auditors which now reports to Gould.

Developing a risk assessment and creating an audit plan

Gould built Harley-Davidson's first risk model by using an Excel spreadsheet to assess the company's risk and control environment, including evaluation of internal control, the degree of change in specific business units, regulatory impact, the information systems and the role of IT in the business process and the impact of outsourcing, as well as quantitative risk factors, such as business unit size in terms of budget and sales.

Senior management conducted self-rating in terms of these different attributes, which helped Gould further define the audit unit risks for each business unit. He then ranked the risks that management identified, creating the basis for the risk model.

"I had the benefit of using the results of Sarbanes-Oxley testing that had taken place prior to my joining Harley-Davidson," Gould says. "There had been a director of financial compliance, and he spearheaded the controls testing before we formed the IA function, so I used those metrics, along with issues that our external auditors had raised." To round out the risk model, Gould used his own judgment based on years of internal audit experience with companies such as Whirlpool Corporation, Arthur Andersen and Protiviti.

A presentation was made to senior management, which outlined the IA mission, the audit plan and the strategy for building an audit function. To staff his team, Gould looked for individuals with diverse backgrounds, including SEC/financial reporting knowledge, Sarbanes-Oxley knowledge, CPA and accounting backgrounds, IT expertise, as well as manufacturing and operational experience for focusing on business process areas.

The first auditor was hired in February 2004 and the first audit, on Harley-Davidson's treasury unit, was conducted a few weeks later. At the end of the audit, Gould issued a customer satisfaction survey and received high marks. "They felt we focused on the most important issues," he says. "It was value-added."

Performance measurement continues to play an important role for Gould, who issues customer satisfaction surveys after each audit his team performs. The surveys use a five-point scale. "With a score of three or lower, I place a personal phone call to find out why," he says. "Most of the time I am explaining or clarifying the audit scope. It's a learning process for the company." Other performance measures include report cycle time, audit plan completion and budget vs. actual comparisons.

Year Two SOX improvement ahead

In February 2005, Gould and his team conducted a brainstorming exercise to increase the efficiency of the SOX audit process and sharpen the focus on control design and operational effectiveness, compliance with policies and laws and other major enterprise-wide tasks and initiatives, such as systems development projects.

The internal audit team collaborated on allocating resources based on risk. They developed approaches to reevaluate key processes and related applications within the scope of SOX and challenged controls that may be redundant or operational in nature; standardized the SOX testing, documentation and review procedures; put in place a regular monitor process to monitor change events for the Section 302 disclosure requirements, and strengthened the entity-level controls evaluation process. The findings will enable the IA function to reallocate its resources beyond SOX to higher risk audit areas.

"Instead of treating each process with the scope of SOX the same, we reviewed our audit approach, based on a high, medium and low assessment of risk. We also identified several processes that are now out of the audit scope because materiality did not merit inclusion," Gould says. "In the high-risk areas, we will perform walkthrough reviews at interim, and we will perform detailed sampling and testing at both interim and final. In the medium-risk areas, our team will conduct a walkthrough at the beginning of the year and testing on the back half of the year. Finally, in low-risk areas, we will ask management to complete a self-assessment, which IA will validate."

Lessons learned

To build an audit team from the ground up, Gould points out that it is important to focus on COSO requirements, fraud risk management and strategic risk management, which is one of the new COSO components. "The more that audit can be viewed as adding value beyond traditional compliance and operational auditing, the further the function will get," Gould says.

> *"The more that audit can be viewed as adding value beyond traditional compliance and operational auditing, the further the function will get."*
>
> *– Rob Gould, director of internal audit, Harley-Davidson*

In 2004, the IA team focused 75 percent of its time on Sarbanes-Oxley. Now that audit reports are standardized, well organized and meet the approval of the Audit Committee and senior management, Gould plans to focus on more thorough audit planning and leveraging automated work papers and to further streamline the audit function. "The number-one challenge in 2005 is to integrate the Sarbanes 404 project so that it becomes a process rather than a big project. We want to drive 25 percent of our resource hours away from Sarbanes-Oxley," Gould says.

"My goal is significant reduction of total hours by leveraging existing documentation and automation, increasing control awareness and improving training of control ownership," says Gould. "We want to be free to expand the work IA is doing in traditional audit areas. So far, we are well on our way to achieving our goal."

Interview with Rob Gould, director of internal audit, February 2005.

KOMATSU®

IMMEDIATE IMPACT AND ENDURING EFFECT: KOMATSU'S INTERNAL AUDIT GOAL

Komatsu America Corp., the United States-based subsidiary of Komatsu Limited, a Tokyo, Japan-based global manufacturer of construction and mining equipment and other industrial equipment with fiscal 2004 revenue of about $11.5 billion, has 141 consolidated and 44 non-consolidated subsidiaries, 32 plants, and many distributors around the world. Komatsu America Corp. represents Komatsu Limited's largest business segment in terms of sales outside Japan.

Phil Bertram has been director of internal audit at Komatsu since 1997. He was hired to build an IA function within the company, with a mandate to establish a fundamental audit program that covered the business risks of Komatsu America Corp. and its subsidiaries.

"I recently heard Richard Chambers of The Institute of Internal Auditors say that internal auditors should create immediate impact and enduring effect," Bertram says. "I have adopted that as our goal."

Komatsu is in the midst of tremendous growth, stemming in part from improvements in the global mining economy, which in turn has led to an increased demand for the company's equipment. Though business is strong, Komatsu faces other challenges.

According to Bertram, one of the company's biggest challenges in the past few years has been cultural. To bridge the divide between American and Asian management styles, it had become imperative to build consensus where it did not exist. One key issue was that Japanese employees were accustomed to being responsible for their own business functions, without someone monitoring their processes, as internal auditors often do.

> *"When I was brought on board, my initial challenge was to find out from all the senior executives what kept them up at night. We still try to stay on top of business and process risk to make sure we are addressing the high-risk and high-payback opportunities."*
>
> *Phil Bertram, director of internal audit, Komatsu*

In an effort to create a better understanding between the two cultures, the company recently conducted training sessions for senior managers, illustrating how American and Japanese employees could better integrate with each other. "Those training sessions helped provide insight into how both groups worked so that we could all more fully understand each other's decision-making processes and collaborate more effectively," Bertram says. "It was a corporate human resources initiative, but it was well received by everyone who participated."

The vast majority of Komatsu's management is American, and thus the company at large has adopted an American approach to auditing, which is centered around proactively identifying and mitigating risk, improving internal controls and adding value to the business through process improvement.

"When I was brought on board, my initial challenge was to find out from all the senior executives what kept them up at night," Bertram says. "We still try to stay on top of business and process risk to make sure we are addressing the high-risk and high-payback opportunities."

Having recently lost one of its staff members, the IA team consists only of Bertram and a senior auditor. This two-person function must conduct fundamental risk assessments, identify the audit universe, apply a risk assessment methodology, prioritize projects with management and then design the audit plan.

Bertram reports to the executive vice president of finance and control, who in turn reports to the CFO. Perhaps because he reports to executives in the finance function, there is a strong leadership consensus that the focus right now for the Komatsu audit team is Sarbanes-Oxley (SOX) compliance by March 31, 2006.

Leading the Sarbanes-Oxley initiative

As the company's Sarbanes-Oxley project leader, Bertram works with a consultant team from Protiviti toward 2006 compliance for Komatsu America Corp. and some of Komatsu Ltd.'s English-speaking subsidiaries around the world. He and his team are responsible for providing the company with compliance-related strategy and methodologies.

"I've been the project leader since May of 2004," he says. "We have almost finished the initial phase of documentation and evaluation design. At the moment, our challenge is to roll this out and help some of our sister Komatsu Ltd. subsidiaries document, evaluate and test their controls by September 30, 2005. We also must begin our testing phase. We will need to be finished with testing and evaluations by September 2005 so we can develop and implement a plan to sustain our SOX Section 404 compliance effort into fiscal 2006 and get ready for our external auditors to come in and begin their work in the fall of 2006."

Bertram says that he is working on a variety of methodologies with Protiviti, ranging from a highly leveraged approach that introduces documentation to all locations with a mandate from corporate, to an approach that requires auditors to go to each location and document the different processes, to sharing the documentation with a group in a facilitated session, gathering feedback and making adjustments accordingly. "The approaches are varied, but we have to ensure that what we are doing is cost efficient," says Bertram.

With a staff of two, adding Sarbanes-Oxley to an already-full workload might seem unreasonable; however, according to Bertram it makes sense. "What we are doing with Sarbanes at the moment fulfills what needs to be audited," he says. "We are gathering documentation and evaluation of controls. Of course, operational audits are put on hold right now due to lack of time. One challenge we will face is how to combine operational audits and business process improvement with the auditing and review of management's testing of internal financial controls."

Making a big difference with a small team

As the leader of a two-person staff, Bertram says that he is "the chief cook and bottle washer." He has to strategize, review, audit and follow up, always striking a balance between those four roles. To get projects done, and issue reports in a timely fashion, he often "borrows" auditors where he can, either through a guest auditor program, taking people from other business areas to conduct certain audits or outsourcing. Currently, he outsources his IT audit function.

"Depending on what I'm doing I use other various outside experts," he says. "To conduct an audit in South America, I found an outsourcer with Portuguese language skills, located someone in one of our South American subsidiaries who had an audit background, and put them on a team together so that they could do an audit in Brazil."

Bertram needs to be resourceful. The excellent results his audit team is achieving have brought on more management requests, such as requests to investigate fraud and other impropriety. Bertram, who is the compliance officer for the company's code of conduct, works often with the legal team.

He also partners extensively with the company's various business units. "We conduct front-end planning on all of our projects by talking to the controllers and the functional or business process owners, requesting information ahead of time to identify the goals of the audit and getting their feedback up front," Bertram says. "We have always positioned audit as being here to help the business run more effectively and efficiently. Everyone responds well to that message, because there is not an excess of staff here at Komatsu. Managers generally look forward to the help and insight we provide."

Plans for the future

Ideally, Bertram would like to see his department gain another seven to eight staff members. In the meantime, the advent of Sarbanes and the need for management to document controls has somewhat changed IA's approach to covering risk. "We realize that we can and should use some form of control self-assessment to choose our audit plan," he says. "We are going to focus on process by location, not location by process. Our challenge is to do enough work to come up with our own conclusions with regard to the quality of internal controls, which should support management's conclusions, and help the external auditors by decreasing some of their work."

Currently, Bertram measures audit performance by monitoring auditor productivity, chargeable hours and whether or not his team "gets the job done." He issues closed audit reports that outline recommendations, issues and action steps. Bertram also measures resolution of audit findings and conducts a 360-degree survey that asks auditees to opine on the value of the audit work.

"One thing I've learned is that I am here to make the business better," he says. "By collaborating and listening, we can provide better service and meet the needs of management."

Interview with Phil Bertram, director, internal audit, January 2005.

Manulife Financial

MANAGING DRAMATIC GROWTH: MANULIFE'S INTERNAL AUDIT GROUP

Manulife Financial Corporation, which was established in Toronto in 1887, operated as a mutual insurance organization until 1999, when it became a publicly listed company in Toronto, New York, Hong Kong and the Philippines. Today, Manulife provides financial protection and wealth management products and services on a global basis.

Manulife operates with eight separate divisions and operations in 14 countries around the world. In U.S. dollars, the company's assets are $147 billion, with funds under management of $278 billion and net income for 2004 of $2 billion. Although it is a Canadian company, approximately 60 percent of Manulife's business is based in the United States, 30 percent in Canada, and 10 percent in Asia and Japan.

The company has grown dramatically in the past 10 years, culminating in 2004 in a merger with John Hancock Financial Services, a move that combined two companies of approximately the same size. Today, Manulife is Canada's largest insurance company and one of the world's leading insurance companies.

Manulife's audit team

In addition to the John Hancock merger, Manulife also acquired the operations of a number of small and medium Canadian companies, and acquired a mid-sized Japanese life insurance company in 1999. As a result of these mergers and acquisitions, Manulife's audit team has grown from a staff of 30 in 1996 to a current staff of 90.

"We have audit offices in six cities and four countries – Canada, the United States, China and Japan," says Richard Gourlay, senior vice president and chief auditor for Manulife. "This reflects the geographical structure of our company. Each of our main audit operating units is geographically based. My philosophy is to have my auditors close to the customer because it gives us a much better understanding of the local environments they operate in and allows us to provide day-to-day services to local management."

The five geographically based audit group heads that report directly to Gourlay are located in Toronto and Waterloo, Ontario; Boston; Hong Kong; and Tokyo. An actuarial audit group also reports to Gourlay.

"Previously I reported to the CFO, but now I report administratively to the general counsel," Gourlay says. "In light of Sarbanes-Oxley, we decided it was more appropriate that I report to General Counsel, who is the senior executive with the least conflict from an independence point of view." From a functional perspective, Gourlay reports to the Audit and Risk Management Committee.

Years of change

In recent years, the biggest change that Manulife has faced, from a cultural viewpoint, has been the John Hancock merger. "We conducted due diligence of the John Hancock audit group prior to the merger," says Gourlay. "While they were using a sound approach to the auditing, it was very

different from our approach. We recognized early on that it would be a major challenge to merge the two departments. The decision was made to adopt Manulife's audit approach and introduce that approach to the combined audit team."

The differences in the two audit methodologies were dramatic in terms of risk-based audit approach, definition of an audit unit, sample sizes, report formats, audit rating systems and audit management systems. "The decision was to go Big Bang," says Gourlay. "Two weeks after the deal was closed, at the end of April 2004, we had the entire John Hancock audit staff trained in our audit approach. For every audit that commenced after closing, we have used our approach."

"The lesson I learned from putting two large audit groups together is that, in hindsight, we did it the right way," he says. "We conducted due diligence, developed a formal project plan and devised a tight timeline for integrating the department."

The profiles of Manulife's audit professionals are varied. From a general perspective, Gourlay says that he looks for a combination of skills in his auditors, primarily focusing on technical knowledge, fundamental intelligence and communications expertise. Upon joining Manulife, he says, he realized that actuaries are a critical component of any insurance company. "We had to bring actuaries on staff to audit pricing risk and reserve valuation risk," he says. "We now have three actuaries, with a plan to increase that number to five. Additionally, we have a core of IT auditors who are responsible for technical IT audits including ensuring that our myriad data center outsource partners are appropriately managing IT controls. Exploring the interrelationship between Manulife and outsourcers is an ongoing project." The majority of the auditors are generalists and represent a mix of external audit and business operations experience.

Objectives

As is the case with most Canadian financial services internal audit groups, Manulife is top-down risk focused, in part stemming from the Canadian regulatory environment. "We are an assurance-based audit group whose objective is to provide an opinion on the adequacy of risk management," Gourlay says. "Our objective has been to not only provide management with the results of individual audits but also to provide an opinion to the Audit and Risk Management Committee annually, that each risk in a framework of inherent risks is appropriately managed across the company on a global basis."

To achieve that objective, Gourlay and his team created a risk framework. "At the time, Manulife did not have an enterprise risk management group, so we conducted a great deal of research into insurance industry risks," he says. Once its initial research was completed, the audit group developed a framework of inherent risks and obtained senior management approval of this framework.

It then created an audit approach that would allow sufficient audit coverage every year for high-risk audit units to support an opinion on the adequacy of management of each risk in the risk framework. The audit approach Manulife adopted is comprised of two main components:

1. **Key Risk Audits.** This component of the audit approach consists of full-scope audits, conducted on a cyclical basis. If an audit unit is defined as a high-risk audit unit, it is normally audited every three years and moderate risk units every four years.

2. **Key Risk Reviews.** These reviews are conducted in the off years for high-risk audits. These reviews are designed to identify changes in structure, organization or procedures; involve limited testing; and provide Gourlay a level of assurance that the recommendations of the previous Key Risk Audit have been implemented and that there has been no significant deterioration in risk management since the last audit.

"The Key Risk Review is conducted through management discussion, limited testing and the review of what we call a management self-assessment (MSA) questionnaire," Gourlay says. "We decided early on that, in addition to delivering an audit report, we wanted to deliver a questionnaire that management could use to assess its risk management. Management conducts this assessment each year that we conduct a Key Risk Review. This has become a popular by-product of our audits, because it outlines the risks that must be managed by the business units, which are agreed to by management as part of our planning process. Also, it allows management of moderate-risk units to step back and assess themselves annually, if they choose to."

"Our approach is an efficient and effective way of auditing with limited resources," says Gourlay. "It allows you to focus on the high and moderate risks of a much bigger audit unit. With our approach, we risk assess each process in a business function and if a process is not a high or moderate risk, we do not audit the process.

– Richard Gourlay, senior vice president and chief auditor, Manulife

Manulife differs from many insurance companies in that its audits tend to be large. "We have moved from auditing processes to auditing business functions," Gourlay says. In 1996, Manulife reduced its audit universe from 950 audit units to 175 audit units. As a result of the merger with John Hancock, the company has 250 audit units worldwide.

For example, for the individual life insurance business, the Manulife audit team looked at the business cycle and identified six business functions or audit units. "We look at how products are developed and priced; the ways in which our sales force distributes the product, which gets into business practice risk or what I call market conduct risk, and how they are compensated for selling the product; how the policies are underwritten and recorded; how the policy is administered over the rest of its life cycle; how the actuarial reserves are calculated; and the general financial management of the business. Within all these categories we may be looking at hundreds of individual processes, and this gives our auditors a chance to examine the interrelationship of risk processes within a business unit, rather than focusing only on the risks of a single process."

"Our approach is an efficient and effective way of auditing with limited resources," says Gourlay. "It allows you to focus on the high and moderate risks of a much bigger audit unit. With our approach, we risk assess each process in a business function and if a process is not a high or moderate risk, we do not audit the process. Even more importantly, to properly audit risk management, you have to conduct it at a business function level, because it is difficult to audit top-down risk management from a business process level, since risks are generally viewed at the business level."

An independent audit group

Manulife's management views the audit team as a group that is uniquely positioned to provide an objective opinion on the company's risk management. "We operate in a professional environment where we maintain strong working relationships with management, and provide risk-based audit services to the businesses. However, we are an independent audit function and I make no bones about that. I know the current trend is for internal auditors to become consultants, but I think unequivocally that internal auditors' prime mandate is to provide an opinion to the audit committee on the adequacy of risk management."

Particularly in the wake of corporate governance reform, Gourlay's opinion on auditor independence and objectivity rings true. As a Canadian company, Manulife is defined as a foreign private issuer, and its first year of Sarbanes-Oxley compliance is 2006. "From day one, we made a decision that ownership of Sarbanes-Oxley initiatives is with the corporate controllers group and the CFO," he says. "In the initial six months, we worked closely with the corporate controllers to develop the documentation templates. We conducted two pilots of the templates to ensure their efficacy and we participated in steering committees. We have maintained independence of the process but have actively participated in it."

While the actual documentation related to Sarbanes-Oxley has been created by Manulife's many business units, the audit group was actively involved in quality assurance reviews (QAR) related to the first rounds of documentation. A full-time project manager was appointed in 2004 within the corporate controllers group to assume responsibility for documentation. Management testing will be conducted by an independent testing group reporting to the project manager.

"The role that the audit team plays in all of this is that we will complete a QAR of the testing in order to provide management with assurance that testing is done in accordance with the policies developed by the corporate controllers group," says Gourlay. "On an ongoing basis, we decided to incorporate Sarbanes-Oxley-related testing in the audits and reviews that we normally complete; work that, in many cases, was being done anyway."

Challenges

One of the most significant challenges Gourlay and his group face is to complete the full integration of the John Hancock audit group. "We are in the midst of doing that right now," he says. "For example, John Hancock does not use Lotus Notes for its audit systems and we do, so we are exploring ways to adopt a common system. We also are implementing a QAR process so that we can conduct quality reviews in each group annually.

"We have experienced dramatic growth and change in the past few years, and we are actively managing that change and moving forward."

Interview with Richard Gourlay, senior vice president and chief auditor, February 2005.

Posteitaliane

RESHAPING AUDIT AT POSTE ITALIANE

Poste Italiane is a financial services and postal organization that provides customers with integrated products, communication, logistic and financial services throughout Italy. With 14,000 post offices across the nation, the organization is vast and complex. As a result, effective, uniform and proactive internal auditing has been a challenge to implement.

Three years ago, Carolyn Dittmeier became the director of internal audit (IA) at Poste Italiane, reporting directly to the CEO and the president of the company. Prior to this, she had started up and headed the Corporate Governance Services consultancy within KPMG, following several years as chief audit executive for Edison (previously Montedison), a major Italian multinational listed on the U.S. and other foreign stock exchanges. As an American in Italy since 1982, Dittmeier has adopted a flexible business style that combines Anglo-Saxon management techniques with Italian innovation and adaptability.

At the onset of her tenure with the Poste Italiane group, Dittmeier was asked to reengineer the IA function, transforming it from its traditional role as inspector to a role that encompasses a modern audit approach, capable of activating continuous improvement in company control measures and process effectiveness.

"I reorganized the department by implementing a strategic plan to introduce information systems and new analysis methodology, in order to structure business process audits over a vast number of operational units in a consistent yet flexible manner."

– Carolyn Dittmeier, director of internal audit, Poste Italiane

"This was my mandate, and we called it the Internal Audit Reshaping Program," says Dittmeier. "I reorganized the department by implementing a strategic plan to introduce information systems and new analysis methodology, in order to structure business process audits over a vast number of operational units in a consistent yet flexible manner."

The reshaping program

The IA structure at Poste Italiane consists of approximately 600 auditors, most of whom are located outside of headquarters, operating throughout the national territory at branches, post offices and other decentralized operational units. In order to provide high-quality tools, four primary staff units were created. The first unit focuses on IA standards and procedures related to risk and control analyses of the constantly changing core business processes and procedures. This group creates audit programs as a platform for a strong compliance audit function; establishes general professional standards and detailed operating instructions; and communicates these standards in continually updated audit manuals.

Another unit is dedicated to planning and reporting. "With 14,000 post offices and 140 branches, we have to plan our audits based on risk-scoring techniques, strong rotational audit coverage policies and statistical risk assessment," says Dittmeier.

Ethics governance policies related to the United States Foreign Corrupt Practices Act is the focus of a third unit. This unit is comprised of Poste Italiane staff dedicated to dealing with the compliance programs with regard to ethics and fraud issues.

The fourth unit involves audit training and professional development. The group continuously deploys new methodology in audit management skills, communication skills and technical areas, which is fundamental to the strategic professional development of Poste Italiane auditors, who were previously trained as inspectors and investigators.

"These four units are all new, and are base drivers to the Reshaping Program. They are an extremely dynamic group," says Dittmeier.

During the Reshaping Program, Dittmeier and her team focused heavily on the planning and reporting sector in order to develop a reporting system that aggregates audit results and produces condensed reports based on the work of the function's 600 auditors. "We now produce a management information report called Internal Control Panel. This report publishes executive summary numbers stemming from the audits throughout the territories," says Dittmeier. "This is an innovative and important performance measurement tool for the company as a whole, because in addition to using it within our department, we also export it to top and middle management, so that they can appreciate the status of internal controls in the company based on our compliance auditing of processes.

"An important part of the Reshaping Program was to introduce a new organizational audit group called operational auditing," says Dittmeier. "Operational auditors are consultants who analyze the adequacy of processes in terms of internal control systems related to a comprehensive range of business objectives, including customer satisfaction, profitability, security, information, etc. In large part, we created operational auditing by hiring from the outside because of its more advanced consulting nature.

"Another interesting feature of our new structure is that one area feeds into another," she says. "The operational audit group feeds important process information into our unit focused on standards and procedures for compliance audit programs. These groups come to better understand the processes and can map them out more effectively, which results in better audit procedures for the large number of auditors working throughout Italy. Simultaneously, the Internal Control Panel produced from our compliance auditing feeds important information to our operational auditors in red flags on defective processes. Lastly, our compliance auditors can support operational audit by performing test work that measures the level of the process defects that operational audit analyses reveal. Any audit report that can actually measure with accuracy the degree of inefficiency and potential loss caused by a process defect is a high impact audit report. The interrelations and synergy between the audit areas is, in my mind, quite powerful."

Prior to the Reshaping Program, the IA function was inspective in nature and in mission, with little programming and planning. Now the core functions of auditing are divided into four areas:

1. Financial services

2. Postal services

3. Corporate processes, such as purchasing or HR

4. IT auditing, working in an integrated service approach with non-IT activities

Within each of these three areas there is a head of compliance auditing and a head of operational auditing. The structures break down into approximately 50 percent financial, 40 percent postal and 10 percent other processes. "The auditing sector for corporate processes is also new," says Dittmeier. "The previous inspector role had only focused on core business financial and postal areas. Also, IA had to accelerate the process of helping the company bring itself up to speed in efforts to comply with the many regulatory requirements emerging in the financial and banking sector."

Internal auditor skills

The Reshaping Program required that the IA staff be brought to a new level of competence and awareness. "We created a training unit, and implemented a training course for operational auditing," says Dittmeier. "Most of the auditors we needed came from outside the company. However, I maintained the 500 existing auditors who had a great number of years in the postal system. With these auditors, it was a question of training them gradually, giving them the basics of compliance auditing with a methodology behind it."

The Reshaping Program training strategy began with establishing both the operational methodology and a new audit culture within the group. This took place through consistent, effective communication. "I believe that communication skills are half the problem or half the answer," Dittmeier says. "In an auditor, I look for strong communication and analytical skills. In fact, a main aspect of the Reshaping Program was to develop competency levels for each person. One of the competencies is general process knowledge, another is audit technique and a third is communication and analytic skills. Auditors must be able to effectively communicate and summarize significant information."

New audit tactics for higher impact

The operational methodology is a fundamental component of the new face of internal auditing at Poste Italiane. As an ex-government agency, there were many opportunities for efficiencies. Significant points in the audit methodology include:

- IA reports that require management agreement on results and include action plans – which are also agreed on by management. "This was new for the company," says Dittmeier. "In addition, due to the complexity of the company, action plans that can be formulated on a local level will not necessarily resolve the problem, so we gather the results in the Internal Control Panel report and bring the problem to a higher level of management to establish broader, more comprehensive plans of action. Finding who can make the change is a key element in the management process of this department."
- A preliminary data analysis, which is being introduced "gradually but with great determination," according to Dittmeier. She and her team are attempting to better target actual risks within the single audit project by giving auditors the tools to look at significant data that can help them decide which areas need the most attention. "We are gradually renewing this IA function, and it is not always easy," she says. "It took us two years to get here; the first part was standardizing audit procedures on a process basis, and now we are introducing analysis and making the audit more flexible."
- A centralized planning process to identify the business units with the highest risk, based on risk scoring. "We look at the units on the basis of size factors and control vulnerabilities in order to make a unified national planning process – rather than the decentralized planning process that was in place previously. We achieve many efficiencies this way."

Another important feature of the Reshaping Program is the way in which the audit team measures its performance. The team introduced a system called Time Monitoring, which monitors and measures average cycles for audit projects, as well as the amount of time invested in professional development and the amount of time spent on various other tasks, such as administrative work. Time Monitoring is conducted on a person-by-person or group-by-group basis.

Audit performance is also measured by management-by-objective (MBO) guidelines, which include the quantity and quality of audit reports issued, the contributions by audit managers to the innovation and development of new audit procedures, and the specific objectives that can be applied to each individual.

The MBO system is top down, so that the objectives of Dittmeier and her team are articulated downward to the various audit managers. "In addition, for the first time in my experience, I have managed to put audit results in the MBO system of company management," Dittmeier says. "This means that operational management is partially measured by audit results. For example, if a branch is responsible for 2,000 post offices, some of them will be audited. If any get poor results, this will be looked at in the performance measurements in the MBO system."

Results

Across the enterprise, the perception of the internal auditors has changed drastically, from inspectors to professionals who contribute to and help the company in a variety of ways by improving processes and managing risks. Through the audit style and communication approach Dittmeier has spearheaded, employees throughout Poste Italiane realize that they have a lot to learn about company procedures and that the auditors can help them to close their own knowledge gaps. It has been a radical change in only three years.

The next step in the Reshaping Program is to introduce a more centralized method of monitoring myriad databases within the company. Audit has never had direct access to these databases, and establishing access will represent an incredible efficiency and effectiveness driver for the IA function.

A second challenge is advancing the professional competencies of the auditors throughout the territories, while the third challenge relates to the control culture of the company. "It's improving but there is a long way to go," says Dittmeier.

As president of The IIA in Italy

Dittmeier is president of The Institute of Internal Auditors (IIA) in Italy. Here, too, she considers herself a leader of change. "My mission is one of significant reorganization, because the association has a lot of hidden potential," she says. "In my philosophy, you need to activate big changes in the beginning or you won't do it at all."

"I have been the president of The IIA in Italy since April 2004, and people say that more has happened since then than happened in the previous three years. I have established a strategic approach by setting up a series of support committees for the IIA chapter (for example, committees dedicated to research, professional development programs, benchmarking, financial sector, etc.) and this has sparked a renewed interest in the chapter. We are bringing in new services and professional training programs, because an important part of our mission is to develop the professional capacity of the internal auditor, and to make our profession a key reference point for corporate and control governance in general."

"For the first time, we have a true strategic plan in place," she says. "We want to raise awareness of the chapter and the profession in general. Leadership in the market must know about internal auditing; they must feel it, see it, understand it and appreciate it."

Interview with Carolyn Dittmeier, director, internal audit, December 2004.

QANTAS: A LEADING AUSTRALIAN AIRLINE DEVELOPS A NEW FACE OF INTERNAL AUDIT

The kangaroo symbol used by Qantas Airways represents this Australian company's proud history of reliability, safety, engineering excellence and customer service. As a leading national brand and Australia's largest domestic and international airline, Qantas employs about 35,000 employees across a global network spanning 140 destinations in Australia, Africa, the Americas, Asia-Pacific, the UK and Europe. Last year, Qantas reported AUD$12 billion in revenues.

The Qantas Group is structured into three business portfolios: Flying Businesses, Flying Services and Associated Businesses. A fourth group, the Corporate Center, provides ongoing support for segments in the three business portfolios. The Flying Business portfolio includes brand-name airlines, such as Qantas, QantasLink, Australian Airlines and Jetstar. The Flying Services portfolio comprises segments focused on airports and catering, as well as a group dedicated to engineering, technical operations and maintenance services. Finally, the Associated Businesses portfolio of Qantas is composed of Qantas Holidays (a tour wholesaler), Freight, Qantas Defense Services (providing engineering services to the Australian air force and government) and Qantas Consulting.

Rob Kella has been the head of Internal Audit at Qantas for two years. His IA team consists of 17 auditors and one support person, all of whom work closely with the company's 200 multi-disciplined specialists dedicated to a wide range of risk, control and assurance issues. These specialists work in a variety of business areas, including Group Security, Group Safety, Group Environment, Occupational Health Services, Aviation Health and Legal. These groups are involved in establishing operational risk policy and monitoring the application of that policy within the business. The IA team works with the control and monitoring functions of these groups.

"On a rotational basis, we work with these risk, control and assurance groups to ensure their auditing methods are robust," says Kella. "We need to ensure ourselves that we can rely on their findings because with the range of risks we face, some 35,000 employees worldwide and AUD$12 billion in revenues, it would be extremely difficult for an 18-person audit team to provide complete coverage. Fortunately, in addition to our external auditors, Internal Audit has these other groups acting in an assurance capacity. Executive management and our Audit Committee expect Internal Audit to work with these groups to provide an overall assurance view."

Kella reports functionally to the Audit Committee and administratively to the CEO. Before he arrived, executive management changed the administrative reporting line from the CFO to the CEO. "On my arrival, the CFO encouraged me to strengthen these reporting lines and increase the involvement of the CEO and the Audit Committee in the audit process," he says. "Today, the CEO and the Audit Committee are involved in major policy decisions coming out of the department. I typically interact monthly with the Audit Committee chairperson to keep him apprised of the progress of audit programs and matters regarding risks, controls and compliance."

IA goals and objectives

According to Kella, the IA mandate at Qantas has always been to improve the effectiveness of the company's risk management, internal control and compliance systems. "That has always been front and center," he says. "We test the systems in place to provide assurance on the efficacy of those systems and work with management to improve them over time."

Prior to the business being privatized as a major Australian public company in 1995, the Australian government owned Qantas. In the highly regulated airline industry, organizations operate under many controls. "Risk is a concept you don't have to sell," Kella says. "This is a business with a significant amount of strategic, operational and financial risk. In light of the corporate governance reforms that have taken place in Australia and worldwide in recent years, our task is to make the group's risk and control system as effective, integrated and commonly understood within the business as possible."

In the past two years, Kella has worked with executive management to further refine the organization's strategy on risks and controls, communicating information about risk, developing a common risk and control language to be used in all areas of the enterprise, and reducing duplication of control systems. "We want to make the control environment as simple and well understood as possible," he says.

Qantas has modelled its internal control framework on COSO, so that its control framework includes compliance, operational and financial reporting controls, and that these components work together seamlessly, incorporating the control environment, risk assessment, control activities, information and communication, and monitoring.

"Qantas had an existing Group Risk function when I arrived, which profiled risk at a group and segment level," Kella says. "Soon after arriving I met with the head of Group Risk and we agreed that co-locating his group with the IA function would assist our two groups to work more effectively. As a result, we have used outcomes from Group Risk's processes to drive our audit planning and methodology and worked together in improving the company's risk management framework."

Kella reorganized the internal audit function to align with the structure of the business. He has four managers, one associated with each of the business portfolios: Flying Businesses, Flying Services, Associated Businesses and the Corporate Center. "We needed a direct and effective way to gather information and deepen our understanding about the specific risks in each business portfolio," he says. "With this organizational structure, we can gather data on key challenges and risks, processes, controls within the processes, and how the risks relate to those controls. From there we manage a continuous queue of audit work with six monthly updates as part of a more formal planning process." The IA team designs six monthly plans that are driven by business challenges, the group's assessment of risks, trends and cycles, as well as particular incidents that may have occurred in the business.

As part of a monitoring and tracking system, monthly self assessments and quarterly reporting on the implementation status of action plans help Internal Audit stay abreast of management progress and process improvement. Internal Audit is also working with Group Risk to develop quarterly risk and control scorecards for each of the segments.

"To help us determine our level of success, in addition to self-assessment, scorecards and peer reviews, we consider factors such as audit plan relevance to the business, reporting and findings, feedback on controls and compliance and management input – in effect, no surprises," Kella says.

Although IA forms its own view, it also works closely with the corporate center, segments, executive management and the Audit Committee to gather agreement and endorsement of the audit work completed. "Our reports do not include recommendations; instead they are populated with agreed management actions. The environment here is open and collegial," Kella says. "Yes, there are times when we disagree, and during those times we are aware that the IA function has both an enforcement and a consulting orientation, so we apply judgment as to when to use each one." As a result of this collaboration and mutual respect, the relationship between the auditors and management is strong. "There are some 60 former auditors across the business," Kella points out. "Our group is seen as a place to develop management, risk and control skills before moving into the business."

Internal auditor skills

In building the internal audit team, Kella looks more for accounting and business backgrounds than engineering or health and safety expertise. "Because of our organizational structure, the real innate skills I'm looking for include problem-solving, communication, an ability and eagerness to learn, a desire to continuously improve, and a comfort level for dealing with a variety of people and business issues," Kella says. Primarily important to him is an orientation toward risks and controls. "This is our bread and butter," he says. "Our auditors must have a strong grasp of risks and controls and how to evaluate them in terms of consequence and likelihood."

Corporate governance

The corporate governance evolution in Australia, as in many other regions of the world, has had an impact on Qantas. In addition to executive management's desire to increase the focus on risk management and control, it is one of the key reasons for re-positioning the head of Internal Audit at Kella's level and developing a more robust IA team. "Bringing me in was the start of re-positioning the department overall, giving it more access to leadership and to information," he says. "Everything the board sees, I see. Qantas recognized that it needed an independent and objective internal audit department, staffed by personnel with a viewpoint on issues across the enterprise."

An important part of Kella's mandate is to work with management to create a more integrated risk management framework and formalized internal control structure. While Qantas is not subject to Sarbanes-Oxley regulations, because the company does not trade in the United States, it is looking to continuously improve its risk management framework and prepare more formal documentation of its control framework, including financial, operational and compliance control documentation. "The whole initiative is driven by the need to demonstrate the efficacy of our controls and how frequently they are assessed," Kella says. "This has been led in part by the Audit Committee and executive management."

Technology

Kella's IA team leverages technology as much as possible, including Lotus Notes, data analytics, transactional risk modeling, ratings and scoring tools, and data profiling and trend analysis. "We are developing tools that are either part of our audit process or that we can leave behind with the business so that they can evaluate their progress and the strength of their controls," he says. "In addition, our data analytics team is looking into the implementation of continuous monitoring to assist in timely identification of control failures."

Challenges ahead

According to Kella, while progress has been made overall, further refinements are needed in the audit planning process at Qantas. He wants to ensure his group is auditing the right things at the right times. "As our business matures in terms of developing an integrated risk management structure, our planning processes will need to evolve with it," he says.

The other challenge Kella cites is finding and retaining talented auditors. "I never stop recruiting," he says. "This business attracts highly qualified and ambitious individuals who are eager to work for an airline. Once we develop our auditors to the appropriate skill level, it is often hard for our department to hold on to them due to their desire to progress their career elsewhere in the business."

Interview with Rob Kella, head of internal audit, March 2005.

INTEGRATED RISK MANAGEMENT AND ASSURANCE AT ROYAL MAIL

Royal Mail Holdings plc has annual sales in excess of £9 billion and more than 190,000 employees. Every working day, Royal Mail collects, processes and delivers around 84 million items to 27 million addresses in the United Kingdom for prices that are among the lowest in Europe. Each week it serves 28 million customers through a network of post offices and the parcels business delivers around 1 million parcels per day across 34 countries for 180,000 customers.

The marketplace in which Royal Mail operates is changing rapidly, and the business is transitioning from its historical position as the United Kingdom's monopoly provider of mail services to operating in a liberalized market. Royal Mail is providing an increasingly wide range of services to meet new demands in response to the next milestone in its history: full competition with private companies in the marketplace in 2006.

Derek Foster is Royal Mail's internal audit and risk management director and has been with the business for three years. Foster joined Royal Mail from General Motors Europe, where he held senior audit and finance line positions. Foster has a 30-strong team and is supported by heads of:

- **Risk Management** – Kevin Fairbotham has been the head of risk management at Royal Mail for just over a year. He is a veteran risk manager and internal auditor, with experience at both Deloitte & Touche and Arthur Andersen.
- **Internal Audit** – Peter Tansley recently joined the group from TUI, a German-headquartered travel business, where he was the European head of operational audit.
- **Business Risk Solutions** – Kamran Malik has been with Royal Mail for three years. Prior to this, he worked in various finance roles in the transport industry for over 10 years on a worldwide basis, including five years at TNT and as finance director for an international courier company.

The challenge for audit and risk management

"It is important to put in context the scale of the challenges faced by Royal Mail," says Foster. "On the one hand, the industry is experiencing threats such as e-substitution. At the same time, the big players are consolidating and looking at acquisitions, and new entrants are targeting profitable segments. Meanwhile, the industry regulator is progressing with an accelerated liberalization of the market in the U.K."

"What that adds up to is a business that needed to get fit for competition very quickly and that was inevitably going to experience significant strains on its system of control in the process. We needed to make sure that we were set up to support the business through this scale of challenge."

Internal audit and risk management – the function

Risk Management, Internal Audit and Business Risk Solutions are the building blocks of Royal Mail's approach – each part of this "triangle" brings individual skills and competencies that are harnessed together to deliver integrated risk management and assurance to Royal Mail. Internal audit and risk

management (IA & RM) support two key committees that oversee Royal Mail's governance processes – these are the Audit and Risk Committee and the Corporate Risk Management Committee.

Risk Management is responsible for policy, procedures, standards, and for facilitating the risk identification process, and Internal Audit for assurance on controls and risks. Business Risk Solutions is a team that works with business management to help identify and deploy solutions to business risks.

The planned activities for the year are compiled in a similar way to many organizations. A risk-based approach is taken, and the plan is created with reference to inherent risk areas, areas of major change, input from senior management, etc. Also, assignments are often triggered from other parts of the triangle. For example, an internal audit assignment, on conclusion, can sometimes result in a client request for Risk Solutions assistance to help with a gap analysis to identify additional work required, or a root cause analysis to help ensure deeper-seated issues are addressed. Equally, an initial risk profiling exercise by Risk Solutions can be followed up by an audit at an appropriate point to assess the effectiveness of controls around risks identified.

"One of the criticisms sometimes faced by risk management functions historically," says Foster, "has been a lack of connection to business reality on the ground; one of the criticisms sometimes faced by internal audit functions historically has been lack of appreciation of the real risks to the business. This way of working helps avoid both issues by getting both disciplines to speak the same language."

Organizing for maximum impact

There are a number of ways the Internal Audit and Risk Management function in Royal Mail looks to maximize the impact and value-add of its service. Among these are:

- **Key linkages:** The risk team and auditors liaise closely with Royal Mail's business planning team. This means that when the annual business plans are being compiled, IA & RM can help ensure that all relevant risks are factored into the plans.
- **Embedding of risk:** The business direction is that risk management is embedded into business as usual activities. IA & RM support this objective by raising awareness of risk around the organization, helping deploy risk identification and assessment techniques, and insisting that risk is transparently considered in project management and change proposals.
- **Collating various assurance activities:** Similar to many large organizations, Royal Mail has a number of assurance activities around the business that address specific risks. IA & RM prepare a summarized report that brings together these disparate sources of assurance for the Audit and Risk Committee. "It is important to give the Audit Committee of any business as comprehensive a picture as possible of the risk and control environment," says Foster. "We clearly distinguish between our independent assessment and the results of assurance providers in specific risk areas."
- **Liaison with unit risk functions:** The IA & RM team works with risk teams embedded with RM's business units to ensure that maximum impact is delivered for Royal Mail's investment in risk and control assurance. IA & RM are also represented on the risk and internal control committees operated by key business units.
- **Early identification of issues:** IA & RM place a lot of emphasis on looking to identify issues and weaknesses as early as possible to prevent problems arising or solve them promptly. This is done in a number of ways including: reviews of major projects on commencement to ensure they are set up to succeed, with appropriate resource and senior management buy-in; use of gap analyses to identify areas where more organizational focus is needed; and ongoing review of a suite of leading indicators of control and performance.

Development of people

IA & RM have developed a team with a mix of competencies. A number of professionals joined the department from within the Royal Mail organization but a number of people also come from external auditing firms. In-house professionals generally follow an accounting-based qualification route. However, the staff also has internal audit, risk management or other relevant qualifications. "Without question, the skills we seek in auditors now are broader business skills, such as the ability to identify and manage risk and analyze processes, rather than crunching numbers," says Fairbotham.

"It sounds obvious," says Foster, "but the key is people. We encourage training, secondments inside and outside the department, multi-tasking and stretch assignments. However, two things are not negotiable: the first is independence – we make sure that what we do is transparently objective and independent; the second is evidence – we feel strongly that our offering has to be fact-based. These are ways of working we insist on as a team."

Goals and objectives

The department has a charter supported by a detailed Destination Statement that sets out the function's goals, objectives and how it seeks to add value to the business. The Destination Statement states:

> "IA & RM will be Royal Mail's centre of excellence in risk management and assurance. We will add value by serving as a trusted business partner to the board and senior managers, helping them to identify and reduce their corporate risks and providing independent assurance on the effectiveness and efficiency of controls.
>
> We will be, for Royal Mail, both a source of competitive advantage and a key part of a lean, effective governance framework. We will deliver cost-effective and timely products that will enable the Board and senior managers to understand, evaluate and manage business challenges, and to obtain confirmation that the challenges are being addressed.
>
> We will offer highly trained, technically qualified and flexible resources to deliver commercially focused, creative and integrated products across Royal Mail. We will set high performance standards and proactively manage development of our people. In these ways, IA & RM will also be a key talent developer for future senior management resources."

"There is still much to do," says Foster. "This is our way of reminding ourselves which way is North."

Future challenges

"Our function is now more risk-focused, leaner, more connected to business activities, and is identifying and helping address issues earlier," says Foster. "The challenge, given the amount of change in our business and the industry, is to try to identify and hopefully help deal with the new or emerging risks that come with this level of change and the new business environment."

Interview with Derek Foster, internal audit and risk management director, January 2005.

STARBUCKS: CONTROL, COMPLIANCE, TEAMWORK

The first Starbucks coffeehouse opened in Seattle in 1971. At that time, no one could have known that Starbucks would one day be as ubiquitous a brand as any the world has ever seen. Recognized in 2003 as "Most Trusted Brand" by *AdWeek*, the company has grown from its single location on the West Coast, to a current total of over 8,000 stores worldwide. Starbucks is widely associated with high-quality coffee and excellent customer service, and it is heralded for promoting the European coffeehouse culture in the United States.

Starbucks' company-operated retail stores accounted for about 85 percent of its net revenues during fiscal 2003. In addition, specialty operations help develop the Starbucks brand outside its retail stores through a number of channels, including foodservice accounts, North American retail store licensing, grocery channel licensing, warehouse club accounts, international retail store licensing, direct-to-consumer marketing and joint ventures. Specialty operations accounted for about 15 percent of net revenues for Starbucks in fiscal 2003.

Financial reporting and compliance have been the focal point for Starbucks' internal audit (IA) team over the past two years. Kiko Harvey, vice president of internal audit since 2001, says the IA team is focused on corporate-level entity risk, information technology systems and corporate governance.

Starbucks has a relatively small audit shop, with five full-time employees. To establish effective risk and control coverage, the IA team uses co-sourcing to supplement their internal audit services. "It involves a lot of collaboration," says Harvey. "Between 30 and 60 auditors from our service provider may work on our account during the year, and we meet and communicate with them regularly. We use this relationship primarily for international auditing and IT audit resources. This year, we also have been leveraging this resource to prepare for Sarbanes-Oxley Section 404 compliance. Because of the company's September year-end, Starbucks is required to implement 404 in fiscal 2005."

Preparing for Sarbanes-Oxley

It was two years ago that Starbucks began preparing for the eventual adoption of Section 404. The internal audit team incorporated control maturity matrices in their audit reports to build the linkage between the control objectives, risks and control activities and have used these control maturity matrices to evolve the testing plan for SOX 404.

"We recognized that Sarbanes-Oxley 404 documentation and testing would be a significant undertaking for a company our size," says Harvey. "Internal Audit had a large inventory of control documentation gathered in one central location because of the nature of the work we have been doing. That meant we were in a good position to take management's documentation and organize it into the format that we needed to develop and execute the testing plans."

Lessons learned

According to Harvey, the primary lesson to pass on to other audit shops preparing for Sarbanes-Oxley is that the first year is going to be difficult. "You are creating documentation and laying down work papers for the first time. In many cases, that can be very resource intensive. The second year will be better," she says.

"We did a couple of things right," she adds. "We conducted a pilot test, so we had an accurate sense of how long testing would take. In 2003, we performed a full trial testing run of a significant transaction cycle and gained an understanding of the average number of hours needed to perform each test. We were surprised and pleased to have stayed pretty true to our pilot thus far. Although we do plan to become more efficient over time, this exercise has enabled us to understand the resources we need to successfully complete the work on time.

"Also, the work paper tool we selected became extremely important to us. We were fortunate to have made good choices. We were able to change direction when we discovered early on that we could not use the documentation tool to effectively administer our testing. It just did not lend itself to work paper reviews, coaching notes and the other activities that go along with auditing. Instead, we decided to use our existing audit work paper tool to better control the testing process. We are very happy with the results."

Although this type of testing and compliance readiness has been disruptive to the company, feedback from leadership and management has been overwhelmingly positive. "There has been a tremendous amount of understanding and interest in the Sarbanes-Oxley project. We are not experiencing pushback or delays from leadership or the other groups with whom we interact, and that helps," she says.

"Sarbanes-Oxley will most likely change IA functions at public companies over the coming years. The recruiting for internal auditors will begin to focus much more on CPAs, and the audits we perform will be more financially oriented rather than operational. Internal audit teams will begin to work extensively with the external auditors, and communication and coordination of efforts will improve."

– Kiko Harvey, vice president of internal audit, Starbucks

Harvey notes that Sarbanes-Oxley testing can be distracting to a company because it represents incremental audit hours that had not been there before. She notes, "Internal audit teams typically focus on one area or business process at a time, but with Sarbanes-Oxley testing we have to look at every key business process every year, and with a focus heavily weighted toward financial reporting controls, rather than the operational controls that were such a large part of our focus in the past. Our businesses are not used to all being audited at the same time. There has been an onslaught of activity and communication across the organization, so it's been a unique and sometimes challenging situation."

Goals

A clear goal for Harvey over the past year has been to develop a sustainable and efficient process for managing compliance with Sarbanes-Oxley code sections 302 and 404 related to financial reporting. Once that process is consistent and repeatable, the IA team plans to transfer some of the work to the businesses. While the businesses have been participating, and they own the control activities and objectives, it is incumbent on the IA team to design a logical assembly of testing, in a way that streamlines the information, centralizes it in one location and creates an easier process for external auditors to access the information and internal auditors to manage it.

"We have regularly scheduled audits on our existing audit plan, and much of the work we are doing in 404 applies to what we would typically do in an audit. We had to determine how to leverage the testing that we were doing to support Sarbanes-Oxley and then add on the operational and compliance testing that is also a part of a full scope internal audit. Our goal is to take advantage of the work that we are doing in Sarbanes-Oxley to fulfill our ongoing IA plan."

Predictions

"Sarbanes-Oxley will most likely change IA functions at public companies over the coming years," Harvey predicts. "The recruiting for internal auditors will begin to focus much more on CPAs, and the audits we perform will be more financially oriented rather than operational. Internal audit teams will begin to work extensively with the external auditors, and communication and coordination of efforts will improve."

Harvey says that, as a group, she and her team have developed an enormous knowledge of how things get done at Starbucks, in all facets of the business. The future challenge becomes how to share the information with the rest of the organization.

Looking forward, Harvey says, "In 2005 and into the future, we expect to bring more of the currently co-sourced Sarbanes-Oxley work in-house and increase our in-house resources to provide a broader range of internal audit services to Starbucks. While we will continue to support management with their testing of the controls over financial reporting, we will need to have a dual focus from now on that includes the more traditional audit areas as well. Although the project has been challenging, it has been interesting work. We hope to see benefits from this exercise in future years."

Interview with Kiko Harvey, vice president of internal audit, June 2004.

ABOUT PROTIVITI INC.

Protiviti is a leading provider of independent internal audit and business and technology risk consulting services. We help clients identify, assess and manage operational and technology-related risks encountered within their industries, and assist in the implementation of processes and controls to enable their continued monitoring. Protiviti assists companies with Sarbanes-Oxley compliance efforts by helping them to document their internal control over financial reporting and disclosure controls and procedures, design and recommend improvements in processes and controls, and organize and manage projects for complying with the Sarbanes-Oxley Act.

Protiviti, a wholly owned subsidiary of Robert Half International Inc. (NYSE: RHI), has more than 40 locations in North America, Europe, Asia and Australia.

Internal audit services

Protiviti provides a full spectrum of services, technologies and skills to management, directors and the internal audit community. We provide world-class professionals and state-of-the-art methodologies and tools. Our network allows us to offer the right resources at the right time and in the right place to meet your needs, and we offer a creative and flexible approach to quality assurance reviews, from a standard compliance report to a full transformation of your capabilities. We also provide ongoing assistance for your internal staff and systems.

Among the services Protiviti's internal audit practice provides include:

- Audit committee advisory
- Co-sourcing and specialized resource enhancement
- Full outsourcing
- Internal audit technology and tool implementation
- Internal audit quality assessments and readiness reviews
- Internal audit transformation
- Information technology audit services
- Start-up and development advice

Information technology internal audit co-sourcing and information technology-related Sarbanes-Oxley compliance solutions

Protiviti provides a broad range of IT internal audit co-sourcing and outsourcing solutions. Our IT internal auditors have broad expertise to assist in all aspects of IT audit services, from the defining of the audit universe and performing the risk assessment, the annual planning and scoping process to the execution of all types of technology-related internal audits. We also provide consulting services around technology risk and control aspects of Sarbanes-Oxley compliance. We provide expertise in documenting critical business processes, identifying risks and mitigating controls, analyzing performance gaps, and recommending and implementing action plans to improve controls.

We help companies understand and evaluate technology risks related to:

- Technology audit planning and risk assessments
- Application control review and internal audits
- Security assessments and internal audits
- Business continuity
- Technology process controls reviews and internal audits
  - Change control and management
  - Security administration
  - Data center operations and problem management
  - Asset management

KnowledgeLeader℠
provided by protiviti®

KnowledgeLeader is a subscription-based website launched in 1998 to help internal audit professionals find tools and best practices that improve the quality and efficiency of their work.

Since that time, KnowledgeLeader has been publishing interviews with chief audit executives on a monthly basis. Within these "Performer Profiles," audit leaders from a variety of companies and industries share their tips and techniques for managing risk and improving business processes. They discuss the challenges they have successfully faced in managing their function within the organization, and provide insights and "lessons learned" for their peers. There is now a library of over 90 audit director profiles on the KnowledgeLeader site.

Other tools and resources available on KnowledgeLeader include:

- **Hot issues** – Weekly informative articles about business risks, internal auditing and IT. Each issue offers actionable advice for improving business performance and managing risk.
- **Checklists and guides** – There are over 300 checklists and guides available. They include questionnaires, best practices, templates, and other tools for managing risk, conducting internal audits and leading an internal audit department.
- **Analyst reports** – To keep members apprised of risks and opportunities in information technology, KnowledgeLeader features white papers from leading IT research analysts.
- **Work programs** – A wide variety of sample internal audit and IT audit work programs can be downloaded and customized.
- **Policies and procedures** – To help members review, update, or create internal policies and procedures, there are many finance, technology and HR policy samples available.
- **Industry news** – Premium business and industry news is provided in real-time on the website.
- **Hubs** – Hubs provide access to the articles and tools, grouped into special "themed" areas for easy access:
  - Business Continuity
  - Business Ethics and Fraud
  - COSO
  - Internal Audit
  - Sarbanes-Oxley
  - Self-Assessment
  - Security
  - Technology

Other resources found on KnowledgeLeader include methodologies and models, white papers, conferences and events, online CPE courses, certification information, audit and accounting standards and organizations, and best business links.

To learn more about KnowledgeLeader, sign up for a complimentary 30-day trial by visiting **www.knowledgeleader.com**. Members of The Institute of Internal Auditors are eligible for a subscription discount.

NOTES

NOTES

NOTES

North America

UNITED STATES
+1.888.556.7420
www.protiviti.com

CANADA
+1.416.350.2181
www.protiviti.ca

Europe

FRANCE
+33.1.42.96.22.77
www.protiviti.fr

ITALY
+39.02.655.06.301
www.protiviti.it

UNITED KINGDOM
+44.207.930.8808
www.protiviti.co.uk

Asia-Pacific

AUSTRALIA
+03.9672.4200
www.protiviti.com.au

CHINA
(86 21) 63915031
www.protiviti.cn

JAPAN
+81.3.5219.6600
www.protiviti.jp

SINGAPORE
+65.6220.6066
www.protiviti.com.sg

Protiviti is a leading provider of internal audit and risk consulting services. We help clients identify, assess and manage operational and technology-related risks encountered in their industries, and assist in the implementation of the processes and controls to enable their continued monitoring. We also offer a full spectrum of internal audit services focused on bringing the deep skills and technological expertise to enable business risk management and the continual transformation of internal audit functions.

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

protiviti.com