

# Predicting the unpredictable\*

Protecting Transportation & Logistics companies against fraud, reputation and misconduct risk



\*connectedthinking

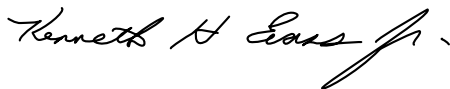


## Welcome

The potential for corporate fraud and misconduct to easily spread from a small brush fire into a full-blown firestorm has garnered the attention of regulators, with the United States Securities and Exchange Commission, the Public Company Accounting Oversight Board and the Federal Sentencing Commission all having recently addressed this topic. While it may not be possible to eliminate the risk of fraud altogether, a company can at least identify it early and minimize its damage with proper planning, policies and procedures.

This report provides step-by-step guidance on how to develop an effective antifraud program that addresses not only financial statement risk, but also reputation, operational, legal and strategic risks. In addition, it provides a summary of fraud schemes that are common to the transportation & logistics industry.

Fraud management makes good business sense. A company that establishes an effective antifraud program will go a long way toward maintaining or restoring investor confidence in the integrity of its financial results. Equally important, reducing fraud will help a company to lower costs, improve profitability, protect its reputation and mitigate liability. We believe this report is a valuable blueprint to help transportation & logistics companies achieve these goals.



Kenneth H. Evans Jr.  
US Transportation & Logistics Leader



Jonny Frank  
Fraud Risks & Controls Leader

For more information about the services offered by PricewaterhouseCoopers' Global Transportation & Logistics Practice, please visit our website at [www.pwc.com/transport](http://www.pwc.com/transport) or contact one of the regional professionals listed on page 51 of this report.

For more information about our Fraud Risks & Controls practice, please visit our website at [www.internalaudit.com](http://www.internalaudit.com) or contact one of the Fraud Risks & Controls professionals listed on page 52 of this report.



# Table of contents

5	Introduction	22	Operational risk: Protecting the bottom line
6	SEC and Public Company Accounting Oversight Board (PCAOB) require senior management to implement effective antifraud programs and controls	23	Legal risk: Protecting against criminal, regulatory and civil liability
6	Limitations of “Sarbanes” antifraud programs and controls	23	Strategic risk: Protecting the future
7	Recent amendments to United States Sentencing Guidelines require an effective compliance program	23	Leveraging Sarbanes to mitigate other risks at minimal incremental cost
9	Common transportation & logistics sector fraud schemes	24	Five-step plan for leveraging Sarbanes antifraud program
10	Financial statement manipulation	24	Step 1: Hold individual business unit leaders accountable
12	Asset misappropriation	25	Step 2: Balance accountability and responsibility
12	Unauthorized receipts or expenditures	25	Step 3: Expand the scope of the risk assessment
13	Aiding and abetting	25	Step 4: Don’t just look at financial reporting controls
13	Fraud by senior management or employees with significant role in financial reporting	25	Step 5: Consult your independent auditor
13	Disclosure fraud	27	Closing thoughts
15	Five-step antifraud program implementation plan	29	Appendices
16	Step 1: Establish a baseline	30	Appendix A: Antifraud program and controls assessment grid
16	Step 2: Conduct a fraud risk assessment	34	Appendix B: Antifraud program and controls responsibilities matrix
17	Step 3: Evaluate design and validate operating effectiveness	38	Appendix C: Conducting a fraud and reputation risk assessment
18	Step 4: Address residual financial reporting fraud risks	42	Appendix D: Fraud auditing process
18	Step 5: Standardize process for incident investigation and remediation	44	Appendix E: Antifraud program implementation
21	Mitigating reputation, operational and legal risks	45	Appendix F: Comparison of antifraud programs and controls and United States Sentencing Guidelines
21	Sarbanes integrated audit reaches only financial reporting risk		
22	Reputation risk: Protecting your most precious asset		



# Introduction

At the beginning of the 20th century, 146 factory workers died during a fire at the Triangle Waist Company in New York City, some of whom jumped out of windows, plunging to their deaths ten floors below. Termed by one historian as “the fire that changed America,”<sup>1</sup> public outrage prompted elected officials and regulators to enact fire prevention and detection codes, which, until that horrific event, had been successfully blocked by the real estate and manufacturing industries.

Will the scandals that have rocked corporate America over the past few years have a similar historical impact? Will historians dub Enron and WorldCom and the like as the frauds that changed America? Public outrage over corporate fraud has resulted in new legislation, regulations and professional standards, which, like the changes following the Triangle Waist fire, focus on prevention and timely detection. For the first time, corporate fraud is a key agenda item for boards of directors, senior management, and independent auditors.

---

1 D. Drehle, “Triangle: The Fire That Changed America” (Atlantic Monthly Press 2003).

## SEC and PCAOB require senior management to implement effective antifraud programs and controls

Companies subject to the Sarbanes-Oxley Act (Sarbanes)<sup>2</sup> must now implement “antifraud programs and controls.”<sup>3</sup> Seemingly innocuous, this new requirement creates significant new responsibilities for businesses, including the requirements for (1) audit committee oversight, (2) a fraud risk assessment, (3) internal audit activities relative to prevention and detection of fraud, and (4) procedures for handling complaints and the reporting of fraud to the audit committee and independent auditor.<sup>4</sup>

Securities and Exchange Commission (SEC) rules implementing Sarbanes §404 refer explicitly to controls related to the *prevention, identification and detection* of fraud. The regulations require corporate management to evaluate and test the design and operating effectiveness of antifraud controls on an annual basis.<sup>5</sup> Independent auditors evaluate and test the design and operating effectiveness of antifraud controls as a part of the integrated audit.<sup>6</sup> Deficiencies in antifraud programs and controls ordinarily result in a finding of a significant deficiency to the audit committee.<sup>7</sup> The auditor must issue an adverse opinion if it concludes that the deficiencies rise to a material weakness.<sup>8</sup>

This white paper focuses on a strategy for developing and implementing effective antifraud programs and controls within the transportation & logistics sector, beginning with an overview of common transportation & logistics sector fraud schemes. The white paper addresses Sarbanes antifraud programs focused exclusively on financial reporting risk, followed by a discussion of leveraging Sarbanes efforts to address other significant risks implicated by fraud and misconduct, including reputation, operation, legal, compliance and strategic risk.

The appendices provide additional information about Sarbanes antifraud programs. Appendix A summarizes laws, regulations and auditing standards. Appendix B includes a grid that enables companies to benchmark individual antifraud program components. Appendix C depicts the fraud risk assessment processes. Appendix D depicts the process of auditing residual fraud risks. Appendix E provides a one page summary of the entire process.

PricewaterhouseCoopers’ (PwC’s) previous whitepaper, *Key Elements of Antifraud Programs and Controls*, identifies the key elements of an effective antifraud program based on the core principles shared by the new laws, regulations and standards and considers the application of the Committee of Sponsoring Organizations (COSO) of the Treadway Commission, “Internal Control – Integrated Framework to Antifraud Programs and Controls” (COSO-Internal Controls). Another PwC whitepaper, *The Emerging Role of Internal Audit in Mitigating Fraud and Reputation Risk*, considers tactics for implementation of Sarbanes antifraud programs and controls. Copies of both whitepapers can be obtained from PwC’s internalaudit.com website.

## Limitations of “Sarbanes” antifraud programs and controls

Fraud is a broad concept that refers generally to any intentional act committed to secure an unfair or unlawful gain. The SEC and PCAOB requirements focus only on fraud that could have a more than inconsequential or material effect on the company’s financial statements.<sup>9</sup>

Some fraud and misconduct risks have *no* financial statement impact – these risks fall outside the scope of the audit of internal controls over financial reporting. Audit committees, management, shareholders and other stakeholders therefore should not rely upon antifraud programs implemented solely

2 Sarbanes-Oxley Act of 2002, 15 U.S.C. §7201 (2002) (Sarbanes).

3 For an in-depth discussion, see PricewaterhouseCoopers whitepaper *Key Elements of Antifraud Programs and Controls*, available at [www.cfodirect.com/News and Analysis/Corporate Governance/Key Elements of Antifraud Programs and Controls](http://www.cfodirect.com/News and Analysis/Corporate Governance/Key Elements of Antifraud Programs and Controls) (December 2003).

4 Public Company Accounting Oversight Board (PCAOB), “An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements” (hereinafter PCAOB Auditing Standard No. 2) Paragraph 24 (PCAOB Release No. 2004-001, dated March 9, 2004).

5 According to the rule, “Controls subject to such assessment include, but are not limited to controls related to the prevention, identification, and detection of fraud. The nature of a company’s testing activities will largely depend on the circumstances of the company and the significance of the control. However, inquiry alone generally will not provide an adequate basis for management’s assessment.”

6 PCAOB Auditing Standard No. 2 Paragraphs 88-107.

7 PCAOB Auditing Standard No. 2 Paragraph 139.

8 PCAOB Auditing Standard No. 2 Paragraph 175.

9 SEC registrants should note that SEC Staff Accounting Bulletin (SAB) 99, which provides guidance to determine materiality when fraud is discovered, rejects the frequently used rule of thumb that a misstatement or omission that is less than 5 percent of some factor (e.g., net income or net assets) is immaterial. SAB 99 requires that a determination of materiality consider both the “quantitative” and “qualitative” aspects of the particular matter being analyzed. 17 Code of Federal Regulations Part 211, August 12, 1999. The PCAOB has adopted the same approach for the audit of internal controls. PCAOB Auditing Standard No. 2 Paragraphs 22-23.

to meet SEC and PCAOB requirements to address wider-ranging fraud and misconduct risks. Conversely, companies can apply the same approach and framework to design and implement programs and controls to meet all types of fraud and reputation risk.

## Recent amendments to United States Sentencing Guidelines require an effective compliance program

Legal and compliance, for example, illustrate a fraud and misconduct risk that extends beyond Sarbanes. Effective November 1, 2004, the United States Sentencing Commission amended the existing United States Sentencing Guidelines (USSG) to provide greater guidance to organizations and courts regarding the criteria for an effective program to prevent and detect violations of the law. This amendment responds to section 805(a)(2)(5) of the Sarbanes-Oxley Act of 2002, Public Law 107-204, which directed the Commission to review and amend the guidelines and related policy statements to ensure that the guidelines are sufficient to deter and punish organizational criminal misconduct.

The USSG establishes minimum steps for an effective compliance program and provides guidance for their implementation. The November 2004 amendments, among new requirements, mandate entities to assess periodically the risk that violations of law will occur, including an assessment of (1) the nature and seriousness of such violations of the law, (2) the likelihood that certain violations of the law may occur because of the nature of the organization's business, and (3) the prior history of the organization. The entity must then take appropriate steps to reduce the risk of violations of law identified by the risk assessment and ensure that its compliance program is being followed and is working effectively, including using monitoring and auditing systems that are designed to detect violations of the law.

The amended USSG shares many common elements with Sarbanes requirements for antifraud programs and controls. Appendix F cross-references the USSG and Sarbanes elements.



# Common transportation & logistics sector fraud schemes

The integrated audit comprises two portions – an audit of internal controls over financial reporting integrated with the financial statement audit. Auditors consider fraud in both portions.

The internal controls portion of the audit includes three components. First, management must “design and implement programs and controls to prevent, deter, and detect fraud.”<sup>10</sup> Second, management must assess and the auditor must evaluate management’s assessment of the entity’s antifraud programs and controls.<sup>11</sup> Third, the independent auditor must conduct its own assessment and separately evaluate design and validate operating effectiveness of general and specific antifraud programs and controls.<sup>12</sup>

In a separately issued FAQ, the PCAOB has explained that the internal controls portion of the audit reaches fraud risks having a *direct* or *indirect* financial statement impact. Revenue recognition fraud, for example, has a direct financial statement impact. Fines and penalties resulting from fraud or misconduct, e.g., a violation of the Foreign Corrupt Practices Act (FCPA), exemplify an indirect financial statement impact.

Under the financial statement portion of the audit, the auditor designs procedures to provide reasonable assurance that the financial statements are free of material misstatement due to error or fraud. Auditing standards define fraud as comprising fraudulent financial reporting or misappropriation of assets. The financial statement portion of the audit generally addresses only frauds risks having a potential *direct* financial statement impact.

---

10 PCAOB, Auditing Standard No. 2 Paragraph 25.

11 Id. at Paragraph 40.

12 Id. at Paragraph 24.

PwC organizes these fraud and misconduct schemes into six broad categories based on Sarbanes-Oxley PCAOB auditing standards:



Following are a few of the most common schemes impacting the transportation & logistics sector:

## Financial statement manipulation

### Improper revenue recognition

**Timing estimates** refer to the manual adjustments made to the financials to record revenue in accordance with US GAAP. EITF 91-9 states that revenue and direct costs may be recognized when the shipment is completed or revenue can be allocated between reporting periods based on relative transit times in each reporting period with expenses recognized as incurred. In some cases, the company neither knows the exact transit times for each shipment nor the exact date that individual shipments are completed. Because of this, management must use estimates to adjust the amount of revenue recognized. As a result, there is the potential for management to manipulate the estimate to over- or understate the amount of revenue recognized in a period.

**Revenue leakage** occurs when there are discrepancies between the quantity of items shipped, and the quantity of items for which revenue is being recognized. This is a very important issue for the transportation industry because, in many cases, companies ship thousands of items per day. This scheme can also occur when a transportation move involves inter-company handoffs. Where the company's systems do not link the shipping, billing, and revenue recognition functions,

the auditor should ensure that management is performing a reconciliation of the items shipped to the revenue being recognized. In addition, this reconciliation will help ensure that the company is not recognizing revenue multiple times for the same shipment.

**Customer side agreements** frequently occur when an organization enters a written or oral agreement outside the normal reporting channels to boost sales figures. Sales personnel often craft side agreements to obtain undeserved commissions, and management may enter into them to inflate revenue.

**Backdated agreements** refer to posting a date on a document earlier than the actual creation date for purposes of deception, and recognizing a transaction in the wrong financial period.

**Round-tripping** is recording transactions between or among companies for which the transaction provides no economic benefit to any partner. Round tripping, which is most commonly associated with the technology and energy industries, typically occurs to meet analyst expectations regarding gross revenue targets. It can also occur at transportation companies.

**Accounts receivable indicators** are certain trends within accounts receivables which indicate premature revenue recognition. For example, spikes in accounts receivable balances at quarter-end and year-end dates suggest that management may be manually accruing revenues for transportation services before the earning process is complete.

**Holding the books open for extended time after period end to include additional revenues** allows companies to record additional end-of-period revenues that are invoiced and shipped after the end of a reporting period.

**Over-accrual of rebates payable to customers** can occur when a company pays rebates to customers based on the amount of work performed over a certain period of time. Intentionally over-accruing the liabilities during the "good times" allows the company to build up a reserve which can be relieved to recognize additional revenue in later periods.

**Recording fictitious transactions** refers to companies creating fictitious orders for either existing or fictitious customers. False supporting documentation is often created to support the nonexistent sale.

**Reporting revenue based on gross sales** allows the company to overstate its revenue by recording total invoice value of sales, without deducting for customer discounts, allowances, or returns.

**Sham related party transactions** are transactions between related parties which are often difficult to audit, as they are not always accounted for in a manner that communicates their substance and effect with transparency. The possibility of collusion always exists given that the parties are, by definition, related.

### Overstatement of assets/understatement of liabilities

**Improper capitalization of expense** occurs when a company capitalizes items which should be expensed as incurred and, as a result, overstates assets and net income. There is some broad authoritative guidance which provides capitalization standards, but the wide variety and volume of items which are subject to the standards in this industry give rise to the risk of certain items being misclassified.

**Understatement of insurance liabilities** occurs when management intentionally underestimates the anticipated number, and ultimate cost, of accident claims. Due to the nature of the transportation & logistics industry, claim expenses (e.g., property damage, worker's compensation, FELA, health and liability) can be material. By understating the company's exposure to claims, management can understate claim reserves and, consequently, overstate earnings.

**Understatement of environmental liabilities** can occur when management fails to report environment health and safety compliance issues. Compliance errors can lead to failure to detect environmental risks, which can be costly.

**Improper withholding of funds** can also occur when a transportation company acts as a broker to help independent contractors obtain various lines of insurance. If the company accepts insurance premiums from contractors but does not remit the premiums to the insurance company on a timely basis or renew the policies, there is the risk that the company may not have adequate reserves for claims for the periods the contractors are not insured by third parties.

**Overstatement of trade receivables** occurs when an entity overstates its accounts receivable, for example, by the creation of fictitious receivables. In addition, an entity may understate the allowance for doubtful accounts by applying improper estimating techniques, fraudulently changing

receivable dates so that they appear to be more current, or devising other ways to avoid or delay the write-off of receivables that may become uncollectible. In all instances, the net value of accounts receivable is artificially inflated. One area to consider in the transportation industry is the receivable for accessorial charges; management may be including receivables for accessorial charges on its balance sheet which are not valid or collectible.

**Over-accrual of vendor rebates and receivables** can occur when the company receives discounts or rebates from their vendor suppliers based on purchase volumes reaching a certain threshold, or other factors. Fraud occurs if the company intentionally recognizes the vendor allowance or rebate in an amount, or in a period, contrary to that which is acceptable under GAAP.

### Other areas of fraudulent financial reporting

**Improper journal entries** are sometimes the vehicle used by management to account for many different fraud schemes discussed elsewhere, but sometimes, improper journal entries can become a scheme in and of itself. These journal entries might occur during the consolidation process when "top-side" adjustments are made. There have also been instances where management has utilized improper reclassification or elimination entries to manipulate the financial statements. Due to the complexity of most companies today, material misstatements of the financial statements can occur through improper journal entries at the sub-consolidation or even in the subsidiary ledgers.

**Manipulation of significant estimates** is another common area of fraudulent financial reporting. The following list contains examples of significant estimates that may be at risk for transportation sector companies:

- Customer programs and incentives
- Pension and OPEB accounting
- Accounting for taxes
- Valuation of goodwill or long-lived assets
- Restructuring and severance reserves
- Legal/litigation reserves
- Self-insurance reserves

**Improper inter-company or suspense account activity** is not always well controlled. Fraud can occur when management utilizes these inter-company or suspense accounts in order to misstate the financial statements. Common fraud schemes include improper elimination of intercompany profit, inconsistent treatment of transactions between two subsidiaries, or utilization of inter-company transactions to mask deteriorating trends in a particular segment or market.

**Improper accounting for significant unusual transactions** has become an area of focus for the SEC in recent years. The release of FIN 46 is a direct result of the issues arising from improper accounting for transactions such as acquisitions, divestitures, joint venture arrangements, alliance agreements, special purpose entities and other similar transactions. In addition, improper accounting for long term purchase commitments may also lead to fraudulent financial reporting.

## Asset misappropriation

Most asset misappropriation schemes implicate operational risk rather than financial reporting risk. The financial statements are impacted only if the statements erroneously overstate the asset that has been misappropriated. For example, misappropriation of inventory results in a misstatement, only if the financial statements report erroneously the inventory.

**Fraudulent disbursements** comprise a wide range of fraud schemes which result in cash being inappropriately sent from the company to another party. Examples of fraudulent disbursement schemes include payments to ghost employees, fictitious vendors, pay-and-return schemes, over-billing schemes, unauthorized overtime schemes, and expense report schemes. The decentralization of operations in the transportation & logistics industry makes it very susceptible to fraudulent disbursements.

**Cash skimming** probably began shortly after the introduction of currency as a form of payment. Cash skimming is often a result of a lack of segregation of duties in the areas of cash receipt and cash application. Sophisticated schemes include not recording payments received against the customer's account and then writing off receivable balances left unpaid.

**Cargo theft** occurs in a range of freight-forwarding and storage operations, but the greatest risk is during truck and container transportation or when vehicles are in the process of being loaded or unloaded. Cargo theft not only affects the victimized transportation companies and their insurers – the illegal sale of stolen cargo also undercuts prices in legitimate businesses.

**Industrial espionage** illustrates the theft of trade secrets, intellectual property and other soft assets, some of which have recorded financial statement value.

**Lapping** generally involves stealing one customer's payment and then using a subsequent payment, usually from another customer, to cover the payment from the first customer's account. The perpetrator, for example, steals the payment intended for customer A's account. When a payment is received from customer B, the thief credits it to A's account. And when customer C pays, that money is credited to B.

## Unauthorized receipts or expenditures

PCAOB auditing standards refer to unauthorized receipts and expenditures and unauthorized acquisition, disposition or use of assets. Unlike financial statement manipulation, entities and individuals do not perpetrate these fraud schemes with the objective of misstating the financial statements.

These frauds nonetheless impact the financial statements – directly and/or indirectly. Overcharging customers exemplifies an unauthorized receipt having a direct financial statement impact inasmuch as the financial statements recognize income and include assets that should not be recognized by the entity and which will result in a restatement if discovered and material. Bribery illustrates an unauthorized expenditure that typically has an indirect financial statement impact inasmuch as the potential fine, penalty or other sanction could lead to a material misstatement.<sup>13</sup>

**Bribery of government officials (domestic and foreign)** are endemic to all industries and sectors that sell to governments, require regulatory approval, or are subject to customs, inspection, or other government oversight. The size and scope of capital expenditure projects such as airline terminal construction and railroad infrastructure expansion make the

transportation industry particularly susceptible to bribery. In addition, transportation companies often do not have mature Foreign Corrupt Practices Act compliance programs like other sectors, such as defense contracting and health care.

**Commercial bribery**, in the transportation industry, may be as significant of a risk as government bribery as a result of decentralized operations. Commercial bribery can involve any step along the supply and sales chains and take many forms, including kickbacks to procurement departments or vendors, slotting fees, etc.

**Tax evasion** is a classic example of how a company can employ fraud to avoid expenses. Highly taxed regions encourage the company to record revenue in lower tax districts or off-book to engage in sales and income tax fraud.

**Improper labor practices** are another way to avoid expenses by fraud – whether that means failing to pay the minimum wage, not allowing drivers to use mandatory rest periods, or encouraging operators to work more than the legal number of hours per day. It can be argued that these are also internal control issues, as improper labor practices, such as hiring illegal immigrants or pressuring employees to work off the clock, will also have an impact on the company's overall financial statements, and represent an unauthorized expenditure of company assets.

**Fraud against employees** for instance, where the employer fails to make pension fund contributions or insurance premiums, is another illustration of costs and expenses avoided by fraud.

## Aiding and abetting

Aiding and abetting refers to facilitating others to engage in fraud or misconduct. U.S. law treats the facilitator as if it committed the underlying crime.

Prosecutors and regulators, as well as private litigants, over the past several years have placed and continue to place considerable greater emphasis and scrutiny on aiding and abetting liability. Given this trend, entities should consider the possible scenarios under which one of its employees or agents might facilitate a third party entity to violate the law.

## Fraud by senior management or employees with significant role in financial reporting

PCAOB auditing standards provide that fraud of “any magnitude” by senior management should be regarded as “at least a significant deficiency and as a strong indicator of a material weakness.”<sup>14</sup> The PCAOB defines senior management as the principal executive and financial officers signing the company's certifications as required under Section 302 of Sarbanes, as well as any other members of management who play a significant role in the company's financial reporting process.

Fraud risks related to senior management financial misconduct typically relate to conflicts of interest, inappropriate receipt of goods or services from vendors, misuse of corporate assets, or insider trading.

## Disclosure fraud

Disclosure fraud occurs if the entity intentionally omits or misstates material information from public filings – whether they be in the audited financial statements or unaudited filings such as the Management's Discussion & Analysis portion of the 10k. The SEC has placed renewed emphasis on disclosure, including, for example, holding a company liable for disclosure fraud for failing to disclose channel stuffing practices, notwithstanding that the practices conformed to GAAP.



# Five-step antifraud program implementation plan

This section provides an overview for the development and implementation of an antifraud program. A one-page visual representation of this five-step plan is provided in Appendix E at the end of this paper.

## Step 1: Establish a baseline

### Form a project team

At the outset of undertaking an antifraud program, companies will inevitably vary in their approach. There is no single answer. Some companies will assign this task to internal audit, or to a Sarbanes project team. Others develop a separate, multi-disciplinary team drawn from internal audit, compliance, ethics and legal. PwC endorses the multi-disciplinary approach. Whatever the decision is, the formation of a project team (referred to as the “team” within this section of the paper) is a vital component of Step 1.

### Assess existing antifraud programs and controls

Virtually every public transportation & logistics company has some components of an antifraud program in place. Appendix B provides an example of a tool that companies can use to assess their existing antifraud program relative to benchmarks identifying best practices, general compliance, and deficiency levels, based on the new mandates required under Sarbanes and its implementing regulations and auditing standards.

Because the requirement for an antifraud program is new, many public companies need to take supplemental action to avoid significant deficiencies or material weaknesses. The previous PwC whitepaper, *Key Elements of Antifraud Programs and Controls* on the elements of an effective antifraud program describes the areas where many companies will need to take supplemental action to avoid significant deficiencies or material weaknesses.<sup>15</sup>

### Develop a remediation plan

A thorough assessment will identify shortfalls within the plan, which can be addressed in a remediation plan. Appendix B includes a tool for designing a remediation plan and delegating responsibility among the board of directors, management, business unit leaders, and internal audit.

### Communicate with audit committee and independent auditor

Management should establish and maintain solid lines of communication with the audit committee and independent auditor, specifically discussing: (i) the status and scope of the organization’s antifraud controls, and (ii) the remediation plan to cure deficiencies. A bilateral communication will allow

management to understand the expectations of its primary stakeholders and to align its activities to address these expectations. Communication, moreover, is required under Sarbanes §302, if a significant deficiency is discovered.

## Step 2: Conduct a fraud risk assessment

How can management develop antifraud controls without first identifying its fraud risks? Prior to Sarbanes, few companies assessed fraud risk on a comprehensive and recurring basis, rather than in an informal or haphazard manner.

A fraud risk assessment process, performed independently or integrated with the enterprise risk assessment process, is a cornerstone of an antifraud program that anticipates, rather than reacts to, fraud and misconduct. An effective fraud risk assessment may identify previously unidentified risks and strengthen the ability of the organization to prevent and detect fraud and misconduct before they become a headline-grabbing corporate embarrassment.

Fraud risk assessment expands upon traditional risk assessment. It can be scheme and scenario-based rather than based on control risk or inherent risk. The assessment considers the various ways that fraud and misconduct can occur by and against the company. Fraud risk assessment also considers vulnerability to management override and potential schemes to circumvent existing control activities, which may require additional compensating control activities. The focus is on how fraud can be perpetrated and then concealed.

### Develop an inventory of fraud risks

Developing an inventory of a fraud risks is a pessimist’s utopia, as the team seeks to envision any and all incidents that might negatively impact the company. PwC recommends that this step focus on inherent fraud risks, that is, without regard to existing controls or probability of occurrence. Sample techniques include:

- Industry research
- Existing event inventories
- Brainstorming
- Focus groups
- Web-based and other surveys
- Process flow analysis
- Field interviews and focus groups

<sup>15</sup> Areas most likely requiring attention include (i) developing a systematic fraud risk assessment process, (ii) implementing a standardized process to track, investigate and remediate allegations or suspicions of fraud, (iii) linking control activities to identified risks, (iv) testing design and operating effectiveness, and (v) auditing and monitoring for fraud.

Some entities, hoping to save time and costs, limit event identification inquiries to senior management. PwC urges management to resist this temptation and to expand the assessment to include a broad range of sources – lower level employees who understand the inner workings of the company and business almost always serve as an invaluable, yet often ignored, information source.

### Assess likelihood

Transportation & logistics companies that have undergone either a Sarbanes review or enterprise-wide risk assessment will be familiar with assessing likelihood of occurrence. For the purposes of this evaluation, likelihood should be considered without regard to controls. PCAOB auditing standards refer to three levels of likelihood:

- Remote (likelihood of event occurring is slight)
- More than remote (likelihood of event occurring is reasonably possible, but less than likely)
- Probable (event is likely to occur)

Predicting likelihood of fraud is even more risky than the local television weatherman predicting fair skies on a holiday weekend. Just as the weatherman is blamed when it rains, so too will the team be blamed, if a risk categorized as “remote”, actually occurs. And the consequences will likely be worse than a group of angry television viewers.

The team must dig into the factors and circumstances that would give rise to the impacting event. Does, for example, the potential event involve intentional conduct? If so, query whether any incentives or pressures exist that would motivate the intentional conduct. Absent a motivation, it is unlikely that the event would occur.

### Gauge potential significance and financial statement impact

The Fraud Risk Assessment must also consider the significance of the fraud risks to the financial statements:

- Inconsequential
- More than inconsequential
- Material

Preventability is essential. If the event is perceived to be preventable, the potential harm to the entity is much greater. Risk events that are perceived by stakeholders to be preventable are events within the control of the organization.

Next, if preventable, consider whether the stakeholder will perceive the event as a systemic flaw or as an isolated occurrence. All other things being equal, the impact of a systemic flaw will be much harsher. The organization’s response will also be critical. A perceived ineffective response aggravates the harm to reputation. An effective response conversely may not only preserve the company’s reputation, but may also enhance it.

Attempting to measure the significance of an event (and management’s response) that has not yet occurred is both difficult and risky. Importance varies by stakeholder and is highly fact specific. Beware therefore of too hastily dismissing a potential event as being clearly inconsequential. Additional guidance about the fraud risk process appears in a separate PwC whitepaper, *The Emerging Role of Internal Audit in Mitigating Fraud and Reputation Risks*.<sup>16</sup>

### Step 3: Evaluate design and validate operating effectiveness

Evaluation of control activities intended to prevent or detect fraud includes two components: design effectiveness and operating effectiveness. Evaluating design effectiveness, which is often overlooked, considers whether, if the identified controls operate as designed, the fraud risk will be adequately mitigated. Evaluating design effectiveness often requires input from a fraud subject matter expert knowledgeable of the ways that a fraudster will seek to collude, override or otherwise circumvent fraud control activities.

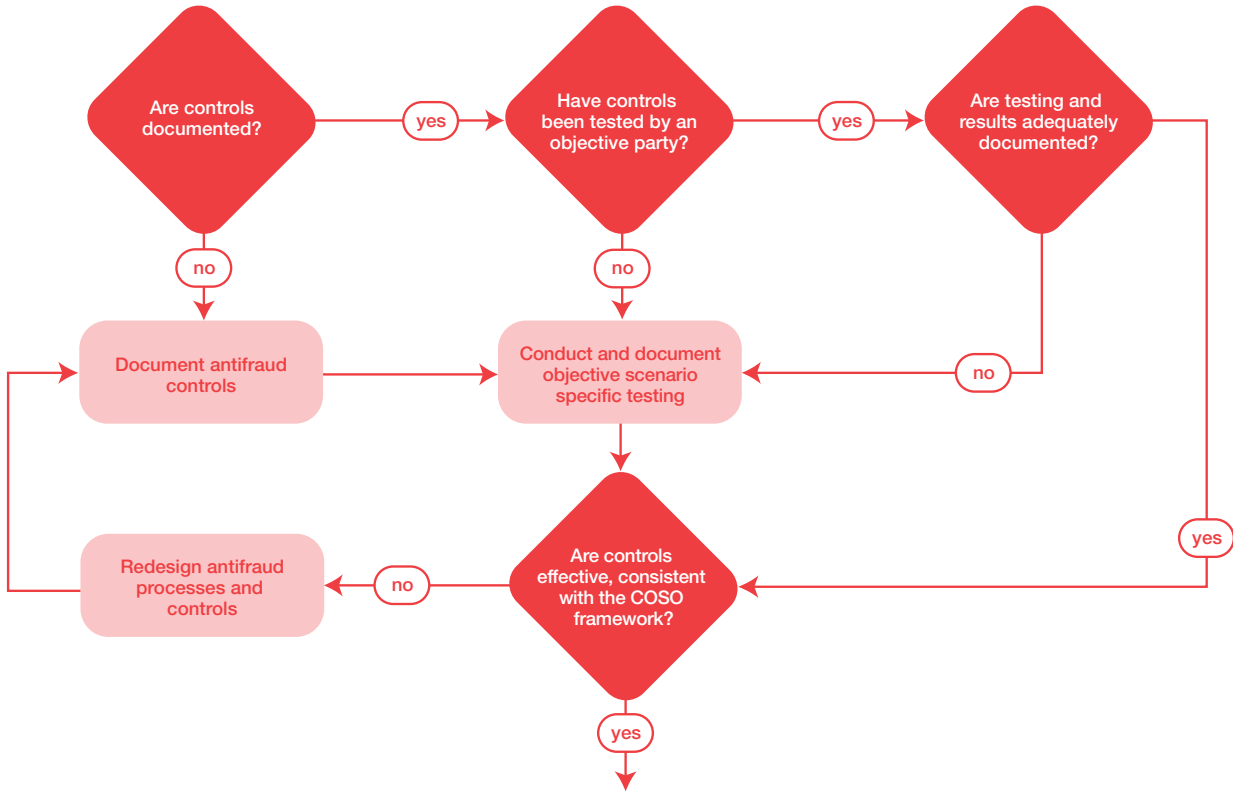
Validating operating effectiveness evaluates whether a properly designed control is not operating as designed and whether the persons performing the control possess the necessary authority, skill and qualifications to perform the control effectively.

Management can evaluate and test their antifraud programs and controls using the workflow shown at the top of page 18.

Management must conduct its own evaluation and testing of design and operating effectiveness. It cannot rely upon the independent auditor’s evaluation and testing of its antifraud programs and controls. (Nor can the independent auditor’s evaluation rely upon management’s evaluation and testing.) The company faces a possible qualified or adverse opinion if it fails to conduct and document an adequate assessment.<sup>17</sup>

<sup>16</sup> www.internalaudit.com. See also, J. Frank, *Fraud Risk Assessments* (Internal Auditor, April 2004).

<sup>17</sup> PCAOB Auditing Standard No. 2 Paragraphs 40, 42, 178.



### Step 4: Address residual financial reporting fraud risks

Management must assign internal audit, or some other function, to address residual financial reporting fraud risks. The internal audit function should re-evaluate its annual internal audit plan based on the results of the fraud risk assessment and testing of the design and operating effectiveness of antifraud programs and controls. Management and internal audit should be able to document that the internal audit plan addresses residual fraud risks; that is, fraud risks that are not adequately mitigated by antifraud programs and controls.

PCAOB auditing standards require that the independent auditor consider the adequacy of internal audit activities regarding fraud.<sup>18</sup> It is, at a minimum, a significant deficiency and a strong indicator of a material weakness if the independent auditor concludes that the internal audit function is ineffective.<sup>19</sup>

### Step 5: Standardize process for incident investigation and remediation

Fraud and misconduct are going to occur. Every large transportation & logistics company will suffer some level of internal and external misconduct, just as any moderate-sized municipality suffers some level of crime.

But companies must develop a standardized process for responding to allegations or suspicions of fraud. Transportation & logistics companies cannot wait until fraud is detected to develop an investigative process.

#### The investigative process

A company’s investigative process varies depending upon its size and complexity. The investigative process at smaller companies can be relatively informal, whereas the process at large, multinational organizations will likely require significant structure. By way of illustration, one Fortune 50 company has an investigative process that includes:

18 PCAOB Auditing Standard No. 2 Paragraph 24.  
 19 PCAOB Auditing Standard No. 2 Paragraph 140.

- An Office of Global Ethics & Compliance (ECO) that oversees investigations on a global basis.
- Ethics & Compliance Committees (ECC) established by charter in each of the organization's geographic regions.
- A separate Code of Conduct for conducting investigations.
- Standard global processes for categorizing, referring, investigating and reporting allegations of fraud and misconduct, including hotline calls.
- Participation by internal audit in all investigations.
- A global database that (1) enables the ECO and regional ECC to monitor and oversee all regional investigations; (2) facilitates the investigative work and best practices among the functional subject-matter experts; and (3) streamlines compliance reporting to management and the Audit Committee.

The investigative process must be capable of tracking all fraud allegations. The PCAOB requires management to certify in writing that it has described "any material fraud and any other fraud that although not material, involves employees who have a significant role in the company's internal control over financial reporting."<sup>20</sup> Management cannot meet its obligation, absent an adequate tracking process.

## Remediation

The investigation determines "what happened." Remediation generally involves five additional elements:

- Performing fraud audit procedures to assess whether (i) the wrongdoers engaged in other, unrelated wrongdoing, and/or (ii) similar misconduct occurred elsewhere in the organization
- Considering whether to self-report misconduct to government authorities

- Taking disciplinary and legal action against wrongdoers
- Recovering/restoring losses and other damages
- Learning from an incident to improve controls and prevent recurrence

In addressing control failures, management needs to consider the roots of how and why specific instances of fraud and/or misconduct were able to occur. Fraud, almost by definition, demonstrates a failure of controls, except in situations where detective controls are shown to be effective by identifying a fraud in a timely fashion.

In the final analysis, management must be prepared to explain to the audit committee and independent auditor (i) why the controls failed, and (ii) what action has been taken to prevent a recurrence.

<sup>20</sup> PCAOB Auditing Standard No. 2 Paragraph 142(f).



# Mitigating reputation, operational and legal risks

## Sarbanes integrated audit reaches only financial reporting risk

Although fraud and misconduct broadly impact the entity, the Sarbanes integrated audit reaches only risks that materially impact the financial statements. Equally important risks, including reputation, operational, legal and compliance risk, however, *falls outside* the scope of the audit of internal controls over financial reporting.

Audit committees, management, investors and other stakeholders, therefore, should take caution that SEC and PCAOB “antifraud programs and controls” do not address these issues. Nor should they assume or expect that the independent auditor considers these risks in the integrated audit of internal controls over financial reporting and the financial statements.

Conversely, transportation & logistics companies can apply the same approach and framework to design and implement programs and controls to broaden SEC and PCAOB antifraud programs and controls to reach fraud and misconduct risks that fall outside the scope of the audit of internal controls over financial reporting. Companies, for example, can draw on scheme and scenario risk assessments to identify “what could go wrong” and then link the risks to existing controls to assess whether the risk is adequately mitigated. At a minimum, independent auditors, audit committees, management, shareholders and other stakeholders should understand and manage expectations regarding the scope and audit of company controls to protect the company’s reputation and prevent and detect fraud and misconduct risk.

### Reputation risk: Protecting your most precious asset

What is a company's greatest asset? Ask that question of any CEO, analyst, employee, customer or supplier and the likely answer will be – "Reputation." Ask those same stakeholders to name the company's greatest risk, and the answer remains the same – "Reputation."

PwC's 2004 CEO survey conducted in association with the World Economic Forum reflects just how seriously fraud and reputation risk is perceived among company executives. Of the 1,400 CEOs responding to that study, 35 percent identified reputation risk as either "one of the biggest threats" (10 percent) or "a significant threat" (25 percent) to their business growth prospects.<sup>21</sup>

Corporate reputation, while it may not explicitly appear on the balance sheet, is a valuable asset. A strong reputation has both operational value and financial value. Generally speaking, most would agree that a good corporate reputation attracts customers, investors, and talented employees, leading to higher profits.<sup>22</sup> In some instances, customers are even willing to pay a premium price to companies with a positive reputation for product and service quality. A good reputation can also result in a higher credit rating, making it easier – and cheaper – to tap the capital markets.

A strong reputation not only helps a company attain stronger earnings, but it also helps to sustain profitable growth. In one study, an Australian business school professor compared the after-tax return on total assets (ROA) against companies listed over an eleven year period in Fortune's "Most Admired Companies." The study determined that:

(1) Good corporate reputations increase the length of time that firms spend earning superior financial returns (carry-over effect).

(2) Good corporate reputations may reduce the length of time that firms spend earning below-average financial returns (a lead-indicator effect).<sup>23</sup>

Today, reputation, brand and other intangible assets represent a significant proportion of a company's enterprise value. PwC research indicates that intangible assets may represent over 60 percent of a company's market value. Indeed, reputation is so crucial that the insurance industry is even developing an insurance product to cover loss of reputation.<sup>24</sup>

Despite the importance of reputation, few transportation & logistics companies have a comprehensive framework, approach, and infrastructure in place to identify and manage reputation risks, including evaluating related controls, and allow them to respond quickly and effectively if a damaging event were to occur. Without such a plan, they are exposed to ever-expanding business land mines and booby traps, particularly in this sector, which receives substantial local and national media exposure.

### Operational risk: Protecting the bottom line

Fraud in operations likewise presents significant risk. Operations fraud, even if the financial statements are accurate, significantly impacts the bottom line and opportunities.

According to PwC's Global Economic Crime Survey, the bigger you are, the harder you fall: companies with more employees are more likely to have suffered from economic crime. Further, the survey reports that no industry is safe as over 30 percent of the respondents in each of the industries interviewed suffered fraud. Another study of more than 450 public companies reported that three out of every four organizations experienced fraud during the prior 12 months, which is 13 percentage points higher than the last time a similar survey was conducted.<sup>25</sup>

A single fraud-related failure can result in a multibillion-dollar loss. In fact, a 2004 study of 508 fraud cases by the Association of Certified Fraud Examiners (ACFE) suggested that fraud can cost the typical U.S. organization roughly six percent of a company's annual revenues.<sup>26</sup> That figure, when applied to the U.S. Gross Domestic Product, translates into a fraud-related loss of approximately \$749 billion for U.S.-based companies in 2005.<sup>27</sup> This study also suggested that the median loss for a fraud in the transportation & logistics industry was \$225,000.

21 7th Annual Global CEO Survey, 2004, PricewaterhouseCoopers.

22 R. Alsop, The 18 Immutable Laws of Corporate Reputation 10 (2004); G. Dowling, Creating Corporate Reputations 12 (2001).

23 G. Dowling, Creating Corporate Reputations (2001).

24 R. Harris, Picking Up The Pieces, CFO Magazine (August 2004).

25 Findings from KPMG's 2003 Fraud Survey.

26 Association of Certified Fraud Examiners: 2004 Report to the Nation on Occupational Fraud and Abuse. The ACFE study involved 508 occupational fraud cases reported by certified fraud examiners that involved U.S.-based companies.

27 Based on advance estimate of 2005 Gross Domestic Product released by the Bureau of Economic Analysis on January 27, 2006.

### Legal risk: Protecting against criminal, regulatory and civil liability

The transportation & logistics sector faces substantial legal and compliance risk. Regulated segments are vulnerable to license suspensions, debarment, fines and other sanctions resulting from fraud and misconduct. Unregulated segments confront potential criminal and civil fines and/or private lawsuits arising from fraud and misconduct.

Transportation & logistics companies, as previously noted, can apply Sarbanes efforts toward meeting the 2004 USSG amendments. Qualifying as having an effective USSG compliance program provides a critical benefit, particularly if the entity should become the subject of any government investigation. Having an effective compliance program can help to avoid prosecution or other government action and, at a minimum, will reduce fines and penalties.

### Strategic risk: Protecting the future

Transportation & logistics companies must consider fraud and misconduct in developing and executing strategic decisions. They, for example, should consider fraud and misconduct risk associated before entering high risk geographic markets or industry segments. And, prior to entering into a merger or acquisition, transportation & logistics companies must consider the risk of becoming associated with individuals or company that engages in illegal or immoral business practices.

### Leveraging Sarbanes to mitigate other risks at minimal incremental cost

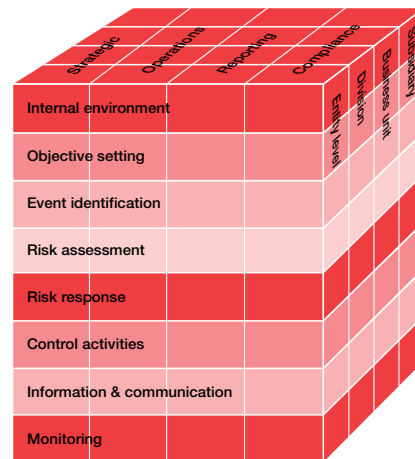
Expanding the Sarbanes antifraud program to address all misconduct risks involves little additional cost. The cost savings opportunities alone will more than pay for the entire antifraud and misconduct management program, while also potentially achieving USSG protection and mitigating reputation, legal, and strategic risk.

### Expand to COSO-ERM

Most companies apply COSO-Internal Controls to satisfy Sarbanes requirements. In September 2004, the Treadway Commission issued Enterprise Risk Management – Integrated Framework (COSO-ERM), authored by PwC, which expands upon the COSO-Internal Controls model. COSO-ERM serves as an excellent foundation for leveraging Sarbanes to address other fraud and misconduct risks.

Following is a broad overview of the COSO-ERM “cube”, and a five-step plan for leveraging Sarbanes and COSO-ERM at minimal incremental cost.

### COSO-ERM



### Objectives

COSO-ERM broadens the objectives listed on the top of the COSO-Internal Controls “Cube” model. The top side of the COSO-ERM cube represents the company’s objectives:

1. Strategic – relating to the corporate mission and high-level goals
2. Operations – relating to use of corporate assets and resources
3. Reporting – relating to the reliability of corporate reporting
4. Compliance – relating to compliance with law<sup>28</sup>

28 COSO-ERM at 21. COSO-ERM lists four objectives whereas COSO-Internal Controls lists three. COSO-ERM adds the “Strategic” objective which was not included in the COSO-Internal Controls model. Effective reputation risk management requires consideration of reputation risk in developing strategic objectives. Reputation risk, for example, is an important, but often absent consideration for transportation & logistics companies in determining whether a company should make an acquisition or enter into a joint venture. Another difference is that COSO-ERM refers to “Reporting”, whereas COSO-Internal Controls uses the phrase, “Financial Reporting”. COSO-ERM thus expands “Reporting” to include all internal or external reports of the entity, and not just published financial statements. Every corporate communication potentially impacts reputation, whether it is an advertising claim to the general public or an internal employee memo.

COSO-ERM adds “strategic” as an objective category and expands the reporting objective to include all reporting, and not just financial reporting as described in COSO-Internal Controls.

### Deeper than corporate

The right side of the cube depicts the company’s organizational structure. COSO-ERM distinguishes Entity, Division, Business Unit, and Subsidiary levels.

Effective fraud and misconduct risk management programs drill deep below the corporate level and perhaps even deeper than that required under Sarbanes. The least financially significant business unit might nonetheless pose huge reputation or legal risk. Transportation & logistics companies cannot afford to overlook business units that are immaterial to the financial statements or engage in a non-core business activity.

The selection process, of course, presupposes that the company has the appropriate staffing and competency to identify potential reputation risks – many of which vary by geographic market and business sector. PwC can help by leading the initial effort or by supplementing the company’s effort on an as needed basis. As members of their local business communities, PwC offices spread across 144 countries are well-positioned to identify unique geographic risks. Likewise, PwC’s industry specialists can help identify reputation risks unique to a particular business segment.

### Components of risk management

The front side of the cube depicts the eight components of Enterprise Risk Management, expanding from the five components in COSO – Internal Control.<sup>29</sup>

1. Internal Environment – relating to corporate culture and mission
2. Objective Setting – aligning objectives, mission and risk appetite
3. Event Identification – anticipating potential events that, if they occur, would impact the organization’s ability to realize objectives

4. Risk Assessment – evaluating likelihood and significance of potential events within a company’s core activities (product development, health & safety, environmental and employment policies)
5. Risk Response – responding by avoiding, accepting, reducing and sharing risks
6. Control Activities – implementing response through policies and procedures
7. Information and Communication – capturing and sharing relevant information across the organization
8. Monitoring – scrutinizing risk management through combination of ongoing management activities and after-the-fact separate evaluations

## Five-step plan for leveraging Sarbanes antifraud program

PwC has developed a Five-Step Plan for leveraging prior Sarbanes efforts and COSO-ERM to address all misconduct risk. *Steps 1 and 2* recommend obtaining senior management and Audit Committee support to hold individual business unit leaders accountable and form a senior-level, multidisciplinary team. *Steps 3 and 4* apply concepts from COSO-ERM and Sarbanes Antifraud Programs and Controls to expand the fraud and misconduct risk assessment, evaluate all antifraud – not just financial reporting – controls, and monitor residual risks. Finally, *Step 5* recommends consulting with your independent auditor.

### Step 1: Hold individual business unit leaders accountable

Managing fraud and misconduct risk demands active and visible backing from senior management. Senior management, in turn, must persuade business unit and function leaders to take ownership of managing fraud and misconduct.

Managing these risks cannot be left to the risk management, internal audit, legal, compliance, brand management or other corporate shared-services centers. The business unit and function leaders must take an active role in the process. Not only does this approach reinforce accountability, but individual

<sup>29</sup> The five components of COSO-Internal Control are (1) control environment, (2) risk assessment, (3) control activities, (4) information and communication, and (5) monitoring.

business unit and function leaders are best situated to assess reputation risks and root causes, as they have the deepest understanding of their business areas. One Fortune 500 company formally reinforces ownership and accountability by requiring the individual business unit and function leaders to make formal presentations to senior management and/or the Audit Committee.

### Step 2: Balance accountability and responsibility

Managing fraud and misconduct risk, however, requires coordination; takes time away from other duties, and can be expensive, depending upon the required level of coaching and consultation. To achieve balance, PwC recommends a hybrid approach. Under this model, business unit leaders remain accountable, but supported by a senior multidisciplinary team, comprised of outside consultants and representatives from the key business processes, who are responsible for implementing the fraud and misconduct management plan.

### Step 3: Expand the scope of the risk assessment

A Sarbanes fraud risk assessment addresses only financial reporting risks. Expanding the risk assessment to identifying potential fraud and misconduct that give rise to reputation, operation legal, compliance, and strategic risk is the single most important action step. Events range from the obvious to the obscure.<sup>30</sup> Investing time and resources into event identification will identify previously unidentified risks and enable companies to prevent, detect, and mitigate potentially damaging scenarios – whether they damage reputation, reduce earnings, or expose the company to civil, criminal, or regulatory liability.

### Step 4: Don't just look at financial reporting controls

Sarbanes antifraud programs look exclusively at internal controls over financial reporting. To gain broader coverage, the controls assessment must include all controls intended to prevent and detect misconduct risk, regardless of how the entity labels those controls activities.

The process should be fairly simple, if the company's control activities are well organized. As a benchmark, most companies should be able to link approximately 60 to 70 percent of identified misconduct risks to an existing Sarbanes-documented and tested control activity.

Sarbanes control activities split between preventive and detective controls. Management of reputation, operations, compliance and misconduct risks employs a third control consideration: a ready response plan to mitigate the reputation damage from the event, which PwC refers to as a "responsive" control.

Evaluating design and validating operating effectiveness or preventive and detective controls forces the entity to distinguish between inherent and residual risks. Residual risks are fraud and misconduct risks that are not adequately mitigated by antifraud programs and controls. As with financial reporting risks, companies should assign internal audit, or some other function, to address these residual risks.

This method of developing a risk response to events helps companies to develop well-thought out reputation risk strategies that don't rely on sheer luck. Linking identified risks to specific preventive, detective and responsive control activities forces the company to decide whether to avoid or accept a reputation risk and, if accepted, on what basis.

### Step 5: Consult your independent auditor

The independent auditor can serve a vital role in fraud and reputation risk management, subject to SEC and entity-specific independence rules. Seeking the auditor's assistance will reduce cost and gain an independent perspective, which can be helpful in dealing with government authorities.

The independent auditor, for example, can assist to evaluate the design and validate the operating effectiveness of general and specific reputation and compliance controls, since the auditor will have already considered many of these issues as a part of the internal controls portion of the integrated audit. At a minimum, the entity should inform the independent auditor of the scope of its fraud and risk management program to ensure a mutual understanding of which aspects are covered under Sarbanes.

30 COSO-ERM, p. 41.



# Closing thoughts

As we said at the beginning of this report, fraud management makes good business sense. It can help a company maintain investor confidence in the integrity of its financial results, reduce costs, improve profitability, protect its reputation, and mitigate liability. However, the elements discussed in this whitepaper must all work together to form an effective antifraud program, and thus should be considered in the aggregate as an integrated system.

In summary:

Common fraud schemes impacting the transportation & logistics sector can be classified in the following ways:

- Financial statement manipulation
- Misappropriation of assets
- Unauthorized receipts and expenditures
- Aiding and abetting
- Fraud by senior management
- Disclosure fraud

To develop and implement an effective antifraud program, you should:

1. Establish a base line
2. Conduct a Fraud Risk Assessment
3. Evaluate design and validate operating effectiveness
4. Address residual financial reporting fraud risks
5. Standardize processes for incident investigation and remediation

Audits of internal controls under Section 404 of the Sarbanes-Oxley Act of 2004 only address risks that materially impact the financial statements. Equally important risks that fall outside the scope of the audit of internal controls include:

- Reputation risk
- Operational risk
- Legal risk
- Strategic risk

You can leverage prior Sarbanes efforts and COSO-ERM to address all misconduct risk by:

1. Holding individual business unit leaders accountable
2. Balancing accountability and responsibility
3. Expanding the scope of the risk assessment
4. Broadening your look beyond financial reporting controls
5. Consulting with your independent auditor



# Appendices

Appendix A: Antifraud program and controls assessment grid

Appendix B: Antifraud program and controls responsibilities matrix

Appendix C: Conducting a fraud and reputation risk assessment

Appendix D: Fraud auditing process

Appendix E: Antifraud program implementation

Appendix F: Comparison of antifraud programs and controls and United States Sentencing Guidelines

## Appendix A: Antifraud program and controls assessment grid

Following is a practice aid that a company can use to assess its existing antifraud programs and controls. The criteria work together to form an effective antifraud program, and thus should be considered in the aggregate as an integrated system. A singular, deficient element does not necessarily rise to the level of a “significant deficiency.” Conversely, the absence of multiple elements should raise a concern about the adequacy of the program or a COSO framework control component. Any deficiencies should also be evaluated in the aggregate to consider whether they combine in a way that creates a significant deficiency and whether significant deficiencies when aggregated become a material weakness.

Element	Criteria	Assessment ranking		
		Best practice	Generally in compliance	Deficient
<b>Control environment</b>				
Management Accountability	Management should: (1) effectively implement the company’s antifraud programs and controls, and (2) take appropriate actions involving circumvention of internal controls over financial reporting.	Management: (1) demonstrates that internal controls, including those addressing fraud, are important, (2) implements antifraud programs and controls including codes of ethics and conduct, and (3) takes appropriate, consistent remediation action in instances of violations.	Management takes sufficient actions with respect to prevention, detection, investigation, remediation, and monitoring of fraud and fraud controls.	Management fails to conduct oversight of antifraud programs and controls. Remediation, including disciplinary action, is inconsistent.
Board of Directors and Audit Committee Oversight	The Board and Audit Committee should provide oversight over: (1) management’s antifraud programs and controls, (2) management’s assessment of fraud risk, (3) control activities over fraud risks identified by the assessment, (4) monitoring and auditing for fraud, (5) investigation of alleged or suspected fraud, and (6) remediation.	The Board and the Audit Committee: (1) actively conduct oversight of management’s antifraud program, (2) seek the views of internal audit, the independent auditor, and others regarding the topic of fraud. The charter expressly addresses fraud oversight as an essential function of the Audit Committee.	The Board and Audit Committee provide oversight.	The Board and Audit Committee fail to provide oversight and do not sufficiently consider fraud risk.
Codes of Ethics and Conduct	Written standards that are reasonably designed to deter wrongdoing and to promote honest and ethical conduct. Operating effectiveness evidenced through communication plan, annual confirmation process, training, management and Audit Committee involvement and oversight.	Documented and effective codes of conduct should include and be effectively communicated to all employees. Code should address: (1) conflicts of interest, (2) related party transactions, (3) accuracy of accounting records, (4) illegal acts, and (5) compliance with laws and regulations.	Documented and effective code of conduct with only minor deficiencies. Applies to all individuals in an accounting or financial reporting oversight role.	Code omits topics specified in SEC’s Final Rules or is not operating effectively. Ineffective communication to all covered persons.

Element	Criteria	Assessment ranking		
		Best practice	Generally in compliance	Deficient
Ethics Hotline/ Whistleblower Program	Documented procedures for the receipt, retention and treatment of complaints and confidential, anonymous submission of concerns by employees or third parties.	Ethics hotline with a documented process and proven effectiveness as evidenced by employee and third-party awareness, encouragement of use, and appropriate and timely response. Program operates independently of management and with Audit Committee oversight.	Ethics hotline that appears to be of proper design and effectiveness but potentially with perceived low volume of use.	Ethics hotline or whistleblower program omits elements (design or operating) in SEC rules.
Hiring and Promotion Procedures	Established standards for hiring and promotion including background investigations and maintenance of all information in the personnel files for all positions of trust in an organization.	For new hiring and promotions of personnel in positions of trust, conduct full-scope background investigations, including interviews with independent references. Similar investigations conducted for strategic third parties such as vendors, joint venture partners, consultants, and customers. All results documented. Background investigations should include educational background, employment history, and criminal record.	Performs public record background investigations on personnel hired or promoted into positions of trust.	Fails to perform substantive background investigations for individuals being considered for employment to a position of trust.
Investigative Process	Standardized procedure for tracking, responding to, investigating and assessing allegations of fraud, whether or not material, potentially including a 10A investigation by independent counsel.	Written plan and process for tracking and responding to allegations of misconduct. Where appropriate, investigative process allows for investigation independent of management. Audit Committee and external auditors advised of all significant deficiencies in internal controls and of any fraud involving management or other employees who have significant role in internal controls.	In the absence of a written process, company demonstrates that a process exists for tracking and responding to allegations, notwithstanding a lack of a written plan.	Inadequate process for responding to allegations for suspicions of fraud.
Remediation	Documented process of assessing and improving relevant internal controls, taking appropriate action against violators and communicating results both internally as well as to the necessary external parties.	Improves relevant internal controls, takes appropriate action against violators and communicates results both internally as well as to the necessary external parties. Evidence and documentation of Audit Committee involvement.	Takes appropriate disciplinary action and considers need for additional action to prevent recurrence.	Fails to take consistent remedial action with regard to identified significant deficiencies, material weaknesses, actual fraud or suspected fraud.

Element	Criteria	Assessment ranking		
		Best practice	Generally in compliance	Deficient
<b>Risk assessment</b>				
Process for Assessing Risk	Systematic rather than haphazard; considers fraud schemes and circumvention of existing controls; active oversight by Audit Committee.	Fully documents fraud risk assessment process; process includes interviews of personnel at various levels of organization, occurs periodically throughout organization and in response to significant events, e.g., acquisitions, entry into new markets/products; active oversight by Audit Committee.	Assesses fraud risk on systematic basis; Audit Committee review.	Fails to assess fraud risk on systematic basis; haphazard or informal process for fraud risk assessment; inadequate evidence of Audit Committee involvement and review.
Frauds Considered	Consideration of fraudulent financial reporting, misappropriation of assets, unauthorized or improper receipts and expenditures, and fraud by senior management should all be demonstrated.	Assesses exposure from each of the categories of fraud risks considered.	Addresses all fraud risks that have a more than remote likelihood of having a material impact upon the financial statements.	Absence of adequate documentary evidence of management's risk assessment process and the Audit Committee's involvement and review.
Likelihood and Significance of Fraud	Consideration of the likelihood of each fraud risk as probable, reasonably possible, or remote; consideration of significance of fraud as inconsequential, more than inconsequential or material should be demonstrated.	Evaluates comprehensively the likelihood and significance of each identified fraud risk.	Substantially evaluates likelihood and significance of each fraud risk. Management provides sufficient explanation where risk assessment process does not consider risks that are more than remote and more than inconsequential.	Management's risk assessment process does not identify the level or likelihood and significance considered. Management fails to provide and explanation where risk assessment process does not consider risks that are more than remote and more than inconsequential.
Consideration of Organizational Levels	Consideration of fraud at the company-wide business unit and significant account levels should all be demonstrated.	Assesses fraud risk at all levels of the organization.	Assesses fraud risk at all significant levels, accounts and locations of the organization.	Fails to consider significant business units or significant processes in the fraud risk assessment.
Circumvention of Controls and Management Override	Effectively designed internal controls should be in place to respond to the assessment of risk of management override.	Audit Committee specifically considers vulnerability of existing controls and risk of management override.	Fraud risk assessment process addresses circumvention of existing controls and potential for management override.	Fails to adequately consider risk of: (1) circumvention of controls, and (2) management override.
<b>Control activities</b>				
Linkage with Risk Assessment	Effective control activities should be designed and implemented to mitigate identified fraud risks.	Company links control activities to all identified fraud risks. Active oversight by Audit Committee to ensure design and operating effectiveness.	Company can link control activities to identified fraud risks and evaluates for design and operating effectiveness.	Fails to link control activities to identified fraud risks; control activities deficient in design or operating effectiveness.
<b>Information and communication</b>				
Training	Demonstrated frequency and sufficiency of proper training courses provided to all employees on fraud risk and antifraud programs and controls.	Provides comprehensive and frequent relevant training to all employees. Maintains records documenting types of training and employees trained.	Provides adequate training to employees regarding fraud related issues.	Fails to provide adequate or effective training regarding code of ethics and other fraud areas.

Element	Criteria	Assessment ranking		
		Best practice	Generally in compliance	Deficient
Knowledge Management	Demonstrated capabilities in place to collect and share information regarding identified fraud risks, strengths and weaknesses of antifraud control activities, allegations of fraud, and remediation efforts.	Clear communication of antifraud policies and procedures flows down, up, and across the organization. Employees fully understand relevant aspects of the antifraud program and understand what behavior is acceptable and unacceptable. Strong knowledge sharing regarding fraud risks, control activities, allegations of fraud, and remediation efforts.	Shares some but not all fraud-related information.	Fails to collect or share information regarding fraud risks, control activities and remediation of identified misconduct.
Information Systems and Technology	Elements that should be addressed are inclusion of technology in management's fraud risk assessment, effective IT security and controls, adequacy of fraud detection and monitoring tools, and ability to investigate computer misuse.	Information systems and technology addresses: (1) consideration of technologically enabled fraud in management's fraud risk assessment; (2) IT security controls, (3) inappropriate modification to computer programs, (4) system override, (5) segregation of duties, (6) adequacy of fraud detection and monitoring tools, and (7) ability to investigate computer misuse.	Information systems and technology addresses some, but not all of elements 1 through 7.	Fails to: (1) consider information technology in fraud risk assessment, (2) maintain security and access controls, (3) employ information technology to prevent and detect fraud, or (4) have an ability to investigate computer misuse.
<b>Monitoring</b>				
Monitoring by Management	Management should have a process of assessing the quality of the antifraud programs and controls over time through ongoing monitoring activities as well as separate periodic evaluations.	Monitors antifraud controls, programs and policies on an ongoing and periodic basis; management considers possibility of fraud in day-to-day operations; management uses results of fraud assessment and IT system to monitor for fraud.	In absence of written process, company can demonstrate that management monitors for indicia of fraud as part of day-to-day operations.	Management fails to include possibility of fraud in its monitoring of day-to-day operations.
Internal Audit Evaluations	The internal audit function in an organization should conduct separate fraud evaluations with a documented plan, approach, scope, and results of review with knowledgeable and experienced staff.	Internal audit actively considers fraud risk in developing audit cycle. Internal audit builds fraud auditing modules into routine audits and special projects. Internal audit includes fraud-experienced internal auditors.	In absence of written process, company can demonstrate that: (1) internal audit considers fraud in developing and executing internal audit cycle, and (2) department includes internal auditors with training and experience in fraud auditing.	Fails to either: (1) consider fraud in planning internal audit cycle, (2) conduct fraud auditing procedures, or (3) include routine fraud auditing in the scope of the internal audit function's annual audit cycle. Failure to include knowledgeable and experienced fraud professionals in the internal audit function.

## Appendix B: Antifraud program and controls responsibilities matrix

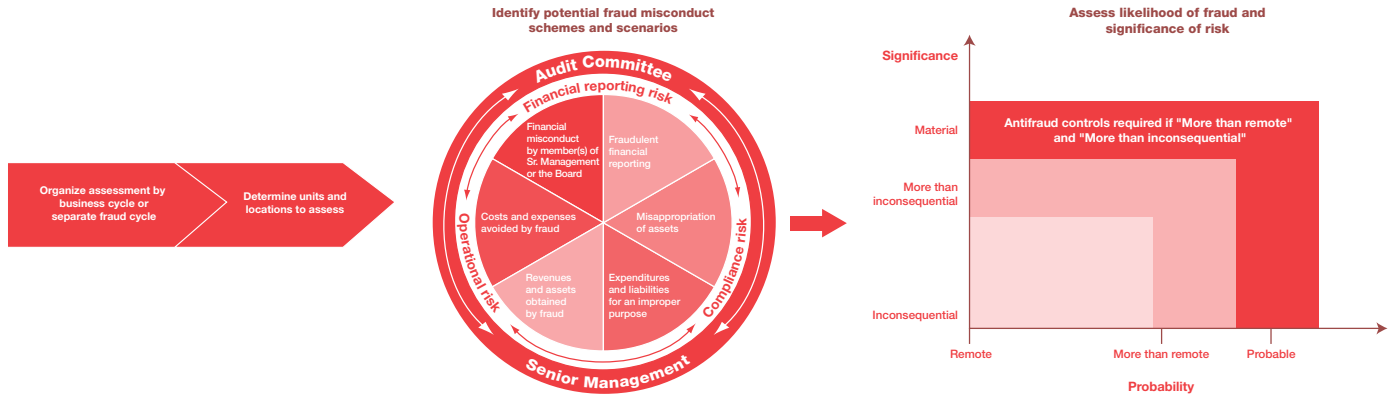
Date of assessment		Responsibility				
Element	Criteria	Board of Directors	Management	Internal Audit	Other	Documentation
<b>Control environment</b>						
Management Accountability	Management should: (1) effectively implement the company's antifraud programs and controls, and (2) take appropriate actions involving circumvention of internal controls over financial reporting and other fraudulent behaviors.					
Board of Directors and Audit Committee Oversight	The Board and Audit Committee should provide oversight over: (1) management's antifraud programs and controls, (2) assessment of fraud risk, (3) controls activities over fraud risks identified by the assessment, (4) monitoring and auditing for fraud, (5) investigation of alleged or suspected fraud and (6) remediation.					
Codes of Ethics and Conduct	Written standards that are reasonably designed to deter wrongdoing and to promote honest and ethical conduct. Operating effectiveness evidenced through communication plan, annual confirmation process, training, management and audit committee involvement and oversight.					
Ethics Hotline/ Whistleblower Program	Documented procedures for the receipt, retention, and treatment of complaints and confidential, anonymous submission of concerns by employees or external third parties.					

Date of assessment		Responsibility				
Element	Criteria	Board of Directors	Management	Internal Audit	Other	Documentation
Hiring and Promotion Procedures	Established standards for hiring and promotion including background investigations and maintenance of all information in the personnel files for all positions of trust in an organization. Background investigations should include educational background, employment history and criminal record.					
Investigative Process	Standardized procedure for responding to, investigating and assessing allegations or suspicions of fraud, whether or not material, potentially including a 10A investigation by independent counsel.					
Remediation	Documented process of assessing and improving relevant internal controls, taking appropriate action against violators, and communicating results both internally as well as to the necessary external parties.					
<b>Risk assessment</b>						
Process for Assessing Risk	Systematic rather than haphazard; considers fraud schemes and circumvention of existing controls; active oversight by Audit Committee.					
Frauds Considered	Consideration of fraudulent financial reporting, misappropriation of assets, unauthorized or improper receipts and expenditures, and fraud by senior management should all be demonstrated.					

Date of assessment		Responsibility				Documentation
		Board of Directors	Management	Internal Audit	Other	
Element	Criteria					
Likelihood and Significance of Fraud	Consideration of the likelihood of each fraud risk as probable, reasonably possible or remote; consideration of significance of fraud as inconsequential, more than inconsequential or material should be demonstrated.					
Consideration of Organizational Levels	Consideration of fraud at the company-wide, business unit, and significant account levels should all be demonstrated.					
Circumvention of Controls and Management Override	Effectively designed internal controls should be in place to respond to the assessment of risk of management override.					
<b>Information and communication</b>						
Training	Demonstrated frequency and sufficiency of proper training courses provided to all employees on fraud risk and antifraud programs and controls.					
Knowledge Management	Demonstrated capabilities in place to collect and share information regarding identified fraud risks, strengths and weaknesses of antifraud control activities, allegations of fraud, and remediation efforts.					
Information System and Technology	Elements that should be addressed are: inclusion of technology in management's fraud risk assessment, effective IT security and controls, adequacy of fraud detection and monitoring tools, and ability to investigate computer misuse.					

Date of assessment		Responsibility				
Element	Criteria	Board of Directors	Management	Internal Audit	Other	Documentation
<b>Monitoring</b>						
Monitoring by Management	Management should have a process of assessing the quality of the antifraud programs and controls over time through ongoing monitoring activities as well as separate periodic evaluations.					
Internal Audit Evaluations	The internal audit function in an organization should conduct separate fraud evaluations with a documented plan, approach, scope and results of review with knowledgeable and experienced staff.					
<b>Control activities</b>						
Linkage with Risk Assessment	Effective control activities should be designed and implemented to mitigate identified fraud risks.					
Evaluate Design and Operating Effectiveness of Specific Preventive or Detective Antifraud Control	Not applicable - varies based upon control.					

## Appendix C: Conducting a fraud and reputation risk assessment



A properly executed fraud and reputation risk assessment will identify significant cost-savings opportunities which fall directly to the bottom line. These cost savings should far exceed the costs of the antifraud program. A major study of the insurance industry, for example, demonstrated that antifraud programs generated seven dollars for every dollar invested.<sup>31</sup> Likewise, a separate benchmarking analysis and research by the General Counsel Roundtable found that each additional dollar of compliance spending saves organizations, on average, \$5.21 for every one spent in heightened avoidance of legal liabilities, harm to the organization’s reputation and lost productivity.<sup>32</sup> That’s more than a five-to-one payback.

### Organize the assessment

The fraud and reputation risk assessment process may be integrated around the organization’s existing business cycles or be established as a separate cycle for this purpose. Organizing around an existing business cycle can simplify the process; the team can *specifically* consider fraud and reputation risks associated with revenue.

The downside to this approach is that the team may miss a fraud or reputation risk that does not fit neatly into a particular business cycle.

An alternative is to create a separate cycle focused on fraud and reputation risk. In doing so, however, consider a more innocuous title for the cycle, such as “safeguarding of assets,” because of the anxiety-producing nature of a fraud descriptor.

### Determine units and locations to assess

To be effective, fraud and reputation risk assessments must be conducted at the company-wide, business-unit and significant account levels. Risk assessments should also be conducted when special circumstances arise, such as changed operating environments, the introduction of new products, mergers and acquisitions, the entry of new markets, and corporate restructurings.

At public companies, the team should liaise with the Sarbanes-Oxley readiness team because of its ongoing work with the organization’s significant business units, accounts and locations. Note, however, the fraud risk assessment process may well require a broader reach, given that reputation risk is not synonymous with financial significance.<sup>33</sup>

Multinational companies, for example, often conduct business at higher-risk locations. While such locations may not be financially material to the organization as a whole, there may be potential fraud and reputation risks associated with doing business in such markets, and both senior management and the Board of Directors need to be apprised of such risks.

31 “Insurance Fraud: The Quiet Catastrophe,” Insurance Research and Publications, Conning and Co., 1996. The Conning study, which sought to project returns on investment for combating insurance fraud, defined ROI as the ratio of money saved to money spent preventing fraud. It found that the average ROI across the insurance industry for 1995 was \$6.88 for every dollar spent on fighting fraud. (Source: Coalition Against Insurance Fraud.)

32 “Seizing the Opportunity, Part One: Benchmarking Compliance Programmes,” © 2003 Corporate Executive Board, General Counsel Roundtable.

33 Likewise, PCAOB auditing standards emphasize that an auditor must apply qualitative, as well as a quantitative, factors when identifying significant accounts and processes. Thus, an account, which is quantitatively immaterial to a financial statement audit, might be material to an audit of internal controls. PCAOB Auditing Standard No. 2, Paragraphs 60 – 70.

## Identify potential fraud and misconduct schemes & scenarios

Organizations can damage their reputations or be defrauded in myriad ways. A critical step in the risk assessment process is to identify the organization's universe of potential risks – without regard to probability of occurrence (that consideration follows). A starting point is to determine what fraud schemes and scenarios typically affect your organization's industries and locations. Next, you must tailor these schemes and scenarios to your organization.

Developing a scheme- and scenario-based database for a company is a formidable challenge, as we know from first-hand experience. PwC tracks new and emerging fraud by company, industry and geography. We also maintain an extensive database of scheme- and scenario-based information, drawing source material from the media, reporting services, subject matter experts and industry associations. For the most common schemes, our fraud subject matter experts have identified the:

- Mechanics of the scheme and sub-scheme.
- Scheme indicia.
- Antifraud preventive and detective control activities.
- Fraud auditing detection procedures.

Senior management and the Audit Committee are responsible for all six categories in the wheel depicted in the graphic above. Yet, many companies assign no internal organization to prevent and detect fraud. A company's risk assessment process must address all six categories of fraud and misconduct to avoid being cited for a "significant deficiency." Management and the team will need requisite fraud expertise to develop scheme- and scenario-based databases and repositories and will need to know (1) the technicalities associated with the scheme, (2) the indicia to look for to determine whether the scheme is occurring, (3) what controls are available to prevent and detect the scheme, and (4) how to detect the fraud in the normal course of business.

Identifying the universe of potential fraud schemes is a significant task. Our list of generic fraud schemes represents the tip of the iceberg. Fraud schemes and scenarios differ drastically by product and service sector and geography. For example, sales and marketing schemes are quite common in the Asian market whereas procurement fraud is more widespread in Central and South America. On the other hand, the types of schemes affecting a transportation & logistics company differ from those affecting a bank or insurance company.

As a result, the typical major transportation & logistics company may face hundreds of fraud and reputation risks. To develop scheme descriptions requires a deep knowledge of fraud, the industry or industries in which the company operates, and the geographies and jurisdictions where it conducts business.

Management can draw relevant information from individual business units about industries and geographies served. Note, however, that it is one thing to be an industry and geographic expert – but quite another to be expert about how fraud and misconduct occur and can be mitigated. For example, for international operations, the country manager is a critical starting point, but management must probe more deeply to surface relevant insights. Publicly available information about fraud schemes tends to be quite limited and generic in nature, reflecting both the reticence of companies to share information about such matters as well as the scant attention given to fraud prevention and detection prior to Sarbanes-Oxley.

The team also needs to understand the risks and ramifications posed by each scheme. In assessing fraud-related risks, for example, senior management and the Audit Committee may be far more willing to risk a monetary loss as opposed to the loss of reputation or the possibility of criminal or civil sanctions.

**Assess likelihood of fraud and significance of risk**

Fraud risk assessments, like traditional risk assessments, consider the likelihood that a particular fraud will occur. The PCAOB auditing standards specify the following risk levels.<sup>34</sup>

- Remote
- More Than Remote/Reasonably Possible
- Probable

An organization should address risks that have “more than a remote” likelihood of occurring to avoid a significant deficiency. Fraud risks deemed to be remote can be ignored, although it is advisable for the assessment team to document that the organization had considered the risk before determining it to be remote.

Next, assess the significance of fraud risks with a more than remote likelihood of occurring. In this context, the PCAOB auditing standards refer to:

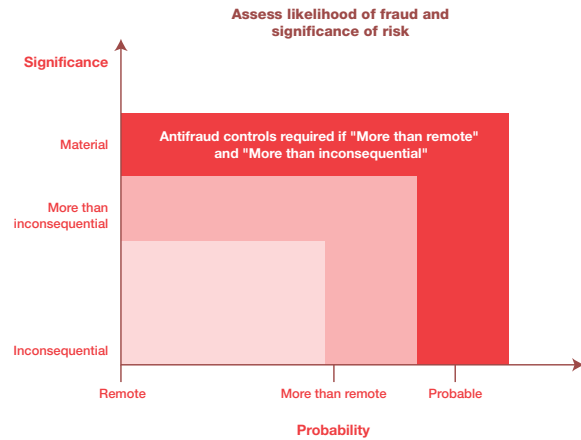
- Inconsequential
- More Than Inconsequential
- Material

The PCAOB defines inconsequential as a misstatement that a reasonable person, “after considering the possibility of further undetected misstatements” would find to “clearly be immaterial to the financial statements.”<sup>35</sup> The standard further provides, “If a reasonable person could not reach such a conclusion regarding a particular misstatement, that misstatement is more than inconsequential.”

Do not be fooled by the term “material.” Do not limit the scope of the fraud risk assessment to material frauds. Materiality refers to the significance of an item to the users of a set of financial statements.<sup>36</sup> SEC registrants should note that SEC Staff Accounting Bulletin No. 99 (SAB 99), which provides guidance in determining materiality when fraud is discovered<sup>37</sup>, rejects the frequently used rule of thumb that a misstatement or omission that is less than 5 percent of some factor (e.g., net income or net assets) is immaterial. SAB 99 requires that a determination of materiality consider both the “quantitative” and “qualitative” aspects of the particular matter being analyzed.

Fraud rises to the level of material if a reasonable person – say a shareholder or lender – would consider it important. When evaluating significance, management should consider the impact of the fraud scheme individually and in the aggregate. Some frauds, such as travel and expense fraud, might be inconsequential on an individual basis but be significant on a combined basis.

Transportation & logistics companies should address fraud risks that are “more than inconsequential” in amount to avoid a significant deficiency. Although an organization can ignore fraud risks deemed to be inconsequential, based on cost-benefit considerations, it should document why this determination was reached.



34 PCPCAOB Auditing Standard No. 2 refers to Financial Accounting Standards Board Statement No. 5, Accounting for Contingencies (FAS No. 5), which uses the terms probable, reasonably possible and remote. The PCAOB defines “more than remote” as reasonably possible or probable.

35 PCAOB Auditing Standard No. 2 Paragraph 9.

36 Financial Accounting Standards Board (“FASB”) Statement of Financial Accounting Concepts No. 2, Qualitative Characteristics of Accounting Information (“CON 2”) describes materiality as “the omission or misstatement of an item in a financial report is material if, in light of surrounding circumstances, the magnitude of the item is such that it is probable that the judgment of a reasonable person relying upon the report would have been changed or influenced by the inclusion or correction of the item.”

37 17 Code of Federal Regulations Part 211, August 12, 1999.

## Link antifraud controls

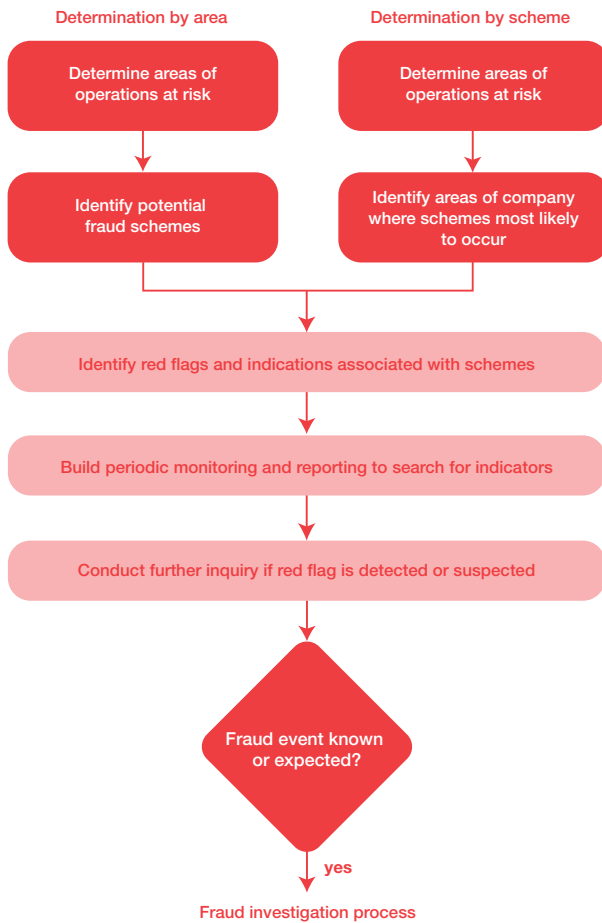
The team may use a table similar to that shown below to link antifraud risks to existing controls.

Next, the company should identify the control activities which mitigate those fraud and reputation risks that have a more than remote likelihood of occurring and that are more than inconsequential in amount. As a rule of thumb, antifraud controls generally include controls designed to *prevent* fraud and those designed to *detect* fraud *in a timely fashion* when it occurs.<sup>38</sup> Management should expect to tie 70 to 80 percent of identified fraud risks to existing control activities such as approvals, authorizations, verifications, reconciliations, segregation of duties, reviews of operating performance and security of assets.

Conversely, the assessment will likely reveal that no control activities exist to mitigate 20 to 30 percent of the identified risks. Management must decide whether to develop controls for areas lacking appropriate controls. In doing so, management will need to conduct a cost-benefit analysis to compare the costs of controlling a risk to the benefits of mitigating or eliminating that risk. It is important to document the analysis, should management decide against implementing corrective measures.

Business unit, process or objective	Fraud category	Fraud scenario	Sample antifraud controls	
			Preventive	Detective
Procurement	Asset overstatement/ liability understatement	Improper change in payment terms	Ability to create or change credit limits and payment terms is restricted to credit personnel and approved by management.  §302 certification confirmations contain specific reference to the absence of undisclosed payment terms.	Reporting exists to monitor changes in payment terms in the system.  The collections group monitors the A/R to identify changes in payment term trends.
Inventory	Misappropriation of assets	Inventory shrinkage	Physical security of all inventories under dual control.	Periodic physical inventory.  Investigation and reconciliation of inventory differences.

## Appendix D: Fraud auditing process



Many companies will need to assemble or develop fraud expertise within the internal audit function. Today’s antifraud and risk-mitigation environment requires a broad range of skills and experience. Internal audit must be aware of potential schemes and scenarios affecting the industries and markets in which the company does business, and it must be conversant with and able to identify the indicia of these schemes. What’s more, internal audit must have a solid understanding of measures intended to prevent and detect fraud and be able to evaluate and test antifraud control effectiveness. In addition, internal audit must be knowledgeable about fraud auditing and forensic investigation techniques.

For most internal audit functions, many of these skill sets will be new, for until now, relatively little emphasis has been placed on fraud prevention and detection. Running investigations into “what happened” differs substantially from performing fraud risk assessments, testing antifraud control activities and conducting fraud audits. Moreover, a company cannot achieve needed skills and expertise by simply hiring an investigator or former law enforcement agent.

Management can pursue a number of options to obtain the breadth of resources needed to address antifraud and risk mitigation concerns. Some large companies are creating internal units within internal audit to address prevention, detection, investigation and remediation of fraud. Some companies have the internal audit function borrow internal resources or enter into co-sourcing relationships in order to ensure compliance with the new requirements.<sup>39</sup>

### Fraud auditing vs. fraud investigation

Fraud auditing (as opposed to fraud investigation) is a new field, largely being defined in response to today’s environment. Like traditional forms of auditing, fraud auditing focuses on the risks of fraud, the probability of the occurrence of fraud and the significance of a fraud event or series of events.

Fraud auditing combines aspects of forensic investigation and standard auditing techniques and generally requires knowledge of how frauds occur in various industries and a firm grounding in the indicia of fraud schemes that appear during an audit. The mere indicia of a fraud scheme do not, in and of themselves, indicate that a fraud has occurred. There may be perfectly legitimate reasons for any given fraud indicia to arise as part of the audit process.

By contrast, fraud investigation, or forensic accounting, is an inquiry into specific allegations or suspicions of fraud. Fraud investigations focus on determining the nature, extent, cause and resolution of identified or suspected fraudulent events. Only those indicia that are subsequently found to be fraudulent in nature become the focus of a fraud investigation. The discipline of fraud investigation embraces specialty skill sets beyond those typically required to conduct fraud risk assessments and audits.

<sup>39</sup> Every member of the internal audit department needs to have some level of fraud training, even if the department retains specialized resources. Such training should address common fraud schemes and scenarios and provide the grounding needed for an internal auditor to assess fraud risk and identify fraud indicators.

Fraud auditing work plans typically include the following components:

### Interviewing

The fraud auditor must identify the individuals who would have knowledge (first-hand or otherwise) of the existence of fraud or of facts that would indicate that fraud might be occurring. This means that the fraud auditor would need to interview a broader range of personnel than would otherwise normally be interviewed. Moreover, fraud auditing interviews need to be conducted in person, since it is virtually impossible to obtain targeted information by telephone or via e-mail.

### Analytics

Fraud auditors, like auditors of financial statements, rely heavily upon analytics, although fraud auditors are likely to disaggregate analytics to a lower threshold. For example, a fraud auditor might consider revenue month by month rather than quarter by quarter or year by year.

### Management override and circumvention of controls

Fraud auditors always consider the possibility of management override or circumvention of controls. Thus additional procedures are needed to test for this possibility.

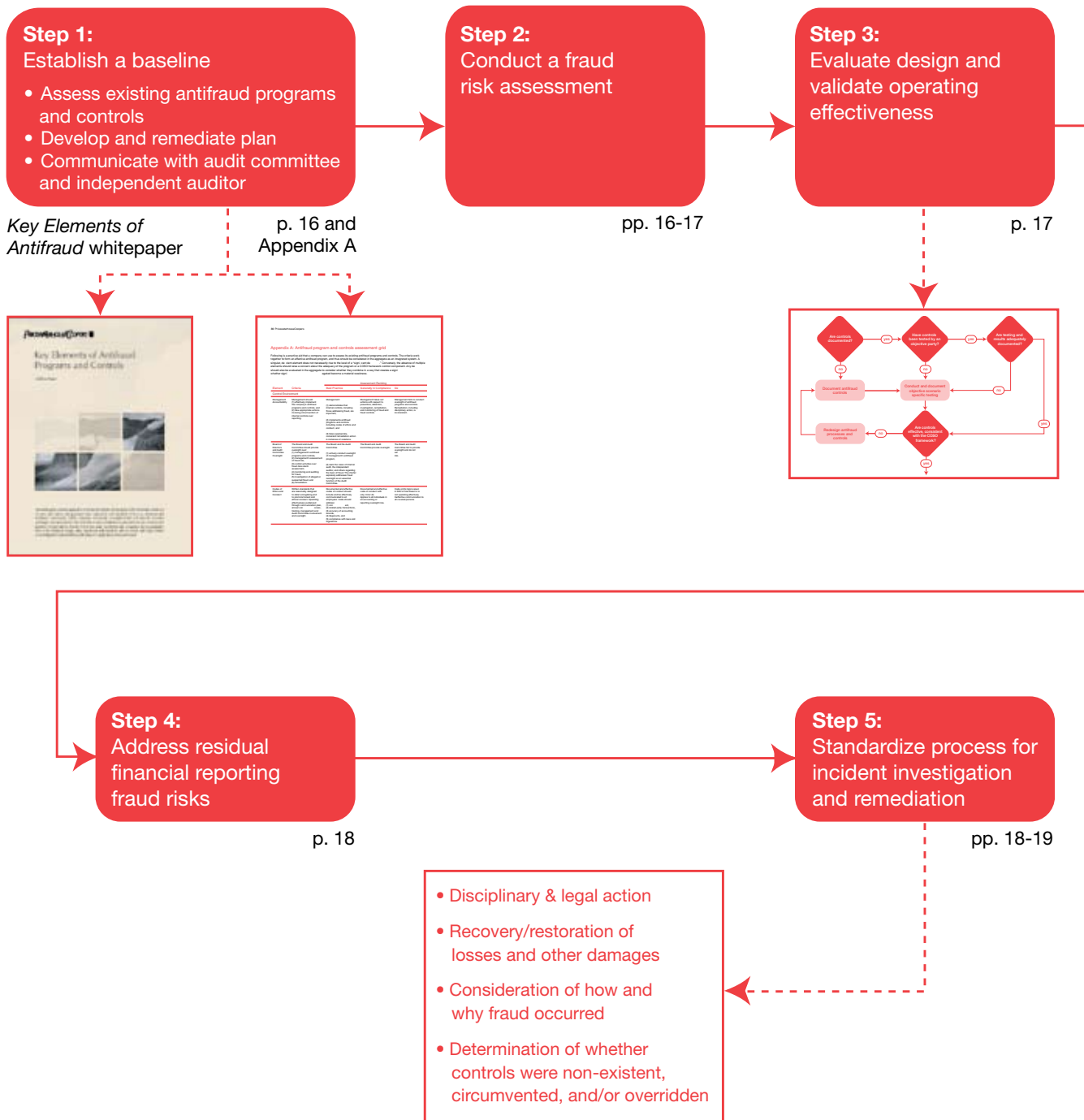
### Computer-Assisted Auditing Techniques (CAATs)

CAATs are essential because of their ability to search massive amounts of data. Historically, due to lack of market demand, however, fraud-related CAATs have not matured to an ideal level of technical sophistication, although a number of CAAT tools are available and substantial research and development is underway. CAATs should be considered an integral part of every fraud audit.

### Targeted testing of transactions

A fraud auditor must also consider targeted (as opposed to random) testing of transactions. For example, a fraud audit targeting improper revenue recognition might focus on round dollar transactions, transactions ending in 999, or transactions occurring after the closing date.

## Appendix E: Antifraud program implementation



## Appendix F: Comparison of antifraud programs and controls and United States Sentencing Guidelines

The following document compares the requirements of an effective compliance program under the amended USSG to the requirements for antifraud programs and controls using the COSO framework. The criteria for both minimal compliance and best practice implementation have been displayed for each element of the COSO framework. Then each element of an effective compliance and ethics program, as dictated by the USSG, was linked to the related element of the COSO framework.<sup>40</sup>

Element	Criteria	Best practice	USSG
<b>Control environment</b>			
Management Accountability	Management should: (1) effectively implement the company's antifraud programs and controls, and (2) take appropriate actions involving circumvention of internal controls over financial reporting.	Management: (1) demonstrates that internal controls, including fraud, are important, (2) implements antifraud programs and controls including codes of ethics and conduct, and (3) takes appropriate, consistent remediation action in instances of violations.	An organization shall exercise due diligence to prevent and detect criminal conduct. ( <b>§8B2.1.a.1</b> )  Specific individual(s) within the organization shall be delegated day-to-day operational responsibility for the compliance and ethics program. Individual(s) with operational responsibility shall report periodically to high-level personnel and, as appropriate, to the governing authority, or an appropriate subgroup of the governing authority on the effectiveness of the compliance and ethics program. ( <b>§8B2.1.b.2.C</b> )
Board of Directors and Audit Committee Oversight	The Board and Audit Committee should provide oversight over: (1) management's antifraud programs and controls, (2) assessment of fraud risk, (3) control activities over fraud risks identified by the assessment, (4) monitoring and auditing for fraud, (5) investigation of alleged or suspected fraud, and (6) remediation.	The Board and the Audit Committee: (1) actively conduct oversight of management's antifraud program, (2) seek the views of internal audit, the independent auditor, and others regarding the topic of fraud. The charter expressly addresses fraud oversight as an essential function of the Audit Committee.	The organization's governing authority shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight with respect to the implementation and effectiveness of the compliance and ethics program. ( <b>§8B2.1.b.2.A</b> )
Codes of Ethics and Conduct	Written standards that are reasonably designed to deter wrongdoing and to promote honest and ethical conduct. Operating effectiveness evidenced through communication plan, annual confirmation process, training, management and Audit Committee involvement and oversight.	Documented and effective codes of conduct should include and be effectively communicated to all employees. Code should address: (1) conflicts of interest, (2) related party transactions, (3) accuracy of accounting records, (4) illegal acts, and (5) compliance with laws and regulations.	An organization shall otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law. ( <b>§8B2.1.a.2</b> )

<sup>40</sup> Here are a few items to note. 1) The references back to where the requirement is stated in the USSG have been included in the chart. These are all in a bold font. 2) All of the elements of the USSG have been mapped to the COSO framework; this helped to ensure completeness. 3) In some cases there is a "many-to-one" relationship between the COSO framework and the USSG requirements. For example, there are five areas on the risk assessment element of the COSO framework. The USSG contains language requires a risk assessment, but it was only mapped to one of the five risk assessment areas even though it really encompasses them all, particularly with regards to best practices.

Element	Criteria	Best practice	USSG
Ethics Hotline/ Whistleblower Program	Documented procedures for the receipt, retention and treatment of complaints and confidential, anonymous submission of concerns by employees or external third parties.	Ethics hotline with a documented process and proven effectiveness as evidenced by employee and external third-party awareness, encouragement of use, and appropriate and timely response. Program operates independently of management and with Audit Committee oversight.	The organization shall take reasonable steps to have and publicize a system, which may include mechanisms that allow for anonymity or confidentiality, whereby the organization's employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation. (§8B2.1.b.5.C)
Hiring and Promotion Procedures	Established standards for hiring and promotion including background investigations and maintenance of all information in the personnel files for all positions of trust in an organization.	For new and promotions of personnel in positions of trust, conduct full-scope background investigations, including interviews with independent references. Similar investigations conducted for strategic third parties such as vendors, joint venture partners, consultants, and customers. All results documented. Background investigations should include educational background, employment history, and criminal record.	The organization shall use reasonable efforts not to include within the substantial authority personnel of the organization any individual whom the organization knew, or should have known through the exercise of due diligence, has engaged in illegal activities or other conduct inconsistent with an effective compliance and ethics program. (§8B2.1.b.3)
Investigative Process	Standardized procedure for tracking, responding to, investigating and assessing allegations of fraud, whether or not material, potentially including a 10A investigation by independent counsel.	Written plan and process for tracking and responding to allegations of misconduct. Where appropriate, investigative process allows for investigation independent of management. Audit Committee and external auditors advised of all significant deficiencies in internal controls and of any fraud involving management or other employees who have significant role in internal controls.	
Remediation	Documented process of assessing and improving relevant internal controls, taking appropriate action against violators and communicating results both internally as well as to the necessary external parties.	Improves relevant internal controls, takes appropriate action against violators and communicates results both internally as well as to the necessary external parties. Evidence and documentation of Audit Committee involvement.	<p>The organization's compliance and ethics program shall be promoted and enforced consistently throughout the organization through (a) appropriate incentives to perform in accordance with the compliance and ethics program; and (b) appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct. (§8B2.1.b.6)</p> <p>After criminal conduct has been detected, the organization shall take reasonable steps to respond appropriately to the criminal conduct and to prevent further similar criminal conduct, including making any necessary modifications to the organization's compliance and ethics program. (§8B2.1.b.7)</p>

Element	Criteria	Best practice	USSG
<b>Risk assessment</b>			
Process for Assessing Risk	Systematic rather than haphazard; considers fraud schemes and circumvention of existing controls; active oversight by Audit Committee.	Fully documents fraud risk assessment process; process includes interviews of personnel at various levels of organization, occurs periodically throughout organization and in response to significant events, e.g., acquisitions, entry into new markets/products; active oversight by Audit Committee.	The organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement set forth in subsection (b) to reduce the risk of criminal conduct identified through this process. (§8B2.1.c)
Frauds Considered	Consideration of fraudulent financial reporting, misappropriation of assets, unauthorized or improper receipts and expenditures, and fraud by senior management should all be demonstrated.	Assesses exposure from each of the categories of fraud risks considered.	
Likelihood and Significance of Fraud	Consideration of the likelihood of each fraud risk as probable, reasonably possible, or remote; consideration of significance of fraud as inconsequential, more than inconsequential or material should be demonstrated.	Evaluates comprehensively the likelihood and significance of each identified fraud risk.	
Consideration of Organizational Levels	Consideration of fraud at the company-wide business unit and significant account levels should all be demonstrated.	Assesses fraud risk at all levels of the organization.	
Circumvention of Controls and Management Override	Effectively designed internal controls should be in place to respond to the assessment of risk of management override.	Audit Committee specifically considers vulnerability of existing controls and risk of management override.	
<b>Control activities</b>			
Linkage with Risk Assessment	Effective control activities should be designed and implemented to mitigate identified fraud risks.	Company links control activities to all identified fraud risks. Active oversight by Audit Committee to ensure design and operating effectiveness.	
<b>Information and communication</b>			
Training	Demonstrated frequency and sufficiency of proper training courses provided to all employees on fraud risk and antifraud programs and controls.	Provides comprehensive and frequent relevant training to all employees. Maintains records documenting types of training and employees trained.	The organization shall take reasonable steps to communicate periodically and in a practical manner its standards and procedures, and other aspects of the compliance and ethics program, to the members of the governing authority, high-level personnel, substantial authority personnel, the organization's employees, and, as appropriate, the organization's agents by conducting effective training programs and otherwise disseminating information appropriate to such individual's respective roles and responsibilities. (§8B2.1.b.4)

Element	Criteria	Best practice	USSG
Knowledge Management	Demonstrated capabilities in place to collect and share information regarding identified fraud risks, strengths and weaknesses of antifraud control activities, allegations of fraud, and remediation efforts.	Clear communication of antifraud policies and procedures flows down, up, and across the organization. Employees fully understand relevant aspects of the antifraud program and understand what behavior is acceptable and unacceptable. Strong knowledge sharing regarding fraud risks, control activities, allegations of fraud, and remediation efforts.	
Information Systems and Technology	Elements that should be addressed are inclusion of technology in management's fraud risk assessment, effective IT security and controls, adequacy of fraud detection and monitoring tools, and ability to investigate computer misuse.	Information systems and technology addresses: (1) consideration of technologically enabled fraud in management's fraud risk assessment; (2) IT security controls, (3) inappropriate modification to computer programs, (4) system override, (5) segregation of duties, (6) adequacy of fraud detection and monitoring tools, and (7) ability to investigate computer misuse.	
<b>Monitoring</b>			
Monitoring by Management	Management should have a process of assessing the quality of the antifraud programs and controls over time through ongoing monitoring activities as well as separate periodic evaluations.	Monitors antifraud controls, programs and policies on an ongoing and periodic basis; management considers possibility of fraud in day-to-day operations; management uses results of fraud assessment and IT system to monitor for fraud.	<p>High-level personnel of the organization shall ensure that the organization has an effective compliance and ethics program, as described in this guideline. Specific individual(s) within high-level personnel shall be assigned overall responsibility for the compliance and ethics program. (§8B2.1.b.2.B)</p> <p>The organization shall take reasonable steps to ensure that the organization's compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct. (§8B2.1.b.5.A)</p> <p>The organization shall take reasonable steps to evaluate periodically the effectiveness of the organization's compliance and ethics programs. (§8B2.1.b.5.B)</p>
Internal Audit Evaluations	The internal audit function in an organization should conduct separate fraud evaluations with a documented plan, approach, scope, and results of review with knowledgeable and experienced staff.	Internal audit actively considers fraud risk in developing audit cycle. Internal audit builds fraud auditing modules into routine audits and special projects. Internal audit includes fraud-experienced internal auditors.	





# PricewaterhouseCoopers Global Transportation & Logistics practice

PricewaterhouseCoopers' Transportation & Logistics practice provides industry-focused assurance, tax and advisory services to over 250 public and private companies. Below is a list of Transportation & Logistics industry leaders.

## Global Transportation & Logistics Leader

Franz-Josef Schwarzhof  
+49 211 981 2902

## European Transportation & Logistics Leader

Andreas Baur  
+41 58 792 51 00

## Transportation & Logistics Business Development and Marketing

Peter Kauschke  
+49 211 981 2167

## Australia

Don Munro  
+61 2 8266 7328

## Belgium

Peter van den Eynde  
+32 3 259 33 32

## Canada

Robert Glenny  
+1 514 205 5119

## China/HK

Alan Ng  
+852 2289 2828

## Denmark

Bo Schou-Jacobsen  
+45 39 45 36 39

## France

Jean-François Châtel  
+33 1 56 57 83 25

## Germany

Klaus-Dieter Ruske  
+49 211 981 2877

## India

Amrit Pandurangi  
+91 11 5135 0505

## Italy

Luciano Festa  
+39 6 57025 2465

## Mexico

Martha Elena Gonzalez  
+52 55 5263 58 34

## Netherlands

Michel Adriaansens  
+31 10 4075 271

## New Zealand

Grant Burns  
+64 9 355 8034

## Central and Eastern Europe

Aleksander Domaradzki  
+48 22 523 4160

## Singapore

Soh Kok Leong  
+65 6236 3788

## South Africa

Akhter Moosa  
+27 12 429 0546

## South America

Henrique Luz  
+55 11 3674 3897

## Spain

Miguel Martin Rabadan  
+34 91 568 4172

## Sweden

Eva Blom  
+46 8 555 333 88

## Switzerland

Andreas Baur  
+41 58 792 51 00

## United Kingdom

Clive Hinds  
+44 1727 89 2379

## United States

Kenneth H. Evans Jr.  
+1 305 375 6307

## PricewaterhouseCoopers Fraud Risks & Controls Practice

PwC Fraud Risks & Controls (FR&C) assists PwC clients and audit teams to mitigate reputation, legal, operational and strategic risk arising from fraud and misconduct. FR&C includes originally-trained accountants, auditors, and investigative attorneys who have been retrained in laws, professional standards, methodology and antifraud technologies to assess fraud and misconduct risk, develop and evaluate antifraud programs and control activities, design fraud audit detection procedures, and standardize processes for incident response and remediation.

**Jonny Frank**

New York, NY, US  
+1 646 471 8590

**Paul Kinney**

Belfast, United Kingdom  
+44 0 28 9041 5514

**Will Kenyon**

London, United Kingdom  
+44 0 207 212 2623

**George Prokop**

Washington, DC, US  
+1 703 918 1148

**Chris Kelkar**

Los Angeles, CA, US  
+1 213 356 6345

**David Jansen**

New York, NY, US  
+1 646 471 8329

**Michael Carey**

Boston, MA, US  
+1 617 530 6487

**Dave Oldham**

New York, NY, US  
+1 646 471 7474

Please visit our website at [www.internalaudit.com](http://www.internalaudit.com).



