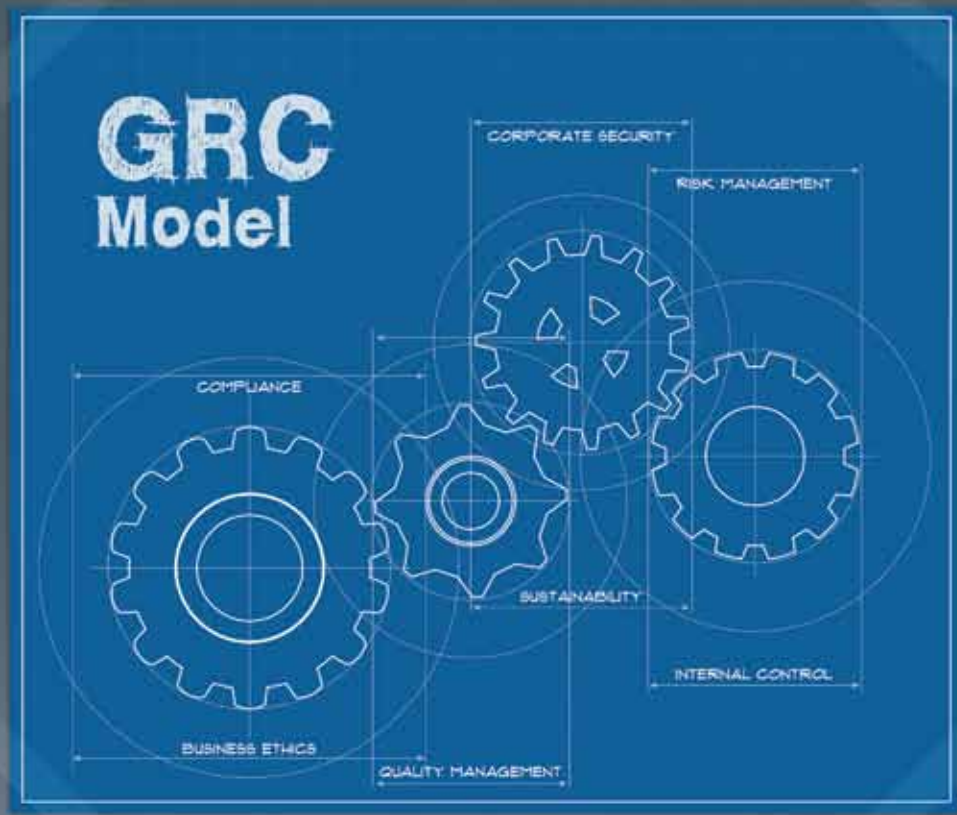




# The GRC Toolbox



# The Use of Integrated Methods to Fight Fraud

Governance, risk management and compliance (GRC) aims to eliminate corporate “silos” and to integrate organizational management, protection against fraud and theft and regulatory adherence. However, those who devise GRC programs often underestimate fraud risk. CFEs can help by heightening their employers’ and clients’ awareness and understanding of fraud and by showing them how GRC can help detect and prevent it.

**R**evenue had soared suddenly in the Asia-Pacific region of a U.S.-headquartered aerospace multinational while its business had tailed off elsewhere. Eager to celebrate this success and spur his North American and European managers back into growth, the CEO toured several plants throughout the Far East and publicly lavished praise on its regional director. At the same time, he let it be known that he wanted innovative strategies to restore market share lost on both sides of the Atlantic. The CEO was confident that his plan would work. He had a good team; they simply needed to be reminded of their dispensability.

Just as the company’s Gulfstream G650 touched down and taxied across the runway at JFK, the CEO’s smartphone vibrated. Jet-lagged, he wearily retrieved it from his jacket. A text message from his personal assistant asked that he accept a call at home that evening from the vice president of internal audit on a matter of great urgency.

“I can’t even leave town for a few days without someone getting into a cold sweat,” he thought. Several hours later, he too was unnerved, spilling his gin and tonic when the internal audit chief revealed there were unmistakable signs of revenue overstatement in the Asia-Pacific region.

“How bad?” the CEO asked.

“Very bad.”

“How could this be?” the CEO exclaimed. “I was just there. The place is booming!”

“You saw what they chose to show you. Apparently they just made up last year’s numbers and paid off everyone who was in a position to jeopardize their performance bonuses. We noticed it as soon as we looked.”

But they had not looked soon enough, the CEO ruefully realized. While he had been focused on motivating the troops, his best-laid plan had been lacking — in governance, in risk management and in compliance. Later, a fraud examination would reveal that he and the Asia-Pacific regional director had been passive stewards. The company had not conducted adequate background checks on its local hires and had not trained its expat staff on doing business ethically in an emerging market and complying with the U.S. Foreign Corrupt Practices Act. Perhaps worse, the home office had not noticed that the company’s code of ethics had never been translated into other languages.

**By Robert Tie**

The CEO saw that the board was going to crucify him, the press would humiliate them all and the company's shares would take a solid hit. Plus, the regulators would have to be dealt with. It was infuriating, the CEO thought. A few days later, thousands of investors joined him in this sentiment.

This fictional case study exemplifies one of many kinds of the corporate fraud that increasingly plagues all nations. While it is avoidable, there are not enough signs that businesses are doing everything possible to significantly mitigate it.

### NEEDED: RESULTS

Despite two financial mega-crises in one decade, there are indications fraud still may not be seen as a lethal threat to the global financial system and the welfare of every nation's citizens. Over the past 10 years, failures in governance and accounting destroyed billions in investors' savings and widespread conflicts of interest evaporated additional billions in homeowners' equity. Two of the most important laws in generations — the Sarbanes-Oxley Act of 2002 and the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 — have led to the imprisonment of many who engineered these catastrophes.

Nevertheless, according to the ACFE's 2010 "Report to the Nations," 5 percent of global GDP, or nearly \$3 trillion, was lost to fraud in 2009. The U.S.'s share of those losses — \$700 billion — was slightly larger than its massive defense budget. Most other nations suffer generally the same proportion of fraud-related damage as America. Yet much more must be done to rein in these losses, and skillfully applied anti-fraud measures should be a central ingredient in the action plan.

The hope among fraud fighters is that organizations will better integrate their governance, risk management and compliance (GRC) and anti-fraud programs, creating synergies and efficiencies that will better detect and deter fraud. For that coordination to occur, though, leaders have to recognize the ubiquity and seriousness of the fraud threat. This article offers suggestions and practical tips on how CFEs can spread fraud awareness throughout their organizations and improve their own enterprise-wide fraud detection capabilities.

### WHAT IS GRC?

Norman Marks is a vice president and GRC evangelist for enterprise software giant SAP. A former corporate chief risk officer and head of internal audit, he also is an Institute of Internal Auditors' (IIA) blogger ([www.theiia.org/blogs/marks](http://www.theiia.org/blogs/marks)) and columnist and a fellow of the Open Compliance and Ethics Group (OCEG), a GRC-focused nonprofit organization.

Marks likes to cite an incisive quote by Lee Dittmar, a principal of Deloitte Consulting. In a paper on GRC, Dittmar said, "In the complex and constantly changing sea of acronyms, abbreviations and other abstractions, there is one that is simultaneously met with affirmation and apathy, confirmation and confusion, and recognition and rejection. I am of course writing about GRC."

THE HOPE AMONG FRAUD FIGHTERS IS THAT ORGANIZATIONS WILL BETTER INTEGRATE THEIR GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE (GRC) AND ANTI-FRAUD PROGRAMS, CREATING SYNERGIES AND EFFICIENCIES THAT WILL BETTER DETECT AND DETER FRAUD. FOR THAT COORDINATION TO OCCUR, THOUGH, LEADERS HAVE TO RECOGNIZE THE UBIQUITY AND SERIOUSNESS OF THE FRAUD THREAT.

As a practical example of these contradictory reactions, Marks notes that some executives embark on a GRC program whose potential outcome may be as dicey as the very risks it aims to mitigate.

"They do it because everyone else is doing it, and they don't want to lag behind their peers and the competition," he said.

The latest numbers support this view. Forrester Research predicted that spending on GRC software, consulting and related services is growing at a breakneck pace and will likely soar from \$2.6 billion in 2010 to \$24 billion in 2015.

To explain GRC, Marks cited OCEG's definition:

"... a system of people, processes and technology that enables an organization to understand and prioritize stakeholder expectations; set business objectives that are congruent with values and risks; achieve objectives while optimizing risk profile and protecting value; operate within legal, contractual, internal, social and ethical boundaries; provide relevant, reliable and timely information to appropriate stakeholders; and enable the measurement of the performance and effectiveness of the system."

OCEG said these activities most commonly take place across business, administrative or support units focused on governance, strategy and business performance management, risk management, compliance, internal control, corporate security, legal, information technology, business ethics, sustainability and corporate social responsibility, quality management, human capital and culture and audit and assurance or finance.

Marks also recommended comparing the following characteristics of a) *fragmented* or ineffective and b) *federated* or effective GRC implementations. Fragmented GRC, Marks said, is a prickly tangle of controls and practices buried inside functional or geographic "silos" with hundreds — or even thousands — of isolated activities. It is bewilderingly complex and duplicative, even as it leaves major gaps uncovered and fails to deliver desired results. In contrast, Marks said, federated GRC is the more efficient model. Everyone works together, sharing best practices

and using common tools to rely on each other's work. This model does not require unilateral ownership, but must be cooperative and well coordinated.

Sounds good, but businesses will have to identify appropriate strategic and tactical guidelines and best practices to get there. OCEG and other such organizations can help in that respect. Likewise, CFEs need their own source of practical instruction and resources if they are to provide effective leadership to their employers and clients on using GRC to anticipate, detect and stop fraud.

### MISSING THE POINT

Stark, but apt, comparisons — like the cost of fraud in the U.S. equaling the defense budget — put the dimensions of fraud in sharp relief. Nevertheless, in late 2010 KPMG LLP's Audit Committee Institute (ACI), whose 1,200 members serve on the boards of companies around the world, reported that a survey of its members revealed that oversight of fraud risk was a "great" concern for only 6 percent of them.

Imagine yourself in a general session at an ACI conference. When asked, only 72 of the 1,200 attendees raise their hands to say, "Yes, fraud is a great concern to me." The other 1,128 believe either that fraud is not a big threat or that their

organizations' controls are so good that the audit committees need not be particularly worried about fraud risk.

What does concern them, then? As recently as April 2011, the ACI's latest member survey showed that members were more concerned with other major risks, including the Gulf oil spill, WikiLeaks' disclosures of classified information, political unrest in the Middle East and North Africa, and the earthquake and tsunami in Japan. Because such geopolitical factors are of major importance and danger, audit committees should not be accused of sleeping at the wheel. But they need to be more attentive to fraud risk.

In the April ACI survey, tone at the top ranked fifth and ensuring audit committee effectiveness was seventh (!) among member concerns, but there was no high-ranking mention of fraud or the collateral damages it can inflict on an organization, including debarment from government markets, such as the Medicare and Medicaid programs or corporate reputation damage that shrinks market share. Furthermore, in its summary of the conference, the ACI highlighted a keynote speaker who emphasized that "the main task for boards is not governance, but leadership." The aerospace CEO mentioned in the opening case study would have agreed — before his epiphany, but not after it.

## NEW COURSE!



# Fraud Risk Management

**CPE Credit: 16**

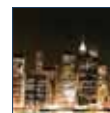
*Course Level: Specialized*

*Prerequisite: None*

With organizations losing an estimated 5 percent of their annual revenues to fraud, the need for a strong anti-fraud stance and proactive, comprehensive approach to combating fraud is clear. This course will explain how organizations can integrate anti-fraud initiatives into their risk management programs by:

- *Identifying, assessing and managing fraud risks from all sources*
- *Establishing an anti-fraud culture and promoting fraud awareness throughout the organization*
- *Developing a system of internal controls to address the entity's fraud risks*
- *Addressing and responding to any identified instances of fraud*

**Your next chance to attend this exciting course:**



**October 13-14, 2011  
New York, NY**

For more information or to register, visit [ACFE.com/FRM](http://ACFE.com/FRM)



## APPLYING GRC TO FRAUD

The ACFE has created and is continuing to develop a series of GRC resources for its members. The goal is to enhance members' GRC knowledge and help them develop the skills they need to guide their organizations in designing and implementing GRC programs that are effectively integrated with their existing anti-fraud programs. For example, the ACFE recently premiered a two-day live seminar, "Fraud Risk Management" and a one-day seminar, "Fraud-Related Compliance." Additionally, the ACFE offers a number of self-study courses on GRC issues related to fraud. New resources will be available next year, including a course on using data analysis as part of an effective compliance program.

CFEs also can take independent action to strengthen their skills. In April 2011, Marsh Inc. and the Risk and Insurance Management Society (RIMS) released "Excellence in Risk Management VIII," the latest in a series of surveys that began in 2004. Marsh, a subsidiary of Marsh & McLennan Companies Inc., is a global insurance brokerage and risk advisory firm. RIMS is a global association for risk management professionals.

The survey results included responses from more than 1,000 risk managers and C-level, finance and other executives. It found that 80 percent said senior leadership's expectations of their organization's risk management departments have increased over the past three years. When C-suite respondents were asked in what areas expectations have grown:

- 61 percent said they want to see risk managers integrate deeper with operations.
- 60 percent said risk managers need to execute day-to-day activities more effectively.
- 58 percent said risk managers should do more to lead enterprise risk management activities within the organization.
- 54 percent said risk managers need to provide better quantification and analysis on risk management, develop greater understanding of non-insurance risks and increase their involvement in the organization's overall business strategic planning efforts.

Based on the survey responses, Marsh and RIMS offered recommendations for risk managers. While most CFEs are not risk managers, these recommendations provide sound advice on both giving and receiving information about fraud risks in an organization:

- Look for leadership opportunities in your organization's advancement in enterprise risk management. Whether it is making sure risk management is on the agenda at appropriate meetings, creating or improving a cross-functional risk committee or leading the entire effort, be a catalyst. As the risk manager at one health care organization put it, the firm's new emphasis on ERM means her department now has a "chance to shine."

- Continue to break down organizational silos. Embrace senior management's goal to integrate deeper with operations. Focus risk management efforts on the value you can add to the organization in achieving the organization's strategic and operational objectives.
- Get out of the office when possible and see how your company actually does business.
- Look for allies in other departments. You may find, for example, that your finance department shares the desire to improve the firm's technology. Or that your IT director has some thoughts on better protecting the company's digital assets. The key is to have the conversations.
- Understand the analytical tools and methodologies that are available to help you dig deeper into your company's risk issues. It is important to find the appropriate tools, use them effectively and share the results with decision makers.

Pam Rogers of Marsh Risk Management Optimization in Minneapolis and Jason Lelio, CFE, CPA, CFF, of Marsh Forensic Accounting and Claims Services in Boston emphasized that the survey addressed all organizational risks and did not analyze or comment on fraud risk in particular.

Respondents to the Marsh/RIMS survey ranked total cost of risk (TCOR) highest among key performance indicators (KPIs) for the risk management function. However, Rogers said that TCOR doesn't focus on fraud much, if at all.

Because fraud claims are unpredictable, Rogers said, fraud losses generally are not reserved for the balance sheet. In contrast, workers' compensation or automobile liability or general liability policies have predictable volume and losses. So, they are reportable on the liability side of the balance sheet, and, therefore, are counted in TCOR. Thus, survey respondents' most popular KPI does not fully encompass the costs of fraud.

"CFEs should note that when an expensive workers' compensation claim causes a high TCOR number, that gets a lot of attention," Rogers said. "Safety programs are put in place. But, if a risk — such as fraud — doesn't generate a significant TCOR value, it's that much more difficult to get resources to mitigate it."

Lelio added that estimating the potential for fraud losses is difficult because the range of the loss impact can be so great.

"No one knows how much an employee is going to steal," he said. "Every company thinks that it will be able to control losses. But clients tell me all the time that they had no idea that they could suffer such a significant fraud loss. And that's why they often underinsure themselves. Even though fraud policy premiums are not too expensive, companies don't buy enough coverage because they can't imagine employees scheming together to defraud the company for that much money." Lelio added that this is why it is important to periodically perform a fraud risk assessment.

"If you put good controls around your fraud risk indicators, it helps limit your potential fraud exposure. Whether it's rising



## Tip:

**BUDDY UP TO A FINANCIAL OR OPERATIONS ANALYST... SEE HOW HE OR SHE USES THE APPLICATION, AND SOON YOU'LL BE TAPPING INTO THE DATA WAREHOUSE YOURSELF, FOLLOWING UP ON POTENTIAL RED FLAGS OF FRAUD.**

shrinkage numbers or employee expense report thefts, you have to plan your internal audits to identify these red flags before you experience a significant loss," he said.

Rogers said CFEs can help generate support for fraud mitigation efforts by becoming members of their organizations' risk committees. They should build networks of people who feed them information about what is going on in their organizations, she said.

"CFEs also can contribute to fraud detection and prevention by facilitating discussions on fraud risk," Lelio said. "It's important to educate the entire organization about fraud risk and to get high-level support so that all employees know management takes fraud seriously. It's a great fraud deterrent when employees know the company and its executives are alert to the risk of employee fraud."

### CFEs AROUND THE ORGANIZATION

Marks recommends that CFEs seeking software for GRC tasks should first ask whether any of their organizations' existing applications could help them identify fraud indicators and provide the analytics they need.

In-house financial analysts, who review trends and variances to help management, often have IT-supported software already running on corporate databases that CFEs can learn to use.

CFEs at first should not seek to *create* reports to access relevant data, Marks said. They should instead ask to be able to run and have access to the same reports that the financial analysts are using, which will reveal trends in the businesses and fluctuations in revenue. Once CFEs become familiar with the reports and understand how the data reveals potential fraud indicators, Marks said, then they can ask to create their own reports. Such software typically enables users to design their own reports, rather than having to request them from IT departments.

"Buddy up to a financial or operations analyst," Marks said. "See how he or she uses the application, and soon you'll be tapping into the data warehouse yourself, following up on potential red flags of fraud."

### MISSION: CRITICAL

Marks reminded CFEs that they can improve fraud awareness and anti-fraud programs by guiding and putting to good use the activities of people in other parts of the organization. For example, financial and operations analysts are in a good position to identify potential frauds if they are alert to the possibility and know what red flags to look for. Without anti-fraud guidance, however, their attention likely will remain focused only on their own accounting and reporting needs.

"You need better coordination than that to manage risk for the whole enterprise," he said.

Marks believes this is where CFEs can make a major contribution. The most effective CFEs are those who evolve their role and interdepartmental visibility, changing how others throughout their organizations perceive and interact with them, he said.

"Educate your colleagues in other departments," Marks advised. He encourages CFEs to help the governance, risk management and compliance staffs build fraud risk assessments and monitoring into their activities. "Foster communication and cooperation in fraud prevention and detection. Show them how to work together to anticipate fraud risk and build appropriate controls and other anti-fraud measures into business strategy as they formulate it," he said.

As CFEs become more familiar with GRC, they should continually combine that growing knowledge with their fundamental anti-fraud skills.

"Understand your organization's business and its processes," Marks said. "Learn how to use existing monitoring tools to perform better fraud risk assessments and identify the not-so-obvious frauds — the ones that go undetected and do the most damage."

Once again, crisis presents opportunity — in this case, for CFEs to infuse their organizations' governance, risk management and compliance programs with anti-fraud awareness and action. 🔍

---

**Robert Tie** is a New York business writer. His email address is: [bob@roberttie.com](mailto:bob@roberttie.com).

---