

ANTI-FRAUD PROGRAMS AND CONTROLS

PREFACE

This appendix discusses and provides examples of programs and controls that management can implement to help deter, prevent, and detect fraud. Management may develop and implement some of these programs and controls in response to specific identified risks of material misstatement due to fraud. In other cases, these programs and controls may be a part of the entity's enterprise-wide risk management activities.

As discussed in paragraph .02, management is responsible for designing and implementing systems and procedures for the prevention and detection of fraud and, along with those responsible for oversight of the financial reporting process, for creating a culture and environment that promotes honesty and ethical behavior. However, because of the characteristics of fraud described in paragraphs .03 through .12, a material misstatement due to fraud may occur notwithstanding the presence of programs and controls such as those described in this Appendix.

In obtaining an understanding of the entity and its environment, the auditor also obtains an understanding, principally through inquiries of management and others (see paragraphs .19 through 27) of programs and controls established by management to mitigate specific risks of fraud, or that otherwise help to prevent, deter, and detect fraud. The information provided on the following pages has been developed to assist auditors in obtaining such an understanding. However, the absence of such programs and controls does not affect the auditor's ability to perform an audit in accordance with generally accepted auditing standards.

INTRODUCTION

Almost all organizations experience fraud and abuse of one form or another, ranging from minor employee theft and unproductive behavior to immaterial misappropriation of assets to material fraudulent financial reporting. Material financial statement fraud can have a significant adverse effect on an entity's market value, reputation, and ability to achieve its strategic objectives. A number of highly publicized cases have heightened the awareness of the effects of fraudulent financial reporting and led many organizations to be more proactive in taking steps to prevent or deter its occurrence. Misappropriation of assets, though often not material to the financial statements, can nonetheless result in substantial losses to an entity if a dishonest employee has the incentive and opportunity to commit fraud.

The risk of fraud can be reduced through a combination of prevention, deterrence and detection measures. However, fraud is often difficult to detect because it often involves concealment through falsification of documents or collusion. Therefore, it is important to place a strong emphasis on fraud prevention, which may reduce opportunities for fraud to take place, and fraud deterrence, which could persuade individuals that they should not commit fraud because of the likelihood of detection and punishment. Moreover, prevention and deterrence measures are much less costly than the time and expense required for fraud detection and investigation.

An entity's management has both the responsibility and the means to implement measures to reduce the incidence of fraud. The measures an organization takes to prevent and deter fraud also can help to create a positive workplace environment that can enhance the entity's ability to recruit and retain high quality employees.

Research suggests that the most effective way to implement measures to reduce wrongdoing is basing them on a set of core values that are embraced by the entity. These values provide an overarching message about the key principles guiding all employees' actions. This provides a platform upon which a more detailed code of conduct can be constructed, giving more specific guidance as to permitted and prohibited behavior, based on applicable laws and the company's values.

This appendix identifies measures entities can implement to prevent, deter and detect fraud. Broadly stated, there are three fundamental activities — that is, (1) create and maintain a *culture* of honesty and high ethics, (2) *evaluate* the risks of fraud, and implement the processes, procedures and controls needed to mitigate the risks and reduce the opportunities for fraud, and (3) develop an appropriate *oversight* process. Although the entire management team shares the responsibility for implementing and monitoring these activities, with oversight from the board of directors, the entity's chief executive officer (CEO) should initiate and support such measures. Without the CEO's active support, these measures are less likely to be effective.

The information presented in this appendix generally is applicable to entities of all sizes.

However, the degree to which certain programs and controls are applied in a smaller entity, and the formality of their application, are likely to differ from larger entities. For example, management of a smaller entity (or the owner of an owner-managed entity), along with those charged with governance of the financial reporting process, is responsible for creating a culture of honesty and high ethics. However, the entity may not have a written code of conduct or formally documented ethics policies. Management also is responsible for implementing a system of internal control commensurate with the nature and size of the business, but smaller entities may find that certain types of control activities are not relevant because of the involvement of and controls applied by management.

CREATING A CULTURE OF HONESTY AND HIGH ETHICS

It is the organization's responsibility to create a culture of honesty and high ethics and to clearly communicate acceptable behavior and expectations of each employee. Such a culture is rooted in a strong set of core values (or "value system") that provides the foundation for employees as to how the company conducts its business. It also allows an entity to develop an ethical framework that covers (1) fraudulent financial reporting, (2) misappropriation of assets, and (3) corruption.¹

Creating a culture of honesty and high ethics may include the following:

Setting the tone at the top

Management must be made aware that they are expected to set the standard with respect to ethical behavior within the entity. Research in moral development strongly suggests that honesty can best be reinforced when a proper example is set—sometimes referred to as "the tone at the top." The management of an entity cannot act one way and expect others in the entity to behave differently. Management must show employees through its actions that dishonest or unethical behavior will not be tolerated.

For example, statements by management regarding the absolute need to meet operating and financial targets can create undue pressures that may lead employees to commit fraud in order to achieve them. Setting unachievable goals for employees can give them two equally unattractive choices: to fail or to cheat. In contrast, a statement from management that "we are aggressive in pursuing our targets, while requiring truthful financial reporting at all times" clearly indicates to employees that integrity is a requirement. This message also conveys that the entity has "zero tolerance" for unethical behavior, including fraudulent financial reporting.

The cornerstone of an effective anti-fraud environment is a culture with a strong value system. This value system often is reflected in a code of conduct.² The code of conduct should reflect the core values of the entity and guide employees in making appropriate decisions during their workday. The code of conduct might include such topics as ethics,

¹ Corruption includes bribery and other illegal acts as described in Section 317, *Illegal Acts by Clients*.

² An entity's value system also could be reflected in an ethics policy, a statement of business principles, or some other concise summary of guiding principles.

confidentiality, conflicts of interest, intellectual property, sexual harassment, and fraud.³ In order for a code of conduct to be effective, it should be communicated to all personnel in an understandable fashion. It also should be developed in a participatory and positive manner that will result in both management and employees taking ownership of its content.

Creating a positive workplace environment

Research results indicate that wrongdoing occurs less frequently when employees have positive feelings about an entity than when they feel abused, threatened, or ignored. Without a positive workplace environment there are more opportunities for poor employee morale, which can provide incentives for and affect an employee's attitude about committing fraud against a company. Factors that detract from a positive work environment and may increase the risk of fraud include:

- Top management that does not seem to care about or reward appropriate behavior,
- Negative feedback and lack of recognition for job performance,
- Perceived inequities in the organization,
- Autocratic rather than participative management,
- Low organizational loyalty or feelings of ownership,
- Unreasonable budget expectations or other financial targets,
- Fear of delivering "bad news" to supervisors and/or management,
- Less than competitive compensation,
- Poor training and promotion opportunities,
- Lack of clear organizational responsibilities
- Poor communication practices or methods within the organization.

Employees should be encouraged and empowered to help create a positive workplace environment and support the entity's values and code of conduct. They should be given the opportunity to participate in developing and updating the entity's code of conduct, to ensure that it is relevant, clear and fair. Employees should be given the means to obtain advice internally before making decisions that appear to have significant legal or ethical implications. They should also be encouraged and given the means to communicate concerns about potential violations of the entity's code of conduct, without fear of retribution. Involving employees in this fashion also may effectively contribute to the oversight of the entity's code of conduct and an environment of ethical behavior (see "Developing an Appropriate Oversight Process").

³ Although the discussion in this appendix focuses on fraud, the subject of fraud often is considered in the context of a broader set of principles that govern an organization. Some organizations, however, may elect to develop a fraud policy separate from an ethics policy. Specific examples of topics in a fraud policy might include: a requirement to comply with all laws and regulations and explicit guidance regarding making payments to obtain contracts, holding pricing discussions with competitors, environmental discharges, relationships with vendors, and maintenance of accurate books and records.

Hiring and promoting appropriate employees

Not all people are equally honest or have equally well-developed personal codes of ethics. Many people, when faced with sufficient pressure and a perceived opportunity, will behave dishonestly rather than face the negative consequences of honest behavior. But the threshold at which dishonest behavior starts will vary among individuals. If an entity is to be successful in preventing fraud, it must have effective policies that minimize the chance of hiring or promoting individuals with low levels of honesty, especially for positions of trust.

Proactive hiring and promotion procedures may include:

- Conducting background investigations on individuals being considered for employment or for promotion to a position of trust⁴,
- Thoroughly checking a candidate's education, employment history, and personal references,
- Training new employees about the entity's values and code of conduct,
- Incorporating into regular performance reviews an evaluation of how each individual has contributed to creating an appropriate workplace environment in line with the entity's values and code of conduct, and
- Periodic objective evaluation of compliance with the entity's values and code of conduct.

Training

Employees should be trained at the time of hiring about the entity's values and its code of conduct. This training should explicitly cover expectations of all employees regarding (1) their duty to communicate certain matters, (2) a list of the types of matters, including actual or suspected fraud, to be communicated along with specific examples, and (3) information on how to communicate those matters. There also should be an affirmation from senior management regarding employee expectations and communication responsibilities. Such training should include an element of "fraud awareness," the tone of which should be positive but nonetheless stress that fraud can be costly (and detrimental in other ways) to the entity and its employees.

In addition to training at the time of hiring, employees should receive refresher training periodically thereafter. Some organizations may consider ongoing training for certain positions, such as purchasing agents or employees with financial reporting responsibilities. Training should be specific to an employee's level within the organization, geographic location, and assigned responsibilities. For example, training for senior manager level personnel would normally be different from that of non-supervisory employees, and training for purchasing agents would be different from that of sales representatives.

⁴ Some organizations also have considered follow-up investigations, particularly for employees in positions of trust, on a periodic basis (e.g., every five years) or as circumstances dictate.

Confirmation

Requiring periodic confirmation by employees of their responsibilities may deter individuals from committing fraud and other violations and may identify problems before they become significant. Such confirmation may include statements that the individual understands the entity's expectations, has complied with the code of conduct, and is not aware of any violations of the code of conduct. Although people with low integrity may not hesitate to sign a false confirmation, most people will want to avoid making a false statement in writing. Honest individuals are more likely to return their confirmations and to disclose what they know (including any conflicts of interest or other personal exceptions to the code of conduct). Thorough follow-up by internal auditors or others regarding non-replies may uncover significant issues.

Discipline

The way an entity reacts to incidents of alleged or suspected fraud can send a strong deterrent message throughout the entity, helping to reduce the number of future occurrences. The following actions should be taken in response to an alleged incident of fraud:

- A thorough investigation of the incident should be conducted,⁵
- Appropriate and consistent actions should be taken against violators,
- Relevant controls should be assessed and improved
- Communications and training should occur to reinforce the entity's values, code of conduct, and expectations.

Expectations about the consequences of committing fraud must be clearly communicated throughout the entity. For example, a strong statement from management that dishonest actions will not be tolerated, and that violators may be terminated and referred to the appropriate authorities, clearly establishes consequences and can be a valuable deterrent to wrongdoing. If wrongdoing occurs and an employee is disciplined, it can be helpful to communicate that fact, on a no-name basis, in an employee newsletter or other regular communication to employees. Seeing that other people have been disciplined for wrongdoing can be an effective deterrent, increasing the perceived likelihood of violators being caught and punished. It also can demonstrate that the entity is committed to an environment of high ethical standards and integrity.

⁵ Many entities of sufficient size are employing anti-fraud professionals, such as certified fraud examiners, who are responsible for resolving allegations of fraud within the organization and also assist in the detection and deterrence of fraud. These individuals typically report their findings internally to the corporate security, legal, or internal audit departments. In other instances, such individuals may be empowered directly by the board of directors or its audit committee.

MANAGEMENT’S EVALUATION OF THE PROCESSES AND CONTROLS NEEDED TO MITIGATE THE RISKS OF AND REDUCE THE OPPORTUNITIES FOR FRAUD

Neither fraudulent financial reporting nor misappropriation of assets can occur without a perceived opportunity to commit and conceal the act. Organizations should be proactive in reducing fraud opportunities by (1) identifying and measuring fraud risks, (2) taking steps to mitigate identified risks, and (3) implementing and monitoring appropriate preventive and detective internal controls and other deterrent measures.

Identifying and Measuring Fraud Risks

Management has primary responsibility for establishing and monitoring all aspects of the entity’s fraud risk assessment and prevention activities.⁶ Fraud risks often are considered as part of an enterprise-wide risk management program, though they may be addressed separately.⁷ The fraud risk assessment process should consider the vulnerability of the entity to fraudulent activity (i.e., fraudulent financial reporting, misappropriation of assets, and corruption) and whether any of those exposures could result in a material misstatement of the financial statements. In identifying fraud risks, organizations should consider organizational, industry, and country-specific characteristics that influence the risk of fraud. Management may want to consider evaluating the specific risk of fraud by considering the risk factors discussed in paragraphs 31 and 32.

The nature and extent of management’s risk assessment activities should be commensurate with the size of the entity and complexity of its operations. For example, the risk assessment process is likely to be less formal and less structured in smaller entities. However, management should recognize that fraud can occur in organizations of any size, and that almost any employee may be capable of committing fraud given the right set of circumstances. Accordingly, management should develop a heightened “fraud awareness” and an appropriate fraud risk management program, with oversight from the board of directors or audit committee.

Mitigating Fraud Risks

It may be possible to reduce or eliminate certain fraud risks by making changes to the entity’s activities and processes. An entity may choose to sell certain segments of its operations, cease doing business in certain locations, or reorganize its business processes to eliminate unacceptable risks. For example, the risk of misappropriation of funds may be reduced by implementing a central lockbox at a bank to receive payments instead of receiving money at the entity’s various locations. The risk of corruption may be reduced

⁶ Management may elect to have internal audit play a proactive role in the development, monitoring, and ongoing assessment of the entity’s fraud risk management program. This may include an active role in the development and communication of the entity’s code of conduct or ethics policy, as well as in investigating actual or alleged instances of non-compliance.

⁷ Some organizations may perform a periodic self-assessment using questionnaires or other techniques to identify and measure risks. Self-assessment may not be particularly useful in identifying the risk of fraud due to a lack of experience with fraud (although many organizations experience some form of fraud and abuse, material financial statement fraud or misappropriation of assets is a rare event for most) and because assessing employee attitudes is inherently difficult.

by closely monitoring the entity's procurement process. The risk of financial statement fraud may be reduced by implementing shared services centers to provide accounting services to multiple segments, affiliates or geographic locations of an entity's operations. A shared services center may be less vulnerable to influence by local operations managers and may be able to implement more extensive fraud detection measures cost effectively.

Implementing and Monitoring Appropriate Internal Controls and Other Measures

Some risks are inherent in the environment of the entity, but most can be addressed with an appropriate system of internal control. Once fraud risk assessment has taken place, the entity can identify the processes, controls and other procedures that are needed to mitigate the identified risks. Effective internal control will include a well-developed control environment, an effective and secure information system, and appropriate control and monitoring activities.⁸

In particular, management should evaluate whether appropriate internal controls have been implemented in any areas management has identified as posing a higher risk of fraudulent activity, as well as controls over the entity's financial reporting process (see SAS No. 55, *Consideration of Internal Control in a Financial Statement Audit* (AICPA Professional Standards, vol. 1, AU sec. 319.50). Because fraudulent financial reporting may begin in an interim period, management also should evaluate the appropriateness of internal controls over interim financial reporting.

Fraudulent financial reporting by upper-level management typically involves override of internal controls within the financial reporting process. Because management has the ability to override controls, or to influence others to perpetrate or conceal fraud, the need for a strong value system and a culture of ethical financial reporting becomes increasingly important. This helps to create an environment where other employees will decline to participate in committing a fraud and will use established communication procedures to report any requests to commit wrongdoing.⁹ The potential for management override also increases the need for appropriate oversight measures by the board of directors or audit committee as discussed further below.

Fraudulent financial reporting by lower levels of management and employees may be deterred or detected by appropriate monitoring controls, such as having higher-level managers review and evaluate the financial results reported by individual business units or subsidiaries. Unusual fluctuations in results of particular reporting units may indicate potential manipulation by departmental or business unit managers or staff.

⁸ The report of the Committee of Sponsoring Organizations (COSO) of the Treadway Commission, *Internal Control—Integrated Framework*, provides reasonable criteria for management to use in evaluating the effectiveness of the entity's system of internal control.

⁹ Many organizations have implemented a process for employees to report on a confidential basis any actual or suspected wrongdoing, or potential violations of the code of conduct or ethics policy. For example, some organizations use a telephone "hotline" that is directed to or monitored by an ethics officer, fraud officer, general counsel, internal audit director, or another trusted individual responsible for investigating and reporting incidents of fraud or illegal acts.

DEVELOPING AN APPROPRIATE OVERSIGHT PROCESS

To effectively prevent or deter fraud, an entity should have an appropriate oversight function in place. Oversight can take many forms and can be performed by many within and outside the entity.

Management

Management is responsible for overseeing the activities carried out by employees, and typically does so by implementing and monitoring processes and controls such as those discussed previously. However, management also may initiate, participate in, or direct the concealment of a fraudulent act. Accordingly, the audit committee (or the board of directors where no audit committee exists) has the responsibility to oversee the activities of senior management, and to consider the risk of fraudulent financial reporting involving the override of internal controls or collusion (see further discussion below).

Audit Committee or Board of Directors

The audit committee (or the board of directors where no audit committee exists) should evaluate management's identification of fraud risks, implementation of anti-fraud measures, and creation of the appropriate "tone at the top." An entity's audit committee should encourage senior management (in particular, the chief executive officer) to implement appropriate fraud deterrence and prevention measures to better protect investors, employees, and other stakeholders. The audit committee's evaluation and encouragement not only helps to make sure that senior management takes its responsibility seriously, but also can serve as a deterrent to senior management engaging in fraudulent activity (i.e., demonstrating that the audit committee takes its oversight responsibility seriously).

The audit committee also plays an important role in helping the board of directors to fulfill its oversight responsibilities with respect to the entity's financial reporting process and the system of internal control. In exercising this oversight responsibility, the audit committee should consider the potential for management override of controls or other inappropriate influence over the financial reporting process. For example, the audit committee may obtain from the internal auditors and independent auditors their views on management's involvement in the financial reporting process and, in particular, the ability of management to override information processed by the entity's financial reporting system (e.g., the ability for management or others to initiate or record non-standard journal entries). The audit committee also may consider reviewing the entity's reported information for reasonableness compared with prior or forecasted results, as well as with peers or industry averages. In addition, information received in communications from the independent auditors¹⁰ can assist the audit committee in assessing the strength of the entity's internal control and the potential for fraudulent financial reporting.

¹⁰ See SAS No. 60, *Communication of Internal Control Related Matters Noted in an Audit* (AICPA Professional Standards, vol. 1, AU sec 325) and SAS No. 61, *Communication with Audit Committees* (AICPA, Professional Standards, vol. 1, AU sec. 380).

If senior management is involved in fraud, the next layer of management may be the most likely to be aware of it. As a result, the audit committee (and other directors) should consider establishing an open line of communication with members of management one or two levels below senior management to assist in identifying fraud at the highest levels of the organization or investigating any fraudulent activity that might occur.¹¹ The audit committee typically has the ability and authority to investigate any alleged or suspected wrongdoing brought to its attention. Most audit committee charters empower the committee to investigate any matters within the scope of its responsibilities, and to retain legal, accounting, and other professional advisors as needed to advise the committee and assist in its investigation.

Internal Auditors

An effective internal audit team can be extremely helpful in performing aspects of the oversight function. Their knowledge about the entity may enable them to identify indicators that suggest fraud has been committed. They also have the opportunity to evaluate fraud risks and controls and to recommend action to mitigate risks and improve controls. Moreover, internal audits can be both a detection and a deterrence measure. Internal auditors may conduct proactive auditing to search for corruption, misappropriation of assets, and financial statement fraud. This may include the use of computer-assisted audit techniques to detect particular types of fraud. Internal auditors also can employ analytical and other procedures to isolate anomalies and perform detailed reviews of high-risk accounts and transactions to identify potential financial statement fraud. The internal auditors should have an independent reporting line directly to the audit committee, to enable them to express any concerns about management's commitment to appropriate internal controls or to report suspicions or allegations of fraud involving senior management.

Independent Auditors

Independent auditors can assist management and the board of directors (or audit committee) by providing an assessment of the entity's process for identifying, assessing, and responding to the risks of fraud. The board of directors (or audit committee) should have an open and candid dialogue with the independent auditors regarding management's risk assessment process and the system of internal control. Such a dialogue should include a discussion of the vulnerability of the entity to fraudulent financial reporting and the entity's exposure to misappropriation of assets.¹²

¹¹ *Report of the NACD Best Practices Council: Coping with Fraud and Other Illegal Activity, A Guide for Directors, CEOs, and Senior Managers* (1998) sets forth "basic principles" and "implementation approaches" for dealing with fraud and other illegal activity.

¹² This dialogue may take place in connection with the communications to the audit committee described in paragraphs 80 and 81.