

Predicting the unpredictable*

Protecting Aerospace & Defense companies against fraud, reputation and misconduct risk



*connectedthinking

PRICEWATERHOUSECOOPERS 



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. This increased attention to fraud by United States regulators has led to improvements in corporate antifraud programs and provides a good roadmap for others to consider. In short, it is no longer sufficient to simply react appropriately to issues brought to management's attention. Companies should proactively consider fraud risks as part of their antifraud programs and controls rather than passively waiting for government or customer auditors or the press to find fraud or misconduct.

While it may not be possible to eliminate the risk of fraud altogether, with proper planning, policies and procedures, your company can at least identify it early and minimize its damage. Furthermore, the aerospace and defense industry is unique in that the programs are large, competition is high, and the compliance area is complex with significant penalties for non-compliance, creating additional incentives and pressures that can lead to fraud.

This white paper provides step-by-step guidance on how to develop an effective antifraud program. You will learn that an effective antifraud program goes beyond financial statement risk to cover such areas as reputation, operational, legal and strategic risks. In addition, we have provided a summary of fraud schemes that are common to the aerospace and defense industry.

Fraud management makes good business sense. Companies that establish effective antifraud programs will go a long way toward helping to maintain or restore investor confidence in the integrity of a company's financial results. Equally important, reducing fraud will help your company reduce costs, improve profitability, protect its reputation and mitigate liability. We believe this white paper is a valuable blueprint to help you achieve these goals.



Gregg Agens
Global Aerospace & Defense Leader



Jonny Frank
Fraud Risks & Controls Leader

For more information about the services offered by PricewaterhouseCoopers' Global Aerospace & Defense Practice, please visit our website at www.pwc.com/aerospaceanddefence or contact one of the regional professionals listed on the inside back cover of this report.

For more information about our Fraud Risks & Controls practice, please visit our website at www.internalaudit.com or contact one of the Fraud Risks & Controls professionals listed on the inside back cover of this report.

Table of contents

Introduction	1
SEC and Public Company Accounting Oversight Board (PCAOB) require senior management to implement effective antifraud programs and controls	2
Going beyond “Sarbanes” antifraud programs and controls	2
Recent amendments to United States sentencing guidelines requirements of an effective compliance program	3
Common Aerospace & Defense sector fraud schemes	5
Unauthorized receipts and expenditures	6
Financial statement manipulation	7
Misappropriation of assets	10
Aiding and abetting	10
Fraud by senior management or employees with significant role in financial reporting	10
Disclosure fraud	11
Five-step antifraud program implementation plan	13
Step 1: Establish a base line	14
Step 2: Conduct a fraud risk assessment	14
Step 3: Evaluate design and validate operating effectiveness	15
Step 4: Address residual financial reporting fraud risks	16
Step 5: Standardize processes for incident investigation and remediation	16
Mitigating reputation, operational, legal and strategic risks	19
Sarbanes integrated audit reaches only financial reporting risk	19
<i>Reputation risk – Protecting your most precious asset</i>	20
<i>Operational risk – Protecting the bottom line</i>	20
<i>Legal risk – Protecting against criminal, regulatory and civil liability</i>	20
<i>Strategic risk – Protecting the future</i>	21
Leveraging Sarbanes to mitigate other risk at minimal incremental cost	21
Five-step plan for leveraging Sarbanes antifraud program	22
<i>Step 1: Hold individual business unit leaders accountable</i>	22
<i>Step 2: Balance accountability and responsibility</i>	22
<i>Step 3: Expand the scope of the risk assessment</i>	23
<i>Step 4: Don’t just look at financial reporting controls</i>	23
<i>Step 5: Consult your independent auditor</i>	23
Closing thoughts	25
Appendices	27
Appendix A – Antifraud program and controls assessment grid	28
Appendix B – Antifraud program and controls responsibilities matrix	33
Appendix C – Conducting a fraud and reputation risk assessment	37
Appendix D – Fraud auditing process	41
Appendix E – Antifraud program implementation	43
Appendix F – Comparison of antifraud programs and controls and United States sentencing guidelines	44

Introduction

The U.S. Government Department of Defense budget approximates \$500 billion per annum. As government spending has increased, so have prosecutions of contractor fraud. Since 1986, the government has recovered over \$17 billion under the False Claims Act.¹ Headlines of procurement fraud in Afghanistan, Iraq, the War on Terrorism and reconstruction from Hurricane Katrina would indicate that investigations, prosecutions and recoveries will continue.

In July 2002, President Bush established the Corporate Fraud Task Force under the Department of Justice. In less than two years time, the Task Force had obtained over 500 corporate fraud convictions, with corporate fraud charges still pending against more than 900 defendants and 60 CEOs and presidents in connection with over 400 filed cases.

In February 2005, the Justice Department created a Procurement Fraud Working Group led by U.S. District Attorney Paul J. McNulty to supplement other fraud detection initiatives. Aimed at combating fraud among defense and homeland security contractors, Mr. McNulty said, “It is imperative that we take action to prevent, deter and prosecute those unscrupulous contractors whose theft of critically needed resources threatens America’s safety and defense.” Current ideas and initiatives of this working group include:

1. Enhanced efforts to detect ethics violations and conflicts of interest by current and former agency officials.
2. Placement of investigators at major procurement offices to work with agency employees who are directly involved in the negotiation of government contracts.
3. Improved training of special agents and auditors in conducting investigations of procurement fraud, bribery, and conflicts of interest.
4. Use of computer data-mining and other programs to uncover and detect procurement fraud.²

Public outrage over Enron and WorldCom frauds resulted in the establishment of new legislation, regulations and professional standards which focus on prevention and timely detection of fraud. For the first time, corporate fraud is a key agenda item for boards of directors, senior management and independent auditors.

¹ Contractor fraud during the U.S. Civil War resulted in the 1863 enactment of the False Claims Act, including provisions for Qui tam actions (“whistle blowers”). The 1986 amendments to the Act following Justice Department “Operation Ill Wind” investigations increased whistle blower incentives and contractor penalties.

² Paul J. McNulty, “Combating Procurement Fraud: An Initiative to Increase Prevention and Prosecution of Fraud in the Federal Procurement System,” 18 February 2005, U.S. Department of Justice, Eastern District of Virginia.

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

Companies subject to the Sarbanes-Oxley Act (Sarbanes)³ must now implement “antifraud programs and controls.”⁴ Seemingly innocuous, this requirement creates significant 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.⁵

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.⁶ Independent auditors evaluate and test the design and operating effectiveness of antifraud controls as a part of the integrated audit.⁷ Deficiencies in antifraud programs and controls ordinarily result in a finding of a significant deficiency to the Audit Committee.⁸ The auditor must issue an adverse opinion if it concludes that the deficiencies rise to a material weakness.⁹

This white paper focuses on a strategy for developing and implementing effective antifraud programs and controls within the aerospace and defense sector, beginning with an overview of common aerospace and defense sector fraud schemes. The white paper addresses Sarbanes antifraud programs focused 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 includes a grid that enables companies to benchmark individual antifraud program components. Appendix B includes a matrix to assist companies in assigning responsibilities in implementing an antifraud program. 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 white paper, *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” (COSO-Internal Controls) to antifraud programs and controls. Another PwC white paper, *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 white papers can be obtained from PwC's internalaudit.com website.

Going beyond “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 related to internal control over financial reporting focus only on fraud that could result in a misstatement that is more than inconsequential to the company's financial statements.¹⁰ Only controls specifically intended to address the risk of fraud that have a reasonably possible likelihood of having a material effect on the financial statements are considered.

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 to meet Sarbanes-Oxley §404 requirements to address wider-ranging fraud and misconduct risks. However, companies can apply the same implementation plan to design programs and controls to meet all types of fraud and reputation risk.

Fraud drains earnings, exposes companies, senior management and the Board to criminal and civil liability, and, worst, threatens

³ Sarbanes-Oxley Act of 2002, 15 U.S.C. §7201 (2002) (Sarbanes).

⁴ For an in-depth discussion, see PricewaterhouseCoopers white paper, “Key Elements of Antifraud Programs and Controls,” available at www.cfodirect.com/News and Analysis/Corporate Governance/Key Elements of Antifraud Programs and Controls (December 2003).

⁵ 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).

⁶ 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.”

some of aerospace and defense companies' most valuable assets – reputation and brand value. Yet, it was not until the post-Enron environment that many companies paid much attention to fraud risk management. Aerospace and defense companies are more accustomed to the risks of fraud, particularly unauthorized transactions, than many industries, having been the subject of public scrutiny in the past. However, the post-Enron environment has reemphasized the need for vigilance in the prevention of fraud.

At first, companies concentrated exclusively on satisfying regulatory requirements that SEC registrants implement “antifraud programs and controls” as an element of “internal controls over financial reporting.” These initial programs thus focused exclusively on financial statement fraud.

But fraud runs much deeper and wider than whether the financial statements are correct; a fraud can devastate a company, and yet have no financial statement impact. Having satisfied the regulatory hurdle, many aerospace and defense companies are now expanding their antifraud programs to address a broader range of risks: operation, strategic, legal, compliance, reputation as *well as* financial reporting fraud risk. Stated differently, companies are moving from having financial reporting controls that include an antifraud program to having a fraud risk management program, which happens to also meet regulatory requirements for financial reporting controls.

Mature fraud management programs view fraud more opportunistically in addition to managing risk. Fraud management, for example, almost always identifies significant cost savings opportunities. Similarly, aerospace and defense companies expanding to new markets, products and services can leverage antifraud programs and controls to gain a competitive and strategic advantage.

Aerospace and defense companies used to rely upon their security or investigations department for advice on fraud prevention and detection. The growing interest in fraud has given rise to a new specialty – fraud management – which combines a foundation in risk management, controls and auditing with knowledge of how frauds occur at aerospace and

defense companies, coupled with a firm grounding in the indicia of fraud schemes being monitored or audited.

Recent amendments to United States sentencing guidelines requirements of an effective compliance program

Legal and compliance risks, for example, illustrate a fraud and misconduct implication 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 best practices elements.

7 PCAOB Auditing Standard No. 2 Paragraphs 24-28.

8 PCAOB Auditing Standard No. 2 Paragraph 139.

9 PCAOB Auditing Standard No. 2 Paragraph 175.

10 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 considers 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 22-24.



Common Aerospace & Defense sector fraud schemes



The foundation of a successful antifraud program begins with a thorough risk assessment by management and the design and implementation of internal controls to prevent, deter and detect fraud.

PwC's Fraud Risks & Controls Practice organizes fraud and misconduct schemes into six broad categories as seen in the diagram on the left.

The following pages include some of the most common fraud schemes impacting the aerospace and defense sector that management should consider when conducting its risk assessment and evaluating its antifraud programs and controls.

Unauthorized receipts and 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 since 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 since the potential fine, penalty or other sanction could lead to a material misstatement.¹¹

In 1986, the Justice Department started a three-year investigation of fraud in defense procurement, known as Operation Ill Wind, which resulted in the conviction of a number of government officials and civilians. The scandal led Congress to pass the Procurement Integrity Act in 1988, which includes limitations on the pay that procurement officials receive from contractors during the first year of employment after they leave the government, and restricts their ability to provide bid and proposal information to their new employers.

Partly in response to Operation Ill Wind, 32 major defense contractors established The Defense Industry Initiative on Business Ethics and Conduct (“DII”) in June of 1986. DII establishes a code of business ethics and acknowledges the responsibility that defense contractors have to comply with federal procurement regulations as well as their responsibility to the Department of Defense and the public.

However, neither Operation Ill Wind nor DII has eliminated fraud for aerospace and defense companies. In fact, recent high profile procurement violations have rekindled the debate over business ethics. This time, European defense contractors are joining U.S. contractors to consider developing a voluntary code of business ethics which may become a successor to DII. Compliance with federal procurement regulations requires skill and experience, and the avoidance of fraud requires vigilance in the application of corporate antifraud programs.

Bribery of government officials (domestic and foreign) is 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 many aerospace and defense contracts make this industry particularly

susceptible to bribery. Bribery may take forms other than cash payments and can include gifts and favors, including promises of future employment. A company’s use of sales agents or other consultants increases the risk of such payments being made on the company’s behalf. In addition, many companies often do not have mature Foreign Corrupt Practices Act compliance programs.

Commercial bribery may be as significant of a risk as government bribery given the broad, international footprint of the aerospace and defense industry. Commercial bribery can involve any step along the supply and sales chains and takes many forms, including kickbacks to procurement departments or vendors. Commercial bribery can also result in substantial fines or loss of future business.

Failure to submit cost or pricing data that is current, accurate and complete may result in a contract price adjustment, including profit or fee, as government contractors must certify cost or pricing data as a requirement of the Truth in Negotiations Act (TINA). In addition, the government is entitled to penalty amounts and interest from the date of overpayment. Defective pricing results from a failure to disclose factual information that would have a significant effect on price. It includes the underlying factual information of vendor quotes/bids, make/buy decisions, planned M&A activity and changes to production flows that form the contractor’s basis of estimate. In addition to TINA, contractors may be subject to violations of other statutes including false claims, false statements, conspiracy and wire/mail fraud.

Failure to follow accounting practices disclosed in the company’s Cost Accounting Standards (CAS) Disclosure Statement for the measurement, assignment and allocation of costs may result in contract price adjustments. Disclosures that are vague, incomplete or contradictory may lead to a claim against the contractor when found not to follow the government’s interpretation of disclosed practices.

Regulatory reporting requirements for aerospace and defense companies are generally rigorous and range from quality, domestic content requirements, health and environmental concerns, to product safety and labor law compliance. Additionally, many aerospace and defense companies conduct significant business with governments and are held to specific cost and price disclosures or are required to meet specific offset requirements. Documentation may be intentionally inaccurate and records manipulated to avert liability and avoid responsibility. Falsification of records could subject the company to significant fines, criminal penalties and the loss of the ability to continue contracting with certain customers.

¹¹ SEC, Staff Accounting Bulletin 99.

Financial statement manipulation

Improper revenue recognition

Intentional manipulation of cost estimates used in the percentage of completion method of contract accounting can result in overstatement or understatement of profitability in the related periods. The percentage of completion method of contract accounting requires the use of extensive estimates of future revenues and costs over the term of the contract. Cost estimates include many elements, often over an extended period of time, and require significant management judgment. Labor estimates, product warranty and performance guarantees, and estimates of incentive fees are easily susceptible to manipulation.

Intentional manipulation of data used to account for separately priced extended warranty and maintenance contracts for services can result in fraudulent deferral of cost recognition or accelerated revenue recognition. Accounting for these services requires significant estimates of the costs of providing the services and estimates of the expected future pattern of those costs. The timing of such costs is dependent upon the specific characteristics of the product and type of coverage provided by the program.

Improper frontloading of revenue recognition can occur when companies intentionally accelerate revenue recognition on contracts that include software and other licensing agreements by failing to appropriately account for those components of the contracts.

Customer side agreements refer to written or oral agreements made between companies and their customers outside the normal contracting process to modify the original contract terms. Sales personnel could craft side agreements to obtain undeserved incentive compensation, and management may enter into them to inflate or even defer revenue. Furthermore, due to the complexity of aerospace and defense products, development and production delays, as well as customer deferrals, are common, which could result in modification of contract terms that may affect revenue recognition. Side agreements could include changes to payment terms, rights of return, guaranteed prices, performance guarantees and warranties, all of which could call into question the propriety of revenue recognition.

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.

Bill & hold sales schemes, especially those resulting from production delays, are another common method of accounting fraud, bypassing the delivery requirement. As its name implies, a

Improper cost and labor charging are common examples of recordkeeping issues which can result in overcharging customers and improper financial reporting. These include mischarging labor or other costs between job orders, improper labor substitution under time & material contracts, or seeking improper recovery of contract research & development costs through independent research & development cost mechanisms.

Price-fixing occurs when companies conspire to set an artificially high price for a product. The financial impacts of recent price-fixing and bid-rigging cases have been substantial.

Unmonitored business units, such as captive insurance companies or other units not core to the broader company's operations or outside the expertise of corporate management, can be susceptible to violating statutory or company regulations, putting the larger organization at risk.

Improper labor practices are another way to avoid expenses by fraud – whether that means failing to pay the minimum wage under the Service Contract Act, Davis Bacon or Fair Labor Standards, failure to properly record time, failure to properly account for uncompensated overtime, or labor substitution. For example, 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 payments of insurance premiums, is another illustration of costs and expenses avoided by fraud.

Improper product component substitutions occur when manufacturers use unauthorized materials or components, leading to poor quality components and possible safety issues, affecting a company's brand and reputation. The aerospace and defense sector has seen these problems surface in the area of substandard fasteners and other commodity items.

Fraudulent or inadequate documentation of safety logs, including aircraft maintenance logs, safety equipment inspections, and repair and warranty certificates, may put airframe manufacturers and subcontractors at significant risk. Safety issues that could have been avoided by proper maintenance will adversely affect the airframe manufacturer's brand and reputation as much as, if not more than, an airline or maintenance shop that may have been involved in fraudulent reporting of flight hours or service records.

legitimate sales order may be received, processed and readied for shipment even though the customer is not ready, willing or able to accept delivery of the product at that time. For example, a seller holds goods or ships them to a different location, such as a third-party warehouse, until the customer is ready to accept shipment and prematurely recognizes revenue immediately or upon shipment to the interim location, often in violation of generally accepted accounting principles (GAAP).

Contingent sales (e.g., consignment sales) are examples of transactions with contingent events that must be satisfied before revenue can be recognized. Although payment for product by the customer may be contingent upon ultimate use of the products, the supplier may prematurely recognize revenue from the sale up front.

Improper cutoff of revenue recognition by holding the books open for extended time after period end allows companies to record additional end-of-period revenues that are invoiced and shipped after the end of a reporting period. Cutoff issues are often accompanied by spikes in accounts receivable balances at quarter-end and year-end dates; however, such increases in receivable balances may also suggest that management may be manually accruing product revenues before the earning process is complete in contract accounting situations.

Early delivery of product occurs when companies attempt to accelerate shipment to customers before they are ready to receive the goods or before all required delivery criteria are met. While the ability to accelerate revenue recognition in the aerospace and defense industry is possible, such behavior is limited due to the pull-through supply chain model of the industry and the typically stringent customer acceptance terms that exist, especially when conducting business with the U.S. Government.

Trade loading/channel stuffing (e.g., loading the trade or the distribution channel) is not pervasive in the aerospace and defense industry because of the pull-through supply chain model, where most inventory is built to order. However, the opportunity may still exist in certain instances. Channel stuffing is a marketing practice that suppliers sometimes use to boost sales at, or close to, the end of a quarter by inducing downstream purchasers or ultimate customers to buy substantially more inventory than they can reasonably utilize. Under normal circumstances, these types of transactions generally result in proper recognition of revenue when accompanied by fixed and determinable payment terms and transfer of title. In certain circumstances, however, inducements to overbuy may be accompanied by side agreements that allow for certain guarantees or provisions.

In another example, inventory may be shipped in excess of the customer's original order. When the customer later disputes the amount of inventory sent to them (typically in the supplier's subsequent accounting period), the supplier may offer deep discounts on the inventory. In this example, revenue is overstated in one period while the rebate is recorded in the subsequent period. To offset the impact of the rebate recorded in the subsequent period, the supplier may initiate other channel stuffing activities to offset the effects of the rebates and/or inventory returns.

Recording fictitious transactions refers to creating fictitious orders for either existing or fictitious customers. False 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.

Related party revenue transactions are sales between parties that may not be at arm's length. Further, the other party may not have the financial wherewithal to remit payment on a timely basis which also calls into question proper revenue recognition.

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 estimates of product performance guarantees, operating cost guarantees and extended warranty programs can be used to manipulate financial results. Management estimates about the future material and labor costs that will be incurred in connection with future maintenance requirements based on projected product performance involve significant judgment. Other product performance information may be manipulated to avoid necessary accruals.

Fraudulent or improper inventory capitalization refers to inflating inventory by improperly capitalizing certain expenditures—such as abnormal production variances or overhead costs, and selling or maintenance expenses—as part of inventory.

Overstatement of inventory counts refers to over-reporting the amount of inventory on hand to increase the value on the books. This can be done a number of ways, including manipulating the physical inventory records. The most famous scandal involves

the “Salad Oil” swindle and the placement of water into storage tanks filled with salad oil. Other examples include sub-standard product substitutions during the physical inventory process, miscalibration of scales and movement of products during the physical inventory count or failure to record physical inventory adjustments.

Inadequate provisioning for excess or obsolete inventory in the aerospace and defense sector may result when companies overstate projected usage requirements. This issue is exacerbated by the long-term business cycle requiring estimates of spares maintenance requirements over extended service lives of aircraft or other equipment.

Overstatement of trade and unbilled receivables can occur when an entity creates fictitious receivables or capitalizes amounts not recoverable under contracts with customers. In addition, an entity may understate the allowance for doubtful accounts by applying improper estimation 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 result is an artificially inflated net value of accounts receivable.

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. An example of this in the aerospace and defense sector relates to companies improperly capitalizing the value of demonstration units or prototypes. Another example relates to overstatement of overhead and other rates affecting amounts unbilled to customers. Long delays between the initial recording in the financial records and government or customer audit or the passing of other milestones which permit subsequent billing and collection make such activity more difficult to detect.

Understatement of claim or self-insurance liabilities occurs when management intentionally underestimates the anticipated number, and ultimate cost, of accident claims. Due to the nature of the aerospace and defense sector, claim expenses (e.g., property damage, product liability, worker’s compensation, 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 environmental, health and safety compliance issues. Compliance errors can lead to failure to detect environmental risks, which can be costly.

Improper accounting for customer rebates and allowances, including volume and other rebate or discount programs due to customers, might result in an understatement of expenses or may call into question the initial revenue recognition.

Other areas of financial statement manipulation

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 aerospace and defense companies:

- Contract revenues and costs
- Warranty/product performance costs
- Customer programs and incentives
- Pension and other postretirement employee benefit plan accounting
- Accounting for taxes
- Valuation of goodwill or long-lived assets
- Restructuring and severance reserves
- Environmental reserves
- Legal/litigation reserves
- Self-insurance reserves

Inter-company or suspense account activity is not always well controlled, and 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 the transaction between the 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 and other regulators in

recent years, resulting in the release of a number of clarifying standards. For example, Financial Accounting Standards Board (FASB) Interpretation Number 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, insurance contracts and other similar transactions. Companies must pay careful attention to ensure that intentional misstatements do not result from unusual transactions, and that all transactions have appropriate business purposes.

Misappropriation of assets

Many asset misappropriation schemes affect 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 there is no adjustment made and the financial statements erroneously report the inventory.

Industrial espionage illustrates the theft of trade secrets, intellectual property and other soft assets, some of which have recorded financial statement value. Failure to protect classified data may result in loss of contracts or civil/criminal prosecution. Companies may export technology in violation of Export Administration Regulations (EAR) and International Traffic in Arms Regulations (ITAR) in the interest of expanding their business to certain emerging markets.

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.

Cash skimming probably began shortly after the introduction of currency as a form of payment. Companies generally have good controls over the receipt of hard cash. More sophisticated schemes include not recording payments received against the customer's account and then writing off receivable balances left unpaid.

Theft or misappropriation of inventory can be represented in its most basic form as employee removal of existing stock. Thefts of inventory from a stop along the supply chain before it has reached the company and distribution center theft rings represent more sophisticated forms of this fraud.

Sales & marketing fraud results when sales personnel and customers collude to share rebates, promotions and discounts.

Outsourcing fraud is becoming prevalent, particularly with the outsourcing of production to overseas locations. Contract manufacturers misappropriate assets by overstating production, by overproducing and misappropriating the excess, and other schemes.

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.

Aiding and abetting

Aiding and abetting refers to facilitating others to engage in fraud or misconduct. For instance, a subcontractor could help a prime contractor to overbill their customer in a variety of ways. A contractor could receive improper assistance in overcharging a customer from a sister company or other related party through multi-tiered profit arrangements or inflated lease transactions. U.S. law treats the facilitator as if he or she committed the underlying crime.

Over the past several years prosecutors and regulators, as well as private litigants, have placed and continue to place 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 Standard No. 2 provides 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."¹² 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.

¹² PCAOB Auditing Standard No. 2 Paragraph 140.

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

Disclosure fraud

Disclosure fraud occurs if the entity intentionally omits or misstates material information from public filings – whether in the audited financial statements or other parts of the document such as the Management Discussion & Analysis portion of the Annual Report on Form 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 did not conform to GAAP.

Additionally, many companies applying for export credit guarantees in Organisation for Economic Co-operation and Development (OECD) countries have a new requirement to disclose all records of corruption within their ranks. The OECD countries, in an effort to curb corrupt behavior of companies operating in developing countries, have introduced new counter-bribery measures, which would deny export credit guarantees to any company with employees that have engaged in corrupt behavior.¹³

Additional disclosures may include company size, use of domestic products, payments to influence federal transactions, affirmative action compliance and debarment and suspension. In addition to financial penalties, failure to make proper disclosures may result in bid protests or contract terminations.

¹³ Michael Peel and Hugh Williamson, “OECD says companies must reveal record on bribery,” *Financial Times*, 16 May 2006.



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 white paper.

Step 1: Establish a base line

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, multidisciplinary team drawn from internal audit, compliance, ethics and legal. PwC endorses the multidisciplinary 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 aerospace and defense company has some components of an antifraud program in place. Appendix A provides an example of a tool that companies can use to assess their existing antifraud program relative to best practices, general compliance and deficiency levels, based on the new mandates required under Sarbanes and its 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 white paper *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.¹⁴

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 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

¹⁴ 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 almost always serve as an invaluable, yet often ignored, information source.

Assess likelihood

Aerospace and defense companies that have undergone either a Sarbanes review or enterprise-wide risk assessment likely will be familiar with assessing the likelihood of occurrence. For the purposes of this evaluation, likelihood should be considered without regard to controls. PCAOB Auditing Standard No. 2 refers to three levels of likelihood:

- Remote (likelihood of event or future event occurring is slight)
- Reasonably possible (likelihood of event or future event occurring is more than remote, but less than likely)
- Probable (event or future event is likely to occur)

Therefore, the likelihood of an event that is “more than remote” is either reasonably possible or probable. 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. For example, does 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 financial statement impact

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

- Inconsequential
- More than inconsequential
- Material

Prevention 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 impact 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. Therefore, beware of too hastily dismissing a potential event as being clearly inconsequential. Additional guidance about the fraud risk assessment process appears in a separate PwC white paper, *The Emerging Role of Internal Audit in Mitigating Fraud and Reputation Risks*.¹⁵

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 the fraud risk will be adequately mitigated if the identified controls operate as designed. 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.

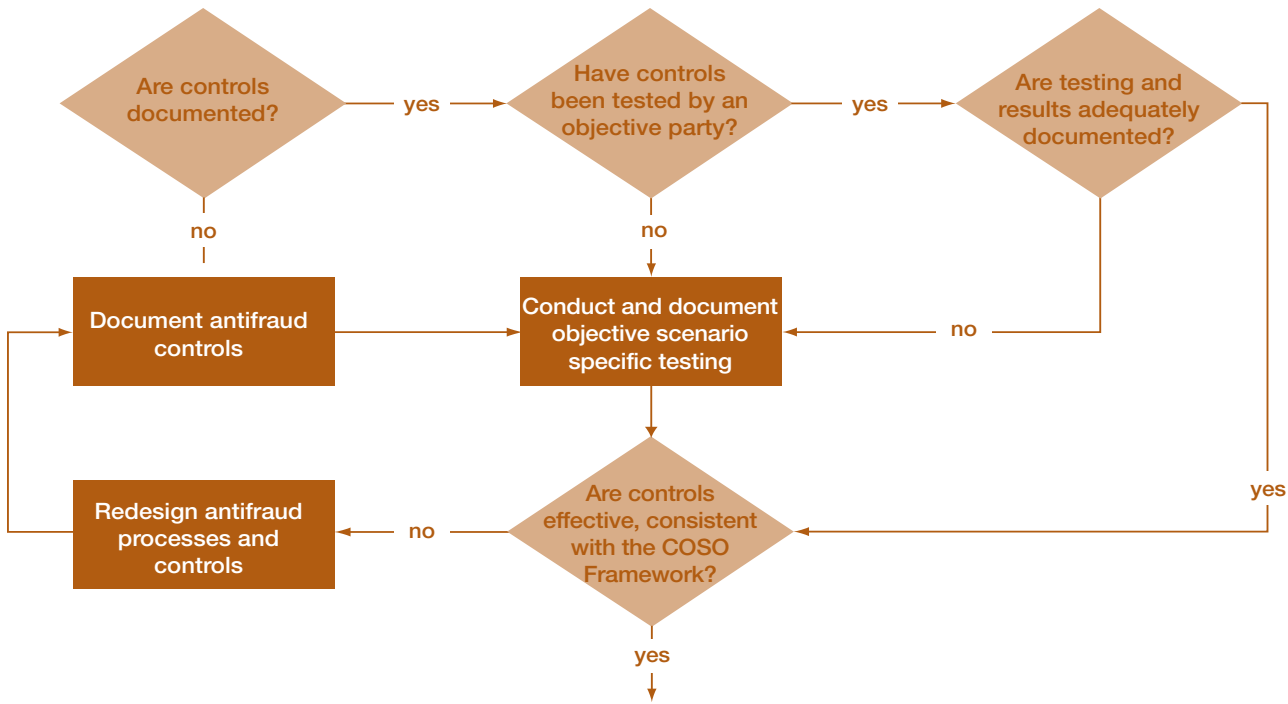
Validating operating effectiveness evaluates whether a properly designed control is not operating as designed and whether the persons performing the control possess the necessary authority, skill and qualifications to perform the control effectively.

Management can evaluate and test their antifraud programs and controls using the workflow on the following page.

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.¹⁶

¹⁵ www.internalaudit.com. See also, J. Frank, “Fraud Risk Assessments,” *Internal Auditor*, April 2004.

¹⁶ 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 Standard No. 2 requires that the independent auditor consider the adequacy of internal audit activities regarding fraud.¹⁷ 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.¹⁸

Step 5: Standardize processes for incident investigation and remediation

Fraud and misconduct are going to occur. Every large aerospace and defense 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. Aerospace and defense 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:

- 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; and

¹⁷ PCAOB Auditing Standard No. 2 Paragraph 24.

¹⁸ PCAOB Auditing Standard No. 2 Paragraph 140.

- A global database that enables the ECO and regional ECC to monitor and oversee all regional investigations, facilitates the investigative work and best practices among the functional subject matter experts, and 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.”¹⁹ 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 the wrongdoers engaged in other, unrelated wrongdoing, and/or whether 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; and
- 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 why the controls failed, and what action has been taken to prevent a recurrence.

¹⁹ PCAOB Auditing Standard No. 2 Paragraph 142(f).



Mitigating reputation, operational, legal and strategic 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, *fall outside* the scope of the audit of internal controls over financial reporting.

Audit committees, management, investors and other stakeholders 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, aerospace and defense 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 2005 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 281 manufacturing and engineering company CEOs responding to that study, 33 percent identified reputation risk as either "one of the biggest threats" (10 percent) or "a significant threat" (23 percent) to their business growth prospects.²⁰

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.²¹ 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) for companies listed over an 11-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).²²

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.²³

Despite the importance of reputation, few companies have a comprehensive framework, approach and infrastructure in place to identify and manage reputation risks, including the evaluation of related controls, to 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 30 percent of the respondents 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.²⁴

A single fraud-related failure can result in a multibillion-dollar loss. In fact, a 2006 study of 1,134 fraud cases by the Association of Certified Fraud Examiners (ACFE) suggested that fraud can cost the typical U.S. organization roughly 5 percent of a company's annual revenues.²⁵ That figure, when applied to the U.S. Gross Domestic Product, translates into a fraud-related loss of approximately \$652 billion for U.S.-based companies in 2005.²⁶ This study also suggested that the median loss for a fraud in the manufacturing and scientific or technical services sectors approximated \$372,000.

Legal risk – Protecting against criminal, regulatory and civil liability

The aerospace and defense sector faces substantial legal and compliance risk. Regulated segments are vulnerable to license suspensions, debarment, fines and other sanctions resulting

²⁰ 8th Annual Global CEO Survey, 2005, PricewaterhouseCoopers.

²¹ R. Alsop, *The 18 Immutable Laws of Corporate Reputation* 10 (2004); G. Dowling, *Creating Corporate Reputations* 12 (2001).

²² G. Dowling, *Creating Corporate Reputations* 16 (2001).

²³ R. Harris, "Picking Up The Pieces," *CFO Magazine*, August 2004.

²⁴ Findings from KPMG's 2003 Fraud Survey.

²⁵ Association of Certified Fraud Examiners: 2006 Report to the Nation on Occupational Fraud and Abuse. The ACFE study involved 1,134 occupational fraud cases reported by certified fraud examiners that involved U.S.-based companies.

²⁶ Based on U.S. Commerce Department first quarter 2006 Gross Domestic Product Growth Estimate.

from fraud and misconduct. Unregulated segments confront potential criminal and civil fines and/or private lawsuits arising from fraud and misconduct.

Aerospace and defense 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**

Aerospace and defense companies must consider fraud and misconduct in developing and executing strategic decisions. For example, they should consider associated fraud and misconduct risks before entering high risk geographic markets or industry segments. And, prior to entering into a merger or acquisition, aerospace and defense companies must consider the risk of becoming associated with individuals or companies that engage 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 Committee of Sponsoring Organizations of 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 using COSO-ERM at minimal incremental cost to address operational, legal, strategic and reputation risks.

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 law²⁷

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.

²⁷ 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 consideration for aerospace and defense 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.

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. The least financially significant business unit might nonetheless pose huge reputation or legal risk. Aerospace and defense companies cannot afford to overlook business units that are immaterial to the financial statements or engage in a non-core business activity.

The identification 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. When identifying such business units beyond those identified for Sarbanes-Oxley purposes, 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 across 148 countries, PwC professionals 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.²⁸

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 impact 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 & 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 existing Sarbanes efforts using COSO-ERM to address all misconduct risk. Steps One and Two recommend obtaining senior management and Audit Committee support to hold individual business unit leaders accountable and form a senior-level, multidisciplinary team. Steps Three and Four 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 Five 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 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 50 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. It 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 are 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.

²⁸ The five components of COSO-Internal Control are 1) control environment, 2) risk assessment, 3) control activities, 4) information and communication and 5) monitoring.

Step 3: Expand the scope of the risk assessment

A Sarbanes fraud risk assessment addresses only financial reporting risks. Expanding the risk assessment to identify potential fraud and misconduct that give rise to reputation, operational, legal, compliance and strategic risk, is the single most important action step.

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 control 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 the majority 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 of 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, compliance, 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 provide an independent perspective, which can be helpful in dealing with government authorities.

The independent auditor, for example, can assist in evaluating the design and validating the operating effectiveness of additional 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.



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 white paper 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 aerospace and defense sector can be classified in the following ways:

- Unauthorized receipts and expenditures
- Financial statement manipulation
- Misappropriation of assets
- Aiding and abetting
- Fraud by senior management
- Disclosur 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 address only those risks that materially impact the financial statements. Equally important risks that exist beyond the scope of the audit of internal controls include:

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

You can leverage existing Sarbanes efforts using 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 companies can use to assess their 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	Best practice	Generally in compliance	Deficient
Control environment				
Management accountability	<p>Management should:</p> <ol style="list-style-type: none"> effectively implement the company’s antifraud programs and controls, and take appropriate actions involving circumvention of internal controls over financial reporting and other fraudulent behaviors. 	<p>Management:</p> <ol style="list-style-type: none"> demonstrates that internal controls, including fraud, are important, implements antifraud programs and controls including codes of ethics and conduct, and takes appropriate, consistent remediation action in instances of violations. 	<p>Management takes sufficient actions with respect to prevention, detection, investigation, remediation, and monitoring of fraud and fraud controls.</p>	<p>Management fails to conduct oversight of antifraud programs and controls. Remediation, including disciplinary action, is inconsistent.</p>
Board of Directors and Audit Committee oversight	<p>The Board and Audit Committee should provide oversight over:</p> <ol style="list-style-type: none"> management’s antifraud programs and controls, assessment of fraud risk, control activities over fraud risks identified by the assessment, monitoring and auditing for fraud, investigation of alleged or suspected fraud, and remediation. 	<p>The Board and Audit Committee:</p> <ol style="list-style-type: none"> actively conduct oversight of management’s antifraud program, and 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. 	<p>Board and Audit Committee provide oversight.</p>	<p>Audit Committee fails to provide oversight and does not sufficiently consider fraud risk.</p>
Codes of ethics and conduct	<p>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.</p>	<p>Documented and effective code of conduct should be effectively communicated to all employees. Code should address:</p> <ol style="list-style-type: none"> conflicts of interest, related party transactions, accuracy of accounting records, illegal acts, and compliance with laws and regulations. 	<p>Documented and effective code of conduct with only minor deficiencies. Applies to all individuals in an accounting or financial reporting oversight role.</p>	<p>Code omits topics specified in SEC’s Final Rules or is not operating effectively. Ineffective communication to all covered persons.</p>

Element	Criteria	Best practice	Generally in compliance	Deficient
Control environment continued				
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 independent 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. Background investigations should include educational background, employment history and criminal record.	For new hires 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.	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 or suspicions 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.

Element	Criteria	Best practice	Generally in compliance	Deficient
Control environment continued				
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.
Risk assessment				
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 impact of fraud	Consideration of the likelihood of each fraud risk as probable, reasonably possible, or remote; consideration of impact of fraud as inconsequential, more than inconsequential or material should be demonstrated.	Evaluates comprehensively the likelihood and impact of each identified fraud risk.	Substantially evaluates likelihood and impact 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 impact considered. Management fails to provide an 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: <ol style="list-style-type: none"> 1. circumvention of controls, and 2. management override.

Element	Criteria	Best practice	Generally in compliance	Deficient
Control activities				
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.
Information and communication				
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.
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: <ol style="list-style-type: none"> 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: <ol style="list-style-type: none"> 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.

Element	Criteria	Best practice	Generally in compliance	Deficient
Monitoring				
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 risk 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: <ol style="list-style-type: none"> 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: <ol style="list-style-type: none"> 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: _____

Element	Criteria	Responsibility				Documentation
		Board of Directors	Management	Internal audit	Other	
Control environment						
Management accountability	<p>Management should:</p> <ol style="list-style-type: none"> effectively implement the company's antifraud programs and controls, and take appropriate actions involving circumvention of internal controls over financial reporting and other fraudulent behaviors. 					
Board of Directors and Audit Committee oversight	<p>The Board and Audit Committee should provide oversight over:</p> <ol style="list-style-type: none"> management's antifraud programs and controls, assessment of fraud risk, controls activities over fraud risks identified by the assessment, monitoring and auditing for fraud, investigation of alleged or suspected fraud, and remediation. 					
Codes of ethics and conduct	<p>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.</p>					
Ethics hotline/whistleblower program	<p>Documented procedures for the receipt, retention and treatment of complaints and confidential, anonymous submission of concerns by employees or external third parties.</p>					

Date of assessment: _____

Element	Criteria	Responsibility				Documentation
		Board of Directors	Management	Internal audit	Other	
Control environment continued						
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 tracking, 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.					
Risk assessment						
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: _____

Element	Criteria	Responsibility				Documentation
		Board of Directors	Management	Internal audit	Other	

Risk assessment continued

Likelihood and impact of fraud	Consideration of the likelihood of each fraud risk as probable, reasonably possible or remote; consideration of impact 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.					

Control activities

Linkage with risk assessment	Effective control activities should be designed and implemented to mitigate identified fraud risks.					
------------------------------	---	--	--	--	--	--

Information and communication

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.					

Date of assessment: _____

Element	Criteria	Responsibility				Documentation
		Board of Directors	Management	Internal audit	Other	

Information and communication continued

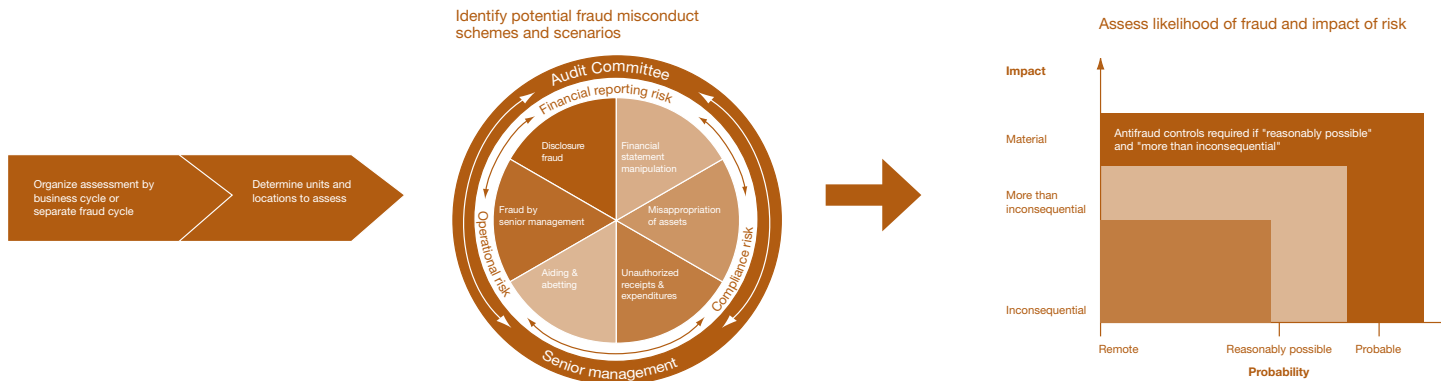
Information system and technology	Elements that should be addressed are inclusion of technology in management's fraud risk assessment, effective IT security and controls, adequacy of fraud detection and monitoring tools, and ability to investigate computer misuse.					
-----------------------------------	--	--	--	--	--	--

Monitoring

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.					

Appendix C – Antifraud program and controls

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.²⁹ 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 in heightened avoidance of legal liabilities, harm to the organization’s reputation and lost productivity.³⁰ 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 & 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.

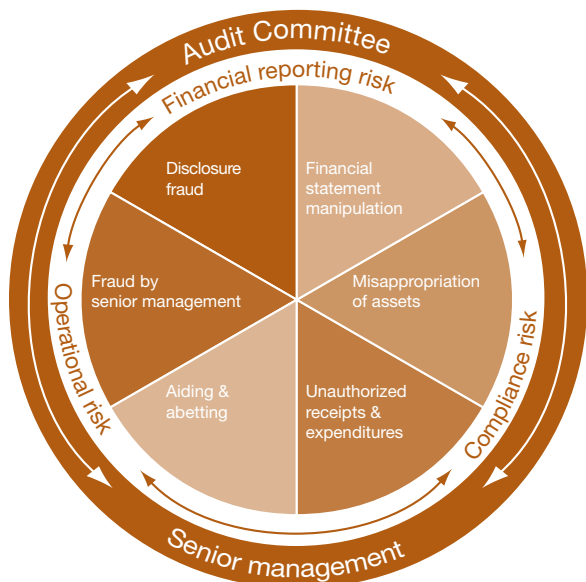
At public companies, the team should liaise with the Sarbanes-Oxley readiness team because of its ongoing work with the organization’s significant business units, accounts and locations. Note, however, the fraud risk assessment process may well require a broader reach, given that reputation risk is not synonymous with financial significance.³¹

²⁹ “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.)

³⁰ “Seizing the Opportunity, Part One: Benchmarking Compliance Programmes,” © 2003 Corporate Executive Board, General Counsel Roundtable.

³¹ 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 misconduct schemes and scenarios



- 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 on the left. 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 an aerospace and defense sector company differ from those affecting a bank or insurance company.

The typical large multinational company, as a result, faces hundreds of fraud and reputation risks. To develop scheme descriptions for aerospace and defense companies requires a deep knowledge of fraud, the industry or industries in which the company operates, and the geographies 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 an expert about how fraud and misconduct occur and can be mitigated. The country manager, for example, 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

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.

Identify potential fraud & 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

32 PCAOB 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.

33 PCAOB Auditing Standard No. 2 Paragraph 9.

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 impact 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:³²

- Remote
- Reasonably possible
- Probable

An organization should address risks that have “a more than 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 impact 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

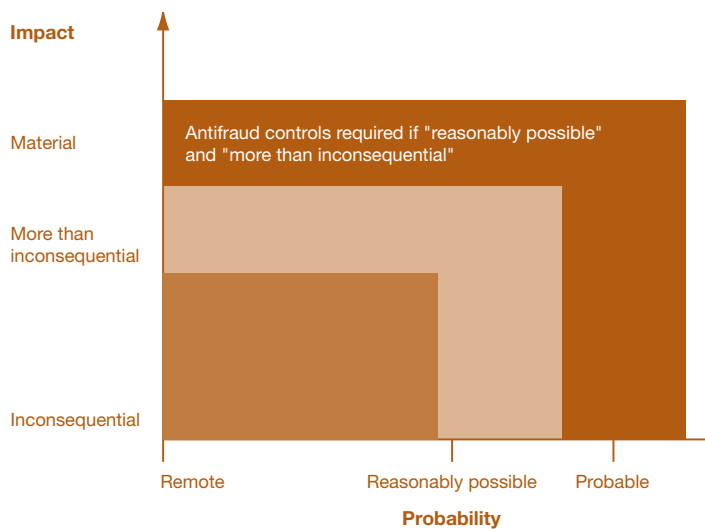
to the financial statements.”³³ The standard further provides, “If a reasonable person could not reach such a conclusion regarding a particular misstatement, that misstatement is more than inconsequential.”

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.³⁴ SEC registrants should note that SEC Staff Accounting Bulletin No. 99 (SAB 99), which provides guidance in determining materiality when fraud is discovered,³⁵ 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 significant on a combined basis.

Aerospace and defense 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.

Assess likelihood of fraud and impact of risk



34 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.”

35 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.

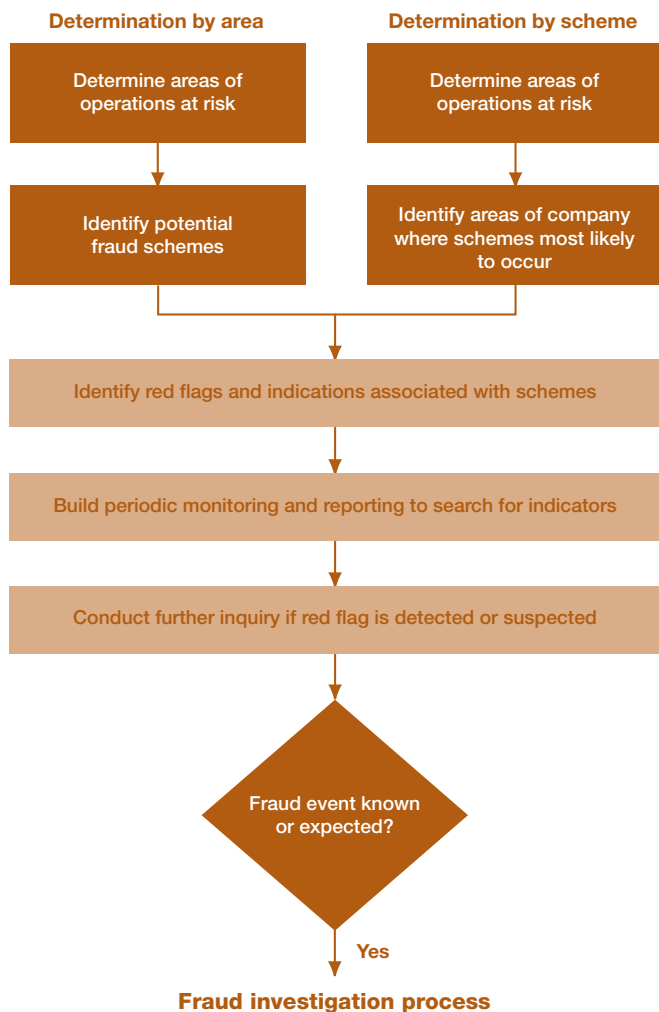
Business unit, process or objective	Fraud category	Fraud scenario	Preventive	Detective
Procurement	Asset overstatement/ liability understatement	Improper change in payment terms	Ability to create or change credit limits and payment terms is restricted to credit personnel and approved by management. §302 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 receivables 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.

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.³⁶ 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 determine 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.

³⁶ PCAOB Auditing Standard No. 2 Paragraph 11.

Appendix D – Antifraud program and controls



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.³⁷

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.

³⁷ 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.

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.

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.

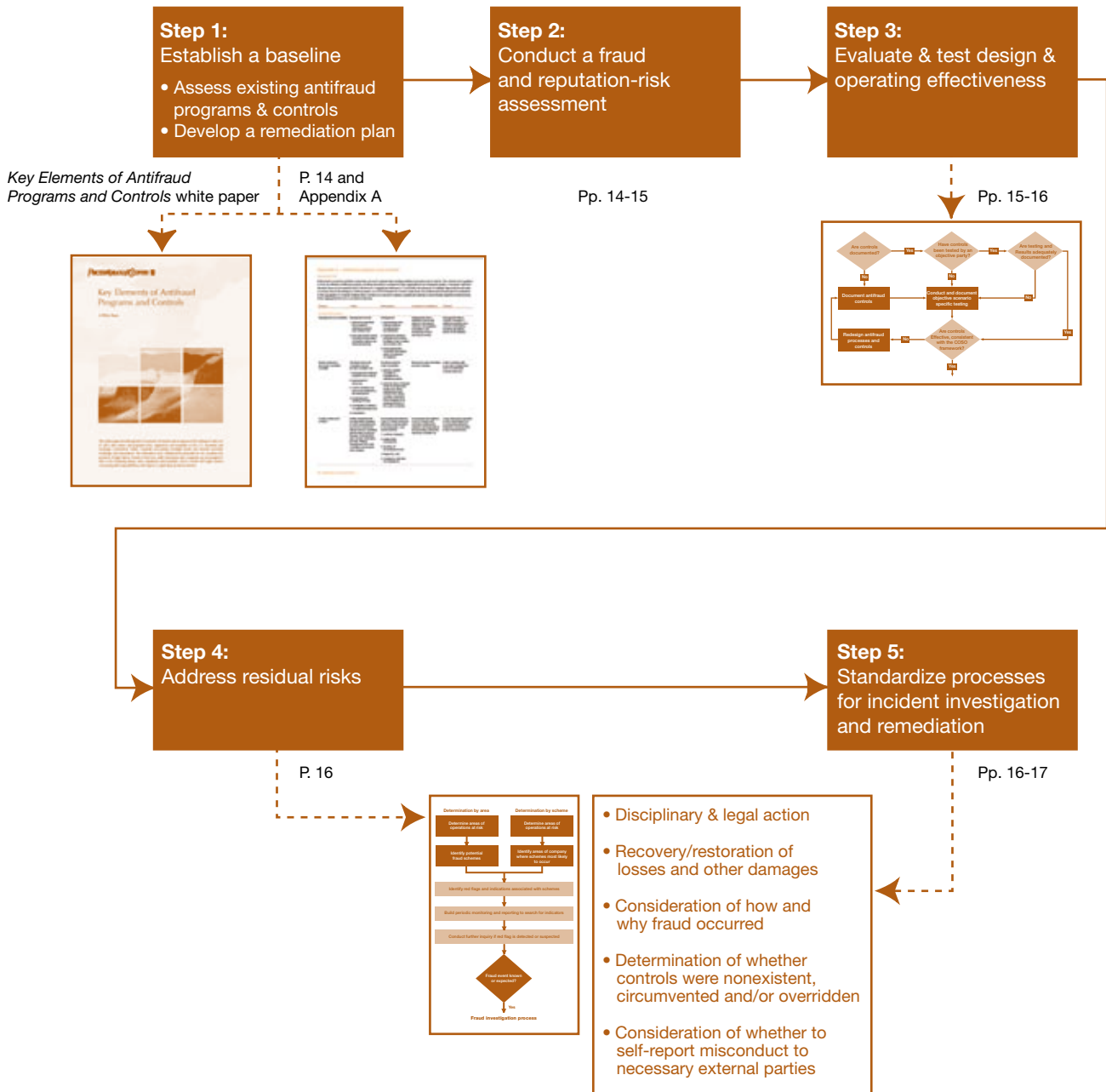
Computer-Assisted Auditing Techniques (CAATs)

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 in amounts just below certain authorization thresholds 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.³⁸

Element	Criteria	Sarbanes best practice	USSG
Control environment			
Management accountability	<p>Management should:</p> <ol style="list-style-type: none"> effectively implement the company's antifraud programs and controls, and take appropriate actions involving circumvention of internal controls over financial reporting and other fraudulent behavior. 	<p>Management:</p> <ol style="list-style-type: none"> demonstrates that internal controls, including fraud, are important, implements antifraud programs and controls including codes of ethics and conduct, and takes appropriate, consistent remediation action in instances of violations. 	<p>An organization shall exercise due diligence to prevent and detect criminal conduct. (§8B2.1.a.1).</p> <p>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. (§8B2.1.b.2.C).</p>
Board of Directors and Audit Committee oversight	<p>The Board and Audit Committee should provide oversight over:</p> <ol style="list-style-type: none"> management's antifraud programs and controls, assessment of fraud risk, control activities over fraud risks identified by the assessment, monitoring and auditing for fraud, investigation of alleged or suspected fraud, and remediation. 	<p>The Board and Audit Committee:</p> <ol style="list-style-type: none"> actively conduct oversight of management's antifraud program, and 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. 	<p>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. (§8B2.1.b.2.A).</p>
Codes of ethics and conduct	<p>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.</p>	<p>Documented and effective codes of conduct should be approved by the Board and/or the Audit Committee, effectively communicated to all employees and confirmed annually with training as appropriate. The codes should be provided to suppliers, customers and other external suppliers as appropriate. The codes should include a description of fraudulent behavior and address compliance with laws and regulations.</p>	<p>An organization shall otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law. (§8B2.1.a.2).</p>

Element	Criteria	Sarbanes best practice	USSG
Control environment continued			
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. Program supported by independent investigations and provides feedback to employees on remediation matters resulting from items reported.	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. Background investigations should include educational background, employment history, and criminal record.	For new hires and promotions of personnel in finance, information technology, sales, procurement and senior management positions, conduct full-scope background investigations, including interviews with independent references. All results documented.	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 or suspicions of fraud, whether or not material, potentially including a 10A investigation by independent counsel.	Written plan provides specific protocol for tracking and responding to allegations of misconduct. Process seeks advice of counsel for difficult decisions. Process evidences active Audit Committee involvement and creates and maintains documentation of the process, proceedings, and resolutions. Process provides for timely follow-up. Where appropriate, investigative process allows for investigation independent of management.	

38 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 italics. 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 that 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	Sarbanes best practice	USSG
Control environment continued			
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.	Provides for consistent actions against violators of policy or those committing fraud, regardless of position in the company. Assesses the need for no-name results to employees. Requires timely follow-up by management on identified control deficiencies contributing to violator's activities. Includes Audit Committee reporting on numbers and types of incidents and actions taken.	<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>
Risk assessment			
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 impact of fraud	Consideration of the likelihood of each fraud risk as probable, reasonably possible or remote; consideration of impact of fraud as inconsequential, more than inconsequential or material should be demonstrated.	Evaluates comprehensively the likelihood and impact of each identified fraud risk.	

Element	Criteria	Sarbanes best practice	USSG
Risk assessment continued			
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.	
Control activities			
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.	
Information and communication			
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).
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.	

Element	Criteria	Sarbanes best practice	USSG
Information and communication continued			
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: <ol style="list-style-type: none"> 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. 	
Monitoring			
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 risk assessment and IT system to monitor for fraud.	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). 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). The organization shall take reasonable steps to evaluate periodically the effectiveness of the organization's compliance and ethics programs. (§8B2.1.b.5.B).
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 Aerospace & Defense Practice

PricewaterhouseCoopers' Aerospace & Defense Practice is a global network of over 70 partners and 2,000 client service professionals who provide industry-focused assurance, tax and advisory services to A&D companies around the world. For example, we provide services to 60 percent of the aerospace and defense manufacturers listed in the *Defense News* Top 100.

Through working with these clients globally and having held senior posts with the sector's major companies, our people can help you deal with the challenges of today's A&D industry.

Our leadership team consists of:

Global Aerospace & Defense Leader

Gregg Agens

Phoenix, AZ, US +1 (602) 364-8290

Aerospace & Defense Client Service Advisor

Jim Thomas

Washington, DC, US +1 (202) 414-1370

United States Aerospace & Defense Leader

Scott Thompson

Hartford, CT, US +1 (860) 240-2153

Aerospace & Defence Industry Analyst

Johnson Imode

London, UK +44 (207) 804 0658

United Kingdom Aerospace & Defence Leader

Ian Chambers

London, UK +44 (0) 20 780 44711

Aerospace & Defense Marketing

Leslie Azia

New York, NY, US +1 (646) 471-0763

France Aerospace Leader

Pierre Chollet

Paris +33 (0) 1 56 57 1218

Anthony White

London, UK +44 (207) 212 4492

France Defence Leader

Stephane Meffre

Paris +33 (0) 1 56 57 8295

Please visit our website at www.pwc.com/aerospaceanddefence

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.

United States

Jonny Frank
New York, NY, US +1 (646) 471-8590

Dave Oldham
New York, NY, US +1 (646) 471-7474

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

Brenda Martin
Chicago, IL, US +1 (312) 298-3163

United Kingdom

Will Kenyon
London +44 (207) 212 2623

Paul Kinney
Belfast +44 (289) 041 5514

India

Vali Nijhawan
New Delhi +91 (11) 5135 0502

South Africa

Colm Tonge
Johannesburg +27 (11) 797 4007

Please visit our website at www.internalaudit.com

Acknowledgements

Special thanks to Paul Bailey, Austin Coventry, Neil Mitchill and Dave Oldham who contributed to the researching and writing of this report and to Leslie Azia and Nancy Newman-Limata for editorial input and review. Thanks also go to the PwC Aerospace & Defense team who provided feedback and to Kimberly Liu for her contribution to the design and publication of this document.

About PricewaterhouseCoopers

PricewaterhouseCoopers (www.pwc.com) provides industry-focused assurance, tax and advisory services for public and private clients. More than 130,000 people in 148 countries connect their thinking, experience and solutions to build public trust and enhance value for clients and their stakeholders.

