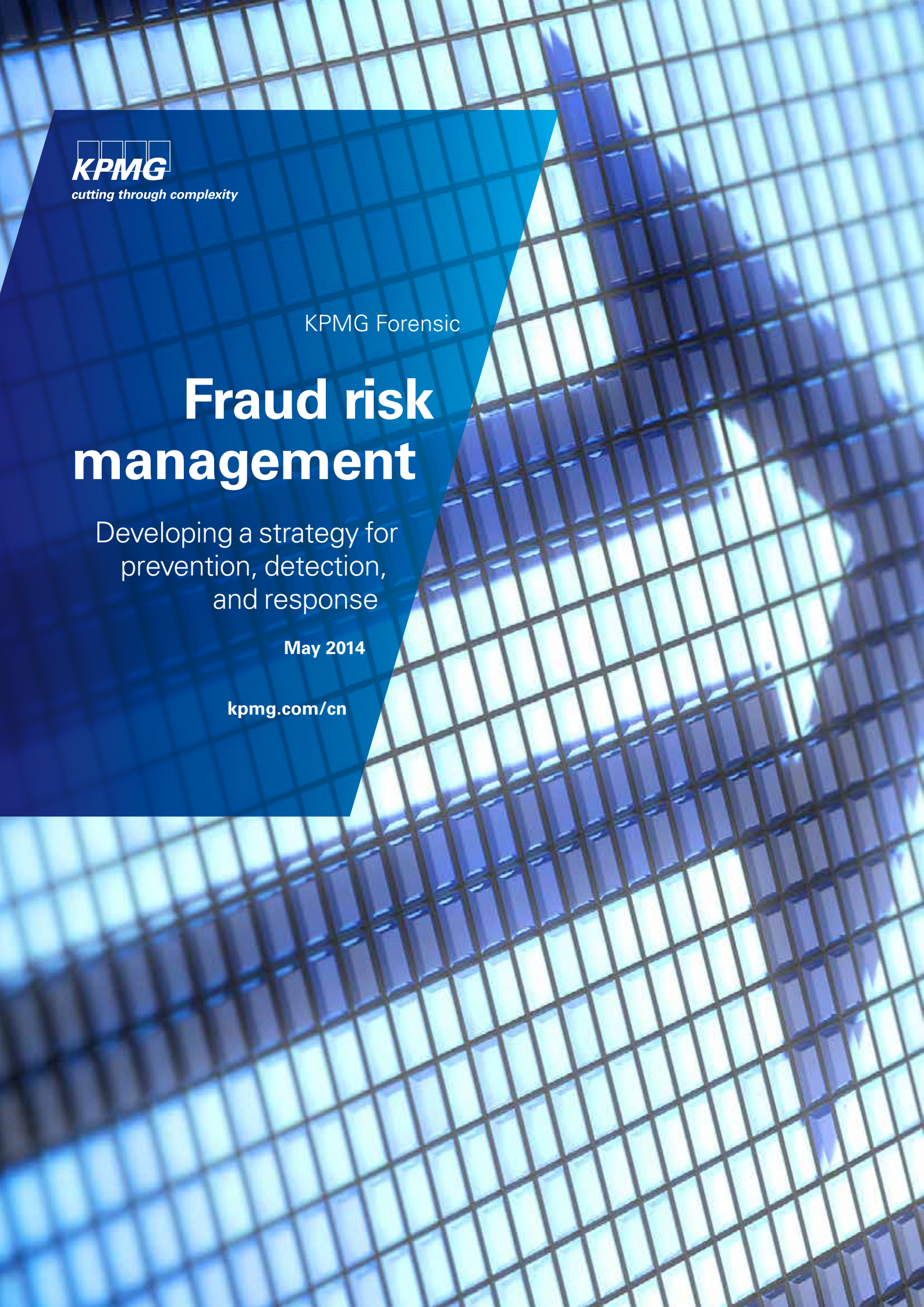


KPMG
cutting through complexity

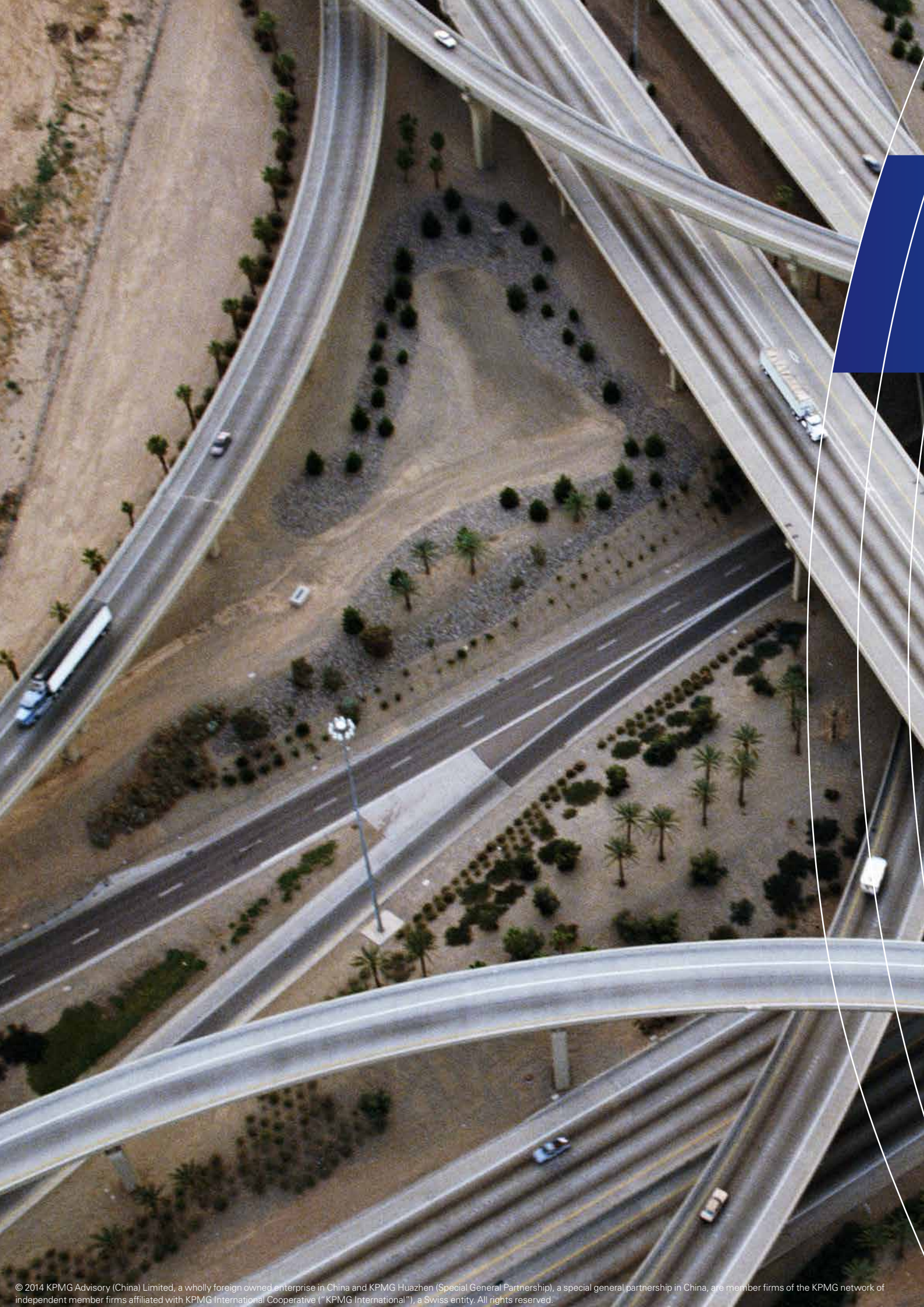
KPMG Forensic

Fraud risk management

Developing a strategy for prevention, detection, and response

May 2014

kpmg.com/cn



Contents

Foreword

Corporate fraud and misconduct remain a constant threat to public trust and confidence in the capital markets. Public sector organisations are also exposed to fraud particularly in the provision of services and the supply chain. As organisations do their best to formulate a comprehensive, proactive strategy to prevent, detect and respond to integrity threats, they can be well served in focusing their efforts upon:

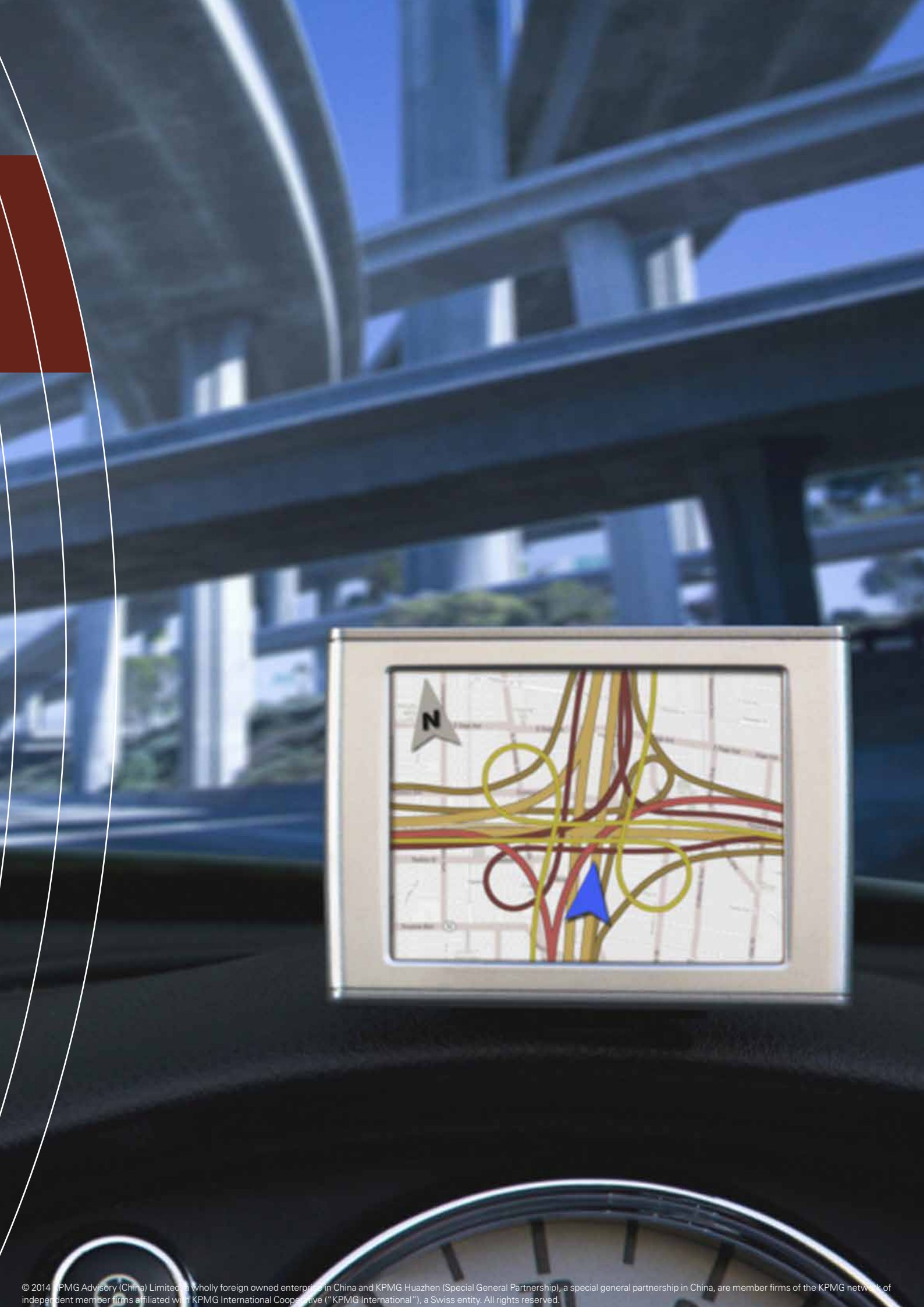
- identifying and understanding the fraud and misconduct risks that can undermine increasingly complex, global business objectives
- evaluating the design and operational effectiveness of corporate compliance programs and related antifraud programs and controls
- meeting antifraud and governance standards promulgated by recognised standard setters
- gaining insight on better ways to design and evaluate controls to prevent, detect, and respond to fraud and misconduct
- reducing exposure to corporate liability, sanctions, and litigation that may arise from violations of law or stakeholder expectations
- deriving value from compliance investments by creating a sustainable process for managing risk and improving performance and
- achieving high levels of business integrity through sound corporate governance, internal control and transparency.

This white paper provides an overview of fraud and misconduct risk management fundamentals. It also provides a road map that organisations can use to move beyond a check-the-box approach to managing the risks of fraud and misconduct and instead, design, implement, and evaluate proactive practices that have been found by leading organisations to be effective.

In addition to these fraud risk management principles we have also referred to laws and guidance applicable in many parts of the world with particular emphasis for countries in the Asia Pacific (ASPAC) region to help organisations gain an understanding of the regulatory landscape for these types of issues.

Grant Jamieson
Partner in Charge,
Forensic Asia Pacific and China

Katy Wong
Partner,
Forensic Hong Kong, Head of Fraud Risk Management Services



Executive summary

In the wake of high-profile corporate scandals and in light of new laws and regulations, executives are increasingly aware of the need to create policies, programs and controls to address fraud and misconduct. While acknowledging that no single approach to risk management exists, this paper spotlights leading practices that organisations have generally found to be effective when building their compliance programs and related antifraud programs and controls. It also offers strategic insights for aligning organisational values with performance.

The business imperative

As organisations do their best to achieve compliance with new laws and regulations, their agenda for doing so increasingly centres on management's ability to:

- understand the fraud and misconduct risks that can undermine increasingly complex and global business objectives
- reduce exposure to corporate liability, sanctions and litigation, and
- achieve high levels of business integrity through sound corporate governance, internal control, and transparency.

Convergence of regulatory challenges

A variety of laws and regulations have recently emerged worldwide, providing organisations with an array of criteria to incorporate into their antifraud and misconduct efforts. These include, among others:

- **Australia:** The Corporate Law Economic Reform Program (Audit Reform & Corporate Disclosure) Act 2004; the Criminal Code Amendment (Bribery of Foreign Public Officials) Act 1999; the Public Interest Disclosure Act 2013; and the Anti-Money Laundering and Counter-Terrorism Financing Act 2006.
- **Canada:** The Canadian Criminal Code.
- **China:** Eighth Amendment of the PRC Criminal Law The Anti-unfair competition Law (1993); the Anti-Money Laundering Law of the People's Republic of China (2007); the Eighth Amendment to the PRC Criminal Law including The Interpretations of the Supreme People's Court and the Supreme People's Procuratorate ("SPC and SPP Interpretation") – Criminal Fraud Cases (2011); and SPC and SPP Interpretation – Bribe-Giving Cases (2012).

Convergence of regulatory challenges

- **Hong Kong:** The Drug Trafficking (Recovery of Proceeds) Ordinance (1993); the Crimes Ordinance (1997) and the Theft Ordinance (1997); the Prevention of Bribery Ordinance (1997); the United Nations (Anti Terrorism Measure) Ordinance (2002); and the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (2012).
- **European Union:** Financial Services Action Plan (FSAP); and the Third Directive on the Prevention of the Use of the Financial System for Money Laundering or Terrorist Financing.
- **Japan:** Standard to address the risks of Fraud in an audit: Established in March 2013 by Business Accounting Council (BSA), an advisory body established within the Japanese FSA.
- **Korea:** Anti-Corruption Act of 2001. An Act established in 2001 focusing on eradicating acts related to government officials and public agencies, and to protect the whistle-blower.
- **Malaysia:** Whistleblowers Protection Act (2010); Malaysian Anti-Corruption Commission Act (2009); Malaysian Code on Corporate Governance (2012); and the Anti-Money Laundering Act (2001).
- **New Zealand:** Protected Disclosures Act 2000; Crimes (Bribery of Foreign Public Officials) Amendment Act 2001; and the Anti-Money Laundering and Countering Financing of Terrorism Act 2009.
- **Singapore:** The Penal Code (enacted 1871); Prevention of Corruption Act (enacted 1960); Securities and Futures Act (enacted 2001); Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (enacted 1999); and the Code of Corporate Governance (enacted 2003).
- **Thailand:** Penal Code of Thailand, Organic Act on Counter Corruption (1999), National Anti-Corruption Commission, Money Laundering Prevention and Suppression Act, Money Laundering Prevention and Suppression Act (1999), Accounting Act (2000)
- **United Kingdom:** Proceeds of Crime Act of 2002; Companies (Audit, Investigations, and Community Enterprise) Act of 2004; the Fraud Act of 2006; and the Bribery Act of 2010.
- **United States:** The USA PATRIOT Act; the Foreign Corrupt Practices Act; the Sarbanes-Oxley Act of 2002; SAS 99, NYSE & NASDAQ listing standards; Public Company Accounting Oversight Board (PCAOB) Standards No. 2 and 5; and amendments to the Federal Sentencing Guidelines and the Dodd-Frank Act.

The key objectives: prevention, detection, and response

An effective fraud and misconduct risk management approach encompasses controls that have three objectives:

- **Prevent** instances of fraud and misconduct from occurring in the first place.
- **Detect** instances of fraud and misconduct when they do occur.
- **Respond** appropriately and take corrective action when integrity breakdowns arise.

Pulling it all together

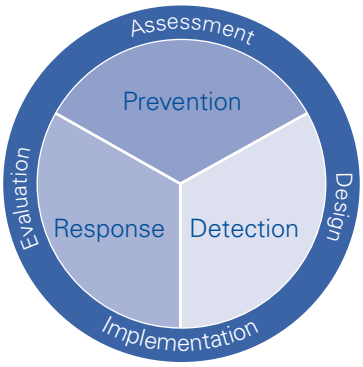
The challenge for organisations is to develop a comprehensive strategy that helps them:

- understand the various regulatory and evaluative frameworks that apply to them
- ensure that controls such as risk assessments, codes of conduct, and whistleblower mechanisms are in place and supported by management and
- create a broad ranging ethics and compliance program that manages and integrates fraud prevention, detection and response efforts.

An ongoing process

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

- **Assessment** of organisational needs based upon the nature of fraud and misconduct risks and existing antifraud programs and control.
- **Design** of programs and controls in a manner consistent with legal and regulatory criteria as well as industry practices that companies and other organisations have generally found to be effective.
- **Implementation** of programs and controls through the assignment of roles, building of internal competencies and deployment of resources.
- **Evaluation** of program and control design, implementation and operational effectiveness.



Defining fraud and misconduct

Misconduct is a broad concept that generally refers to violations of law, regulation, internal policy and expectations for ethical business conduct. While there is no one widely-accepted definition of fraud, it is often defined as a misrepresentation properly relied upon by an individual to that person's detriment or to the unfair advantage of the fraudster. For fraud perpetrated against individuals the above definition may be perfectly acceptable. However, for fraud committed by those in or against an organisation, this definition may not fit as well since it is often difficult or impossible to measure the loss inflicted or gain achieved. As an example of the type of laws designed for the prosecution of fraud we can cite two examples.

The **UK Fraud Act (2006)** which sets out that a person can be guilty of fraud by false representation; by failing to disclose information; or by abuse of position.

Hong Kong – Under Chapter 210, Section 16A of the Theft Ordinance, fraud is deemed to be committed by any person who by deceit (whether or not the deceit is the sole or main inducement):

- dishonestly obtains property belonging to another, with the intention of permanently depriving the other of it
- dishonestly obtains for himself or another any pecuniary advantage
- induces another person to commit an act or make an omission with the intent to defraud, which results in either:

  a) benefit to any person other than the second-mentioned person; or

  b) prejudice or a substantial risk of prejudice to any person other than the first-mentioned person.

For the purposes of this paper, fraud is defined as an intentional deception that drains value from an organisation. Despite the context, the core of what defines an act as fraud is the intent to deceive.

Together, fraud and misconduct typically fall into the following categories, each of which can undermine public trust and damage an organisations reputation:

- Fraudulent financial reporting (i.e., the misrepresentation of financial information).
- Misappropriation of assets (i.e., theft of cash or other assets).
- Other illegal or unethical acts (e.g., bribery, corruption, or market rigging).

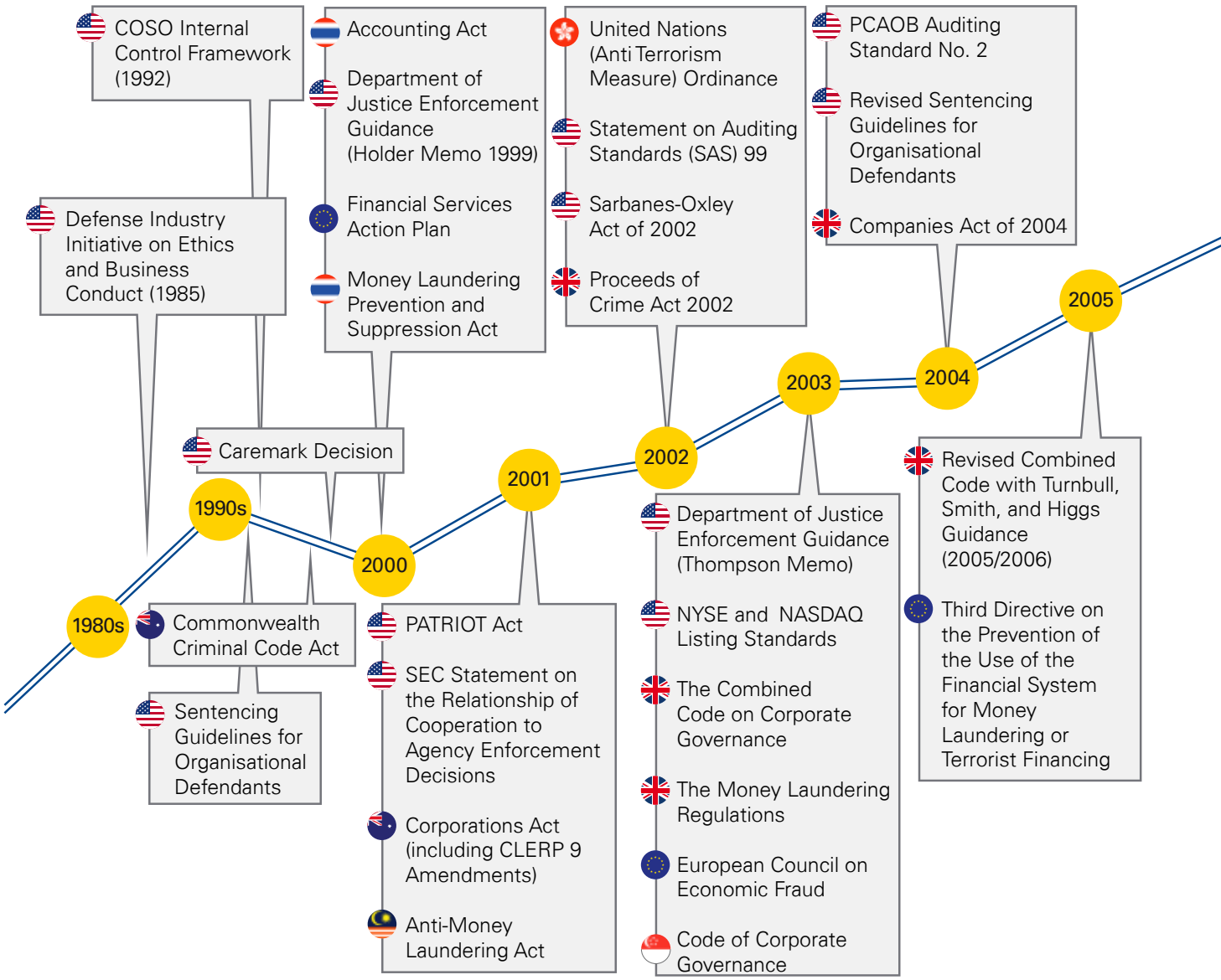
Fraud is a constant risk that latches onto existing weaknesses and has no natural stopping point. This analysis of the problem points to the solution: a recognition that every category of business risk carries an equivalent fraud risk. Fraud should be considered part of a normal business's risk profile, as a potential factor in every operation and function.[1] This white paper sets out to help organisations deal with this ever present risk through ongoing prevention, detection and response activities.

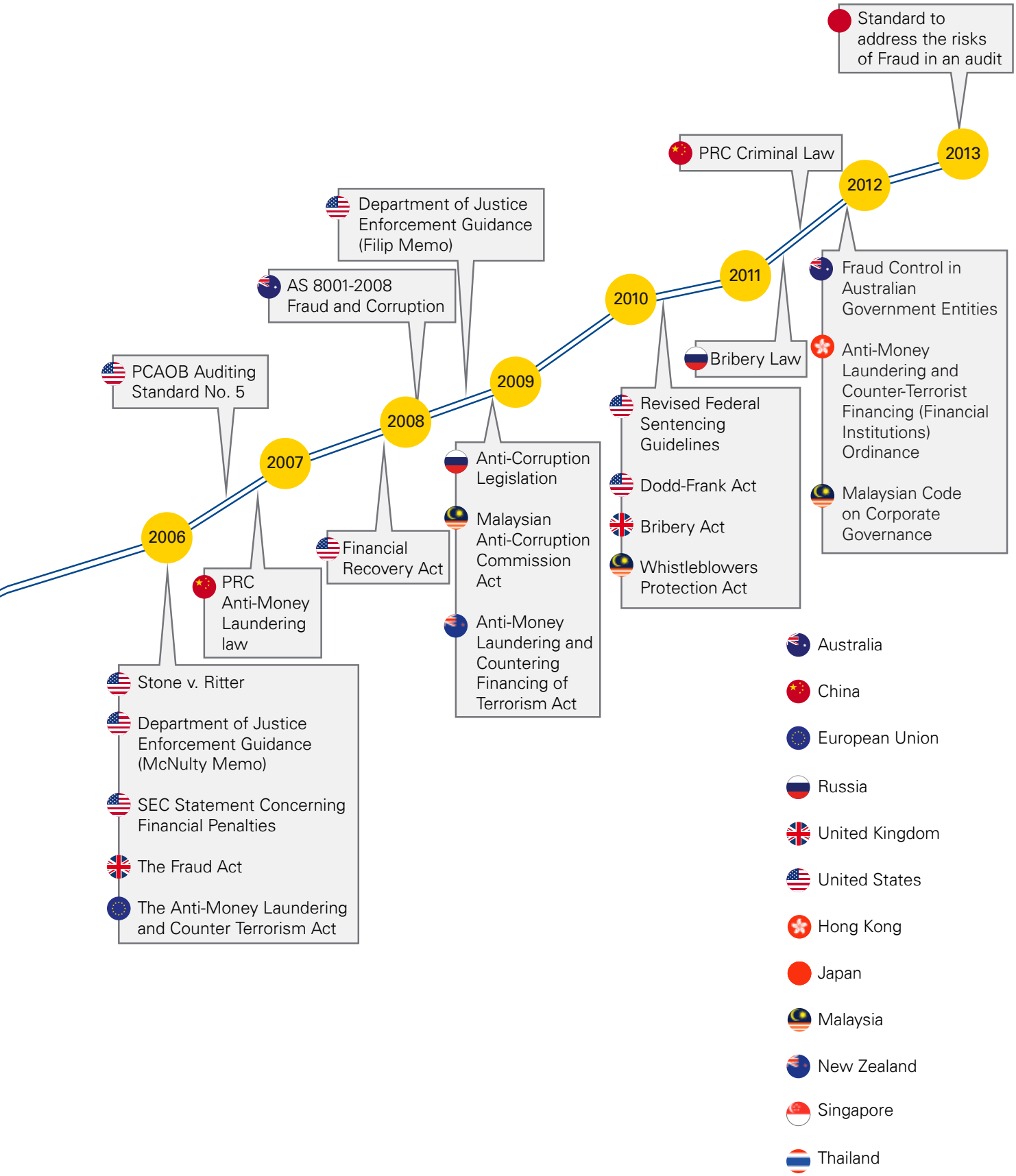
[1] *Corporate and Financial Fraud,* David Luijerink, CCH (UK), 2008.

Convergence of regulatory challenges

Globally, governments have responded to corporate scandals and unethical activity by passing legislative and regulatory reforms that are intended to encourage companies to become more self-governing. The timeline in Figure 1 below provides a representative selection of important global regulations, frameworks and events. Note that a summary of relevant regulations appears in the "Appendix: Selected International Governance and Antifraud Criteria" beginning on page 31.

Figure 1: Timeline of global regulations, frameworks, and events





The key objectives:
prevention, detection, and response

As mentioned above, an effective fraud and misconduct risk management approach is one that focuses on three objectives: establishing policies, programs and controls designed to reduce the risk of fraud and misconduct from occurring, detecting it when it occurs and to taking appropriate corrective action to remedy the harm caused by integrity breakdowns.

Putting it all together

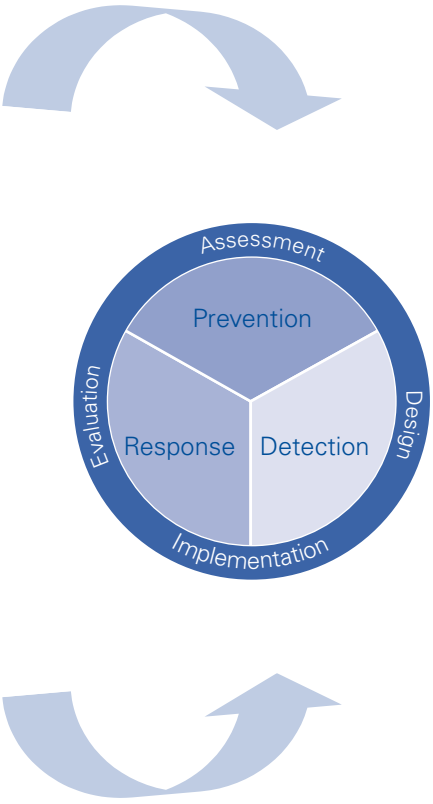
There are a variety of actions that can be undertaken to reduce particularly the opportunity and motivation to perpetrate fraud,[2] and these efforts form part of not only preventing and detecting fraud, but also in responding to instances and in the mitigation to enhance controls. The challenge for companies and other organisations is to ensure that a comprehensive and integrated approach takes place and includes all relevant considerations into account – including applicable control criteria and evaluative frameworks – and enables them to work together.

Doing so helps avoid duplicative effort, resource fragmentation and 'slippage between the cracks' that is associated with a one-off or 'silo' approach.

Such an undertaking begins with understanding the various major control frameworks and criteria that apply to an organisation (see Figure 2). When this categorisation is complete, the organisation 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	AS 8001-2008 Fraud and Corruption	Provides a suggested approach to controlling the risk of fraud and corruption and is intended to apply to all entities.
China	Basic Standard for Enterprise Internal Control (C-SOX)	Introduces comprehensive requirements for an internal control frame work at state-owned entities and listed companies in China. The aim is to enhance the quality of the financial reporting process and strengthen china's capital market.
Hong Kong	Code on Corporate Governance	Sets out the principles of good corporate governance, where listed companies are encouraged to ether comply with the code provisions or provide explanations for any deviations from the code provisions.
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.
Singapore	Code of Corporate Governance	Requires all companies listed on the Singapore Exchange to provide a detailed description of their corporate governance practices and explain any deviations from the Code of Corporate Governance in their annual reports.



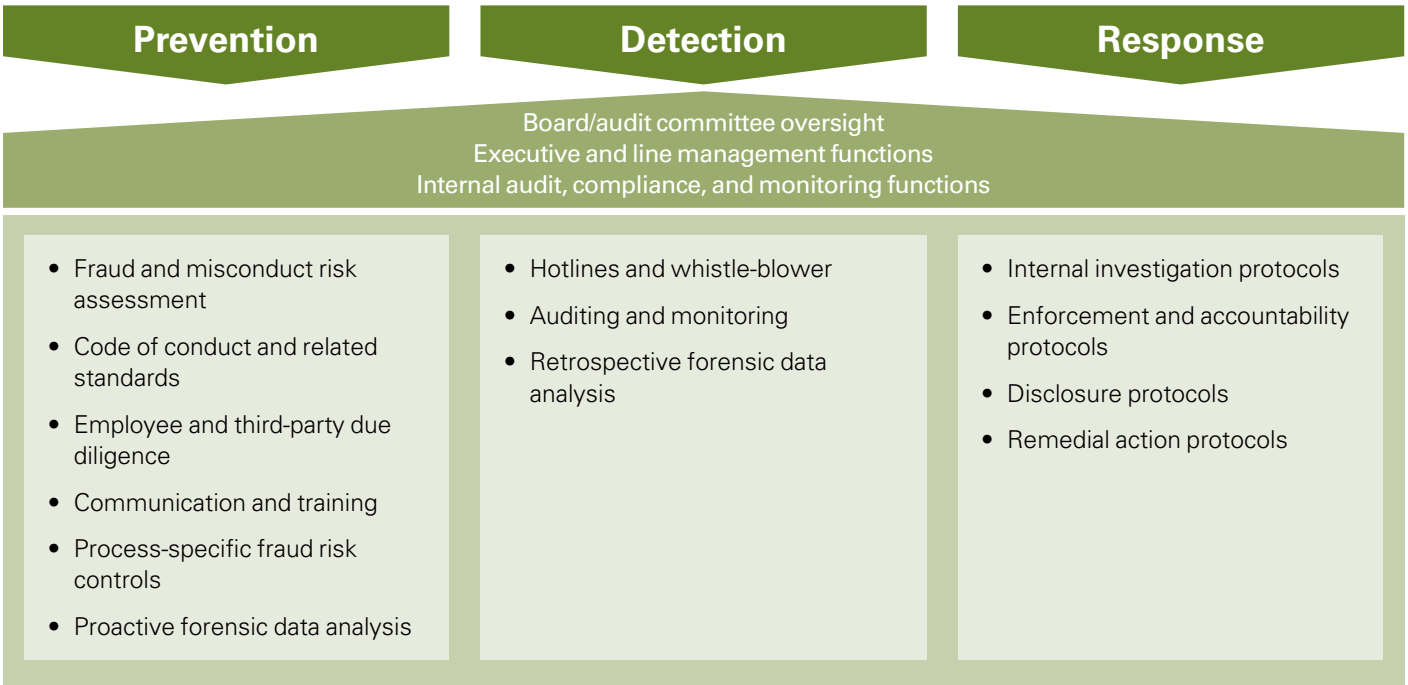
[2] *Corporate and Financial Fraud*, David Luijerink, CCH (UK), 2008.

Jurisdiction	Framework	Relevance
United Kingdom	The Companies Act 2004	Aims to improve the reliability of financial reporting and the independence of auditors and auditor regulation.
United Kingdom	Anti-Bribery Act	Repeals statutory and common law antibribery provisions, replacing them with the crimes of bribery, being bribed, bribing foreign public officials, and failing to prevent bribery.
United States	Federal Sentencing Guidelines	Provides minimum criteria for ethics and compliance programs to prevent and detect violations of law.
United States	Dodd-Frank Act	Establishes a 'bounty program' for whistle-blowers who raise concerns with the government and can receive a portion of the proceeds received by the government.
United States	Sarbanes-Oxley Act	Introduced substantial changes to the corporate governance and financial disclosure requirements of publicly listed companies.

Source: KPMG LLP (US) 2013 and KPMG Australia 2014.

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

Figure 3: Sample Antifraud Program Elements



Source: KPMG LLP (US) 2013.

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 organisation's board of directors plays a critical role in the oversight of programs 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 for ethical and responsible business practices at the highest levels of the organisation.

Directors have not only a fiduciary duty to ensure that the organisation has programs and controls in place to address the risk of misconduct but also a duty to ensure that such controls are effective.[3]

As a practical matter, the board may delegate principal oversight for fraud risk management to a board-level committee (typically the audit committee), which is tasked with:

- reviewing and discussing issues raised during the entity's fraud and misconduct risk assessment process
- reviewing and discussing with the internal and external auditors findings on the effectiveness of the organisation's antifraud programs and controls and
- establishing procedures for the receipt and treatment of questions or concerns regarding questionable accounting or auditing matters.[4]

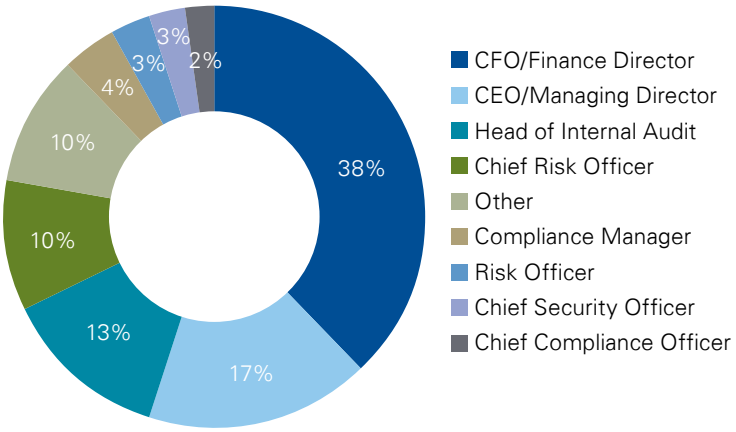
68 percent

Percentage of US employees who reported that their CEO and other senior executives set the right 'tone at the top' on the importance of ethics and integrity.

KPMG Forensic Integrity Survey 2013

Senior management oversight

To help ensure that organisational controls remain effective and in line with regulatory and evaluative criteria, responsibility for an organisation'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). While this critical oversight begins with prevention, it must also follow through to detection and to response efforts.



The chief executive officer is ideally positioned to influence employee actions through his or her personal leadership, specifically by setting the ethical tone of the organisation and playing a crucial role in fostering a culture of high ethics and integrity. The chief executive should lead by example, allocating organisational resources to antifraud efforts, holding management accountable for compliance violations and requiring direct reports to communicate regularly and periodically with their employees on matters related to the organisation's compliance program and related antifraud programs and controls.

Direct responsibility for compliance and antifraud efforts should reside with a high-level individual within the organisation, often a chief compliance or chief risk officer. In many organisations, the chief compliance and/or the chief risk officer reports to the chief executive officer or another member of the executive team (e.g., general counsel) and also has a dotted-line reporting relationship with the board of directors or a board committee.

[3] *In re Caremark Int'l Derivative Litig.*, Del. Ch. 698 A.2d 959 (Del. Ch.1996) and *Stone v. Ritter*, 911 A.2d 362 (Del.Supr. 2006).

[4] The Sarbanes Oxley Act, Section 301 requires that audit committees of issuers listed on U.S. exchanges "establish procedures" for (i) receipt, retention, and treatment of complaints regarding accounting, internal accounting controls, or auditing matters; and (ii) confidential, anonymous submission by employees of concerns regarding questionable accounting or auditing matters. Section 301 was codified as Exchange Act Section 10A(m), which the SEC implemented with Rule 10A-3(b)(3), which may be found at http://taft.law.uc.edu/CCL/34ActRls/rule10A-03.html.

In other organisations the chief risk officer may have direct board accountability. As an example of the role of the chief compliance officer, he or she works together with compliance program staff and designated subject matter experts from relevant functions (e.g., legal, human resources, internal audit, etc.) and coordinates the organisation's approach to preventing, detecting, and responding to fraud and misconduct. When fraud and misconduct issues arise, this individual can draw together the right resources to address the problem and make necessary operational changes.

The chief compliance/chief risk officer, or others tasked by the executive with this role, may also chair a committee of cross-functional managers who, among other activities:

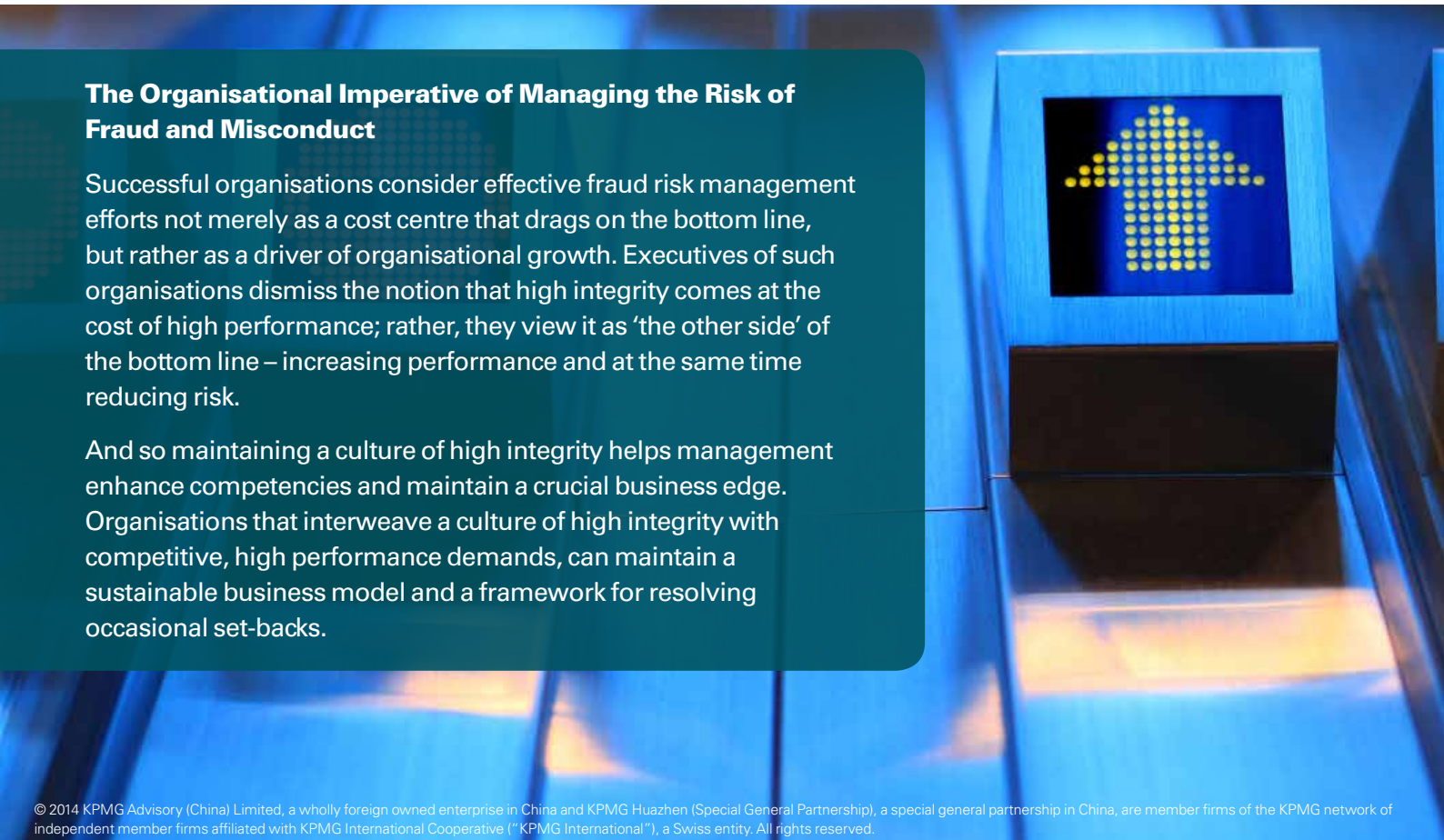
- coordinate the organisation's risk assessment efforts
- establish policies, procedures, and standards of acceptable business practice
- oversee the design and implementation of antifraud programs and controls and
- report to the board and/or the audit committee on the results of fraud risk management activities.

Other organisation leaders, such as department heads, should also have responsibilities in implementing the organisation's fraud risk management strategy. Such individuals are expected to oversee areas of daily operations in which risks arise and serve as subject matter experts to assist the chief compliance/chief risk officer with in their particular areas of expertise or responsibility.

Internal audit function

An organisation's internal audit function is a key participant in antifraud activities, supporting management's approach to preventing, detecting and responding to fraud and misconduct. Such responsibilities represent a change from the more traditional role of internal audit to evaluate the effectiveness of the entity's controls. In general, internal audit may be responsible for:

- assisting in planning and conducting evaluations of the design and operating effectiveness of antifraud programs and controls
- assisting in the organisation's fraud risk assessment and helping draw conclusions as to appropriate mitigation strategies
- considering the results of the fraud risk assessment when developing the annual internal audit plan and
- reporting to the audit committee on internal control assessments, audits, and related activities.



The Organisational Imperative of Managing the Risk of Fraud and Misconduct

Successful organisations consider effective fraud risk management efforts not merely as a cost centre that drags on the bottom line, but rather as a driver of organisational growth. Executives of such organisations dismiss the notion that high integrity comes at the cost of high performance; rather, they view it as 'the other side' of the bottom line – increasing performance and at the same time reducing risk.

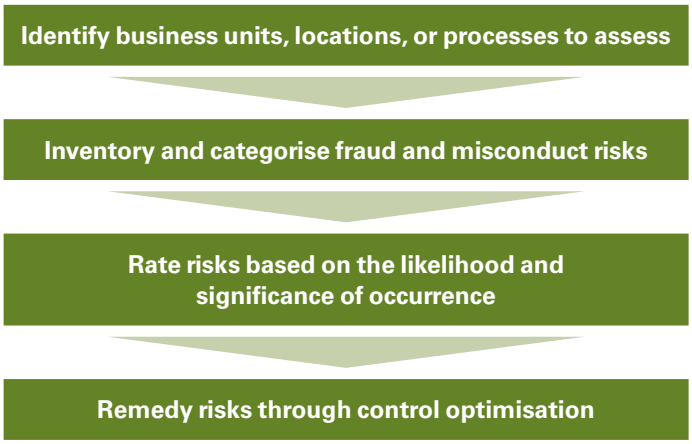
And so maintaining a culture of high integrity helps management enhance competencies and maintain a crucial business edge. Organisations that interweave a culture of high integrity with competitive, high performance demands, can maintain a sustainable business model and a framework for resolving occasional set-backs.

Fraud and misconduct risk assessment

Organisations 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 the organisation's operations, identify gaps or weaknesses in control to mitigate those risks, and develop a practical plan for targeting the right resources and controls to reduce such risks.

Management should seek to ensure that the risk assessment is conducted across the entire organisation, taking into consideration the entity's significant business units, processes and accounts. Throughout this process, subject matter professionals and various control owners provide input as to the relevant risks to achieving organisational objectives as well as the resources and action steps management can use to mitigate such risks. A fraud and misconduct risk assessment typically includes the steps listed in Figure 4, below.

Figure 4: Fraud Risk Assessment Process



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 and ensuring that it remains an ongoing effort, interacting with the organisation's independent auditor to help ensure that assessment results are properly communicated, and helping to ensure that assessment recommendations and mitigation efforts are implemented in a timely manner.

82 percent

Percentage of survey respondents who said that their organisation required management to identify, assess, and manage fraud risk.

KPMG Forensic survey of fraud, bribery & corruption in Australia and New Zealand (2013 issue)

When well executed, fraud risk assessments can help management identify the pressure points and incentives that give rise to some of the most salient integrity-related risks for both organisations and their stakeholders.[5]

Code of conduct

An organisation's code of conduct may be the most important vehicle that management has to communicate to employees key standards of acceptable business conduct. A well-written and communicated code goes beyond restating company policies— such a code sets the tone for the organisation's overall control culture, raising awareness of management's commitment to integrity and the resources available to help employees achieve compliance and integrity goals.[6]

A well-designed code of conduct typically includes attributes such as:

- high-level endorsement from the organisation's leadership, underscoring a commitment to ethics and integrity

[5] *Managing the Risk of Fraud and Misconduct: Meeting the Challenges of a Global, Regulated, and Digital Environment,* Richard H. Girgenti and Timothy P. Hedley. New York: McGraw-Hill, 2011, pg. 123.

[6] ASIC Policy and the ASX Corporate Governance Principles and Recommendations provide guidance and assistance in the conduct of listed companies and are underpinned by the ASX Listing Rules and the provisions of the Corporations Act, for example: Recommendation 3.1 of the current Principles and Recommendations states that companies should establish a code of conduct and disclose the code or a summary of the code.

62 percent

Percentage of US employees who reported that they feel comfortable using an ethics hotline to report misconduct.

KPMG Forensic Integrity Survey 2013

- guidance on values, principles, and strategies aimed at shaping organisational goals and guiding business decisions and behaviours
- simple, concise and positive language that can be readily understood by all employees
- guidance based on each of the company's major policies or key risk areas
- practical guidance on risks based on recognisable 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

59 percent

Percentage of US employees who reported that if employees and managers were to violate standards of conduct, it would be because they believe they will be rewarded based on results, not the means used to achieve them.

KPMG Forensic Integrity Survey 2013

60 percent

Percentage of US employees who reported that if employees and managers were to violate standards of conduct, it would be because they believe that their code of conduct is not taken seriously.

KPMG Forensic Integrity Survey 2013

- a designation of reporting channels and viable mechanisms that employees can use to report concerns or seek advice without fear of retaliation and
- a method for employees to periodically certify or acknowledge that they have received the code, agree to abide by the standards contained therein and pledge to disclose any known or suspected code violations.

Employee and third-party due diligence

An important part of an effective fraud and misconduct prevention strategy is exercising due diligence in the hiring, retention and promotion of employees and relevant third parties. Such due diligence may be especially important in hiring employees who reside in higher-risk geographic locations, are identified as having discretionary authority over the financial reporting process or who have authority in discreet compliance areas. The scope and depth of the due diligence process typically varies based upon the organisation's identified risks, the individual's job function and level of authority and the specific laws of the jurisdiction in which the organisation or the employee resides.[7]

There are also certain situations where screening third parties may be valid. For example, management may wish to screen agents, consultants, vendors, or temporary workers who may have access to confidential information or acquisition targets

[7] One of the minimum requirements announced by the U.S. Sentencing Guidelines for Organisational Defendants calls for the entity 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), available at http://www.ussc.gov/Guidelines/2010_guidelines/Manual_HTML/8b2_1.htm.

that may have regulatory or integrity risks that can materially affect the value of the transaction or the reputation of the organisation.

Due diligence should begin at the start of an employment or business relationship and to the extent permissible, continue periodically throughout. For instance, taking into account in performance evaluations behavioural considerations (such as adherence to the organisation's core values) 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.

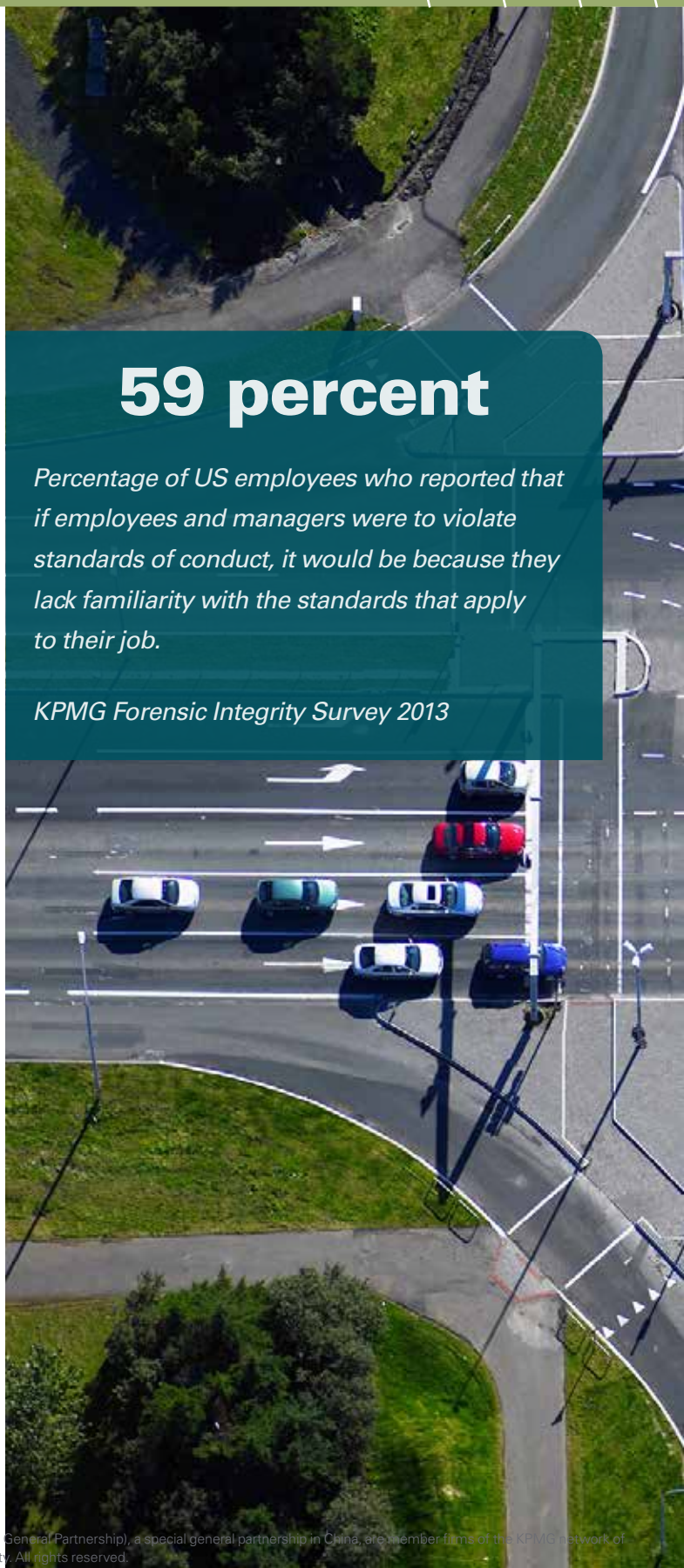
Australian companies listed on the Australian Stock Exchange (ASX) should also consider reviewing requirements to obtain details regards new directors and executives, as a result of a recent recommendation released by the ASX.[8]

Communication and training

Making employees aware of their obligations to mitigate the risks of fraud and misconduct begins with practical communication and training. While many organisations communicate on such issues in an ad hoc manner or by using a one-size-fits-all approach, such efforts may fail to educate employees or provide them with a clear message that their control responsibilities are to be taken seriously.

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

- based upon the results of the fraud and misconduct risk assessment
- tailored to the needs of individual job functions
- integrated with other training efforts, whenever possible
- effective in a variety of settings, using multiple methods and techniques and
- regular and frequent, covering the relevant employee population.

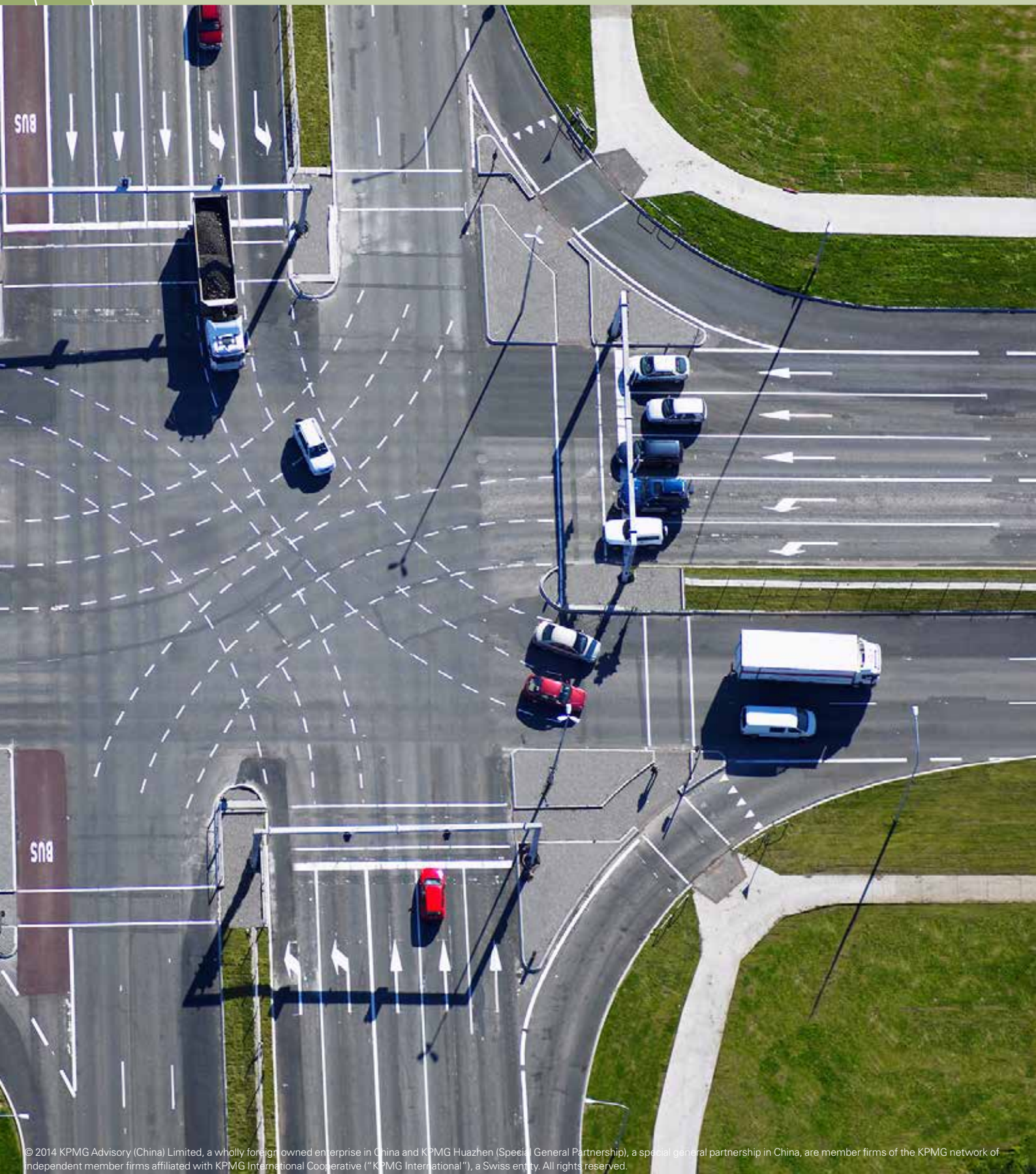


59 percent

Percentage of US employees who reported that if employees and managers were to violate standards of conduct, it would be because they lack familiarity with the standards that apply to their job.

KPMG Forensic Integrity Survey 2013

[8] Recommendation 1.2 of the 3rd ASX Corporate Governance Principles, applicable from 1 July 2014.



Detection

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

Mechanisms for Seeking Advice and Reporting Misconduct

Organisations have a better chance of detecting fraud and misconduct early when they have built a culture where firstly, employees believe they have a stake in the company or see that integrity is a key element of their organisation and secondly, that they have the affirmative obligation to raise their hands and report improper conduct. It is important to understand that employees are more likely to raise concerns when they know where to turn for help, feel comfortable doing so without fear of retaliation and believe that management will be responsive to their concerns.

With the oversight and guidance of senior management, organisations can provide employees with a variety of ways to report concerns, typically requesting that employees follow a process that begins with alerting their own managers, if possible, or a designated human resources or compliance officer. While many organisations offer employees telephone or web-based 'hotlines' that can be used at any time, research suggests that they are often used when normal communication channels are deemed to be impractical or ineffective.

A hotline typically provides a viable method whereby employees, and third-parties if applicable, are encouraged to:

- seek advice before making decisions when the appropriate course of action is unclear and

59 percent

Percentage of US employees who reported that they believed they would be protected from retaliation after reporting misconduct.

KPMG Forensic Integrity Survey 2013

- communicate concerns about potential fraud and misconduct, including questionable accounting or auditing matters.

76 percent

Percentage of US employees who reported that they feel comfortable reporting misconduct to their supervisor.

KPMG Forensic Integrity Survey 2013

A well-designed hotline typically includes the following features:

- **Anonymity**: The organisation's policies 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.
- **Confidentiality:** All matters reported via the hotline are treated confidentially. Hotline operators inform callers that relevant safeguards will protect caller confidentiality, for instance limiting access to personal information (if volunteered). Hotline operators disclose to callers any limitations the organisation may have in preserving caller confidentiality (e.g., callers should have no expectation of confidentiality if the call leads to a government investigation).
- **Follow-up on Non-retaliation:** The organisation's policies prohibit retaliation against employees who in good faith, seek advice or report misconduct. The organisation requires a follow-up with employees periodically after the hotline case has been closed (e.g., at 1, 3, and 6-month intervals) to ensure that they have not experienced retaliation. The company encourages the employees to report any instances of retaliation and takes swift action against those who do retaliate.
- **Organisation-wide Availability:** Employees at international locations are able to use the hotline through features such as real-time foreign language translation and toll-free call routing (or alternatively, have access to local hotlines in specific countries or regions).

- **'Real Time' Assistance:** The hotline is designed to provide an immediate, "live" call response to facilitate a thorough and consistent treatment of a caller's report of misconduct or to provide immediate guidance (if the hotline offers such assistance).[9] Thus, hotline operators need to be appropriately qualified, trained, and, in some situations, authorised to provide advice.
- **Data Management Procedures:** The organisation uses consistent protocols to gather relevant facts, manage and analyse hotline calls, and report key performance indicators to management and the board. This is often accomplished, for example, by using a computerised, back-end case management system to store, organise, prioritise, and route employees reports.
- **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 or a regulatory/compliance risk.
- **Audit Committee Notification:** The hotline includes protocols that specify the nature and timing of allegations that are escalated to the audit committee (particularly important for companies that must comply with the requirements of the US Sarbanes-Oxley Act of 2002).[10]
- **Prominent Communications:** The organisation publicises its hotline prominently. Such communications may include, among others: (i) describing the hotline within the code of conduct, in key organisational publications and training, and at management 'town hall' type meetings; (ii) featuring the hotline telephone number on posters, banners, wallet cards, screen savers, telephone directories or desk calendars; and (iii) communicating illustrative case-studies based on hotline calls to employees (e.g., in newsletters, training programs, or intranet sites) to demonstrate that the organisation values hotline calls and is able to provide assistance to those who use the hotline.

63 percent

Percentage of survey respondents who said that their single largest fraud was either detected through internal controls or as a result of a notification by an employee.

KPMG Forensic survey of fraud, bribery & corruption in Australia and New Zealand (2013 issue)

73 percent

Percentage of US employees who reported that their organisation audits and monitors employee compliance with the code of conduct either formally or informally.

KPMG Forensic Integrity Survey 2013

Auditing and monitoring

Auditing and monitoring systems are important tools that management can use to determine whether or not the organisation's controls are working as intended. They can also facilitate an effective governance process through the evaluation of other characteristics, including ethics and values, performance management, and the assessment and communication of risk.[11]

Since it is impossible to audit every fraud and misconduct risk, management should develop a comprehensive auditing and monitoring plan that is based upon risks identified through a formal risk assessment process.

An auditing and monitoring plan should encompass activities that are tailored in depth to the nature and degree of the risk involved,

[9] Typically, outsourced, third-party hotline vendors only direct questions or concerns to their client organisation's compliance, audit, or legal function for handling, and do not attempt to provide callers with guidance in response to specific questions.

[10] Section 301 of the U.S. Sarbanes-Oxley Act of 2002 requires audit committees to establish procedures for the receipt, retention, and treatment of complaints received regarding accounting, internal accounting controls, or auditing matters and the confidential, anonymous submission by employees of the issuer of concerns regarding questionable accounting or auditing matters. Available at http://taft.law.uc.edu/CCL/SOact/sec301.html.

[11] "Managing the Risk of Fraud and Misconduct: Meeting the Challenges of a Global, Regulated, and Digital Environment," Richard H. Girgenti and Timothy P. Hedley. New York: McGraw-Hill, 2011, pg. 215.

with higher-risk issues receiving priority treatment. Auditing activities (an evaluation of past events typically conducted by internal auditors) and monitoring activities (a real-time evaluation typically conducted by management) should be performed in, but are not limited to, areas where:

- audits are legally required
- 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 organisational change
- laws and regulations have changed significantly or
- governmental agencies are stepping-up or targeting enforcement actions.

An organisation'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 should:

- occur in the ordinary course of operations, including during regular management and supervisory activities
- make use of available technologies to identify risks and control failures
- draw on external information to corroborate internally generated information
- formally communicate identified deficiencies and exceptions to senior leadership, so that the harm to the organisation is appropriately understood and mitigated and
- use results to enhance and modify other controls, such as communications and training, performance evaluations, and discipline.

Forensic data analysis

Our modern digital environment has created a world of big data. Locked within this big data are correlations, patterns, trends, relationships and associations that can provide insight into the nature of organisational, employee and third party fraud and misconduct. To unlock these insights, organisations can deploy sophisticated forensic-based data analytics to help detect fraud and misconduct and understand the root causes of any irregularities. For example, basic forensic data analytics may employ rules-based and behaviour-based routines to ferret out irregularities in manual journal entries, locate ghost employees in payroll records or find non-existent vendors in accounts payable.

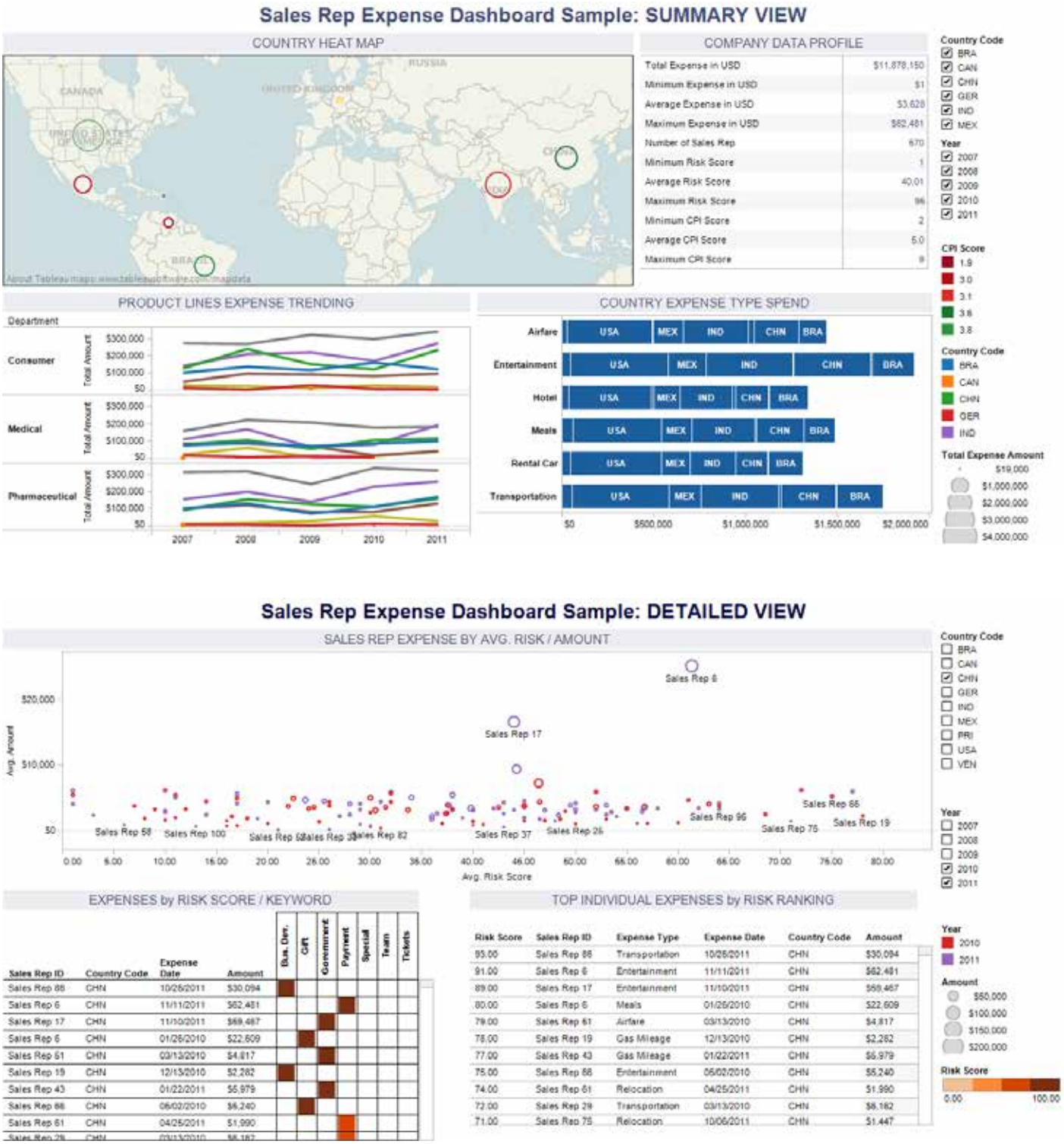
More sophisticated predictive analytic tools employ an array of statistical techniques and modelling to analyse current and historical information to make predictions. Such predictions can support fraud prevention, detection and response strategies by identifying control vulnerabilities, fraudulent transactions in real time and potential suspects during investigations. Regardless of the application, predictive analytic results can be used continuously to refine analytical models to help better support risk mitigation strategies.

Many custom modelling and analytic programs have built-in case management systems, allowing for collaborative work flow in tracking and routing alerts, investigating matters and reporting on instances of fraud and misconduct. Many also incorporate visuals and dashboards similar to the examples of analytic dashboards provided below that profile a company's travel and entertainment expenses by sales representative to help identify bribery or corruption risks (particularly with respect to FCPA, UK Bribery Act, the Australian Criminal Code (Bribing of Public Foreign Officials) and other relevant anti-bribery laws) with a focus on spend in countries with high risk scores.

The power of these analytic tools is often augmented by third party data sources. For example, the Social Security Death Master file, government watch lists and information from credit reporting agencies. All of these are provided in electronic format and are just some examples that can aid organisations in managing transactional risk, screening employees, profiling vendors and ensuring due diligence is performed on third-party intermediaries. Simply put, forensic data analytics can provide a single point of view into desperate data sets to provide insights into previously unknown integrity risks.

The real power of these data-driven tools, however, lies in the fact that they can handle vast amounts of data that is growing at an astounding rate and that resides on nearly countless platforms. For example, data available for analysis may be structured in the form of transactional information or it may be unstructured in the form of company documents, emails and the like. Further, data available for analysis may reside within a company information system, employee smart phone, manufacturing equipment, point of sale systems, GPS sensors and even social network sites. The future of proactive fraud prevention and detection will lay in the seamless, fully integrated use of data analytics platforms, and related tools.

Figure 5: FCPA Dashboard of Sales Rep Expenses



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 an objective and credible assessment of the suspected violation and allow management to 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 typically includes the following attributes, among others:

- oversight by the organisation'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 in house or external legal counsel, selected by the audit or other committee, with little or no ties to the entity's management team, and that can perform an unbiased, independent and qualified investigation
- activities undertaken by investigators who understand the legal dimensions and potential risks of the matter at hand, as well as the necessary investigatory skills
- briefing the organisation's external auditor so that the latter can consider the proposed scope of work in the audit of the organisation's financial statements
- as an expectation of cooperation with investigators, allowing no employee or member of management to obscure the facts that gave rise to the investigation and
- reporting protocols that provide management, the board, external auditors, regulators, and, where appropriate, the public, with information relevant to the investigation's findings in the spirit of full cooperation, self-disclosure and transparency.

Based upon a number of factors, including the nature of the potential misconduct, parties involved, and significance, the organisation 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. By mandating meaningful sanctions, management can send a signal to both internal and external stakeholders that the organisation considers managing fraud and misconduct risk a top priority. Appropriate discipline is also a requirement under leading regulatory and evaluative frameworks.

Organisations would do well to establish and communicate to employees a well-designed disciplinary process which includes 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) and
- uniform and consistent application of disciplinary process regardless of job level, tenure, or job function.

Holding managers accountable for the misconduct of their subordinates is another important consideration. Managers should 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 the organisations 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 and
- enforced the organisations 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 where appropriate:

- voluntarily disclosing the results of the investigation to the government or other relevant body (e.g., to law enforcement or regulatory authorities)
- remedying the harm caused (e.g., initiate legal proceedings to recover monies or other property, compensate those injured by the misconduct, etc.)
- 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 and
- communicating to the wider employee population that management took appropriate, responsive action.

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

55 percent

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

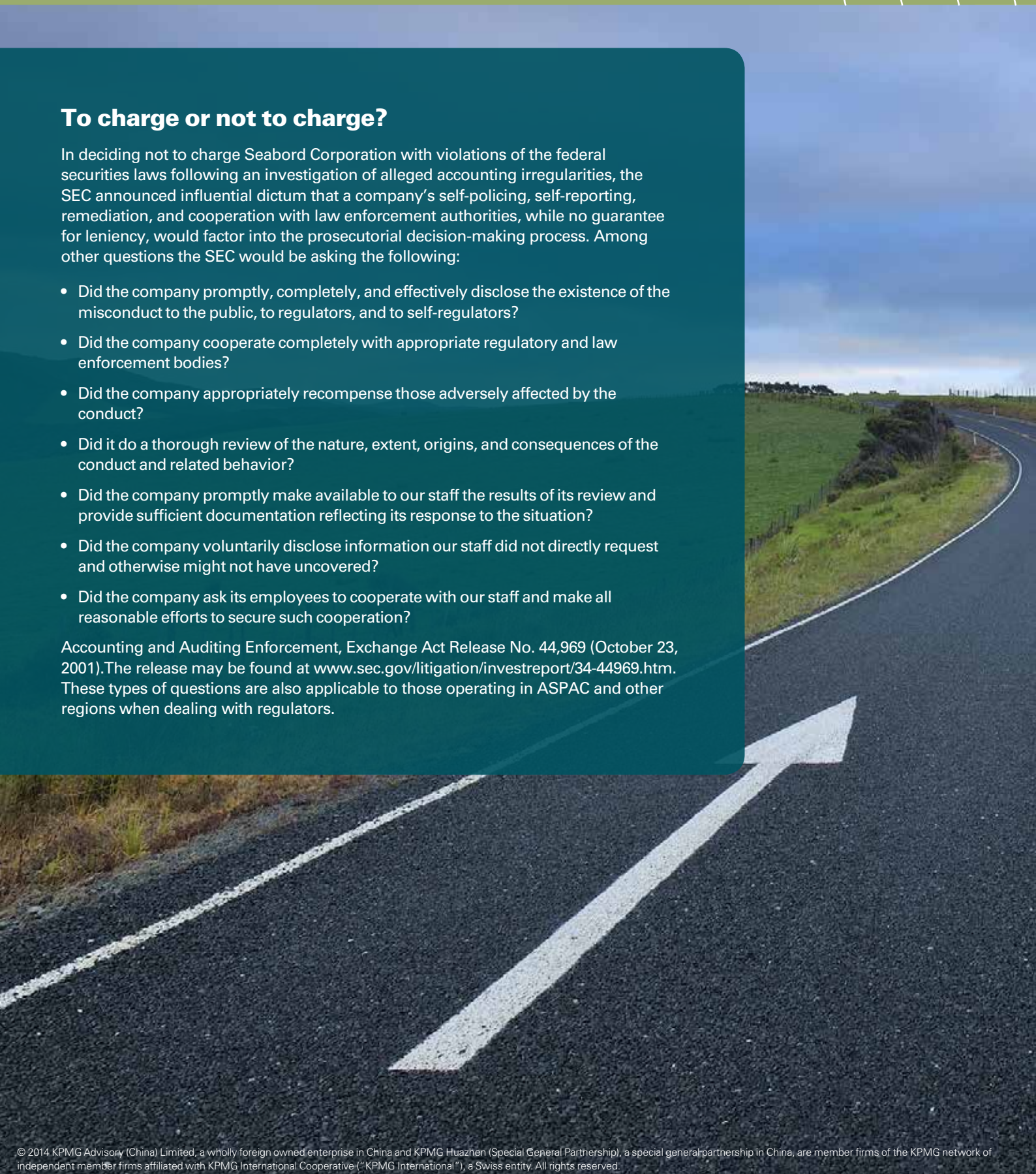
KPMG Forensic Integrity Survey 2013

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. These types of questions are also applicable to those operating in ASPAC and other regions when dealing with regulators.



To fine or not to fine?

In a related opinion, 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 organisation 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:** Assessing the needs of the organisation based on the nature of fraud and misconduct risk that controls are intended to mitigate, as well as the adequacy of existing controls.
- **Design:** Developing controls to prevent, detect, and respond to identified risks and also in a manner consistent with legal and regulatory criteria as well as other relevant leading practices.
- **Implementation:** Deploying a process for implementing 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, and routine monitoring.

Assessment

The nature of fraud and misconduct risks facing an organisation can be as diverse and fluid as the business itself. For example, potential risks of fraud and misconduct for a national bank that has experienced rapid growth through acquisitions are different from those of a global energy company seeking to expand oil exploration in emerging markets. No two organisations have the same risk profile and as such, antifraud measures should be tailored to the unique risks of the organisation, the specific conditions that give rise to those risks, and the targeted resource needs required in balancing risk and control.

The first assessment step is to ascertain the organisation's fraud and misconduct risks and determine how effectively it manages these risks. The scope of this analysis should take into consideration the organisation's key business units, processes, systems, and controls, as well as other relevant factors. The organisation can also identify key stakeholders who may need to be involved. Once the organisation profiles its current state and sets targets for improvements, it can evaluate the 'gaps' 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 effective controls that will protect the organisation from the risks of fraud and misconduct. For an entity to design effective controls, it must first tailor these controls to the risks it is facing as well as to the organisation's unique business environment. When designing controls, management should endeavour to go beyond merely observing 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 organisations have generally found to be effective within the context of such regulatory frameworks). 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 as such will have individualised control considerations. Management would be well served to consider the organisation's unique circumstances when designing fraud controls. For example, 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 organisation's distinct business needs.

Implementation

Once controls have been designed, management should establish a strategy and process for implementing the new controls throughout the organisation 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, it is critical that senior management champion these efforts and for employees to receive clear and frequent communications with respect to when, how, and by whom the controls will be rolled out as well as the manner in which compliance with the new controls will be enforced.

Evaluation

Simply because a control exists is no guarantee that it will operate 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 organisation'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 as well as leading practices that similarly-situated organisations have found to correlate with effective risk management. Management can then undertake 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 organisation'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, management should seek to understand whether the mitigation strategies that were designed and implemented were in fact preventing or detecting the misconduct in question. Similarly, management may have implemented a well-designed code of conduct, but are employees actually using the document and finding it effective in guiding their day-to-day activities?

When such basic questions are addressed management can focus on gathering empirical data on control effectiveness using review and evaluation techniques (e.g., empirically structured audits and 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 that captures 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 organisation'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 organisations 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.

Organisations undertaking this effort should begin by assessing how well they are managing the risks of fraud and misconduct. Identifying and prioritising known risks and existing controls is an important first step. Subsequently, the organisation can determine its ideal future state, perform a gap analysis and prioritise activities that will help enable the development of an ethics and compliance program and related antifraud programs and controls.

Such a program will not only help enable appropriate compliance with legal and regulatory mandates (and potentially avoid fines and penalties related to compliance violations) but also help the organisation align its corporate values and performance and protect its many assets, driving organisational growth and minimising risks.

Appendix

Selected international governance, risk, and compliance criteria

Australia

Criminal Code Act 1995 (Cth)

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 offences 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 (Cth) (Including CLERP 9 Amendments)

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 and
- financial statements must present a true and fair view of the financial position and performance of the entity. (Section 295A)

AUS 210 (2002)

An auditing standard which requires auditors to consider fraud and error in an audit of a financial report.

ASX Listing Rules Guidance Note 9 (2012)

Principle 7 – Listed entities should establish a sound system of risk oversight and management and internal control.

Australian Standard 8001 – 2008 Fraud and Corruption Control (2008)

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

Criminal Code Amendment (Bribery of Foreign Public Officials) Act 1999 (Cth)

This law makes it an offence in Australia for a person to provide, offer or promising a benefit to another person that they are not legitimately due with the intention of influencing a foreign public official in order to obtain or retain a business or business advantage, not legitimately due to the recipient.

Public Interest Disclosure Act (2013) (Cth)

Whistleblower protection scheme providing protection for public sector whistleblowers in Australia.

Fraud Control in Australian Government Agencies (2011)

A guide for management who carry responsibility for the effective and efficient control of fraud risks, both inside and outside the Australian Government.

The Anti-Money Laundering and Counter –Terrorism Financing Act (AML/CTF Act) 2006 (cth)

The Act and its related rules require entities that provide financial services (known as Reporting Entities) to adopt and maintain an AML/CTF program. The AML/CTF programs are divided into Parts A (general) and B (customer identification). In addition entities have a range of reporting obligations such as for international transfers and amounts about a certain threshold. This information is reported to the Australian Transaction Reports and Analysis Centre (AUSTRAC).

China

The Anti-Unfair Competition Law (1993)

The Anti-Unfair Competition Law is the primary legal basis for administrative authorities to crack down on commercial bribery. It prohibits the business operators from offering bribes to sell or purchase merchandise or from giving the other party any unlawful kickbacks. Any commission to an intermediary or discount to any party must be accurately recorded in the accounting books of the company and the party who receives the commission or discount. Otherwise the company and the other party could be punished for commercial bribery.

The Anti-Money Laundering Law of the People Republic of China (2007)

The Anti-Money Laundering Law of the People's Republic of China (the AML Law) came into effect on 1 January 2007, when China became a member of the Financial Action Task Force (FATF). The AML Law and the PRC Criminal Law form the basic legal framework for the prevention, monitoring, regulation, investigation and punishment of money laundering activities in China. Financial institutions must implement measures to fulfil their anti-money laundering obligations under the AML Law and related rules and regulations. Non-financial institutions are also monitored, but to a lesser extent.

SPC and SPP Interpretation – Criminal Fraud Cases (2011)

An organisation and its employees are prohibited from: offering bribes to a state functionary; giving bribes for securing illegitimate benefits; or soliciting and/or accepting bribes in relation to any benefit provided to the briber. It is also prohibited for anyone to obtain public or private money or property by fraud or deceit. This brings China's anti-corruption laws into closer alignment with those in other countries, such as the United States Foreign Corrupt Practices Act.

SPC and SPP Interpretation – Bribe-Giving Cases (2012)

This interpretation of PRC anti-bribery law places more focus on bribe givers by expanding upon existing sentencing thresholds and creating new incentives for voluntary disclosure. It also sets the PRC Criminal Law's threshold as low as CNY10,000 for individual bribes to State Personnel as the floor for criminal liability.

Hong Kong

The Drug Trafficking (Recovery of Proceeds) Ordinance (1993)

This ordinance contains provisions for the investigation of assets that are suspected of being derived from drug trafficking activities, the freezing of assets on arrest and the confiscation of the proceeds from drug trafficking activities upon conviction.

Crimes Ordinance (1997)

This ordinance criminalises the act of forgery of any instrument (i.e. documents, discs, information recorded or stored by electronic means, etc.) and extends to the use and possession of a false instrument by persons who have knowledge of its false nature.

Theft Ordinance (1997)

This ordinance provides for the statutory definition of the criminal offence of fraud and criminalises the misappropriation of property, false accounting and false representations by company officers. It sets out the liability of company officers in certain offences committed by a body corporate which have one of the company officers' consent.

The Prevention of Bribery Ordinance (1997)

This ordinance is the primary anti-corruption legislation in Hong Kong. It criminalises bribery and corrupt transactions in both the public and private sectors. It provides legal power to the Independent Commission Against Corruption for investigating offences under this ordinance.

Selected international governance, risk, and compliance criteria (continued)

The United Nations (Anti-Terrorism Measures) Ordinance (2002)

This ordinance is principally directed towards implementing decisions contained in Resolution 1373 dated 28 September 2001 of the United Nations Security Council (UNSC Resolution 1373) aimed at combating terrorist financing and acts of terrorism. Besides the mandatory elements of the UNSC Resolution 1373, the ordinance also implements the more pressing elements of the special recommendations on terrorist financing developed by the FATF.

The Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (2012)

This ordinance creates the statutory obligations on customer due diligence and record-keeping for specified financial institutions, including insurance institutions. The key features of the ordinance include:

- providing supervisory and enforcement powers to four regulatory authorities, namely the securities and futures Commission, the Hong Kong Monetary Authority, the Office of the Commissioner of Insurance and the Customs and Excise Department
- codifying the customer due diligence and record-keeping obligations of financial institutions into statutory obligations, as set out in Schedule 2 of the ordinance and
- providing supervisory and criminal sanctions for non-compliance with statutory requirements.

Implementing a licensing regime and anti-money laundering framework for remittance agents and money changers.

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 and
- establish internal procedures to train staff to report suspicions to the authorities and to set up preventive systems within their organisations.

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

The European Commission Antifraud Strategy (CAFS) (24/06/2011)

The 2011 CAFS is binding on the Commission and its executive agencies, and updates and replaces the antifraud strategy of 2000. The key objectives of CAFS are to:

- improve and update fraud prevention, detection and investigation techniques
- recover a higher proportion of funds lost due to fraud and
- deter future fraud through appropriate penalties.

The strategy sets out various methods by which antifraud measures will be driven out, together with the support of European Antifraud Office (OLAF). These methods include:

- the introduction of specific antifraud strategies per sector in the Commission; and
- the clarification and enforcement of the different responsibilities of the various stakeholders.

Ensuring that the strategies cover the whole expenditure cycle, and that antifraud measures are proportionate and cost-effective.

Japan

The Business Accounting Council (BSA), an advisory body established by the Japanese Financial Services Authority, issued a *Standard to Address the Risk of Fraud in the Audit* in March 2013. This addresses requirements for auditors to consider matters related to the potential for fraud in financial statements.

Malaysia

Financial Services Act (2013)

This Act provides for the regulation and supervision of financial institutions, payment systems and other relevant entities and the oversight of the money market and foreign exchange market to promote financial stability and for related, consequential or incidental matters.

As per paragraph 56, the business and affairs of an institution shall be managed under the direction and oversight of its board of directors, subject to this Act and any other written law which may be applicable to the institution.

The board of directors shall –

(a) set and oversee the implementation of business and risk objectives and strategies and in doing so shall have regard to the long term viability of the institution and reasonable standards of fair dealing

(b) ensure and oversee the effective design and implementation of sound internal controls, compliance and risk management systems commensurate with the nature, scale and complexity of the business and structure of the institution

(c) oversee the performance of the senior management in managing the business and affairs of the institution

(d) ensure that there is a reliable and transparent financial reporting process within the institution and

(e) promote timely and effective communications between the institution and the Bank on matters affecting or that may affect the safety and soundness of the institution

Malaysian Code on Corporate Governance (2012)

The Malaysian Code on Corporate Governance 2012 which supersedes the 2007 Code establishes the broad principles and specific recommendations on structures and processes which companies should adopt in making good corporate governance an integral part of their business dealings and culture. It advocates the adoption of standards that go beyond the minimum as prescribed by regulation. Listed companies are required to report on their compliance with the MCCG in the annual reports.

Whistleblowers Protection Act (2010)

An Act to combat corruption and other wrongdoings by encouraging and facilitating disclosures of improper conduct in the public and private sector, to protect persons making those disclosures from detrimental action, to provide for the matters disclosed to be investigated and dealt with and to provide for other matters connected therewith.

Malaysian Anti-Corruption Commission Act (2009)

An Act to further and better provide for the prevention of corruption. Principal objects of this Act are to promote the integrity and accountability of public and private sector administration by constituting an independent and accountable anti-corruption body; and to educate public authorities, public officials and members of the public about corruption and its detrimental effects on public and private sector administration and on the community.

Malaysian Institute of Accountants – ISA240

As per ISA240, auditors objectives are:

a) to identify and assess the risks of material misstatement of the financial statements due to fraud

b) to obtain sufficient appropriate audit evidence regarding the assessed risks of material misstatement due to fraud, through designing and implementing appropriate responses and

c) to respond appropriately to fraud or suspected fraud identified during the audit.

Selected international governance, risk, and compliance criteria (continued)

Capital Markets and Services Act (2007)

Requires public listed companies to manage any risks associated with its business and operations prudently. Other than violations in securities trading and submission of false or misleading information, directors and officers can now be held liable for intending to cause wrongful loss to the listed companies.

Anti-Money Laundering Act (2001)

An Act to provide for the offence of money laundering, the measures to be taken for the prevention of money laundering and to provide for forfeiture of property derived from, or involved in, money laundering, and for matters incidental thereto or connected therewith.

Under paragraph 87, where an offence is committed by a body corporate or an association of persons, a person—

(a) who is its director, controller, officer, or partner or

(b) who is concerned in the management of its affairs, at the time of the commission of the offence, is deemed to have committed that offence unless that person proves that the offence was committed without his consent or connivance and that he exercised such diligence to prevent the commission of the offence as he ought to have exercised, having regard to the nature of his function in that capacity and to the circumstances.

Penal Code (Revised 1997)

The Penal Code provides explanations in regards to fraud and dishonesty. It elaborates on a wide scope of offences which include criminal misappropriation of property, criminal breach of trust, cheating/fraud, forgery, counterfeiting and others. Under the penal code, whoever who commits an offence covered within the scope of the act will be liable and punished accordingly

Under paragraph 130 where an offence has been committed by a body corporate in relation to terrorism, any person who, at the time of the commission of the offence, was a person responsible for the management or control of the body corporate, which includes a director, manager, secretary or other similar officer of the body corporate or a person who was purporting to act in any such capacity, shall be guilty of that offence and shall be liable to be proceeded against and punished accordingly.

Securities Commission Act (1993)

Under paragraph 138, where any offence against this Act or any regulations made there under has been committed by a body corporate, any person who at the time of the commission of the offence was a director, a chief executive officer, an officer, an employee, a representative or the secretary of the body corporate or was purporting to act in such capacity, shall be deemed to have committed that offence unless he proves that the offence was committed without his consent or connivance and that he exercised all such diligence to prevent the commission of the offence as he ought to have exercised, having regard to the nature of his functions in that capacity and to all the circumstances.

Securities Industry (Central Depositories) Act (1991)

Under the act, if offences such as falsifications of records or accounts, destruction, concealment, mutilation or alteration of any record, furnishing of false or misleading information are committed by a body corporate, any person who at the time of the commission of the offence was a director, an executive officer or the secretary of the body corporate or was purporting to act in such capacity, shall be deemed to have committed that offence unless he proves that the offence was committed without his consent or connivance and that he exercised all due diligence to prevent the commission of the offence as he ought to have exercised, having regard to the nature of his functions in that capacity and to all the circumstances.

Companies Act (1965)

Requires directors of public companies and their companies to have a system of internal control that will provide reasonable assurance that assets of the company are safeguarded and transactions contained in the financial statements are properly authorised as to give a true and fair view. Other provisions include the duty of an auditor to report on any fraud or dishonesty committed by the company to the Registrar.

Section 304 covers the responsibility for fraudulent trading. It declares that any person who was knowingly a party to the carrying on of the business in that manner shall be personally responsible, without any limitation of liability, for all or any of the debts or other liabilities of the company as the Court directs.

Contracts Act (1950)

Contracts Act provides guidance on fraud implications on contract agreements.

As per paragraph 17, "Fraud" includes any of the following acts committed by a party to a contract, or with his connivance, or by his agent, with intent to deceive another party thereto or his agent, or to induce him to enter into the contract:

(a) the suggestion, as to a fact, of that which is not true by one who does not believe it to be true

(b) the active concealment of a fact by one having knowledge or belief of the fact

(c) a promise made without any intention of performing it;

(d) any other act fitted to deceive and

(e) any such act or omission as the law specially declares to be fraudulent.

New Zealand

Protected Disclosures Act 2000

This legislation promotes the public interest by setting out procedures to be followed when making a disclosure, and provides protection to employees who make disclosures of 'serious wrongdoing', in accordance with the Act.

Crimes (Bribery of Foreign Public Officials) Amendment Act 2001

This Act created an offence with narrow exceptions to corruptly give, or agree to give a foreign public official a benefit with the intent of influencing them in respect of their official capacity in order to obtain or retain business or an improper advantage in business. It introduces an element of extra territoriality enabling New Zealand citizens, residents, and body corporates or corporations solely incorporated in New Zealand to be prosecuted for actions outside of New Zealand.

Anti-Money Laundering and Countering Financing of Terrorism Act 2009

The Act and its related rules require entities that provide financial services (known as Reporting Entities) to adopt and maintain an AML/CTF program. The Act and associated regulations increase reporting entities mandatory requirements to prevent and detect money laundering including a mandatory Audit requirement. The supervising responsibility are split across three government agencies.

Singapore

Penal Code

The Penal Code sets out the general principles of the criminal law of Singapore, as well as the elements and penalties of common criminal offences such as theft, extortion, cheating and fraud.

Prevention of Corruption Act

The Prevention of Corruption Act governs the primary offence of corruption. A number of amendments have been made over the years to provide the relevant authorities with more investigative powers and enhance punishments for offenders.

Futures and Securities Act

The Futures and Securities Act regulates activities and institutions in the securities and futures industry in Singapore. It prohibits market misconduct and prescribes severe penalties for breaches.

Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (CDSA)

The CDSA is the primary legislation to combat money laundering in Singapore and allows for the confiscation of such proceeds. It is mandatory for a person, who in the course of his business or employment, to lodge a suspicious transaction report if he knows or has reason to suspect that any property may be connected to a criminal activity.

Code of Corporate Governance

Requires all companies listed on the Singapore Exchange to provide a detailed description of their corporate governance practices and explain any deviations from the Code of Corporate Governance in their annual reports.

Thailand

Penal Code of Thailand

Thailand's Penal Code addresses corruption in the public sector. Under the Penal Code, the act of giving, offering or agreeing to give property or any benefit to any government official to induce them to wrongfully discharge, omit to discharge or delay a discharge of any of their duties, is punishable by imprisonment not exceeding 5 years or a fine not exceeding ten thousand Thai baht or both.

Organic Act on Counter Corruption (1999) as amended No. 2 (2011)

Thailand's Organic Act on Counter Corruption prohibits officials (including people who were officials within the last 2 years) from unlawfully accepting property or benefits. No particular motive is required. The Act establishes the National Anti-Corruption Commission and regulates the power and duties of its members.

Selected international governance, risk, and compliance criteria (continued)

National Anti-Corruption Commission

Thailand's National Anti-Corruption Commission (NACC) is an independent agency with broad powers of investigation and can independently initiate prosecution. The NACC has seven divisions: Prevention, Suppression, Inspection of Assets and Liabilities, Research, Legal Affairs, International Affairs and Human Resource Development. The NACC has a mandate to examine the assets of politicians or state officials in cases where individuals are accused of accumulating wealth in an unusual manner. The NACC also has the authority to act as the central coordinator for Thailand's international anti-corruption obligations.

Money Laundering Prevention and Suppression Act (1999) amended (2009)

Thailand's Money Laundering Prevention and Suppression Act was passed with the aim of combating the drug trade and other illicit activities, such as corruption, criminal fraud and prostitution. Under this act, it is a crime to transfer, convert, or receive the transfer of funds or property arising from criminal offenses for the purpose of hiding or concealing the source of the funds. It sets out the maximum prison terms and fines for violating the law and for not complying with reporting requirements. The amended Act requires more control from financial institutions and identifies the types of operators that are required to report suspicious transactions.

Accounting Act (2000)

The Accounting Act requires companies to file audited financial statements with the Ministry of Finance annually. Accountants must keep accurate records. Any person who makes a false record is subject to imprisonment for a term of up to two years and a fine not exceeding 40,000 Thai baht. Where the false entry or statement is made by the person obliged to keep such accounts, the penalty is imprisonment of up to 3 years, a fine not exceeding 60,000 baht, or both.

United Kingdom

The Financial Services and Markets Act (2000)

This Act supports the Financial Services Authority's (FSA's) (now the Financial Conduct Authority "FCA") 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 FCA 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, as amended)

The Act strengthened the law on money laundering and set up an Assets Recovery Agency to investigate and recover assets and wealth obtained as a result of unlawful activity. The Assets Recovery Agency has since March 2008 become part of the Serious Organised Crime Agency (SOCA).

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.

The Fraud Act (2006)

The Fraud Act came into effect on January 15, 2007, and supersedes and replaces other legislation.

The Act provides the following statutory definitions of the criminal offence of fraud:

- "Fraud by false representation", which is defined as where a person makes "any representation as to fact or law ... express or implied" which they know to be untrue or misleading
- "Fraud by failing to disclose information", defined as where a person fails to disclose any information to a third party when under a legal duty to disclose such information and
- "Fraud by abuse of position", defined as where a person, who occupies a position in which he/she are expected to safeguard the financial interests of another, abuses that position; this includes where the abuse is through omission.

For all three, the person must have acted dishonestly, and with the intent of making a gain for themselves or anyone else, or inflicting a loss (or a risk of loss) on another.

The Act also provides for corporate criminal liability. Section 12 of the Act states that where an offence against

the Act was committed by a body corporate, but was carried out with the "consent or connivance" of any director, manager, secretary or officer of the body corporate, or any person purporting to be such, then that person and the body corporate itself is liable.

UK Corporate Governance Code (2010, as amended)

The UK Corporate Governance Code (formerly the Combined Code) sets out standards of good practice in relation to board leadership and effectiveness, remuneration, accountability, and relations with shareholders. All companies with a Premium Listing of equity shares in the UK are required under the Listing Rules to report on how they have applied the Code in their annual report and accounts. Some of the provisions of the Code require disclosures to be made in order to comply with them. The new edition of the Code was published in September 2012 and applies to reporting periods beginning on or 1 October 2012. New provisions of the Code include:

- the requirement that companies publish their policy on boardroom gender diversity and report against it annually
- that FTSE 350 companies should put the external audit contract out to tender at least every ten year and
- the requirement that companies provide clear and meaningful explanations when they choose not to apply one of the provisions of the Code, so that their shareholders can understand the reasons for doing so and judge whether they are content with the approach the company has taken.

Bribery Act (2010)

The Act has universal jurisdiction for individuals or commercial organisations with links to the United Kingdom, irrespective of where the crime occurred. The Act repeals all previous statutory and common law provisions in relation to bribery and sets out the following crimes:

- Bribery
- Requesting, agreeing to accept or accepting a financial or other advantage, either for oneself or for another
- Bribery of foreign public officials and
- The failure of a commercial organisation to prevent bribery on its behalf, unless the commercial organisation can demonstrate that it had adequate procedures to prevent such act.

The penalties include imprisonment and an unlimited fine. The Act further provides for the confiscation of property under the Proceeds of Crime Act 2002 and the disqualification of directors under the Company Directors Disqualification Act 1986.

United States

The Sarbanes-Oxley Act of 2002 (Section 404)

Section 404 of the Sarbanes-Oxley Act requires companies and their auditors to evaluate the effectiveness of their internal controls over financial reporting based on a suitable control framework. Most companies in the United States are applying the integrated internal control framework developed by the Committee of Sponsoring Organisations (COSO). Generally speaking, the COSO framework addresses compliance program elements in entity-wide components that have a pervasive influence on organisational behaviour, such as the control environment. Examples 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 and
- appropriateness of remedial action taken in response to violations of the code of conduct.

Corporate Governance Listing Standards

In response to 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 includes standards that require listed

Selected international governance, risk, and compliance criteria (continued)

companies to adopt and disclose codes of conduct for directors, officers, and employees and disclose any code of conduct waivers for directors or executive officers. In addition, the rules of each exchange require listed companies to adopt mechanisms to enforce the codes of conduct.

US Federal Sentencing Guidelines for Organisational Defendants

The federal sentencing guidelines for organisational defendants (first adopted in 1991) establish minimum compliance and ethics program requirements for organisations seeking to mitigate penalties for corporate crimes. Amended in 2004 and again on 2010, these guidelines make it explicit that organisations are expected to 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 organisations 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 are knowledgeable and exercise reasonable oversight over the compliance and ethics program
- assign a high-level individual within the organisation to ensure the organisation has an effective compliance and ethics program and delegate day-to-day operational responsibility to individuals with adequate resources and authority and direct access to the board
- ensure high-level individuals and those with substantial discretionary authority are knowledgeable about the program, exercise due diligence in performing their duties, and promote a culture that encourages ethical conduct and a commitment to compliance with the law
- use reasonable efforts and exercise due diligence to exclude from positions of substantial authority individuals 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
- publicise a system, which may include mechanisms for anonymity and confidentiality, under which the organisation'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 the compliance and ethics program consistently through incentives and disciplinary measures and
- take reasonable steps to respond appropriately to misconduct, including making necessary modifications to the compliance and ethics program.

The Dodd-Frank Wall Street Reform and Consumer Protection Law

The Dodd-Frank Act was enacted to ensure stability in the US financial markets, affecting all US financial institutions, many non-US financial institutions, and many non-financial companies. The Act alters practices in banking, securities, derivatives, executive compensation, consumer protection, and corporate governance. Among others, the Act establishes a 'bounty program' for whistleblowers who raise concerns with the US Securities & Exchange Commission (SEC). The SEC has adopted a final rule to implement the Act's whistleblower award provisions, permitting individuals who provide the SEC with high-quality tips that lead to successful enforcement actions to receive a portion of the SEC's monetary sanctions while attempting to discourage them from side-stepping their company's internal reporting systems.

To be considered for an award, a whistleblower must voluntarily provide the SEC with original information that leads to the SEC's successful enforcement action with monetary sanctions greater than $1 million. An individual whistleblower may be eligible for an award of 10 percent to 30 percent of the monetary sanctions. The final rule, with some exceptions, excludes from eligibility original information obtained by a person with legal, compliance, audit, supervisory, or governance responsibilities for an entity, such as an officer, director, or partner, if the information was communicated to the whistleblower through the company's internal compliance mechanisms, and information

gained by an independent public accountant through the performance of an engagement that is required under the securities laws.

The final rule does not necessarily render a whistleblower ineligible to receive an award if the whistleblower engaged in the same fraud or misconduct that he or she is reporting. Instead, the SEC will consider the nature and severity of the misconduct to determine if the whistleblower may collect an award. The SEC responded to concerns that its whistleblower award program, as originally proposed, might negatively affect a company's internal ethics and compliance processes by providing incentives for a whistleblower to participate in a company's internal compliance and reporting system. However, the rule does not require a whistleblower to report violations of securities laws internally to qualify for an award under the SEC's program.

In determining the amount of an award, voluntary participation in a corporate internal compliance and reporting system may increase the reward while interference with a corporate internal reporting program may reduce the reward. Moreover, the final rule provides that if a whistleblower reports information through the employer's internal compliance and reporting system, and the company subsequently self-reports to the SEC, the whistleblower is credited with the report and is eligible for any resulting award.

Department of Justice Prosecution Policy

In August 2008, the Department of Justice amended its guidelines related to the federal prosecution of business organisations in cases involving corporate wrongdoing. While the guidance states that a compliance program does not absolve a corporation from criminal liability, it does provide factors that prosecutors should consider in determining whether to charge an organisation or only its employees and agents with a crime. These factors include evaluating whether:

- the compliance program is merely a 'paper program' or has been designed and implemented in an effective manner
- corporate management is enforcing the program or tacitly encouraging or pressuring employees to engage in misconduct to achieve business objectives
- the corporation has provided for staff sufficient to audit and evaluate the results of the corporation's compliance efforts
- the corporation's employees are informed about the compliance program and are convinced of the corporation's commitment to it.

Director and Officer Liability

An influential Delaware court broke ground in 1996 with its ***In re Caremark Int'l Inc. Derivative Lit***. decision. The ***Caremark*** case was a derivative shareholder action brought against the board of directors of Caremark International alleging directors breached their fiduciary duties by failing to monitor effectively the conduct of company employees who violated various state and federal laws—which led to the company's plea of guilty to criminal charges and payment of substantial criminal and civil fines.

The court 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. The Caremark case pointed out that the compliance program should provide "timely, accurate information sufficient to allow management and the board, each within its scope, to reach informed judgments concerning both the corporation's compliance with laws and its business performance." It also made clear that a director's fiduciary duty goes beyond ensuring that a compliance program exists, but also that "[t]he director's obligation [also] includes a duty to attempt in good faith to assure that [the compliance program] is adequate…."

Ten years later, the Delaware Supreme Court affirmed the ***Caremark*** standard for director duty in ***Stone v. Ritter***, 911 A.2d 362 (Del. 2006), opining that "Caremark articulates the necessary conditions for assessing director oversight liability" and that the standard is whether there is a "sustained or systematic failure of the board to exercise oversight—such as an utter failure to attempt to assure a reasonable [compliance program] exists…."

Appendix
Selected case studies

Governance, organisational culture, and effective whistle-blowing

The misconduct of one employee can nearly bring an organisation to its knees. This is particularly true when the conduct occurs in an environment where there exists an institutional fear of speaking up and a fundamental lack of oversight – or rather, persistent oversight – at the management and board levels. Such was the case at one of the leading organisations in the United States, where the egregious actions of one employee made headline news, rocked the organisation and resulted in severe consequences.

An independent investigation confirmed that certain employees knew of the offending employee's misconduct, failed to respond appropriately and attempted to cover up the matter. The investigation also determined that governance and oversight at the organisation was seemingly splintered, with different departments operating essentially independently, and that the board was not persistent enough in its inquiries into the matter. Furthermore, certain low-level employees who first-hand knowledge of the misconduct were afraid to come forward with their concerns, for fear of losing their jobs.

When woven together, these facts and circumstances created a perfect storm, amounting to one of the most serious ethical collapses in recent times. And the aftermath has been devastating: senior-level leaders have been terminated, the organisation has been hit with severe fines and penalties, a series of lawsuits have been filed, and the organisation is suffering from extensive reputational and brand damage.

While an effective governance and compliance program might not have prevented this misconduct from happening (no compliance program carries a 100 percent guarantee that fraud and misconduct will not occur), it would have created an environment where employees who witnessed the misconduct were comfortable coming forward, anonymously if they wished, and without fear of retaliation. Additionally, senior leaders and the board would have been expected to demonstrate a firm commitment to ethics and integrity by addressing the allegations of misconduct persistently, swiftly, and decisively.

This white paper set forth leading practices related to organisational governance, ethical cultures, and effective whistle-blowing programs. Specifically, this white paper identifies a variety of controls that organisations should

consider with regard to preventing, detecting, and responding to instances of misconduct, including:

- designing a comprehensive risk assessment program
- ensuring the appropriate level of board and management oversight
- developing policies and procedures that address top risk areas
- integrating various areas of compliance into an organisation-wide compliance program
- instituting training and communications initiatives
- auditing and monitoring compliance activities and
- providing systems and mechanisms through which employees may ask questions and raise concerns, anonymously if they wish – without fear of retaliation.

Effective anti-bribery and anti-corruption programs

There is a not-so-fine line between an effective anti-bribery and anti-corruption program and one that reads well on paper. Walking the talk, as they say, is what really matters.

As confirmed by an internal investigation and also by investigations undertaken by the Department of Justice and the Security and Exchange Commission, a global organisation made improper payments to foreign government officials— directly or indirectly through third party consultants— in order to gain an unfair competitive advantage. Such payments are in violation of the US Foreign Corrupt Practices Act.

As a result of the investigations, the organisation's revenue, profits and stock value fell dramatically. The organisation has since spent hundreds of millions in professional fees. It is faced with a class action lawsuit brought by shareholders and has suffered significant reputational damage. The organisation also underwent massive change at the executive team level.

During the time period when the bribes took place, the organisation had in place a code of conduct, which included an endorsement from the CEO and a section related to anti-bribery and anti-corruption. However, the organisation did not have in place effective procedures, training, or monitoring protocols to help ensure that its employees and third-party consultants were, in practice, living up to the letter and spirit of the code.

Effective compliance and ethics programs are composed of a wide variety of controls intended to prevent, detect, and respond appropriately to misconduct. Code and policy requirements come to life through effective employee and third-party training, monitoring, and auditing. Organisations are expected not only to establish rules and guidelines for employees related to anti-bribery and anti-corruption, but also to empower employees and third parties to make the right business decisions – and to confirm compliance with policy requirements by conducting audits and monitoring the program. Organisations are also expected to take steps to ensure that the third parties with which they conduct business are not conducting business illegally or unethically.

Effective antifraud program

A well designed and embedded antifraud program can not only result in reducing fraud and therefore its negative impact on the organisations bottom line, but can also help reduce or negate potential regulatory sanction.

A financial institution had developed and embedded a comprehensive antifraud program. The program included governance arrangements, fraud risk assessment on products and services, including on proposed new products prior to release, an entity wide fraud awareness program, guidance, and monitoring arrangements.

Sometime later, the institution had suffered an alleged regulatory breach with resulted in the regulator requesting the institution to have an external firm assess whether the organisation had effective compliance programs, which included assessing the appropriateness of the institutions antifraud program.

The review found that the institution did in fact have in place a robust antifraud program. As a result the regulator on that particular issue did not take any action against the firm, being satisfied that the antifraud program was appropriate.

Key Contacts

Australia

David Luijerink
Partner
+61 2 9455 9533
dluijerink@kpmg.com.au

China

Mark Bowra
Partner
+86 21 2212 3883
mark.bowra@kpmg.com

Hong Kong

Katy Wong
Partner
+852 2140 2388
katy.wong@kpmg.com

Japan

Toshifumi Takaoka
Partner
+81 3 5218 6725
toshifumi.takaoka@jp.kpmg.com

Korea

Hee Jun Kim
Director
+82 2 2112 0878
heejunkim@kr.kpmg.com

Malaysia

Ruban Murugesan
Executive Director
+60 3 7721 3388
rmurugesan@kpmg.com.my

New Zealand

Stephen Bell
Partner
+64 9 367 5834
stephencbell@kpmg.co.nz

Singapore

Bob Yap
Partner
byap@kpmg.com.sg
+65 6213 2677

Thailand

Douglas Webb
Executive Director
+66 2677 2766
douglas@kpmg.co.th

kpmg.com/cn

Publication date: May 2014