The Emerging Role of Internal Audit in Mitigating Fraud and Reputation Risks

Internal Audit Services
# Table of Contents

I. Changing Environment Creates Greater Expectations and Expanding Opportunities for Internal Audit  

II. 10-Step Antifraud Action Plan  

   Step 1: Anticipate Questions and Manage Expectations  

   Step 2: Assess Existing Antifraud Programmes and Controls  

   Step 3: Secure Management and Audit Committee Sponsorship  

   Step 4: Assemble Fraud Expertise within Internal Audit  

   Step 5: Organise a Fraud and Reputation-Risk Assessment  

   Step 6: Link Antifraud Control Activities  

   Step 7: Evaluate and Test Design and Operating Effectiveness  

   Step 8: Refine Audit Plan to Address Residual Risk and Incorporate Fraud Auditing  

   Step 9: Establish a Standard Process for Responding to Allegations or Suspicions of Fraud or Misconduct  

   Step 10: Remediate and Prevent Recurrence  

Appendix A: Antifraud Programme and Controls Assessment Grid  

10-Step Antifraud Action Plan
Changing Environment Creates Greater Expectations and Expanding Opportunities for Internal Audit

A number of significant legal, regulatory and standards-setting actions are combining to pressure all players in the financial-reporting process – from directors and senior management to internal and independent auditors – to step up their efforts to combat corporate fraud and misconduct. Some of these actions have broadened the definition of fraud while others have significantly expanded antifraud responsibilities and placed greater emphasis on preventive and detective measures.

This new legal and regulatory structure does more than encourage companies to consider fraud prevention as part of internal controls. As an example, the final SEC implementation rules require CEOs and CFOs to certify the effectiveness of internal controls over financial reporting and disclosures on a quarterly basis. The rules further require management to evaluate and test its internal controls over financial reporting – including its antifraud programmes annually. Management’s annual certification must then be attested to by the independent auditor. Within this regime, a scenario can easily be foreseen where executives who have certified internal controls will be asked to answer for fraudulent activities, misconduct and losses discovered subsequent to their certification. Clearly, in this example, management can anticipate defending the veracity of their certifications in the shadow of antifraud controls subsequently proven to be ineffective.

For internal audit, this environment poses both opportunities and challenges. Corporate auditors who move quickly to develop antifraud action plans (see PricewaterhouseCoopers’ 10-Step Antifraud Action Plan on page 9) will find ample ways to provide added value to their organisations. Conversely, internal audit directors who fail to address rising stakeholder expectations jeopardise their relevance and imperil their job security.

What’s new in today’s more demanding antifraud environment, and why should recent developments be of concern to internal audit professionals?
Changing Legislative and Regulatory Landscape

Sarbanes-Oxley and corresponding regulatory changes have raised the stakes for senior management and the board of directors, who must now view fraud and misconduct as a broad-based threat and address fraud issues in far greater detail. CEOs and CFOs who certify internal controls only to subsequently discover significant fraudulent activity face the loss of reputation and career as well as the potential for harsh punitive measures.

Public Companies Must Implement Antifraud Programmes and Controls

Although federal law previously required public registrants to maintain internal controls, Sarbanes-Oxley now requires management to assert annually as to the effectiveness of those controls. In addition, Securities and Exchange Commission (SEC) rules implementing §404 of Sarbanes-Oxley 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. This requirement, buried within the regulation¹, represents a sea-change: Compliance alone is insufficient; public registrants must now take affirmative, timely action to prevent and detect fraud and misconduct. In today's business environment, an organisation that engages in misconduct may find itself liable on two bases – once for the commission of the offence and again for failing to have controls in place to prevent and timely detect its occurrence.

¹ 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 [footnote omitted]”
New Auditing Standards Require Independent Auditors to Evaluate “Sufficiency” of Internal Audit Activities Related to Fraud

Sarbanes-Oxley created the Public Company Accounting Oversight Board (PCAOB) to regulate public auditing firms. At first blush, the actions of the PCAOB would seem irrelevant to the internal audit function, as it is beyond the jurisdiction of the PCAOB. However, this is not the case. The PCAOB’s proposed auditing standards require independent auditors to evaluate and test the design and operating effectiveness of programmes and controls intended to mitigate the risks of fraud. This evaluation must assess the “[a]dequacy of the internal audit activity and whether the internal audit function reports directly to the audit committee, as well as the extent of the audit committee’s involvement and interaction with internal audit…” Further, PCAOB Auditing Standard No. 2 mandates that the independent auditor cite, at a minimum, “significant deficiency”, and notes that it is a strong indicator of a material weakness if the independent auditor determines the internal audit or risk assessment function to be ineffective.

In short, the PCAOB proposes that independent auditors evaluate the fraud-related activities of an internal audit function on an annual basis. If this evaluation finds an internal audit function to be deficient, the independent auditor must, at a minimum, issue a finding of a significant deficiency to the audit committee. The auditor must issue an adverse opinion if it concludes that the deficiencies rise to a material weakness.

COSO is King

Most companies and auditors in the United States use the COSO framework, authored by PricewaterhouseCoopers, to assert and audit the effectiveness of internal controls. COSO has five key components – control environment, risk assessment, control activities, information and communications, and monitoring. Antifraud programmes and controls must meet each of these components to avoid a finding of a significant deficiency, or worse, a material weakness, in internal controls.

A previous PricewaterhouseCoopers white paper, Key Elements of Antifraud Programmes and Controls, applies each of the five COSO elements to antifraud programmes and controls. In addition to addressing design and operating effectiveness, the white paper provides legal references and lists circumstances that, in and of themselves, are strong indicators of significant deficiencies. Copies of the white paper can be obtained from www.cfodirect.com.

---


3 PCAOB Auditing Standard No. 2 ¶ 140

4 PCAOB Auditing Standard No. 2 ¶ 175

5 www.cfodirect.com / News and Analysis / Corporate Governance / Key Elements of Antifraud Programmes and Controls – 08 Dec 03
Changing Perspective

Companies historically have not viewed fraud prevention as a primary objective of internal control activities. Antifraud initiatives generally were an implicit facet of compliance activities as opposed to part of an explicit programme directed specifically at fraud concerns.

Now, however, control factors are rapidly replacing compliance concerns as the primary drivers of antifraud programmes; in today’s business environment, fraud is a heightened concern for all companies, public and private.

In the past, senior executives, shareholders, auditors and regulators alike tended to view fraud and misconduct as anomalies – infrequent failures of internal controls. As a result of the large number of corporate scandals reported in the early 21st century, however, fraud and misconduct have evolved into mainstream risks linked closely to market, credit, and legal risks as well as risks to reputation.

A 2004 CEO survey conducted in association with the World Economic Forum reflects just how seriously fraud and reputation risk is perceived by executive management. Of the 1,400 CEOs taking part in that PricewaterhouseCoopers study, 35% identified reputation risk as either “one of the biggest threats” (10%) or “a significant threat” (25%) to their business growth prospects6.

And as indicated by the spate of major frauds in recent years, a single fraud-related failure can result in a multibillion-dollar loss. In fact, a 2002 study of 663 fraud cases by the Association of Certified Fraud Examiners (ACFE) suggests that fraud can cost roughly six percent of a company’s annual revenues7. That figure, when applied to the U.S. Gross Domestic Product, translates into a fraud-related loss in the neighbourhood of $600 billion for U.S.-based companies in 2002 – about $4,500 per employee.

---

7 Association of Certified Fraud Examiners: 2002 Report to the Nation on Occupational Fraud and Abuse. The ACFE study involved 663 occupational fraud cases reported by certified fraud examiners that involved U.S.-based companies.
Changing Mindset

Today’s antifraud environment is also characterised by a decided shift from compliance-driven identification and investigation of incidents to proactive prevention and detection embedded into an organisation’s internal controls.

With a compliance-driven approach, the United States Federal Sentencing Guidelines (FSG) serve as the primary benchmark of compliance programme effectiveness. The Guidelines are reactive: they address punitive implications after an occurrence of fraud or other form of corporate misconduct. A negative event of this sort is typically the impetus for an external party (usually the government or criminal defence counsel) to evaluate and test the effectiveness of an FSG-based compliance programme.

In today’s marketplace, however, traditional approaches to compliance are increasingly viewed as being inadequate. For example, a global survey of 160 financial-institution executives conducted in June 2003 by PricewaterhouseCoopers and the Economist Intelligence Unit (EIU) concluded that compliance is a serious gap at the centre of risk management that needs to be bridged and closed. According to the survey analysis, a new, stakeholder-focused, prevention-oriented vision of compliance is needed to bridge this gap. This new vision approaches compliance with financial and operational policies and procedures, as well as commitments to stakeholders, as seriously as it approaches legal and regulatory mandates.

To a growing extent, regulators and investors are now demanding proactive antifraud programmes characterised by a strong focus on the prevention and timely detection of fraud. New legislative and regulatory actions place greater emphasis on internal controls and, in particular, the COSO control framework, authored by PricewaterhouseCoopers and issued in 1992 by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission.

The FSG and COSO frameworks share many attributes. The FSG, which were drafted by lawyers, emphasises governance and “softer” elements, such as training, communications and delegation of authority. COSO considers these same issues under “control environment,” and places additional emphasis on risk assessments, controls and monitoring and auditing.

In December 2003, the United States Sentencing Commission proposed far-reaching changes that would narrow the differences between the FSG and COSO. Specifically, the proposed amendments provide for companies to conduct ongoing risk assessments to form the basis for continuous improvement.

---

8 The PricewaterhouseCoopers/EIU survey, which included executives from 160 financial institutions in North America, Europe and Asia, was conducted in June 2003; copies of results are available at www.PricewaterhouseCoopers.com.


10 PricewaterhouseCoopers has drafted a new set of COSO guidelines – Enterprise Risk Management Framework – which was released for public comment in October 2003. The draft framework emphasises the critical role played by governance, ethics, risk and compliance in enterprise risk management. Copies of the exposure draft are available at www.erm.coso.org.
Changing Expectations of Internal Audit

Of all the players in the financial-reporting supply chain, internal audit is quite possibly the group most affected by the new emphasis on fraud prevention and detection. Internal audit is uniquely *juxtaposed between the audit committee and senior management*, having either a direct or dotted-line relationship to both groups.

Although antifraud roles vary from one organisation to another, there is general agreement that top management *owns* the antifraud responsibility, members of the audit committee provide *active oversight* of antifraud efforts, and internal audit serves as a *critical line of defense* against the threat of fraud, with a sharp focus on risk-monitoring as well as fraud prevention and detection.¹¹

Fraud in many circles is the proverbial hot potato – *too blistering to handle*. Senior management and the audit committee are likely to toss much of the operational responsibility for fraud monitoring to internal audit. High priority is being placed on the need for *internal audit risk assessments* and *fraud audits*, demands that will pressure internal audit to adjust its skill sets accordingly. When incidents of fraud do occur, the audit committee, the CEO and CFO all stand in the direct line of fire from both prosecutors and regulators seeking to determine why a given fraud was neither prevented nor detected earlier. While internal audit may not stand directly in the line of fire, it will share directly in the consequences of failed antifraud programmes. Furthermore, internal audit is likely to take the lead in investigation of reported incidents.

¹¹ *“Management Antifraud Programmes and Controls – Guidance to Help Prevent, Deter and Detect Fraud”* is an exhibit to SAS (Statement on Auditing Standards) 99: Consideration of Fraud in a Financial Statement Audit, published by The Auditing Standards Board in October 2002. The exhibit, which provides examples of antifraud programmes and controls, was co-authored by The Institute of Internal Auditors (IIA) as well as the American Institute of Certified Public Accountants (AICPA), the Association of Certified Fraud Examiners, Financial Executives International (FEI), the Information Systems Audit and Control Association, the Institute of Management Accountants, and the Society for Human Resource Management.
Changing Expectations of Internal Audit – Prevention and Detection of Fraudulent Financial Reporting

An example of how expectations of internal audit are shifting in response to the new environment is in prevention and detection of fraudulent financial reporting.

In the past, many internal audit groups have focused their resources and efforts primarily on the detection of frauds involving the misappropriation of assets. Assessment of risks associated with fraudulent financial reporting and the detection of financial statement fraud have often been left to be addressed by the independent auditor.

In the new environment, management can no longer rely on the work of the independent auditor as a basis for certifying the effectiveness of internal controls over financial reporting. In many organisations, management will look to internal audit to ensure that fraudulent financial reporting risks are addressed through antifraud efforts.

As a result, many internal audit groups will need to strengthen skills necessary to assess the risks of financial statement fraud. The skills necessary will include an understanding of financial reporting standards, skill sets that may have atrophied given the historical focus on the misappropriation of assets.
Changing Opportunities for Internal Audit

For internal audit groups, the fight against fraud has a silver lining. By reducing fraud, a company can cut costs and improve profitability, and to the extent that internal audit can strengthen an antifraud effort, it will create significant organisational value.

According to industry research, antifraud programmes can more than pay for themselves. A major study of the insurance industry, for example, demonstrated that for every dollar invested in antifraud programmes, the return on investment was nearly $7.\(^{12}\) Likewise, a separate benchmarking analysis and research by the General Counsel Roundtable\(^ {13}\) found that each additional dollar of compliance spending saves organisations, on average, $5.21 in heightened avoidance of legal liabilities, harm to the organisation’s reputation and lost productivity. That’s more than a five-to-one payback per dollar of compliance investment.

Changing Roles and Responsibilities

As part of the post-Enron fallout, a series of legislative and regulatory actions have combined to clarify the antifraud roles and responsibilities of principal corporate players.

The board of directors and, in particular, the audit committee, actively oversee the internal controls over financial reporting established by management as well as the process by which management satisfies itself that these controls are operating effectively. Board oversight must be active, not passive, and should extend to:

- Management’s antifraud programmes and controls, including management’s identification of fraud risks and implementation of antifraud measures
- The potential for management override of controls or other inappropriate influence
- Mechanisms for employees to report concerns
- Receipt and review of periodic reports describing the nature, status and eventual disposition of alleged or suspected fraud and misconduct
- An internal audit plan that addresses fraud risk and a mechanism to ensure that internal audit can express any concerns about management’s commitment to appropriate internal controls or to report suspicions or allegations of fraud
- Involvement of other experts – legal, accounting and other professional advisers – as needed to investigate any alleged or suspected wrongdoing brought to their attention

---

\(^{12}\) “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)

\(^{13}\) “Seizing the Opportunity, Part One: Benchmarking Compliance Programmes”, © 2003 Corporate Executive Board, General Counsel Roundtable.
Management is responsible for the design, implementations and execution of the organisation’s antifraud programs and controls. Management must assess fraud risk at the company-wide, business-unit and significant-account levels as well as attest to the quality of the company’s antifraud controls.

Independent Auditors have two, interrelated roles. In their traditional role as auditors of financial statements, independent auditors must plan and perform audits to obtain reasonable assurance that financial statements are free of material misstatements due to fraud or error. And, in their new role as auditors of internal controls over financial reporting, independent auditors must evaluate antifraud programmes and controls, a process that includes an annual examination of the effectiveness of their clients’ internal audit functions. These two functions are interrelated – both SAS 99 and the proposed PCAOB standards provide that auditor evaluation of the control framework necessarily impacts upon the substantive auditing procedures.

The role of Internal Audit will vary – depending on organisational needs, internal audit structure and available competencies. However, this role will likely include:

• Supporting management to construct an auditable antifraud process and programme

• Facilitating fraud and reputation-risk assessments at the corporate, management-unit and business-process levels

• Linking (and documenting) antifraud control activities to identified fraud risks

• Evaluating and testing the design and operating effectiveness of antifraud programmes and controls

• Fraud auditing

• Leading or supporting investigations into alleged or suspected fraud or other misconduct

• Leading or supporting remediation efforts

• Reporting to the Audit Committee about the organisation’s efforts to prevent, detect, investigate and remediate fraud
I. 10-Step Antifraud Action Plan

Given today's environment, a prudent internal audit group will seek to capitalise on antifraud-related opportunities and minimise downside risks. To achieve such a best-of-both-worlds positioning, we advise internal audit functions to develop a strategic and comprehensive planning document to address the role of internal audit in your organisation's antifraud effort. We recommend you consider the following steps in the development of an antifraud action plan.

Step 1: Anticipate Questions and Manage Expectations

Sooner or later, with antifraud efforts rising in importance, an internal audit department should expect to hear the following types of questions from management, the audit committee, or the independent auditor:

- What are the company's fraud and reputation risks?
- What programmes and controls have been implemented to mitigate these risks?
- What is internal audit doing to prevent and detect issues before they emerge into a corporate scandal?

At public companies, such questions are likely to come sooner rather than later, so a proactive internal audit function will anticipate such queries and develop appropriate responses.

It's also critical for internal audit groups to establish and maintain solid lines of communication with senior management and the audit committee. Above all, internal audit needs to discuss and understand the expectations of its primary stakeholders and align its activities to address these expectations.

With the continuing flood of new revelations about corporate fraud, difficult questions are being raised within the investment and financial communities with respect to the role of independent auditors in identifying and preventing fraud. Such questions have contributed to a troublesome gap between the expectations of investors and financial professionals when it comes to the fraud-related roles of independent auditors and their actual roles, in keeping with professional standards. This expectation gap stems, in part, from confusion surrounding the roles of management, the Board and the independent auditor in combating fraud.

It's in the best interests of the internal audit community to avoid creating the kind of long-term “expectation gap” that has plagued the external auditing profession in the fraud arena.
Step 2: Assess Existing Antifraud Programmes and Controls

Virtually every public company already has some components of an antifraud programme in place. Appendix A is an example of a tool to assist you in assessing your company’s antifraud programme.

In many cases, a company will need to take supplemental action to avoid significant deficiencies or material weaknesses. Areas likely to require remedial action, as described in greater detail in PricewaterhouseCoopers’ previous white paper on the elements of an effective antifraud programme\textsuperscript{14}, include the following:

**Fraud Risk Assessments**

How can companies develop effective programmes and controls to mitigate fraud and reputation risk without first identifying the risks that they need to mitigate? Nonetheless, companies rarely commission a proper fraud and reputation-risk assessment.

Fraud and reputation-risk assessments are the cornerstones of an antifraud programme that anticipates, rather than reacts to, fraud and misconduct. Because management and the board likely will turn to internal audit to perform this function, this paper includes a step-by-step guide to performing a fraud risk assessment as well as schematic pull-out illustrating the assessment process.

**Linking Control Activities to Identified Fraud Risks**

Just as companies rarely perform fraud and reputation-risk assessments, they rarely link preventive and detective control activities that mitigate identified risks. Once the fraud and reputation-risk assessment has taken place, the organisation will need to identify, evaluate and test the design and operating effectiveness of its antifraud control activities. Public companies likely will find that it is most efficient to integrate this process with their Sarbanes §404 project planning.

**Fraud Monitoring and Auditing**

Although monitoring and auditing are integral to the COSO framework, public companies rarely monitor or audit specifically for fraud. With some facilitation from internal audit, fraud monitoring can become an integral part of day-to-day operating activities. In addition, internal audit departments must address fraud risk in planning and executing the annual internal audit cycle.

---

\textsuperscript{14} www.ciodirect.com / News and Analysis / Corporate Governance / Key Elements of Antifraud Programmes and Controls -- 08 Dec 03
Step 3: Secure Management and Audit Committee Sponsorship

While ultimately senior management will own antifraud responsibility, we anticipate many companies will toss operational responsibility for antifraud efforts directly to internal audit. Effectively handling the hot potato of antifraud efforts will demand the active sponsorship of senior management and the audit committee. Before accepting operational responsibility for antifraud efforts, internal audit needs to engage senior management and the audit committee in the antifraud effort and persuade its overseers to take strong ownership of the antifraud programme. Developing and enhancing antifraud programmes and controls will flow more smoothly if the organisation understands that senior management and the audit committee are active sponsors of the activity.

Internal audit, moreover, must persuade management of individual business units to take ownership of the fraud and reputation risks affecting their areas. The responsibility to manage fraud and reputation risk cannot be left to a corporate shared-services centre.

With strong backing from the board and management, internal audit is better able to unearth critical information about the organisation’s fraud risks. In many instances, it is middle management and mid-level employees running day-to-day businesses who know where potential risks and skeletons lie.

Obviously, unlocking such information can be tricky, due to fraud-related sensitivities and natural reluctance to talk about the subject. Employees and executives alike can be hesitant to furnish information because they fear suspicion, want to avoid the corporate spotlight, or are harbouring someone’s misconduct (their own, perhaps). As a result, internal audit can be hard-pressed to overcome this hesitancy without the active support of management and the board.
Addressing Resistance

Try these techniques, if you run into resistance from management or the board:

Establish a Dialogue
Fraud, albeit sensitive, is an interesting subject for discussion. Internal audit can quickly engender interest by engaging in one-on-one discussions with your general counsel, director of compliance, or the heads of business units and processes.

To reach a larger audience on antifraud issues, internal audit can publish a newsletter periodically or establish a centre of excellence focusing on fraud. Such vehicles can bring the risks of fraud and misconduct closer to home, making fraud more tangible and less abstract. For example, publishing information about fraud and misconduct occurring within your same industry or geography will naturally lead company officials to question the vulnerability of your company to similar conduct.

Leverage and Engage Sarbanes-Oxley §404 Readiness Projects
Companies lacking effective antifraud programmes and controls will likely be cited for a “significant deficiency” and, quite possibly, a “material weakness” by its independent auditor. A material weakness translates into an adverse opinion about the organisation’s controls. Thus it’s important for internal auditors of public companies to coordinate their fraud-risk assessments with the organisation’s Sarbanes-Oxley readiness effort. At large multinational organisations, in particular, such coordination will also help simplify the process, for Sarbanes-readiness projects identify the company’s significant business units, processes, and locations – information that internal audit can leverage to frame the scope of the organisation’s antifraud effort. In addition, Sarbanes-readiness projects also inventory the organisation’s existing control activities, providing a resource for internal audit to draw upon in linking fraud risks to controls.

Ask Your Independent Auditor for Input
Independent auditing firms are much more focused on fraud as a result of SAS 99, the proposed PCAOB standards, and the legal and reputation risks flowing from the early 21st century corporate scandals. For example, independent auditing firms are developing policies and procedures for Sarbanes-Oxley §404 audits of internal controls. Talk with your independent auditor; ask to speak to their fraud subject-matter experts; and determine your independent auditor’s expectations with respect to the role of internal audit in your organisation’s antifraud effort.

(continued next page)
Host a Fraud Summit

A number of PricewaterhouseCoopers’ clients have adopted the fraud summit technique, with great success. Although members of C-suites and audit committees are concerned about fraud and reputation risk, they rarely discuss these subjects in an organised manner. A fraud and reputation-risk summit provides a dedicated forum for internal audit to facilitate discussion among senior management and audit committee about fraud and risk issues.

Fraud summits can range from 2-4 hours at your corporate headquarters to an offsite retreat. But irrespective of duration, the summit is likely to represent the single greatest opportunity for management to focus directly on the subjects of fraud and reputation risk.

Playing a key role in a fraud summit is one of the best ways for internal audit to demonstrate its capability and willingness to assume a leadership role in your organisation’s efforts to mitigate fraud and risks to reputation. Ideally, internal audit will help organise the summit as well as develop content and facilitate discussion.

A cautionary note: Make the summit an ongoing event. Find reasons to continue the dialogue, perhaps through an internal newsletter, and for the group to meet periodically. Conclude by establishing agreed-upon next-steps and assigned responsibilities.

Step 4: Assemble Fraud Expertise within Internal Audit

The independent auditor’s evaluation of the adequacy of internal audit’s fraud-related activities will, of necessity, consider the depth of fraud expertise within or available to the department. In this respect, IIA (Institute of Internal Auditors) standards mandate that internal auditors have at least a basic knowledge about fraud.16

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 organisation 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 of fraud auditing and forensic investigation techniques.

16 Institute of Internal Auditors, “International Standards for the Professional Practice of Internal Auditing.” §1210
For most internal audit functions, many of these skill sets will be new, for up to 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, an organisation cannot achieve needed skills and expertise by simply hiring an investigator or former law enforcement agent.

To obtain the resources it needs to address antifraud and risk mitigation concerns, internal audit departments can pursue a number of options. Some larger internal audit functions are creating internal units to address fraud and issues stemming from forensic investigations. Other departments are borrowing internal resources or entering co-sourcing relationships. Whatever direction is best for your organisation, just be sure to cover all of your bases.

Each member of an internal audit staff needs to have some level of fraud training, even if the department retains specialised 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.

Training programmes are available through professional associations, such as the Association of Certified Fraud Examiners (ACFE) and the IIA. Other sources of fraud prevention and investigation training in the United States include the MIS Training Institute, public accounting firms and others. When assessing your training options, keep in mind that the most effective antifraud and risk-mitigation training occurs when internal audit contributes substantially to the content and ensures that the training is customised to its needs. And do your best to avoid courses limited to investigations, “war story” sessions, paid infomercials, and canned presentations.
Step 5: Organise a Fraud and Reputation-Risk Assessment

The fraud and reputation risk assessment process involves several steps as depicted below:

**Step 5.1**
Organise Assessment by Business Cycle or Separate Fraud Cycle

**Step 5.2**
Determine Units and Locations to Assess

Facilitating a comprehensive fraud and reputation-risk assessment is the single most important contribution that internal audit can contribute to an organisation’s antifraud programmes and controls. An effective fraud and reputation-risk assessment will identify previously unidentified risks and strengthen the ability of the organisation to prevent and detect fraud and misconduct before they reach scandalous proportions. Furthermore, fraud and reputation-risk assessments can identify cost-savings opportunities far in excess of direct assessment costs.

**Step 5.1: Organising the Assessment**
Internal audit can integrate the fraud and reputation-risk assessment process around the organisation's existing business cycles or establish a separate cycle for this purpose. Organising around an existing business cycle can simplify the process, for if internal audit is evaluating the revenue cycle, for example, the project team can expand the scope of the cycle to specifically consider fraud and reputation risks associated with revenue.

The downside to this approach is that internal audit does not necessarily consider every business cycle. Another downside is that the assessment 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.
Step 5.2: Determine Units and Locations to Assess
To be effective, fraud and reputation-risk assessments must be conducted at the company-wide, business-unit and significant-account levels. Risk assessments should also be conducted when special circumstances arise, such as changed operating environments, mergers and acquisitions, the introduction of new products, the entry of new markets, and corporate restructurings.

At public companies, internal audit should liaise with the Sarbanes-Oxley readiness team because of its ongoing work with the organisation’s significant business units, accounts and locations. However, the fraud risk assessment process may well require a broader reach, given that reputation risk is not synonymous with financial significance.\(^{17}\)

Multinational companies, for example, often conduct business at higher-risk locations. While such locations may not be financially material to the organisation 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 need to be apprised of such risks.

\(^{17}\) The proposed audit standard explains, moreover, that an account might be material to an audit of internal controls even though it is insignificant to the organisation’s financial statements. PCAOB Auditing Standard No. 2 ¶67
Step 5.3: Identify Potential Fraud and Misconduct Schemes and Scenarios

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

Developing a scheme- and scenario-based database for a company is a formidable challenge, as we know from first-hand experience. PricewaterhouseCoopers 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.
In recent years, PricewaterhouseCoopers has identified more than 150 generic fraud schemes, which fall into six basic categories:

- Fraudulent financial reporting
- Misappropriation of assets
- Expenditures and liabilities for an improper purpose
- Revenue and assets obtained by fraud
- Costs and expenses avoided by fraud
- Financial misconduct by senior management\(^{18}\)

For each of these 150 schemes, PricewaterhouseCoopers fraud subject-matter experts identified the:

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

18 PCAOB Auditing Standard No. 2 ¶ 140. The standards define “senior management” to include any member of a senior management who play a significant role in the company’s financial reporting process.
The Six Categories of Fraud and Misconduct

Expectation Gaps Create Opportunities for Internal Audit

Confusion surrounding the roles of management, the Board and the independent auditor in combating fraud relate directly to the diverse nature of fraud, which can be segmented into six distinct categories:

- **Fraudulent Financial Reporting**, e.g., fraud arising from improper revenue recognition, overstatement of assets or understatement of liabilities

- **Misappropriation of Assets**, e.g., embezzlement, payroll fraud, external theft, procurement fraud, counterfeiting or product diversion

- **Improper Expenditures or Liabilities**, e.g., commercial and public bribery

- **Fraudulent Acquisition of Revenues or Assets**, e.g., over-billing or product substitution against third parties, employer fraud against employees

- **Fraudulent Avoidance of Expenses**, e.g., tax fraud, booking revenue off-shore to avoid taxes

- **Financial Misconduct by Senior Management** – includes misconduct of any magnitude

Professional auditing standards (SAS 99) require independent auditors to examine only two of these six areas – *fraudulent financial reporting* and *misappropriation of assets* – and to do so only to the extent that occurrence could lead to a material misstatement.

Senior management and the audit committee, in contrast, are responsible for all six categories. Yet, many companies assign no internal organisation to prevent and detect fraud. For internal audit, this void spells opportunity – and risk. By being proactive, internal audit functions can position themselves to assume leadership of corporate efforts to monitor and oversee the organisation’s antifraud programme and controls.
A company’s risk assessment process must address all six categories of fraud and misconduct to avoid being cited for a “significant deficiency”. In all likelihood, an organisation will look to internal audit to provide the requisite fraud expertise to develop scheme and scenario-based databases and repositories. In turn, internal audit 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 during the course of an internal audit.

Identifying the universe of potential fraud schemes is a significant task. Our list of 150 generic fraud schemes represents the tip of the iceberg. Fraud schemes and scenarios differ drastically by product and service sector and geography. For example, sales and marketing schemes are quite common in the Asian market whereas procurement fraud is more widespread in Central and South America. On the other hand, the types of schemes affecting a bank will differ from those affecting a manufacturer. While both companies may be obtaining assets in a fraudulent manner, the bank might do so by failing to credit interest or by charging improper fees whereas the manufacturer may be short-shipping a distributor to obtain assets fraudulently.

The assessment team also needs to consider the organisation’s individual business processes. As to each step in the process, the team must mull over the various ways that an insider or outsider can manipulate the process to commit fraud for or against the company.

The typical large multinational company, as a result, faces hundreds of fraud and reputation risks. To develop scheme descriptions for your organisation requires a deep knowledge of fraud, the industry or industries in which your organisation operates, and the geographies where you conduct business.
Internal audit can draw relevant information from individual business units about industries and geographies served. Note, however, that it is one thing to be an industry and geographic expert – but quite another to be expert about how fraud and misconduct occur and can be mitigated. The country manager, for example, is a critical starting point, but internal audit 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 Sarbanes-Oxley.

An organisation’s assessment team also needs to understand the risks and ramifications posed by each scheme. The risks tend to fall under three headings – reputation, financial and legal – and have varying implications. In assessing fraud-related risks, for example, senior management and the audit committee may be far more willing to risk a monetary loss as opposed to the loss of reputation or the possibility of criminal or civil sanctions.
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 standard defines “more than remote” as either reasonably possible or probable.

<table>
<thead>
<tr>
<th>SIGNIFICANCE</th>
<th>PROBABILITY</th>
<th>Antifraud controls are required if the likelihood of a fraud scheme is “more than remote” and “more than inconsequential”</th>
</tr>
</thead>
<tbody>
<tr>
<td>Material</td>
<td>Remote</td>
<td>Example fraud scheme #1 (lower risk)</td>
</tr>
<tr>
<td></td>
<td>More than Remote</td>
<td>Example fraud scheme #2 (moderate risk)</td>
</tr>
<tr>
<td></td>
<td>Probable</td>
<td>Example fraud scheme #3 (high risk)</td>
</tr>
<tr>
<td>Inconsequential</td>
<td></td>
<td></td>
</tr>
<tr>
<td>More than Inconsequential</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Example fraud scheme #1** (lower risk)

**Example fraud scheme #2** (moderate risk)

**Example fraud scheme #3** (high risk)

**Step 5.4: Assess Likelihood of Fraud and Significance of Risk**

Fraud risk assessments, like traditional risk assessments, consider the likelihood that a particular fraud will occur. PCAOB Auditing Standards No. 2 specifies the following risk levels:

- Remote
- More Than Remote/Reasonably Possible
- Probable

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

---

19 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 standard defines “more than remote” as either reasonably possible or probable.
Next, assess the significance of fraud risks with a more than remote likelihood of occurring. In this context, the PCAOB Auditing Standards refer to:

- Inconsequential
- More Than Inconsequential
- Material

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.20 SEC registrants should note that SEC Staff Accounting Bulletin (SAB) 99, which provides guidance in determining materiality when fraud is discovered21, rejects the frequently used rule of thumb that a misstatement or omission that is less than 5% 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 analysed. The PCAOB has adopted the same approach for the audit of internal controls.22

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

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

20 Financial Accounting Standards Board (“FASB”) Statement of Financial Accounting Concepts No. 2, Qualitative Characteristics of Accounting Information (“FCON 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.”


22 PCAOB Auditing Standards ¶22-23
Step 6: Link Antifraud Control Activities

Next, internal audit 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. Additionally, internal audit should identify who performs the controls and the related segregation of duties.\(^\text{23}\) Proper assessments of fraud and reputation risk specifically demand that internal audit consider whether and how the controls can be circumvented or overridden by management and others. Internal audit should also consider whether the person performing the control possesses the necessary authority and qualifications.\(^\text{24}\)

Furthermore, internal audit should identify fraud risks which cannot be tied to effectively designed and operating controls. Where control weaknesses result in more than a remote likelihood of fraud loss at more than an inconsequential amount, corrective measures should be considered.

As a rule of thumb, antifraud controls generally include controls designed to prevent\(^\text{25}\) fraud and those designed to detect fraud in a timely fashion when it occurs. What follows is an illustration of how internal audit might document the linkage:

<table>
<thead>
<tr>
<th>Business Unit, Process or Objective</th>
<th>Fraud Category</th>
<th>Fraud Scenario</th>
<th>Sample Antifraud Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Officer Expenses</td>
<td>Financial Misconduct of Management</td>
<td>Over-limit expenditures by corporate officers</td>
<td>Expense authorization limits</td>
</tr>
<tr>
<td></td>
<td>Misappropriation of Assets</td>
<td>Improper reimbursement of officer expenses due to management override</td>
<td>Expense reimbursement policies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>False expense reporting of invalid or non-corporate expenditures</td>
<td>Corporate ethics policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Finance review of officer expenses relative to policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Internal audit testing of the accounts payable and officer reimbursement processes</td>
</tr>
</tbody>
</table>

\(\text{SAMPLE ANTIFRAUD CONTROL LINKAGE CHART}\)

\(^{23}\) PCAOB Auditing Standards No. 2 ¶42

\(^{24}\) PCAOB Auditing Standards No. 2 ¶8

\(^{25}\) PCAOB Auditing Standards No. 2 ¶11
## SAMPLE ANTIFRAUD CONTROL LINKAGE CHART

<table>
<thead>
<tr>
<th>Business Unit, Process or Objective</th>
<th>Fraud Category</th>
<th>Fraud Scenario</th>
<th>Sample Antifraud Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revenue Recognition, Fraud Reporting</td>
<td>Fraudulent Financial Reporting</td>
<td>Improper change in pricing</td>
<td>Access to make changes to pricing files is restricted to individuals with such designated job responsibilities. Establishment and approval is required for all pricing data and discounts are approved by authorised personnel.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Improper change in payment terms</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Reporting exists to monitor changes in payment terms in the system. The collections group monitors the A/R to identify changes in payment-term trends.</td>
</tr>
<tr>
<td></td>
<td>Misappropriation of Assets</td>
<td>Inventory Shrinkage</td>
<td>Physical security of all inventories under dual control</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Periodic physical inventory</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Investigation and reconciliation of inventory differences</td>
</tr>
</tbody>
</table>
Internal audit should expect to tie 70% to 80% of identified fraud risks to existing control activities such as approvals, authorisations, verifications, reconciliations, segregation of duties, reviews of operating performance and security of assets.

Anticipate, conversely, that the fraud and reputation-risk assessment will reveal that no control activities exist to mitigate 20% to 30% of the identified risks. Also anticipate that internal audit will be asked to develop potential controls to address risks lacking control coverage.

Ultimately, management and the board must determine whether to develop controls for areas lacking appropriate controls. In doing so, management will need to conduct a cost-benefit analysis of the costs of controlling a risk vs. the benefits of mitigating or eliminating that risk. It is important to document the analysis, should management decide against implementing corrective measures.
Step 7: Evaluate and Test Design and Operating Effectiveness

Once the fraud and reputation-risk assessment has taken place, internal audit will need to evaluate and test the design and operating effectiveness of antifraud controls. Although the process for evaluating antifraud controls is similar to that for testing other control activities, they differ in one important manner: In evaluating antifraud controls, you also need to address the possibility that management might seek to circumvent or override controls intended to prevent or detect fraud.

It's also important to coordinate your evaluation and testing activities with your independent auditor. PCAOB Auditing Standards No. 1 §115 requires an independent evaluation of antifraud controls and precludes the independent auditor from relying upon internal audit’s testing of antifraud control activities. Given this factor, some organisations will opt to leave the testing to the independent auditor to avoid duplicity of efforts. Others will want to conduct their own testing to identify and cure deficiencies in advance. Organizations preferring the latter option will need to understand the methodology required by PCAOB Auditing Standard No. 2.
Step 8: Refine Audit Plan to Address Residual Risk and Incorporate Fraud Auditing

Internal audit should consider (and document) the results of the fraud and reputation-risk assessment in developing its audit plan. The internal audit plan should be designed to address operating effectiveness and the possible override of those controls identified to mitigate the various fraud risks. In addition, fraud auditing, a new competency, will likely be required to address residual fraud risks, i.e. fraud-related risks that are not mitigated by preventive or detective control activities.

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 being audited. The mere indicia of a fraud scheme do not, in and of itself, indicate that a fraud has occurred. There may be perfectly legitimate reasons for any given fraud indicia to arise as part of the audit process.

By contrast, fraud investigation, or forensic accounting, is an inquiry into specific allegations or suspicions of fraud. Fraud investigations focus on determining the nature, extent, cause and resolution of identified or suspected fraudulent events. Only those indicia that are subsequently found to be fraudulent in nature become the focus of a fraud investigation. The discipline of fraud investigation embraces specialty skill sets beyond those typically required to conduct fraud risk assessments and audits.
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 should 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-Aided Auditing Techniques**
Computer-Aided Auditing Techniques (CAATs) are essential because of their ability to search massive amounts of data. Thus CAATs should be considered an integral part of every fraud audit.
Targeted Testing of Transactions
A fraud auditor must also consider targeted (as opposed to random) testing of transactions. For example, a fraud audit targeting improper revenue recognition might focus on round-dollar transactions, transactions ending in $999, or transactions occurring after the closing date.

FRAUD AUDITING PROCESS

Determination by Area

Determine Areas of Operations at Risk

Identify Potential Fraud Schemes

Identify red flags and indications associated with schemes

Build audit steps to search for indicators

Conduct further inquiry if red flag is detected or suspected

FRAUD INVESTIGATION PROCESS

Fraud event known or expected?

YES
Step 9: Establish a Standard Process for Responding to Allegations or Suspicions of Fraud or Misconduct

Expect fraud and misconduct to occur no matter how diligent your organisation’s antifraud programme and controls. Any organisation that is large enough to support an internal audit function will, by definition, be the victim of internal and external misconduct, just as any moderate-sized municipality will suffer some level of crime, no matter how extensive its anticrime efforts.

Every organisation should develop a standardized process for responding to allegations or suspicions of fraud. It should not wait until fraud is detected to develop an investigative process.

Naturally, the investigative process will vary depending upon the size and complexity of the organisation. At small organisations, the investigative process might be relatively informal, whereas the process at large, multinational organisations will likely require significant structure. By way of illustration, one PricewaterhouseCoopers client, a Fortune 50 company, has an investigative process that includes:

- An Office of Global Ethics and Compliance (ECO) that oversees investigations on a global basis
- Ethics and Compliance Committees (ECC) established by charter in each of the organisation’s geographic regions
- A separate Code of Conduct for conducting investigations
- Standard and global processes for categorising, referring, investigating and reporting allegations of fraud and misconduct, including hotline calls
- Support of the fraud investigation process
- A global database that (1) enables the ECO and regional ECC to monitor and oversee all regional investigations; (2) facilitates the investigative work and best practices among the functional subject-matter experts; and (3) streamlines compliance reporting to management and the audit committee
The investigative process must track all fraud allegations. PCAOB Auditing Standard No. 2 ¶142 requires management to issue a written representation 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.” Management cannot meet this burden without proper tracking process.

The degree to which internal audit is part of the investigative process will vary from one company to another. At many companies, internal audit either conducts investigations or has oversight authority over a specialised investigative unit. Other firms, seeking confidentiality under the work-product doctrine and attorney-client privilege, have internal audit perform these functions on behalf of the General Counsel’s office. Another group of companies opts to exclude internal audit from the investigative process, preferring instead to leave investigations to corporate security, corporate counsel, or outside investigative firms.

At PricewaterhouseCoopers, we believe that internal audit serves a crucial role in the investigative process and should be an integral component of the investigative team, unless legal or independence considerations suggest otherwise. With either a dotted-line or direct reporting relationship to both senior management and the audit committee, internal audit has a unique role within the corporate hierarchy. And with its enterprise-wide focus, internal audit knows the organisation and its players, is familiar with corporate history and politics, has a solid understanding of markets served, and is a proven leader in the fact-finding process. The insights gained from such a broad-based role are invaluable, even if internal audit does not actually lead the investigative team.
Step 10: Remediate and Prevent Recurrence

The investigation determines “what happened.” Remediation generally involves three elements: (1) taking disciplinary and legal action against wrongdoers; (2) recovering/restoring losses and other damages; and, (3) learning from an incident to improve controls and prevent recurrence. At a minimum, internal audit should be highly involved in step 3, even if it is not involved in the investigation or disciplinary processes or in the pursuit of criminal and civil remedies.

Evaluating the Scope of the Investigation
An internal auditor need not be a forensic investigator to evaluate the scope of an investigation. Such an evaluation usually involves two issues: first, has the investigation considered all potential misdeeds of the targets, and second, could the same conduct be occurring elsewhere within the organisation.

Experienced investigators know that wrongdoers rarely confess to all of their misdeeds during initial confessions. Given this fact, internal audit needs to consider whether an investigation has adequately addressed the various ways that the organisation might have been defrauded or otherwise damaged. In addition, internal audit should consider whether similar or related misconduct might be occurring elsewhere.

Addressing Failure in Controls
In addressing control failures, internal audit 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.

Internal audit should determine whether controls were non-existent, circumvented and/or overridden. Likewise, internal audit should be prepared to recommend improvements to address control weaknesses, including potential refinements to the internal audit plan.

In the final analysis, internal audit must be prepared to explain to senior management and the audit committee whether the misconduct in question is likely to recur, or whether new controls can be expected to prevent the problem from recurring.
Some Closing Thoughts

In today’s world of business, fraud and reputation risk have achieved priority status among corporate concerns. With antifraud controls now required by law, senior managements and audit committees alike are asking internal audit groups to play a much stronger role in corporate antifraud efforts.

In response, internal audit needs to evaluate a number of issues:

• What are management’s concerns about fraud? What are the fraud-related concerns of the audit committee?

• When it comes to antifraud efforts, what are senior management’s expectations of internal audit? What are the audit committee’s expectations?

• Does internal audit have clear-cut reporting channels on fraud issues?

• What types of fraud are of particular concern to your industry? To your organisation?

• Does your organisation track fraud cases? Do you measure fraud losses?

If there are gaps between the expectations of senior management and/or the audit committee and your current antifraud focus, move quickly to strengthen the alignment of internal audit with the expectations of these critical corporate overseers. And if internal audit lacks clear-cut reporting channels on fraud and risk-management issues, or if such channels are weak or missing, work with senior management and the audit committee to correct any problems.

When it comes to mitigating fraud and risks to reputation, the role of internal audit can be likened to that of a corporate watchdog. To be more effective in this all-important role, we recommend that you develop an antifraud action plan for internal audit that incorporates elements of the 10-step plan we’ve outlined above.

By reducing fraud, a company can trim costs and improve profitability. What’s more, antifraud efforts can more than pay for themselves. What better way for internal audit to create organisational value?

To learn more about our 10-step antifraud action plan, please contact:

**Jonny Frank**
Partner
Fraud Risks & Controls Practice Leader
646-471-8590
jonny.frank@us.pwc.com

**Jim LaTorre**
Partner
Internal Audit Services Global Leader
703-918-3164
james.a.latorre@us.pwc.com
**Appendix A: Antifraud Program & Controls Assessment Grid**

<table>
<thead>
<tr>
<th>Element</th>
<th>Criteria</th>
<th>Best Practice</th>
<th>Generally in Compliance</th>
<th>Deficient</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Control Environment</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management Accountability</td>
<td>Management should (1) effectively implement the company’s antifraud programmes and controls, and (2) take appropriate actions involving circumvention of internal controls over financial reporting and other fraudulent behaviours.</td>
<td>Management: (1) demonstrates that internal controls, including fraud, are important, (2) proactively implements antifraud programmes and controls including codes of ethics and conduct, and (3) takes appropriate, consistent remediation action in instances of violations.</td>
<td>Management takes sufficient actions with respect to prevention, detection, investigation, remediation and monitoring of fraud and fraud controls.</td>
<td>Management fails to conduct effective oversight of antifraud programmes and controls. Remediation including disciplinary action is inconsistent.</td>
</tr>
<tr>
<td>Board of Directors and Audit Committee Oversight</td>
<td>The Board and Audit Committee should provide oversight over: (1) management's antifraud programmes and controls, (2) assessment of fraud risk, (3) controls activities over fraud risks identified by the assessment, (4) monitoring and auditing for fraud, (5) investigation of alleged or suspected fraud and (6) remediation.</td>
<td>The Board and the Audit Committee (1) actively conduct oversight of management’s antifraud programme, (2) actively seeks 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.</td>
<td>Board and Audit Committee provide adequate oversight.</td>
<td>Audit Committee fails to provide active oversight; passive oversight only; insufficient consideration of fraud.</td>
</tr>
<tr>
<td>Element</td>
<td>Criteria</td>
<td>Best Practice</td>
<td>Generally in Compliance</td>
<td>Deficient</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Codes of Ethics and Conduct</td>
<td>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.</td>
<td>Documented and effective codes of conduct should include and be effectively communicated to all employees. Code should address (1) conflicts of interest, (2) related party transactions, (3) accuracy of accounting records, (4) illegal acts, and (5) compliance with laws and regulations.</td>
<td>Documented and effective code of conduct with only minor deficiencies. Applies to all individuals in an accounting or financial reporting oversight role.</td>
<td>Code omits topics specified in SEC's Final Rules or is not operating effectively. Ineffective communication to all covered persons.</td>
</tr>
<tr>
<td>Ethics Hotline/Whistleblower Programme</td>
<td>Documented procedures for the receipt, retention, and treatment of complaints and confidential, anonymous submission of concerns by employees or external third parties.</td>
<td>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.</td>
<td>Ethics hotline that appears to be of proper design and effectiveness but with perceived low volume of use.</td>
<td>Ethics hotline or whistleblower program omits elements (design or operating) in SEC rules.</td>
</tr>
<tr>
<td>Hiring and Promotion Procedures</td>
<td>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 organisation. Background investigations should include educational background, employment history and criminal record.</td>
<td>For new and promotions of personnel in positions of trust, conducts full scope background investigations conducted, including interviews with independent references. Similar investigations conducted for strategic third parties such as vendors, joint-venture partners, consultants, customers. All results documented.</td>
<td>Performs public record background investigations on personnel hired or promoted into positions of trust.</td>
<td>Fails to perform substantive background investigations for individuals being considered for employment or promotion to a position of trust.</td>
</tr>
<tr>
<td>Element</td>
<td>Criteria</td>
<td>Best Practice</td>
<td>Generally in Compliance</td>
<td>Deficient</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Investigative Process</td>
<td>Standardized procedure for responding to, investigating and assessing allegations or suspicions of fraud, whether or not material, potentially including a 10A investigation by independent counsel.</td>
<td>Written plan and process for 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 a significant role in internal controls.</td>
<td>In absence of written process, company demonstrates that a process exists for responding to allegations notwithstanding a lack of a written plan.</td>
<td>Inadequate process for responding to allegations or suspicions of fraud.</td>
</tr>
<tr>
<td>Remediation</td>
<td>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.</td>
<td>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 active Audit Committee involvement.</td>
<td>Takes appropriate disciplinary action and considers need for additional action to prevent recurrence.</td>
<td>Fails to take consistent remedial action with regards to identified significant deficiencies, material weaknesses, actual fraud, or suspected fraud.</td>
</tr>
<tr>
<td>Element</td>
<td>Criteria</td>
<td>Best Practice</td>
<td>Generally in Compliance</td>
<td>Deficient</td>
</tr>
<tr>
<td>---------</td>
<td>----------</td>
<td>---------------</td>
<td>-------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Process for Assessing Risk</td>
<td>Systematic rather than haphazard; considers fraud schemes and circumvention of existing controls; active oversight by Audit Committee.</td>
<td>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.</td>
<td>Assesses fraud risk on systematic basis; Audit Committee review.</td>
<td>Fails to assess fraud risk on systematic basis; haphazard or informal process for fraud risk assessment; inadequate evidence of audit committee involvement and review.</td>
</tr>
<tr>
<td>Frauds Considered</td>
<td>Consideration of fraudulent financial reporting, misappropriation of assets, unauthorized or improper receipts and expenditures, and fraud by senior management should all be demonstrated.</td>
<td>Assesses exposure from each of the categories of fraud risks considered.</td>
<td>Substantially addresses the six categories of fraud risks.</td>
<td>Absence of adequate documentary evidence of management’s risk assessment process and the Audit Committee’s involvement and review.</td>
</tr>
<tr>
<td>Element</td>
<td>Criteria</td>
<td>Best Practice</td>
<td>Generally in Compliance</td>
<td>Deficient</td>
</tr>
<tr>
<td>---------</td>
<td>----------</td>
<td>---------------</td>
<td>-------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Likelihood and Significance of Fraud</td>
<td>Consideration of the likelihood of each fraud risk as probable, reasonably possible or remote; consideration of significance of fraud as inconsequential, more than inconsequential or material should be demonstrated.</td>
<td>Evaluates comprehensively the likelihood and significance of each identified fraud risk.</td>
<td>Substantially evaluates likelihood and significance of each fraud risk. Management provides sufficient explanation where risk assessment process does not consider risks that are (1) reasonably possible and material, (2) probable and more than inconsequential in amount, or (3) more than remote and more than inconsequential in amount.</td>
<td>Management's risk assessment process does not identify the level or likelihood and significance considered. Management fails to provide an explanation where risk assessment process does not consider risks that are (1) reasonably possible and material, (2) probable and more than inconsequential in amount, or (3) more than remote and more than inconsequential in amount.</td>
</tr>
<tr>
<td>Consideration of Organizational Levels</td>
<td>Consideration of fraud at the company-wide, business unit, and significant account levels should all be demonstrated.</td>
<td>Assesses fraud risk at all levels of the organization.</td>
<td>Assesses fraud risk at all significant levels of the organization.</td>
<td>Fails to consider significant business units or significant processes in the fraud risk assessment.</td>
</tr>
<tr>
<td>Circumvention of Controls and Management Override</td>
<td>Effectively designed internal controls should be in place to respond to the assessment of risk of management override.</td>
<td>Audit Committee specifically considers vulnerability of existing controls and risk of management override.</td>
<td>Fraud risk assessment process addresses circumvention of existing controls and potential for management override.</td>
<td>Fails to adequately consider risks of (1) circumvention of controls and (2) management override.</td>
</tr>
<tr>
<td>Element</td>
<td>Criteria</td>
<td>Best Practice</td>
<td>Generally in Compliance</td>
<td>Deficient</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Control Activities</td>
<td></td>
<td></td>
<td></td>
<td>Fails to link control activities to identified fraud risks; control activities deficient in design or operating effectiveness.</td>
</tr>
<tr>
<td>Linkage with Risk Assessment</td>
<td>Effective control activities should be designed and implemented to mitigate identified fraud risks.</td>
<td>Company links control activities to all identified fraud risks. Active oversight by audit committee to ensure design and operating effectiveness.</td>
<td>Company can link control activities to identified fraud risks, but fails to evaluate for design or operating effectiveness in compliance.</td>
<td>Fails to link control activities to identified fraud risks; control activities deficient in design or operating effectiveness.</td>
</tr>
<tr>
<td>Information and Communication</td>
<td></td>
<td></td>
<td></td>
<td>Fails to provide adequate or effective training regarding code of ethics and other fraud areas.</td>
</tr>
<tr>
<td>Training</td>
<td>Demonstrated frequency and sufficiency of proper training courses provided to all employees on fraud risk and antifraud programmes and controls.</td>
<td>Provides comprehensive and frequent relevant training to all employees. Maintains records documenting types of training and employees trained.</td>
<td>Provides adequate training to employees regarding fraud related issues.</td>
<td>Fails to provide adequate or effective training regarding code of ethics and other fraud areas.</td>
</tr>
<tr>
<td>Knowledge Management</td>
<td>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.</td>
<td>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, controls activities, allegations of frauds and remediation efforts.</td>
<td>Shares some but not all fraud-related information.</td>
<td>Fails to collect or share information regarding fraud risks, controls activities, and remediation of identified misconduct.</td>
</tr>
<tr>
<td>Element</td>
<td>Criteria</td>
<td>Best Practice</td>
<td>Generally in Compliance</td>
<td>Deficient</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Information System and Technology</td>
<td>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.</td>
<td>Information systems and technology address: (1) consideration of technologically enabled fraud in management’s fraud risk assessment, (2) IT security controls, (3) inappropriate modification to computer programmes, (4) system override, (5) segregation of duties, (6) adequacy of fraud detection and monitoring tools, and (7) ability to investigate computer misuse.</td>
<td>Information systems and technology addresses some, but not all of elements 1 through 7.</td>
<td>Fails to either (1) consider information technology in fraud risk assessment, (2) maintain adequate security and access controls, (3) employ information technology to prevent and detect fraud, or (4) have an ability to investigate computer misuse.</td>
</tr>
<tr>
<td>Monitoring</td>
<td>Management should have a process of assessing the quality of the antifraud programmes and controls over time through ongoing monitoring activities as well as separate periodic evaluations.</td>
<td>Monitors antifraud controls, programs and policies on an ongoing and periodic basis; management considers possibility of fraud in day-to-day operations; management uses results of fraud assessment and IT system to monitor for fraud.</td>
<td>In absence of written process, company can demonstrate that management monitors for indicia of fraud as part of day-to-day operations.</td>
<td>Management fails to include possibility of fraud in its monitoring of day-to-day operations.</td>
</tr>
<tr>
<td>Element</td>
<td>Criteria</td>
<td>Best Practice</td>
<td>Generally in Compliance</td>
<td>Deficient</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Internal Audit Evaluations</td>
<td>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.</td>
<td>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.</td>
<td>In absence of written process, company can demonstrate that (1) internal audit considers fraud in developing and executing internal audit cycle and (2) department includes internal auditors with training and experience in fraud auditing.</td>
<td>Fails either to (1) consider fraud in planning internal audit cycle, (2) conduct fraud auditing procedures, or (3) Absence of 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.</td>
</tr>
</tbody>
</table>
10-Step Antifraud Action Plan

**Step 1: Anticipate Questions and Manage Expectations**
- What are the company’s fraud and reputation risks?
- What programs and controls have been implemented to mitigate these risks?
- What is internal audit doing to prevent and detect issues before they emerge into a corporate scandal?

**Step 2: Assess Existing Antifraud Programmes and Controls**

**Step 3: Secure Management and Audit Committee Sponsorship**
- Establish a dialogue
- Leverage and engage Sarbanes-Oxley/404 readiness projects
- Ask your Independent Auditor for input
- Host a fraud summit

**Step 5.1** Organise Assessment by Business Cycle or Separate Fraud Cycle

**Step 5.2** Determine Unit and Location to Assess

**Step 6: Link Antifraud Control Activites**

**Step 7: Evaluate and Test Design and Operating Effectiveness**

Sample Flow Linkage Chart (pages 26-27)
### Step 4: Assemble Fraud Expertise within Internal Audit

Internal audit must (to name a few):
- Be aware of potential schemes and scenarios
- Have a solid understanding of measures intended to prevent and detect fraud
- Be able to perform fraud audits and be knowledgeable of forensic investigations

### Step 5: Organise a Fraud and Reputation-Risk Assessment

- **Step 5.3** Identify Fraud Misconduct Schemes and Scenarios
- **Step 5.4** Assess Likelihood of Fraud and Significance of Risk

### FRAUD AUDITING PROCESS

- Determination by Area
  - Identify areas of company where schemes most likely to occur
- Determination by Scheme
  - Identify red flags and indications associated with schemes
  - Build audit steps to search for indicators
  - Conduct further inquiry if flag is detected or suspected

### FRAUD INVESTIGATION PROCESS

- Identify and evaluate red flags
  - Unusual or unexpected financial transactions
  - Contrary changes in business or operational performance
- Conduct further inquiry if flag is detected or suspected

### Step 8: Refine Audit Plan to Address Residual Risk and Incorporate Fraud Auditing

### Step 9: Establish a Standard Process for Responding to Allegations or Suspicions of Fraud or Misconduct

- Sample investigative process for a Fortune 50 company:
  - Office of Global Ethics and Compliance (ECO)
  - Ethics & Compliance Committees (ECC)
  - A separate Code of Conduct for conducting investigations
  - Standard global processes for categorizing, referring, investigating & reporting
  - Participation by internal audit
  - A global database for ECO & ECC to monitor, facilitate and streamline reporting

### Step 10: Remediate and Prevent Recurrence

Remediation involves:
- Taking disciplinary & legal action
- Recovering/restoring losses & other damages
- Learning from an incident

Prevention involves:
- Consider roots of how and why fraud occurred
- Determine whether controls were non-existent, circumvented and/or overridden
- Explain to senior management and audit committee likelihood of recurrence