KPMG FORENSIC

Fraud Risk Management

Developing a Strategy for Prevention, Detection, and Response

ADVISORY

AUDIT ▪ TAX ▪ ADVISORY

Contents

Foreword

Instances of corporate fraud and misconduct remain a constant threat to public trust and confidence in the capital markets. As organizations strive to achieve compliance with an array of new antifraud laws and regulations that are not prescriptive on the design of controls in this area, management's agenda is focusing on efforts to:

- Understand the fraud and misconduct risks that can undermine their business objectives
- Determine whether antifraud programs and controls are actually effective in reducing instances of fraud and misconduct
- Gain insight on better ways to design and evaluate controls to prevent, detect, and respond appropriately to fraud and misconduct
- Reduce exposure to corporate liability, sanctions, and litigation that may arise from violations of law or market expectations
- Derive practical value from compliance investments by creating a sustainable process for managing risk and improving performance
- Achieve the highest levels of business integrity through sound corporate governance, internal control, and transparency.

This white paper provides an overview of fraud risk management fundamentals, identifies new regulatory mandates from around the world, and spotlights key practices that organizations have generally found to be effective in the current environment.

We hope this perspective provides fresh insights as you consider the risks of fraud at home and abroad, and the effectiveness of controls you rely on to mitigate those risks.

Adam Bates
Global Chairman, KPMG Forensic [SM]

Executive Summary

In the wake of high-profile corporate scandals as well as new regulations worldwide, many business leaders are increasingly aware of the need to create company-specific antifraud measures to address internal corporate fraud and misconduct. While acknowledging that no single approach to fraud risk management can fit every organization's needs, this white paper spotlights key practices that organizations have generally found to be effective when tailoring a company-specific antifraud program, and offers a strategic approach to aligning corporate values with performance.

The Business Imperative

As companies achieve compliance with new antifraud laws and regulations, their agendas center on management's efforts to:

- Understand fraud and misconduct risks that can undermine their business objectives
- Reduce exposure to corporate liability, sanctions, and litigation
- Achieve the highest levels of business integrity through sound corporate governance, internal control, and transparency.

Fraud: Any intentional act committed to secure an unfair or unlawful gain.

Misconduct: A broad concept, generally referring to violations of law, regulations, internal policies, and market expectations of ethical business conduct.

Convergence of Regulatory Challenges

In recent years, a variety of laws and regulations have emerged worldwide, providing organizations with an array of criteria to incorporate into their antifraud efforts. These laws include:

- **Australia**: The Corporate Law Economic Reform Program (Audit Reform & Corporate Disclosure) Act 2004
- **Canada**: The Canadian Criminal Code
- **European Union**: Financial Services Action Plan (FSAP)
- **United Kingdom**: Companies (Audit, Investigations, and Community Enterprise) Act of 2004
- **United States**: The USA PATRIOT Act, the Foreign Corrupt Practices Act, the Sarbanes-Oxley Act of 2002, SAS 99, various NYSE & NASDAQ listing standards, and Public Company Accounting Oversight Board (PCAOB) Standard #2

The Key Objectives: Prevention, Detection, Response

An effective, business-driven fraud risk management approach encompasses controls that have three objectives:

- **Prevent**. Reduce the risk of fraud and misconduct from occurring.
- **Detect**. Discover fraud and misconduct when it occurs.
- **Respond**. Take corrective action and remedy the harm caused by fraud or misconduct.

Pulling It All Together

The challenge for companies is to develop a comprehensive effort to:

- Understand all of the various control frameworks and criteria that apply to them.
- Categorize risk assessments, codes of conduct, and whistleblower mechanisms into corporate objectives.
- Create a broad ranging program that manages and integrates fraud prevention, detection, and response efforts.

An Ongoing Process

Effective fraud risk management provides an organization with tools to manage risk in a manner consistent with regulatory requirements as well as the entity's business needs and marketplace expectations. Such an approach has four phases:

- **Assess Risks**. Identify the scope of the analysis and key stakeholders, profile the current state of fraud risk management, set targets for improvement, and define steps necessary to close the "gap."
- **Design**. Develop a broad ranging program that encompasses controls to prevent, detect, and respond to incidents of fraud or misconduct.
- **Implement**. Deploy a strategy and process for implementing the new controls throughout the organization and assign responsibility for leading the overall effort to a senior individual.
- **Evaluate**. Assess existing controls compared with legal and regulatory frameworks as well as leading practices, such as internal investigation protocols or due diligence practices.

Defining Fraud and Misconduct

Fraud is a broad legal concept that generally refers to an intentional act committed to secure an unfair or unlawful gain.[1] Misconduct is also a broad concept, generally referring to violations of laws, regulations, internal policies, and market expectations of ethical business conduct. Together, they fall into the following categories of risk that can undermine public trust and damage a company's reputation for integrity:

- Fraudulent financial reporting (e.g., improper revenue recognition, overstatement of assets, understatement of liabilities)
- Misappropriation of assets (e.g., embezzlement, payroll fraud, external theft, procurement fraud, royalty fraud, counterfeiting)
- Revenue or assets gained by fraudulent or illegal acts (e.g., over-billing customers, deceptive sales practices, accelerated revenue, bogus revenue)
- Expenses or liabilities avoided by fraudulent or illegal acts (e.g., tax fraud, wage and hour abuses, falsifying compliance data provided to regulators)
- Expenses or liabilities incurred for fraudulent or illegal acts (e.g., commercial or public bribery, kickbacks)
- Other misconduct (e.g., conflicts of interest, insider trading, discrimination, theft of competitor trade secrets, antitrust practices, environmental violations)

Scandals and failures, together with flourishing and cynical greed, may have profound and prolonged effects on public opinions. It is our collective duty and well understood interest to demonstrate that market economy goes together with integrity and common good.

Michel Prada
Chairman of the Autorité des Marchés Financiers French Securities Regulators
Global Public Policy Symposium
October 20, 2005

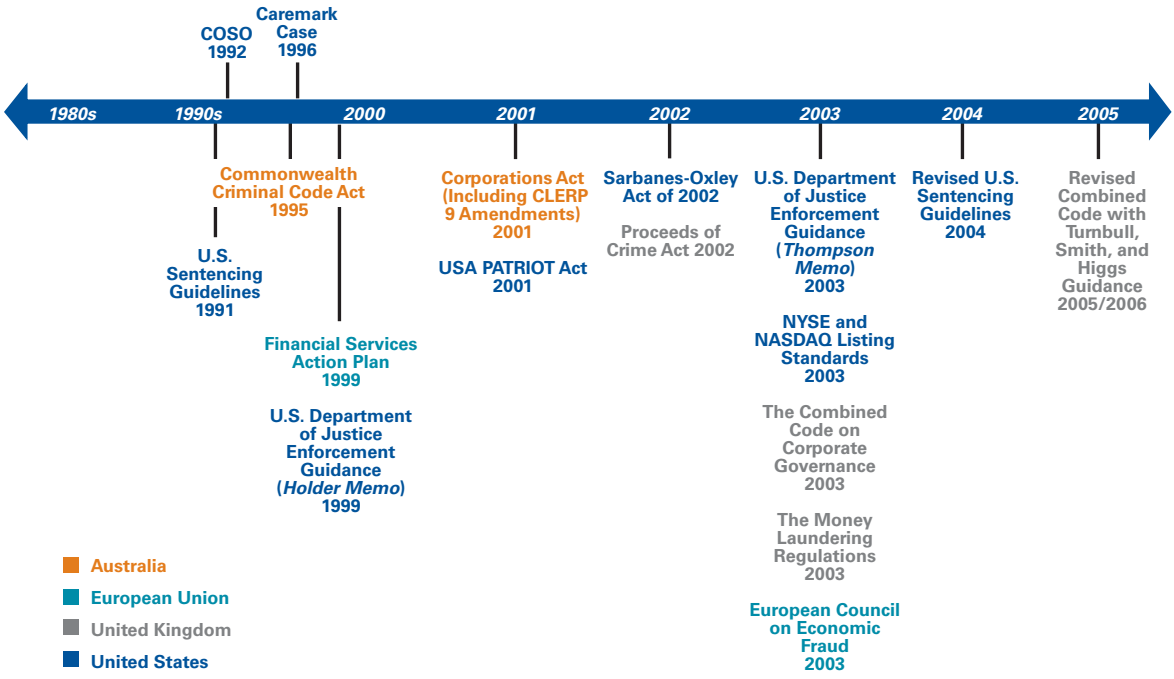
[1] Bryan A. Garner, Editor, *Black's Law Dictionary,* Eighth Edition, West Group, 2004

Convergence of Regulatory Challenges

Governments around the world have responded to corporate scandals and fraudulent activity by instituting legislative and regulatory reforms aimed at encouraging companies to become more self-governing. In recent years, a variety of laws and regulations have emerged, and the timeline in *Figure 1* provides a selection of important global regulations and events.

Note also that a summary of relevant regulations appears in "Appendix: Selected International Governance and Antifraud Criteria" beginning on page 24.

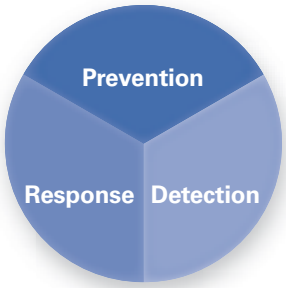
Figure 1: A Timeline



Source: KPMG LLP (U.S.), 2006

> *Undetected financial fraud is one of the greatest risks to an organization's viability and corporate reputation, and it has the capacity to draw into its sphere all associated people, not only the guilty.*
>
> Jeffrey Lucy
> Chairman, Australian Securities and Investments Commission
> November 10, 2005

The Key Objectives: Prevention, Detection, Response



An effective, business-driven fraud and misconduct risk management approach is one that is focused on three objectives:

- **Prevention**: controls designed to reduce the risk of fraud and misconduct from occurring in the first place
- **Detection**: controls designed to discover fraud and misconduct when it occurs
- **Response**: controls designed to take corrective action and remedy the harm caused by fraud or misconduct

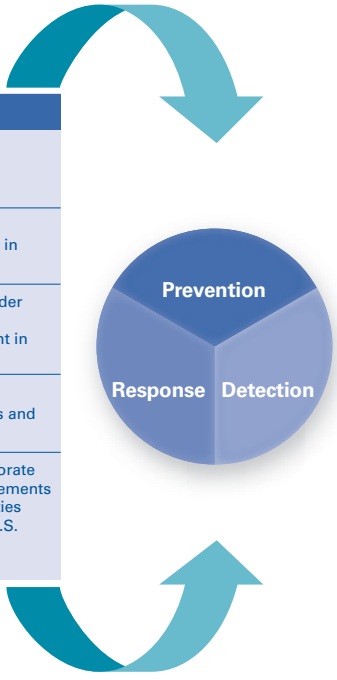
Putting It All Together

Just as there is an array of fraud and misconduct risks facing a company, there is an array of control criteria that various regulatory programs require companies to adopt. The challenge for companies, therefore, is to adopt a comprehensive and integrated approach that takes all relevant considerations into account and enables them to work together. Doing so helps avoid duplicative effort, resource fragmentation, and "slippage between the cracks" associated with a one-off or silo approach.

Such an undertaking begins with understanding all of the various control frameworks and criteria that apply to the company (see *Figure 2*). When this categorization is complete, the organization has the information it needs to create a comprehensive program in which the elements of prevention, detection, and response can be integrated and managed.

Figure 2: Selected International Standards

Jurisdiction	*Framework*	*Relevance*
Australia	Corporations Act 2001 (including CLERP 9 Amendments)	Aims to strengthen the financial reporting framework.
Canada	The Multilateral Instrument 52-109	Promotes an "internal control culture" for improving the quality of financial reporting in Canada.
Netherlands	Corporate Governance Code of Conduct 2004	Seeks to improve transparency in shareholder and management relations as well as the structure and accountability of management in the Netherlands.
United Kingdom	The Companies Act of 2004	Aims to improve the reliability of financial reporting and the independence of auditors and auditor regulation in the United Kingdom.
United States	Sarbanes-Oxley Act of 2002	Introduced substantial changes to the corporate governance and financial disclosure requirements of organizations registered with the Securities and Exchange Commission and listed on U.S. stock exchanges.



Source: KPMG LLP (U.S.), 2006

Figure 3 lists sample elements of a comprehensive program designed to prevent, detect, and respond to fraud.

Figure 3: Sample Antifraud Program Elements

Prevention	*Detection*	*Response*
Board/audit committee oversight Executive and line management functions Internal audit, compliance, and monitoring functions		
• Fraud and misconduct risk assessment • Code of conduct and related standards • Employee and third-party due diligence • Communication and training • Process-specific fraud risk controls	• Hotlines and whistle-blower mechanisms • Auditing and monitoring • Proactive forensic data analysis	• Internal investigation protocols • Enforcement and accountability protocols • Disclosure protocols • Remedial action protocols

Source: KPMG LLP (U.S.), 2006

The next section spotlights some of the common control elements identified in *Figure 3* and offers considerations for their design.

Prevention

Preventive controls are designed to help reduce the risk of fraud and misconduct from occurring in the first place.

Leadership and Governance

Board/Audit Committee Oversight

An organization's board of directors plays an important role in the oversight and implementation of controls to mitigate the risk of fraud and misconduct. The board, together with management, is responsible for setting the "tone at the top" and ensuring institutional support is established at the highest levels for ethical and responsible business practices.

Directors have not only a fiduciary duty to ensure that an organization has programs and controls in place to address the risk of wrongdoing but also a duty to ensure that such controls are effective.[2]

As a practical matter, the board may delegate principal oversight for fraud and misconduct risk management to a committee (typically audit), which is tasked with, among other things:

- Reviewing and discussing issues raised during the entity's fraud and misconduct risk assessment
- Reviewing and discussing with the internal and external auditors findings on the quality of the organization's antifraud programs and controls
- Establishing procedures for the receipt and treatment of questions or concerns regarding questionable accounting or auditing matters.[3]

> *A robust fraud strategy is one that is sponsored at the highest level within a firm and embedded within the culture. Fraud threats are dynamic and fraudsters constantly devise new techniques to exploit the easiest target.*
>
> Philip Robinson
> Financial Crime Sector Leader, Financial Services Authority
> February 27, 2006

[2] *In re Caremark Int'l Derivative Litig.*, Del. Ch., 698 A.2d 959 (1996).

[3] A listed company's audit committee must establish procedures for the receipt, retention, and treatment of complaints regarding accounting, internal accounting controls, or auditing matters, and allow for the confidential, anonymous submission by employees of concerns regarding questionable accounting or auditing matters. See Exchange Act section 10A(m)(4) and SEC Rule 10A-3(b)(3), effective April 2003, which may be found at http://www.sec.gov/rules/final/33-8220.htm.

Senior Management Oversight

To help ensure that fraud and misconduct controls remain effective and in line with governmental standards, responsibility for the organization's fraud and misconduct risk management approach should be shared at senior levels (i.e., individuals with substantial control or a substantial role in policy-making). This critical oversight begins with prevention and must also be part of detection and response efforts.

The chief executive officer is ideally positioned to influence employee actions through his or her executive leadership, specifically by setting the ethical tone of the organization and playing a crucial role in fostering a culture of high ethics and integrity. For instance, the chief executive can lead by example, allocating resources to antifraud efforts and holding senior management accountable for compliance violations.

Direct responsibility for antifraud efforts should reside with a senior leader, often a chief compliance officer who works together with internal audit staff and designated subject matter experts. The chief compliance officer is responsible for coordinating the organization's approach to fraud and misconduct prevention, detection, and response. When fraud and misconduct issues arise, this individual can draw together the right resources to deal with the problem and make necessary operational changes. The chief compliance officer may also chair a committee of cross-functional managers who:

- Coordinate the organization's risk assessment efforts
- Establish policies and standards of acceptable business practice
- Oversee the design and implementation of antifraud programs and controls
- Report to the board and/or the audit committee on the results of the organization's fraud risk management activities.

Other business leaders such as department heads (e.g., product development, marketing, regulatory affairs, human resources) should also participate in responsibilities under the organization's antifraud strategy; they oversee areas of daily operations in which risks arise. Such department heads can serve as subject matter experts to assist the chief compliance officer with respect to their particular areas of expertise or responsibility.

> *Achieving good corporate governance is not solely the responsibility of the directors, investors and regulators; it should be a core objective of senior management. Poor corporate governance weakens a company's potential and at the worst can pave the way for financial difficulties and even fraud.*
>
> Bill Witherell
> Director for Financial and Enterprise Affairs
> Organisation for Economic Co-operation and Development
> CFO Strategies: Corporate Accountability Forum 2004, May 17, 2004

Internal Audit Function

The modern organization's internal audit function is a key participant in antifraud activities, supporting management's approach to preventing, detecting, and responding to fraud and misconduct. KPMG's 2003 Fraud Survey notes that 65 percent of respondents indicated that frauds were uncovered through the work of internal audit. Such responsibilities represent a change from the more traditional role of internal audit (that is, examining the effectiveness of the entity's controls). In general, internal audit should be responsible for:

- Planning and conducting the evaluation of design and operating effectiveness of antifraud controls
- Assisting in the organization's fraud risk assessment and helping draw conclusions as to appropriate mitigation strategies
- Reporting to the audit committee on internal control assessments, audits, investigations, and related activities.

Fraud and Misconduct Risk Assessment

All organizations typically face a variety of fraud and misconduct risks. Like a more conventional entity-wide risk assessment, a fraud and misconduct risk assessment helps management understand the risks that are unique to its business, identify gaps or weaknesses in control to mitigate those risks, and develop a practical plan for targeting the right resources and controls to reduce risk.

Management should ensure that such an assessment is conducted across the entire organization, taking into consideration the entity's significant business units, processes, and accounts.

With input from control owners as to the relevant risks to achieving organizational objectives, a fraud and misconduct risk assessment includes the steps listed in *Figure 4.*

Figure 4: Fraud Risk Assessment Process

Source: KPMG LLP (U.S.), 2006

While management is responsible for performing a targeted risk assessment process and considering its results in evaluating control effectiveness, the audit committee typically has an oversight role in this process. The audit committee is responsible for reviewing management's risk assessment, ensuring that it remains an ongoing effort, and interacting with the entity's independent auditor to ensure that assessment results are properly communicated.

Code of Conduct

An organization's code of conduct is one of the most important communications vehicles that management can use to communicate to employees on key standards that define acceptable business conduct. A well-written and communicated code goes beyond restating company policies—such a code sets the tone for the organization's overall control culture, raising awareness of management's commitment to integrity and the resources available to help employees achieve management's compliance goals.[4]

52%

Percentage of U.S. employees who reported that their codes of conduct are not taken seriously.

KPMG Forensic Integrity Survey 2005 – 2006

A well-designed code of conduct typically includes:

- High-level endorsement from the organization's leadership, underscoring a commitment to integrity
- Simple, concise, and positive language that can be readily understood by all employees
- Topical guidance based on each of the company's major policies or compliance risk areas
- Practical guidance on risks based on recognizable scenarios or hypothetical examples
- A visually inviting format that encourages readership, usage, and understanding
- Ethical decision-making tools to assist employees in making the right choices
- A designation of reporting channels and viable mechanisms that employees can use to report concerns or seek advice without fear of retribution.

> *I submit that having a code of ethics that is not vigorously implemented is worse than not having a code of ethics. It smacks of hypocrisy.*
>
> Roel C. Campos
> Commissioner, U.S. Securities and Exchange Commission
> October 16, 2002

[4] Both the NYSE and the NASDAQ have adopted corporate governance rules that require U.S.-listed companies to adopt and disclose codes of conduct for directors, officers, and employees, and disclose code waivers for directors or executive officers. NYSE Rule 303A(1) may be found at www.nyse.com/about/listed/1101074746736.html, and NASDAQ Rule 4350(n) may be found at http://nasd.complinet.com/nasd/display/display.html?rbid=1189&element_id=1159000635.

Employee and Third-Party Due Diligence

An important part of an effective fraud and misconduct prevention strategy is the use of due diligence in the hiring, retention, and promotion of employees, agents, vendors, and other third parties. Such due diligence may be especially important for those employees identified as having authority over the financial reporting process.

The scope and depth of the due diligence process typically varies based on the organization's identified risks, the individual's job function and/or level of authority, and the specific laws of the country in which the organization resides.[5]

49%

Percentage of U.S. employees who reported that they would be rewarded based on results, not the means used to achieve them.

KPMG Forensic Integrity Survey 2005 – 2006

There are certain situations where screening third parties may be valid. For example, management may wish to screen agents, consultants, or temporary workers who may access confidential information or acquisition targets that may have regulatory or integrity risks that can materially affect the value of the transaction.

Due diligence begins at the start of an employment or business relationship and continues throughout. For instance, taking into account behavioral considerations—such as adherence to the organization's core values—in performance evaluations provides a powerful signal that management cares about not only what employees achieve but also that those achievements were made in a manner consistent with the company's values and standards.

Communication and Training

Making employees aware of their obligations concerning fraud and misconduct control begins with practical communication and training. While many organizations communicate on such issues in an ad hoc manner, efforts taken without planning and prioritization may fail to provide employees with a clear message that their control responsibilities are to be taken seriously.

55%

Percentage of U.S. employees who reported that they lacked understanding of the standards of conduct that apply to their jobs.

KPMG Forensic Integrity Survey 2005 – 2006

[5] One of the minimum requirements announced by the sentencing guidelines for organizational defendants calls for the organization to use reasonable efforts and exercise due diligence to exclude individuals from positions of substantial authority who have engaged in illegal activities. See United States Sentencing Commission, Guidelines Manual, §8B2.1(b)(3) (Nov. 2004) available at http://www.ussc.gov/2005guid/CHAP8.pdf.

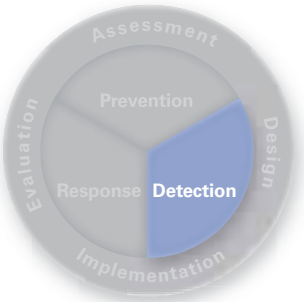
In formulating a training and communications plan, management should consider developing fraud and misconduct awareness initiatives that are:

- Comprehensive and based upon job functions and risk areas
- Integrated with other training efforts, whenever possible
- Effective in a variety of settings, using multiple methods and techniques
- Regular and frequent, covering the relevant employee population.

Senior management must move from thinking about compliance as chiefly a cost center to considering the benefits of compliance in protecting against the legal and reputational risks that can have an impact on the bottom line.

Susan Schmidt Bies
U.S. Federal Reserve Board Governor
The Bank Administration Institute's Fiduciary Risk Management Conference 2004
Current Issues in Corporate Governance
April 26, 2004

Detection



Detective controls are designed to uncover fraud and misconduct when it occurs.

Mechanisms for Seeking Advice and Reporting Misconduct

With the oversight and guidance of senior management, organizations tend to provide employees with multiple channels for reporting concerns about fraud or misconduct. Many typically request that employees follow a process that would begin with alerting their own managers, if possible, or a designated human resources or compliance officer. Telephone "hotlines" are often made available and can be used at any time, although they are usually intended for use when the normal channels are impractical or ineffective. A hotline typically provides a viable method whereby employees, and other third-parties if applicable, are encouraged to:

- Communicate concerns about potential fraud and misconduct, including questionable accounting or auditing matters
- Seek advice before making decisions when the appropriate course of action is unclear.

A well-designed hotline typically includes the following features:

- **Confidentiality**. All matters reported via the hotline are treated confidentially. Hotline operators inform callers that their concerns will be reported only on a "need to know" basis and that relevant safeguards are in place to ensure that such confidentiality is maintained. Hotline operators notify callers if the confidentiality of the matter is subject to any legislative limitations.
- **Anonymity**. The organization's protocols allow for the anonymous submission and resolution of calls. For instance, callers who wish to remain anonymous are given a case tracking number that they can later use to provide additional details related to their question or allegation and/or check the status or outcome of their call.
- **Organization-wide Availability**. Employees at international locations are able to use the hotline through features such as real-time interpreting and toll-free call routing.
- **"Real Time" Assistance**. The hotline is designed to provide an immediate, "live" response to a call to facilitate thorough and consistent treatment of a caller's question or concern as well as to provide immediate guidance. Thus, hotline operators need to be appropriately qualified, trained, and, in some situations, authorized to provide advice.
- **Data Management Procedures**. The hotline operator uses consistent protocols for gathering relevant facts and managing the hotline calls.
- **Classification of Financial Reporting Concerns**. The hotline includes protocols whereby qualified individuals (e.g., internal audit, legal, security) can determine whether the nature of an allegation could trigger a financial reporting risk.

- **Audit Committee Notification**. The hotline includes protocols that specify the nature and timing of allegations that are escalated to the audit committee.
- **Follow-up on Non-retaliation**. The organization's protocols allow for following up with employees periodically after the hotline case has been closed (e.g., at one-, three-, and six-month intervals) to ensure that reporting employees have not experienced retaliation. The company encourages the employees to report any instances of retaliation and takes swift action against those who do retaliate.
- **Prominent Communications**. The organization publicizes its hotline prominently. Such communications may include, among others, (1) describing the hotline within the code of conduct and other key company publications and training; (2) displaying the hotline telephone number on posters, banners, wallet cards, screen savers, telephone directories, or desk calendars; and (3) communicating mini-case-studies based on hotline calls to employees (e.g., in newsletters, training programs, or intranet sites) to demonstrate that the organization values hotline calls and is able to provide assistance to those who use the hotline.

Auditing and Monitoring

Auditing and monitoring systems that are reasonably designed to detect fraud and misconduct are important tools that management can use to determine whether the organization's controls are working as intended. Since it is impossible to audit every fraud and misconduct risk, management should develop a comprehensive auditing and monitoring plan that is based on risks identified through the organization's fraud risk assessment process.

33%

Percentage of Australia/New Zealand employees reporting that early warnings of fraud problems were ignored.

KPMG Fraud Survey 2004

An auditing and monitoring plan should thus encompass activities that are tailored in depth to the nature and degree of the risk involved, with higher-risk issues receiving priority treatment. Auditing activities (an evaluation of past events) and monitoring activities (an evaluation conducted real-time) should be performed in, but are not limited to, areas where:

- There are specific concerns about a key procedure, account, or position
- The company has a history of fraud and misconduct
- There is high employee turnover or organizational change
- Laws and regulations have changed significantly
- Audits are legally required, or governmental agencies are targeting enforcement actions.

An organization's managers involved in auditing and monitoring efforts should not only have sufficient training and experience but also be seen as objective in evaluating the controls for which they are responsible. Optimally, auditing and monitoring protocols should:

- Occur in the ordinary course of operations, including during regular management and supervisory activities
- Draw on external information to corroborate internally generated information
- Formally communicate identified deficiencies and exceptions to the organization's senior leadership, so that the harm to the organization is appropriately understood and mitigated
- Use results to enhance and modify other controls, such as communications and training, performance evaluations, and discipline.

Proactive Data Analysis

Many of the indicators of fraud and misconduct, both actual and potential, reside within an organization's financial, operational, and transactional data, and can be identified using data analysis tools and techniques. Such proactive data analysis uses sophisticated analytical tests, computer-based cross matching, and non-obvious relationship identification to highlight potential fraud and misconduct that can remain unnoticed by management, often for years. The benefits of such an analysis may include, among others:

- Identification of hidden relationships between people, organizations, and events
- A means to analyze suspicious transactions
- An ability to assess the effectiveness of internal controls intended to prevent or detect fraudulent activities
- The potential to continually monitor fraud threats and vulnerabilities
- The ability to consider and analyze thousands of transactions in less time, more efficiently, and cost-effectively than using more traditional forensic sampling techniques
- The ability to consider a company's unique organizational and industry issues.

Transactions can be analyzed using either retrospective or continuous transaction monitoring. Retrospective analyses allow organizations to analyze transactions in one- or two-year increments, enabling organizations to discern patterns that are not visible with shorter-term analyses. Creating the capability to perform retrospective-based proactive forensic data analysis includes steps to:

- Assess the fraud risk profile of systems or processes
- Define the overall objectives of the analysis
- Create a methodology to acquire, extract, and evaluate the data
- Define the analyses to be performed
- Select software tools to be used in performing the analysis
- Perform the analysis, aggregate and prioritize the results, and review and resolve the exceptions identified.

Unlike retrospective-based analyses, continuous transaction monitoring allows an organization to identify potentially fraudulent transactions on, for example, a daily, weekly, or monthly basis. Organizations frequently use continuous monitoring efforts to focus on narrow bands of transactions or areas that pose particularly strong risks.

Response

Response controls are designed to take corrective action and remedy the harm caused by fraud or misconduct.

Investigations

When information relating to actual or potential fraud and misconduct is uncovered, management should be prepared to conduct a comprehensive and objective internal investigation. The purpose of such an investigation is to gather facts leading to a credible assessment of the suspected violation, so management can decide on a sound course of action.

By conducting an effective internal investigation, management can address a potentially troublesome situation and have an opportunity to avert a potentially intrusive government investigation. A well-designed investigative process will typically include the following attributes, among others:

- Oversight by the organization's audit committee, or a special committee of the board, either of which must comprise independent directors who are able to ward off undue pressure or interference from management
- Direction by outside counsel, selected by the audit committee, with little or no ties to the entity's management team, and that can perform an unbiased, independent, and qualified investigation
- Vetting by the organization's external auditor so that the latter can rely on the proposed scope of work in the audit of the organization's financial statements
- A full-cooperation requirement, allowing no employee or member of management to obscure the facts that gave rise to the investigation
- Reporting protocols, providing the external auditors, regulators, and, where appropriate, the public with information relevant to the investigation's findings in a spirit of cooperation and transparency.

Based on a number of factors, including the nature of the potential illegal act, parties involved, and materiality, the organization may decide to use one or more of the above steps. Management would consult with the appropriate oversight functions and internal protocols to determine the steps that best address the allegation.

Enforcement and Accountability

A consistent and credible disciplinary system is a key control that can be effective in deterring fraud and misconduct. Appropriate discipline is, additionally, a requirement under leading regulatory frameworks. By mandating meaningful sanctions, management can send a signal to both internal and external parties that the organization considers managing fraud and misconduct risk a top priority.

47%

Percentage of U.S. employees who reported that wrongdoers would be disciplined fairly regardless of their position.

KPMG Forensic Integrity Survey 2005 – 2006

A well-designed disciplinary process will be communicated to all employees and include company-wide guidelines that promote:

- Progressive sanctions consistent with the nature and seriousness of the offense (e.g., verbal warning, written warning, suspension, pay reduction, location transfer, demotion, or termination)
- Uniform and consistent application of discipline regardless of rank, tenure, or job function.

Holding managers accountable for the misconduct of their subordinates is another important consideration. Managers may be disciplined in those instances where they knew, or should have known, that fraud and misconduct might be occurring, or when they:

- Directed or pressured others to violate company standards to meet business objectives or set unrealistic goals that had the same effect
- Failed to ensure employees received adequate training or resources
- Failed to set a positive example of acting with integrity or had a prior history of missing or permitting violations
- Enforced company standards inconsistently or retaliated against others for reporting concerns.

Corrective Action

Once fraud and misconduct has occurred, management should consider taking action to remedy the harm caused. For example, management may wish to consider taking the following steps, among others, where appropriate:

- Voluntarily disclosing the results of the investigation to the government or other relevant body (i.e., a regulator)
- Remedying the harm caused
- Examining the root causes of the relevant control breakdowns, ensuring that risk is mitigated and that controls are strengthened
- Administering discipline to those involved in the inappropriate actions as well as to those in management positions who failed to prevent or detect such events
- Communicating to the wider employee population that management took appropriate, responsive action.

63%

Percentage of Australian/New Zealand organizations that reported the incident to the police.

KPMG Fraud Survey 2004

Although public disclosure of fraud and misconduct may be embarrassing to an organization, management may nonetheless wish to consider such an action in order to combat or preempt negative publicity, demonstrate good faith, and assist in putting the matter to rest.

To Charge or Not to Charge?

In deciding not to charge Seabord Corporation with violations of the federal securities laws following an investigation of alleged accounting irregularities, the SEC announced influential dictum that a company's self-policing, self-reporting, remediation, and cooperation with law enforcement authorities, while no guarantee for leniency, would factor into the prosecutorial decision-making process. Among other questions the SEC would be asking the following:

- Did the company promptly, completely, and effectively disclose the existence of the misconduct to the public, to regulators, and to self-regulators?
- Did the company cooperate completely with appropriate regulatory and law enforcement bodies?
- Did the company appropriately recompense those adversely affected by the conduct?
- Did it do a thorough review of the nature, extent, origins, and consequences of the conduct and related behavior?
- Did the company promptly make available to our staff the results of its review and provide sufficient documentation reflecting its response to the situation?
- Did the company voluntarily disclose information our staff did not directly request and otherwise might not have uncovered?
- Did the company ask its employees to cooperate with our staff and make all reasonable efforts to secure such cooperation?

Accounting and Auditing Enforcement, Exchange Act Release No. 44,969 (October 23, 2001). The release may be found at www.sec.gov/litigation/investreport/34-44969.htm.

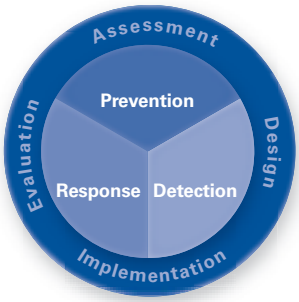
To Fine or Not to Fine?

In a related opinion on January 4, 2006, the SEC opined that in deciding the appropriateness of a civil monetary penalty levied against a corporate settlement of action, the following factors would be examined:

- The presence or absence of a direct benefit to the corporation as a result of the violation.
- The degree to which the penalty will recompense or further harm the injured shareholders.
- The need to deter the particular type of offense.
- The extent of the injury to innocent parties.
- Whether complicity in the violation is widespread throughout the corporation.
- The level of intent on the part of the perpetrators.
- The degree of difficulty in detecting the particular type of offense.
- Presence or lack of remedial steps by the corporation.
- Extent of cooperation with Commission and other law enforcement.

Statement of the Securities and Exchange Commission Concerning Financial Penalties, Release 2006-4 (January 4, 2006). The Statement may be found at http://www.sec.gov/news/press/2006-4.htm.

An Ongoing Process



An effective fraud risk management approach provides an organization with tools to help manage risk in a manner consistent with regulatory requirements as well as the entity's business needs and marketplace expectations. As described below, developing such an approach can be achieved in key phases:

- **Assessment of Risks**. Assessing the needs of the organization based on the nature of fraud and misconduct that risk controls are intended to mitigate and the adequacy of existing controls.
- **Design**. Developing controls to prevent, detect, and respond to identified risks in a manner consistent with legal and regulatory criteria and other leading practices.
- **Implementation**. Deploying a process for implementing the new controls and assigning responsibility to individuals with the requisite level of authority, objectivity, and resources to support the process.
- **Evaluation**. Evaluating the design and operating effectiveness of controls through control self-assessment, substantive testing, routine monitoring, and separate evaluations.

Assessment

The nature of fraud and misconduct risks facing an organization can be as diverse and fluid as the business itself. The risks of fraud and misconduct for a national bank that has experienced rapid growth through acquisitions are different than those of a global energy company seeking to expand crude exploration in emerging markets. Therefore, antifraud measures should be tailored to the unique risks of an organization, the specific conditions that give rise to those risks, and the targeted resource needs required in balancing risk and control.

The first step is to determine what a company's fraud risks are and how effectively the organization manages these risks. To get started, an organization would consider which business units, processes, systems, and controls, among other factors, may need to be included in the scope of the analysis. The organization can also identify key stakeholders who may need to be involved. Once the organization profiles its current state and sets targets for improvements, it can assess the "gap" it must close to reach the desired state and begin defining the necessary steps to get there.

Design

The goal of the control design phase is for management to develop controls that will operate effectively and protect the organization from the risk of fraud and misconduct. However, for an entity to design effective controls, it must first tailor these controls to the risks it is facing as well as the organization's unique business environment.

When designing controls, management should endeavor to do more than observe regulatory requirements (i.e., minimum criteria defined by various regulatory frameworks). Rather, management should take into account the relevance of a variety of leading practices (i.e., practices that similarly situated organizations have generally found to be effective). Incorporating leading practices into the design of fraud controls increases the likelihood that those controls will ultimately prove to be effective.

Each entity is unique and thus will have individualized control considerations. Management would be well served to consider the organization's unique circumstances when designing fraud controls. Control attributes that may be appropriate for a global telecommunications company may be inappropriate for a national bank, and vice versa. Management should seek to design controls that satisfy not only legal requirements but also the organization's distinct business needs.

Implementation

Once fraud controls have been designed, management should establish a strategy and process for implementing the new controls throughout the organization and assign to a senior individual responsibility and resources for leading the overall effort. Meaningful and consistent implementation typically requires a substantial change in workplace culture and practices. Therefore, employees should receive clear and frequent communications with respect to when, how, and by whom the controls will be rolled out as well as the manner with which compliance with the new controls will be enforced.

Evaluation

Simply because a control exists is no guarantee that it is operating as intended. After a control has been operating for a designated period of time, it should be evaluated to determine whether it was designed and implemented to achieve optimal effectiveness. Such an evaluation should first consider those controls identified as "higher risk" before other, lower-priority controls.

On the other hand, simply because a particular control does not yet exist, management should not automatically conclude that the organization's risk management objective is not being met. In the absence of a specific control, other compensating controls may be operating effectively and mitigating the risk of fraud and misconduct.

When evaluating the design effectiveness of a control, management should take into account both regulatory requirements and leading practices that similarly situated organizations have found to correlate with effective risk mitigation. Management can then use a "gap analysis" process to determine whether the control in question

indeed incorporates the required design criteria. For instance, where a design criteria calls for the organization's whistleblower hotline to allow anonymous submission of questions or concerns regarding accounting and auditing matters, management should seek to determine whether the hotline protocols indeed allow for caller anonymity.

To evaluate the operational effectiveness of a particular control, management should focus on the extent to which the control's objectives have been achieved. For example, have the mitigation strategies identified during the fraud and misconduct risk assessment been implemented properly? Similarly, management may have put in place a well-designed code of conduct, but are employees actually using the code to guide their day-to-day activities? In the end, the integrity climate will determine the perceptions employees have of the ability of the organization to prevent, detect, and respond to fraud and misconduct and base their own conduct on those perceptions.

Only when such basic questions are addressed can management focus on gathering empirical data on control effectiveness using review and evaluation techniques (e.g., proactive forensic data analysis). For instance, management may wish to ascertain whether employees truly understand the standards contained in the code of conduct or whether employees feel comfortable calling the hotline. To gather such hard-to-audit qualitative data, management may wish to field a survey of employee perceptions and attitudes. Such a survey can be a powerful tool, generating data that can be benchmarked against prior-year results to note improvements and demonstrate control effectiveness.

An organization's particular situation should be taken into account in conducting an effectiveness evaluation, and such an inquiry should remain ongoing. Management should continuously consider how its risk strategy and control effectiveness are affected by changes in market expectations, external scrutiny, and regulatory or legislative developments.

Conclusion

Faced with an increasing array of rules and standards governing business conduct, many organizations worldwide continue to struggle with how to mitigate the innumerable risks posed by fraud and misconduct.

The development of a broad ranging fraud risk management program is an important step in managing this challenge. Organizations undertaking the effort should begin by assessing how well they are managing fraud risk. Identifying known risks and existing controls is an important first step. Then the organization can determine its ideal future state, perform a gap analysis, and prioritize activities that will help enable the development of a company-specific antifraud program.

Such a program will not only help enable appropriate compliance with regulatory mandates but also help the organization align its corporate values and performance as well as protect its many assets, including its reputation.

Appendix: Selected International Governance and Antifraud Criteria

Australia

Commonwealth Criminal Code Act (1995)

Boards have a responsibility to foster a culture of compliance with Australian law. Under the Criminal Code, a company can be convicted of Commonwealth criminal offenses if it is established that the company had a culture that directed or encouraged, tolerated, or led to noncompliance, or that the body failed to maintain a culture that required compliance with relevant legislation. (Schedule, Part 2.5, Division 12)

Corporations Act 2001 (Including CLERP 9 Amendments) (2001)

Directors must exercise their powers and discharge their duties with care and diligence. (Section 180)

CEO and CFO of a listed entity must make a declaration that:

- An entity's financial records must be properly maintained in accordance with the Act.
- Financial statements for the financial year must comply with the accounting standards.
- Financial statements must present a true and fair view of the financial position and performance of the entity. (Section 295A)

AUS 210 (2002)

Establishes a requirement for auditors to consider fraud and error in an audit of a financial report. (AUS 210)

Australian Stock Exchange Guidance Note 9A (2003)

Requires the board or appropriate board committee to establish policies on risk oversight and management. (Principle 7)

Australian Standard 8001 – 2003 Fraud and Corruption Control (2003)

Provides guidance on fraud and corruption control that is considered best practice.

European Union

The Financial Services Action Plan (FSAP) (1999)

The FSAP is designed to create a single market in financial services throughout the EU. Forty-two legislative measures were contemplated as part of the action plan, many of which focused on securities regulation. As of 2004, these measures are having a tremendous effect on the regulation of EU capital markets and, as with the Sarbanes-Oxley Act, have necessitated major adjustments on the part of issuers, accountants and lawyers, and regulators affected by the legislation.

Third Directive on the Prevention of the Use of the Financial System for Money Laundering or Terrorist Financing (2005/60/EC)

Council Directive 2005/60/EC is an update to two earlier directives in response to concerns about money laundering. This Directive requires member states to:

- Fight against money laundering
- Compel the financial sector, including credit institutions, to take various measures to establish customers' identities

- Urge the financial sector to keep appropriate records
- Establish internal procedures to train staff to report suspicions to the authorities and to set up preventive systems within their organizations.

This Directive also introduces additional requirements and safeguards for situations of higher risk (e.g., trading with correspondent banks situated outside the EU).

United Kingdom

The Financial Services and Markets Act (2000)

This Act supports the Financial Services Authority's (FSA's) goal to reduce the likelihood that business carried on by a regulated person, or in contravention of the general prohibition, can be used for a purpose connected with financial crime. As a result, the FSA requires senior management of regulated firms to take responsibility for managing fraud risks, and firms to have effective systems and controls in place proportionate to the particular financial crime risks that they face.

Proceeds of Crime Act (2002)

The Act has strengthened the law on money laundering and sets up an Assets Recovery Agency to investigate and recover assets and wealth obtained as a result of unlawful activity.

Combined Code on Corporate Governance (2003)

The Financial Reporting Council's (FRC) Combined Code on Corporate Governance sets out standards of good practice in relation to issues such as board composition and development, remuneration, accountability and audit, and relations with shareholders. All companies incorporated in the United Kingdom and listed on the London Stock Exchange are required under the Listing Rules to report on how they have applied the Combined Code in their annual report and accounts, or—where they have not—to provide an explanation.

The current version of the Combined Code was published in July 2003. In recent years, related guidance has been issued including the Turnbull guidance on Internal Control, revised in October 2005; the Smith guidance on Audit Committees; and the Higgs guidance on good practices.

An implementation review carried out by the FRC in 2005 indicated the Code is having a favorable impact on the quality of corporate governance. The results also turned up no appetite for major change, and only two suggested amendments carried strong support. The FRC began consulting on these amendments in January 2006. The main proposals would be to relax the existing provisions to allow the chairman to sit on the remuneration committee and to add a new provision regarding companies including a "vote withheld" box on the annual general meeting (AGM) proxy voting forms, as recommended by the Shareholder Voting Working Group. Consultation on possible amendments to the Code closed on April 21, 2006. If implemented, the intention is that changes would apply to financial years beginning on or after November 1, 2006.

The Money Laundering Regulations (2003)

In the United Kingdom, these regulations require various kinds of businesses to identify their customers under specific circumstances and to retain copies of identification evidence for five years. These regulations apply to banks, check cashing businesses, money transmitters, accountants, solicitors, casinos, estate agents, bureaus de change, and dealers in high-value goods. Employers may be prosecuted for a breach of these regulations if they fail to train staff.

United States

Director and Officer Liability (August 1996)

The Delaware Chancery Court in *In re Caremark Int'l Inc. Derivative Litigation* held that boards of directors that exercise reasonable oversight of a compliance program may be eligible for protection from personal liability in shareholder civil suits resulting from employee misconduct. A director's fiduciary duty goes beyond ensuring that a compliance program exists, but also includes a good faith duty to ensure that the organization's compliance program is adequate.

Department of Justice Prosecution Policy (Original June 1999, revised January 2003)

The Department of Justice's guidance (the *Thompson Memo*) instructs federal prosecutors that while having in place a compliance program does not absolve a corporation from criminal liability, it may provide factors that can be used in determining whether to charge an organization or only its employees and agents with a crime. These factors include evaluating whether:

- The compliance program is merely a "paper program" or is designed and implemented effectively
- Corporate management is enforcing the program or tacitly encouraging or pressuring employees to engage in misconduct to achieve business objectives
- The corporation has sufficient staff to audit and evaluate results of its compliance efforts
- Employees are informed about the program and are convinced of the corporation's commitment to it.

Sarbanes-Oxley Act of 2002

The U.S. government had responded to widespread cases of corporate fraud and misconduct by passing the Sarbanes-Oxley Act of 2002. The Act includes the following sections, among others:

- *Section 301*: Requires audit committees to establish procedures to receive, retain, and treat complaints from employees and others about accounting, internal accounting controls, or auditing matters.
- *Section 404*: Management and external auditors are to evaluate the effectiveness of a company's internal control over financial reporting based on a suitable control framework.
- *Section 406*: Instructs the SEC to issue rules requiring companies to either adopt a code of ethics applicable to senior financial officers or disclose why they do not.

- *Section 806*: Requires all companies regulated by the SEC to have in place a mechanism whereby a whistleblower could report a violation of law or SEC rule, and to protect from retaliation any person who uses that mechanism.
- *Section 1107*: Provides penalties and/or fines for retaliating against any corporate whistleblower, amending section 1513 of Title 18, United States Code.

Most companies in the United States are applying the integrated internal control framework developed by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission for this purpose. Generally speaking, COSO addresses ethics and compliance program elements in company-level components that have a pervasive influence on organizational behavior, such as the control environment. Examples of company-level control considerations include:

- Establishment of the tone at the top by the board and management
- Existence of codes of conduct and other policies regarding acceptable business practices
- Extent to which employees are made aware of management's expectations
- Pressure to meet unrealistic or short-term performance targets
- Management's attitude toward overriding established controls
- Extent to which adherence to the code of conduct is a criterion in performance appraisals
- Extent to which management monitors whether internal control systems are working
- Establishment of channels for people to report suspected improprieties
- Appropriateness of remedial action taken in response to violations of the code of conduct

NYSE Listing Standards Section 303A, Corporate Governance Standards (Modified, November 2004)

Qualitative Listing Requirements for the NASDAQ National Market (Amended, April 2004)

In response to the provisions of the Sarbanes-Oxley Act, both the NYSE and NASDAQ adopted new corporate governance rules for listed companies. While the specific rules for each exchange differ, each have standards that require listed companies to (1) adopt and disclose codes of conduct for directors, officers, and employees and (2) disclose any code of conduct waivers for directors or executive officers. In addition, each exchange requires listed companies to adopt mechanisms to enforce their codes of conduct.

U.S. Sentencing Guidelines Criteria (Amended, November 2004)

The federal sentencing guidelines for organizational defendants establish minimum compliance and ethics program requirements for organizations seeking to mitigate penalties for corporate misconduct. These guidelines make explicit the expectation that organizations promote a culture of ethical conduct, tailor each program element based on compliance risk, and periodically evaluate program effectiveness.

Specifically, the amended guidelines call on organizations to:

- Promote a culture that encourages ethical conduct and a commitment to compliance with the law
- Establish standards and procedures to prevent and detect criminal conduct
- Ensure the board of directors and senior executives exercise reasonable and informed oversight over the compliance and ethics program
- Assign a high-level individual within the organization to ensure the organization has an effective compliance and ethics program, and delegate day-to-day operational responsibility to individuals with adequate resources, authority, and direct access to the board
- Use reasonable efforts and exercise due diligence to exclude individuals from positions of substantial authority who have engaged in illegal activities or other conduct inconsistent with an effective compliance and ethics program
- Conduct effective training programs for directors, officers, employees, and other agents and provide such individuals with periodic information appropriate to their respective roles and responsibilities relative to the compliance and ethics program
- Ensure that the compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct
- Publicize a system, which may include mechanisms for anonymity and confidentiality, whereby the organization's employees and agents may report or seek guidance regarding potential or actual misconduct without fear of retaliation
- Evaluate periodically the effectiveness of the compliance and ethics program
- Promote and enforce consistently the compliance and ethics program through incentives and disciplinary measures
- Take reasonable steps to respond appropriately to misconduct, including making necessary modifications to the compliance and ethics program.

Key Contacts

Tim Hedley
Partner
KPMG LLP in the United States
thedley@kpmg.com
+1 212 872 3496

Gary Gill
Partner
KPMG in Australia
ggill@kpmg.com.au
+61 (2) 9335 7312

Jack de Raad
Partner
KPMG in the Netherlands
DeRaad.Jack@kpmg.nl
+31 20 656 7774

KPMG contributors to this publication include Richard Girgenti, Ori Ben-Chorin, Jim Littley, Graham Murphy, Scott Avelino, Raymond Dookhie, Joel Dziengielewski, Justin Snell, Melissa Dugan, William Rudolph, Jaime Jue, Brad Sparks, Donna Tamura, Remco de Groot, Jack de Raad, Gary Gill, Tim Hedley, Martijn Hin, Muel Kaptein, Carole Law, Peter Morris, Diane Nardin, Shae Roberts, and Aaron Sparks.