KPMG FORENSIC℠

Fraud Risk Management

Developing a strategy for prevention, detection, and response

kpmg.com
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>1</td>
</tr>
<tr>
<td>Executive summary</td>
<td>3</td>
</tr>
<tr>
<td>Defining fraud and misconduct</td>
<td>5</td>
</tr>
<tr>
<td>Convergence of regulatory challenges</td>
<td>7</td>
</tr>
<tr>
<td>The key objectives: prevention, detection, and response</td>
<td>9</td>
</tr>
<tr>
<td>Prevention</td>
<td>11</td>
</tr>
<tr>
<td>Detection</td>
<td>17</td>
</tr>
<tr>
<td>Response</td>
<td>21</td>
</tr>
<tr>
<td>An ongoing process</td>
<td>25</td>
</tr>
<tr>
<td>Conclusion</td>
<td>27</td>
</tr>
<tr>
<td><strong>Appendix</strong></td>
<td></td>
</tr>
<tr>
<td>Selected international governance, risk, prevention, and compliance criteria</td>
<td>29</td>
</tr>
<tr>
<td>Selected case studies</td>
<td>35</td>
</tr>
</tbody>
</table>
Corporate fraud and misconduct remain a constant threat to public trust and confidence in the capital markets. As organizations 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 on the following:

- 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
- 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
- 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 organizations 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 leading organizations have found to be effective.
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 organizations have generally found to be effective when building their compliance programs and related antifraud programs and controls. It also offers strategic insights for aligning organizational values with performance.

The business imperative

As organizations do their best to achieve compliance with new laws and regulations, their agenda for doing so increasingly centers 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
- 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 organizations 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, the Public Interest Disclosure Bill and the Anti-Money Laundering and Counter Terrorism Act.
- **Canada**: The Canadian Criminal Code
- **China**: Eighth Amendment of the PRC Criminal Law.
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 companies 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 whistle-blower mechanisms are in place and supported by management
- Create a detailed ethics and compliance program that manages and integrates fraud prevention, detection, and response efforts.

An ongoing process

Effective fraud risk management provides organizations 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 organizational needs based upon the nature of fraud and misconduct risks and existing antifraud programs and controls
- **Design** of programs and controls in a manner consistent with legal and regulatory criteria as well as industry practices that companies 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 or against an organization, this definition may not fit as well since it is often difficult or impossible to measure the loss inflicted or gain achieved. As such, and for the purposes of this paper, fraud is defined as an intentional deception that drains value from an organization.

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 a company’s 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, market rigging, or conflicts of interest).

Aggressive enforcement by the Criminal Division provides one set of incentives for corporations. Others are sprouting up each and every day, and they are coming from all corners as anti-fraud and corruption enforcement catches up with the globalization of business.

Lanny Breuer
Former Assistant Attorney General,
United States Justice Department, Criminal Division
Compliance Week conference, May 26, 2010
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 29.

Figure 1: Timeline of global regulations, frameworks, and events
As mentioned previously, 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 taking appropriate corrective action to remedy the harm caused by integrity breakdowns.

Putting it all together

The challenge for companies is to adopt a comprehensive and integrated approach that takes 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 organization (see Figure 2). When this categorization is complete, the organization has the information it needs to create a comprehensive program in which the elements of prevention, detection, and response can be integrated and managed.

Figure 2: Selected International Standards

<table>
<thead>
<tr>
<th>Jurisdiction</th>
<th>Framework</th>
<th>Relevance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>AS 8001-2008 Fraud and Corruption</td>
<td>Provides a suggested approach to controlling the risk of fraud and corruption and is intended to apply to all entities</td>
</tr>
<tr>
<td>Netherlands</td>
<td>Corporate Governance Code of Conduct 2004</td>
<td>Seeks to improve transparency in shareholder and management relations as well as the structure and accountability of management in the Netherlands</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>The Companies Act 2004</td>
<td>Aims to improve the reliability of financial reporting and the independence of auditors and auditor regulation</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>Anti-Bribery Act</td>
<td>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</td>
</tr>
<tr>
<td>United States</td>
<td>Federal Sentencing Guidelines</td>
<td>Provides minimum criteria for ethics and compliance programs to prevent and detect violations of law</td>
</tr>
<tr>
<td>United States</td>
<td>Dodd-Frank Act</td>
<td>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</td>
</tr>
<tr>
<td>United States</td>
<td>Sarbanes-Oxley Act</td>
<td>Introduced substantial changes to the corporate governance and financial disclosure requirements of publicly listed companies</td>
</tr>
</tbody>
</table>

Source: KPMG LLP (U.S.) 2013.
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**

<table>
<thead>
<tr>
<th>Prevention</th>
<th>Detection</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Fraud and misconduct risk assessment</td>
<td>• Hotlines and whistle-blower</td>
<td>• Internal investigation protocols</td>
</tr>
<tr>
<td>• Code of conduct and related standards</td>
<td>• Auditing and monitoring</td>
<td>• Enforcement and accountability protocols</td>
</tr>
<tr>
<td>• Employee and third-party due diligence</td>
<td>• Retrospective forensic data analysis</td>
<td>• Disclosure protocols</td>
</tr>
<tr>
<td>• Communication and training</td>
<td>• Process-specific fraud risk controls</td>
<td>• Remedial action protocols</td>
</tr>
<tr>
<td>• Proactive forensic data analysis</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Board/audit committee oversight
Executive and line management functions
Internal audit, compliance, and monitoring functions

Source: KPMG LLP (U.S.) 2013.

The next section spotlights some of the common control elements identified in Figure 3, and offers considerations for their design.
Preventive controls are designed to help reduce the risk of fraud and misconduct from occurring in the first place.

**Leadership and governance**

**Board/audit committee oversight**

An organization’s board of directors plays 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 organization.

Directors have not only a fiduciary duty to ensure that the organization has programs and controls in place to address the risk of misconduct but also a duty to ensure that such controls are effective.¹

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 organization’s antifraud programs and controls
- Establishing procedures for the receipt and treatment of questions or concerns regarding questionable accounting or auditing matters.²

**Senior management oversight**

To help ensure that organizational controls remain effective and in line with regulatory and evaluative criteria, responsibility for an organization’s fraud and misconduct risk management approach should be shared at senior levels (i.e., individuals with substantial control or a substantial role in policy-making). 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 organization and playing a crucial role in fostering a culture of high ethics and integrity. The chief executive should lead by example, allocating organizational 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 organization’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 organization, often a chief compliance officer. In many organizations, the chief compliance 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. The chief compliance officer works together with compliance program staff and designated subject matter specialists from relevant functions (e.g., legal, human resources, internal audit, etc.) and coordinates the organization’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.

---

² 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), which may be found at [http://taft.law.uc.edu/CCL/34ActRls/rule10A-03.html](http://taft.law.uc.edu/CCL/34ActRls/rule10A-03.html).
The chief compliance officer may also chair a committee of cross-functional managers who, among other activities:

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

Other organization leaders, such as department heads, should also have responsibilities for implementing the organization’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 officer within their particular areas of expertise or responsibility.

**Internal audit function**

An organization’s internal audit function is a key participant in antifraud activities, supporting management’s approach to preventing, detecting, and responding to fraud and misconduct. 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 organization’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
- Reporting to the audit committee on internal control assessments, audits, investigations, and related activities.

**The organizational imperative of managing the risk of fraud and misconduct**

Successful organizations consider effective fraud risk management efforts not merely as a cost center that drags on the bottom line, but rather as a driver of organizational growth. Executives of such organizations 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. Organizations 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

Organizations typically face a variety of fraud and misconduct risks. Like a more conventional entity-wide risk assessment, a fraud and misconduct risk assessment helps management understand the risks that are unique to the organization'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 organization, 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 organizational 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

1. Identify business units, locations, or processes to assess
2. Inventory and categorize fraud and misconduct risks
3. Rate risks based on the likelihood and significance of occurrence
4. Remedy risks through control optimization

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 organization’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.

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 organizations and their stakeholders.³

Percentage of U.S. 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

59%

Code of conduct

An organization’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 organization’s overall control culture, raising awareness of management’s commitment to integrity and the resources available to help employees achieve compliance and integrity goals.⁴

A well-designed code of conduct typically includes the following attributes, among others:

- High-level endorsement from the organization’s leadership, underscoring a commitment to ethics and integrity

⁴ Both the NYSE and the NASDAQ have adopted corporate governance rules that require U.S. listed companies to adopt and disclose codes of conduct for directors, officers, and employees, and disclose any code waivers for directors or executive officers. NYSE Listed Company Manual Section 303A.10 may be found at http://www.nyse.com/pdfs/FINAL_FAQ_NYSE%20Listed%20Company%20Manual%20Section%20303A__updated_1_4_10.pdf, and NASDAQ Marketplace Rule 5610 may be found at http://nasdaq.cchwallstreet.com/NASDAQTools/PlatformViewer.asp?selectednode=chap%5F1%5F1%5F4%5F2&manual=%2Fnasdaq%2Fmain%2Fnasdaq%2Dequityrules%2F.
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 organization’s identified risks, the individual’s job function and level of authority and the specific laws of the jurisdiction in which the organization or the employee resides.\(^5\)

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

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 behavioral considerations (such as adherence to the organization’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.

---

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 organizations 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
- Regular and frequent, covering the relevant employee population.

59% Percentage of U.S. 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

76% Percentage of U.S. employees who reported that they feel comfortable reporting misconduct to their supervisor.

KPMG Forensic Integrity Survey 2013
Detected controls are designed to uncover fraud and misconduct when it occurs.

**Mechanisms for seeking advice and reporting misconduct**

Organizations have a better chance of detecting fraud and misconduct early when they have built a culture where employees believe they have a stake in the company and 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, organizations 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 organizations offer employees telephone or Web-based “hotlines” that can be used at any time, research suggests that they are usually 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
- Communicate concerns about potential fraud and misconduct, including questionable accounting or auditing matters.

A well-designed hotline typically includes the following features:

- **Anonymity**: The organization’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 organization 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 nonretaliation**: The organization’s policies prohibit retaliation against employees who, in good faith, seek advice or report misconduct. The organization requires a follow-up with employees periodically after the hotline case has been closed (e.g., at one-, three-, and six-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.
- **Organization-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). Thus, hotline operators need to be appropriately qualified, trained, and, in some situations, authorized to provide advice.

<table>
<thead>
<tr>
<th>59%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Percentage of U.S. employees who reported that they believed they would be protected from retaliation after reporting misconduct.</td>
</tr>
</tbody>
</table>

KPMG Forensic Integrity Survey 2013

---

6 Typically, outsourced, third-party hotline vendors only direct questions or concerns to their client organization’s compliance, audit, or legal function for handling, and do not attempt to provide callers with guidance in response to specific questions.
• **Data management procedures:** The organization uses consistent protocols to gather relevant facts, manage and analyze hotline calls, and report key performance indicators to management and the board. This is often accomplished, for example, by using a computerized, back-end case management system to store, organize, prioritize, 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 U.S. Sarbanes-Oxley Act of 2002).

• **Prominent communications:** The organization publicizes its hotline prominently. Such communications may include, among others: (i) describing the hotline within the code of conduct, in key company 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 organization values hotline calls and is able to provide assistance to those who use the hotline.

### Auditing and monitoring

Auditing and monitoring systems are important tools that management can use to determine whether or not the organization’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.

---

73% Percentage of U.S. employees who reported that their organization audits and monitors employee compliance with the code of conduct either formally or informally.

**KPMG Forensic Integrity Survey 2013**

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, 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 organizational change
- Laws and regulations have changed significantly
- Governmental agencies are stepping-up or targeting enforcement actions.

---

7 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/CCLSOact/sec301.html](http://taft.law.uc.edu/CCLSOact/sec301.html).

An organization’s managers involved in auditing and monitoring efforts should not only have sufficient training and experience but also be seen as objective in evaluating the controls for which they are responsible. Optimally, auditing and monitoring 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 organization is appropriately understood and mitigated
- 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 organizational, employee, and third-party fraud and misconduct. To unlock these insights, organizations 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 behavior-based routines to ferret out irregularities in manual journal entries, locate ghost employees in payroll records, or find nonexistent vendors in accounts payable.

More sophisticated predictive analytic tools employ an array of statistical techniques and modeling to analyze 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 modeling 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 on page 20 that profile a company’s travel and entertainment expenses by sales representative to help identify FCPA risk 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 organizations 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 disparate 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, e-mails, 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

FCPA: Dashboard of Sales Rep Expenses
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 organization’s audit committee, or a special committee of the board, either of which must comprise independent directors who are able to ward off undue pressure or interference from management
- Direction by outside counsel, selected by the audit committee, with little or no ties to the entity’s management team, and that can perform an unbiased, independent, and qualified investigation
- Activities undertaken by investigators who understand the legal dimensions of the matter at hand, as well as the necessary investigatory skills
- Briefing the organization’s external auditor so that the latter can consider the proposed scope of work in the audit of the organization’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
- 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 organization may decide to use one or more of the above steps. Management would consult with the appropriate oversight functions and internal protocols to determine the steps that best address the allegation.

---

**55%**

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

*KPMG Forensic Integrity Survey 2013*
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 organization considers managing fraud and misconduct risk a top priority. Appropriate discipline is also a requirement under leading regulatory and evaluative frameworks.

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

Corrective action
Once fraud and misconduct have 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)
- Remediating 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
- Communicating to the wider employee population that management took appropriate, responsive action.

Although public disclosure of fraud and misconduct may be embarrassing to an organization, management may nonetheless wish to consider such an action in order to combat or preempt negative publicity, demonstrate good faith and assist in putting the matter to rest.
To charge or not to charge?

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

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

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

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

- **Assessment**: Assessing the needs of the organization 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 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 organization 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 organizations have the same risk profile and as such, antifraud measures should be tailored to the unique risks of the organization, 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 organization’s fraud and misconduct risks and determine how effectively it manages these risks. The scope of this analysis should take into consideration the organization’s key business units, processes, systems, and controls, as well as other relevant factors. The organization can also identify key stakeholders who may need to be involved. Once the organization profiles its current state and sets targets for improvements, it can 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 organization 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 organization’s unique business environment. When designing controls, management should endeavor 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 organizations 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 will have individualized control considerations. Management would be well served to consider the organization’s specific 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 organization’s distinct business needs.

### Implementation

Once controls have been designed, management should establish a strategy and process for implementing the new controls throughout the organization and assign to a senior individual responsibility and resources for leading the overall effort. Meaningful and consistent implementation typically requires a substantial change in workplace culture and practices. Therefore, 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 organization's risk management objective is not being met. In the absence of a specific control, other compensating controls may be operating effectively and mitigating the risk of fraud and misconduct.

When evaluating the design effectiveness of a control, management should take into account both regulatory requirements as well as leading practices that similarly situated organizations 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 organization's whistle-blower 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 organization's particular situation should be taken into account in conducting an effectiveness evaluation, and such an inquiry should remain ongoing. Management should continuously consider how its risk strategy and control effectiveness are affected by changes in market expectations, external scrutiny, and regulatory or legislative developments.
Conclusion

Faced with an increasing array of rules and standards governing business conduct, many organizations continue to struggle with how to mitigate the innumerable risks posed by fraud and misconduct. The development of a detailed fraud risk management program is an important step in managing this challenge.

Organizations undertaking this effort should begin by assessing how well they are managing the risks of fraud and misconduct. Identifying and prioritizing known risks and existing controls is an important first step. Subsequently, the organization can determine its ideal future state, perform a gap analysis, and prioritize 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 organization align its corporate values and performance and protect its many assets, driving organizational growth and helping to minimize risks.
Appendix
Selected international governance, risk, and compliance criteria

**Australia**

**Commonwealth Criminal Code Act (1995)**
Boards have a responsibility to foster a culture of compliance with Australian law. Under the Criminal Code, a company can be convicted of Commonwealth criminal offenses if it is established that the company had a culture that directed or encouraged, tolerated, or led to noncompliance, or that the body failed to maintain a culture that required compliance with relevant legislation. (Schedule, Part 2.5, Division 12)

**Corporations Act 2001 (including CLERP 9 Amendments)**
Directors must exercise their powers and discharge their duties with care and diligence. (Section 180) CEO and CFO of a listed entity must make a declaration that:
- An entity’s financial records must be properly maintained in accordance with the Act
- Financial statements for the financial year must comply with the accounting standards
- Financial statements must present a true and fair view of the financial position and performance of the entity. (Section 295A)

**AUS 210 (2002)**
Establishes a requirement for auditors to consider fraud and error in an audit of a financial report.

**Australian Stock Exchange Guidance Note 9A (2003)**
Requires the board or appropriate board committee to establish policies on risk oversight and management (Principle 7).

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

**Criminal Code Amendment (Bribery of Foreign Public Officials) Act**
This law makes it an offense in Australia for a person to provide, offer, or promise 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 advantage, not legitimately due to the recipient.
Public Interest Disclosure Bill (2013)
This legislation, which has passed both houses of parliament and is awaiting royal assent, is the first Australian federal government stand-alone whistle-blower protection scheme and provides protection for public sector whistle-blowers in Australia who report wrongdoing. It requires all federal agencies and entities to report disclosures made by public officials to the Commonwealth Ombudsman or Inspector-General of Intelligence & Security.

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 Act (AML/CTF Act) 2006
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).

European Union
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.

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

- Fight against money laundering
- Compel the financial sector, including credit institutions, to take various measures to establish customers’ identities
- Urge the financial sector to keep appropriate records
- Establish internal procedures to train staff to report suspicions to the authorities and to set up preventive systems within their organizations.

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

The European Commission Anti-Fraud Strategy (CAFS) (24/06/2011)
The 2011 CAFS is binding on the Commission and its executive agencies, and updates and replaces the anti-fraud 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
- Deter future fraud through appropriate penalties.

The strategy sets out various methods by which anti-fraud measures will be driven out, together with the support of European Anti-Fraud Office (OLAF). These methods include:

- The introduction of specific anti-fraud strategies per sector in the Commission
- 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.
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
- "Fraud by abuse of position," defined as where a person who occupies a position in which he or she is 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 United Kingdom 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 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 years
- 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 organizations 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
- The failure of a commercial organization to prevent bribery on its behalf, unless the commercial organization 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 Organizations (COSO). Generally speaking, the COSO framework addresses compliance program elements in entity-wide components that have a pervasive influence on organizational behavior, 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
- 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 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.

U.S. Federal Sentencing Guidelines for Organizational Defendants

The federal sentencing guidelines for organizational defendants (first adopted in 1991) establish minimum compliance and ethics program requirements for organizations seeking to mitigate penalties for corporate crimes. Amended in 2004 and again on 2010, these guidelines make it explicit that organizations 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 organizations to:

- Promote a culture that encourages ethical conduct and a commitment to compliance with the law
- Establish standards and procedures to prevent and detect criminal conduct
- Ensure the board of directors and senior executives are knowledgeable and exercise reasonable oversight over the compliance and ethics program
- Assign a high-level individual within the organization to ensure the organization has an effective compliance and ethics program, and delegate day-to-day operational responsibility to individuals with adequate resources 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
- Publicize a system, which may include mechanisms for anonymity and confidentiality, under which the organization’s employees and agents may report or seek guidance regarding potential or actual misconduct without fear of retaliation
Selected international governance, risk, and compliance criteria (continued)

- Evaluate periodically the effectiveness of the compliance and ethics program
- Promote and enforce the compliance and ethics program consistently through incentives and disciplinary measures
- 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 (the Act) was enacted to ensure stability in the U.S. financial markets, affecting all U.S. financial institutions, many non-U.S. 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 whistle-blowers who raise concerns with the U.S. Securities & Exchange Commission (SEC). The SEC has adopted a final rule to implement the Act’s whistle-blower 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 whistle-blower 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 whistle-blower 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 whistle-blower 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 whistle-blower ineligible to receive an award if the whistle-blower 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 whistle-blower may collect an award. The SEC responded to concerns that its whistle-blower award program, as originally proposed, might negatively affect a company’s internal ethics and compliance processes by providing incentives for a whistle-blower to participate in a company’s internal compliance and reporting system. However, the rule does not require a whistle-blower 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 whistle-blower reports information through the employer’s internal compliance and reporting system, and the company subsequently self-reports to the SEC, the whistle-blower 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 organizations 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 organization 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 a 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, organizational culture, and effective whistle-blowing**

The misconduct of one employee can nearly bring an organization 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 organizations in the United States, where the egregious actions of one employee made headline news, rocked the organization, 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 organization 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 had firsthand 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 for one of the most serious ethical collapses in recent times. And the aftermath has been devastating: senior-level leaders have been terminated, the organization has been hit with severe fines and penalties, a series of lawsuits have been filed, and the organization 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 organizational governance, ethical cultures, and effective whistle-blowing programs. Specifically, this white paper identifies a variety of controls that organizations 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 organization-wide compliance program
- Instituting training and communications initiatives
- Auditing and monitoring compliance activities
- Providing systems and mechanisms through which employees may ask questions and raise concerns, anonymously if they wish, without fear of retaliation.

Effective antibribery and anticorruption programs

There is a not-so-fine line between an effective antibribery 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 organization 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 U.S. Foreign Corrupt Practices Act.

As a result of the investigations, the organization’s revenue, profits, and stock value fell dramatically. The organization 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 organization also underwent massive change at the executive team level.

During the time period when the bribes took place, the organization had in place a code of conduct, which included an endorsement from the CEO and a section related to antibribery and anticorruption. However, the organization 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. Organizations are expected not only to establish rules and guidelines for employees related to antibribery and anticorruption, 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. Organizations are also expected to take steps to ensure that the third parties with which they conduct business are not conducting business illegally or unethically.
Contact us

Richard H. Girgenti
National Practice Leader
KPMG Forensic
KPMG LLP in the United States
212-872-6953
rgirgenti@kpmg.com

Tim Hedley
Partner and Global Lead
Fraud Risk Management Services
KPMG LLP in the United States
212-872-3496
thedley@kpmg.com

kpmg.com