Edwards

Journal of Forensic Accounting
1524-5586/Vol. I(2000), pp. 193-214
© 2000 R.T. Edwards, Inc.
Printed in U.S.A.

Corporate Training Assessment Technique: Risk Factors Associated with Misappropriation of Assets

Carolyn A. Strand*[1], **Kathryn A.S. Lancaster**[2] and **Jerry Thorne**[3]

[1]Seattle Pacific University, Seattle, WA USA
[2]Cal Poly State University, San Luis Obispo, CA USA
[3]North Carolina A&T State University, Greensboro, NC USA

Due to rapid advances in technology, companies are spending record amounts of money on training as they seek to increase employee skills (Armour 1999). Because managers believe that corporate fraud is a growing problem, an important skill for all employees should be the ability to recognize the risk factors that are frequently associated with fraud. A number of instructional cases have been developed that focus on the problems of employee fraud and unethical management practices. Training materials and professional standards now include more detailed information on the subject of fraud and the auditor's responsibility, as well as management's responsibility, with respect to the detection of fraud. The next logical step is to assess employee training on this topic. In particular, can employees recognize risk factors when they are embedded in an actual instance of misappropriation of assets? We offer a case, based on an actual instance of misappropriation of assets, that may be used as a corporate training assessment technique (CTAT). Since training dollars are an important resource allocation decision, assessment of the training that is provided to employees is essential. Further, since effective teaching produces learning, then evaluation of learning is critical to assessing teaching effectiveness. We also include instructions for using the CTAT, teaching notes, and suggestions for developing additional instructional cases.

INTRODUCTION

Due to rapid advances in technology, companies are spending record amounts of money on training as they seek to increase employee skills and to boost retention (Armour 1999). Armour notes that employers spent $60.7 billion on training in the United States in 1998, which is a 26 percent increase from 1993. Wexley and Latham (1991) claim that almost all private and public organizations have formal training and development programs. These authors noted that some organizations spend as much as 15 percent of total payroll on these activities.

Corporate managers know that adequate training for employees can decrease the entity's liability risk, as well as the potential for error, fines and penalties (Clarke 1998; Linares 1999). To decrease an entity's vulnerability to misappropriation of assets, an important skill for all employees should be the ability to recognize risk factors that are frequently associated with this type of employee fraud. Further, since many corporate executives, managers, fraud detection experts, and researchers believe that corporate fraud is a growing problem, this should be an important topic for employee training.

Jurinski and Lippman (1999) note that most fraudulent activities are discovered through internal controls, by other employees noticing fraud, or by internal auditors. However, corporate managers who have responded to the KPMG fraud surveys indicate that they are less confident in their ability to recognize fraudulent activities. In the 1993 study, 96 percent of the managers who participated in the survey indicated they were knowledgeable about the ways in which fraud can occur in an organization. That number dropped to 84 percent in 1995, and to 80 percent in 1998. At the same time, approximately 75 percent of the managers indicated that they consider fraud to be a major problem for business and about two-thirds of the respondents believe the incidence of fraud will increase.

An equally important incentive for organizations to train employees on the topic of misappropriation of assets is the magnitude of losses that result from employee misbehavior. Calhoun and Luizzo (1992) point out that the cost of economic crime in 1990 was at least $114 billion, that one dollar is lost to external crime vis-à-vis eight dollars to internal crime, and that one out of three employees is involved in some type of fraud. However, it is difficult to detect unethical (or illegal) behavior such as fraud while the activity is in progress.

The purpose of this paper is to present a corporate training assessment technique (CTAT) that may be used to appraise corporate training on the topic of fraud. This CTAT was developed using the risk factors and procedures for assessing risk that may arise from misappropriation of assets, identified in paragraphs 18-25 of SAS No. 82, Consideration of Fraud in a Financial Statement Audit, (AICPA 1997).

The rest of the paper is organized as follows. The next section provides a literature review on studies that examine misappropriation of assets and red flags; section three discusses training and assessment techniques. The following section offers suggestions and conclusions. The Appendix contains a case, developed as a corporate training assessment technique, which includes teaching notes to assist the instructor in an evaluation of the effectiveness of corporate training on the topic of misappropriation of assets.

MISAPPROPRIATION OF ASSETS AND RI

Misappropriation of Assets

KPMG's annual fraud surveys indicate that the r
ation of assets. Norman Inkster, President of KI
believes that many factors in current business en
ing, and sophisticated technology – can create o
example, when a company downsizes, layers of r
inated. This usually results in more responsibil
managers might have more opportunities to ove
the detection of misappropriation of assets more

SAS No. 82, paragraph 20, notes that the auditc
employee dissatisfaction or adverse relationship
employees. However, if the auditor does becom
should take these into consideration when asses
SAS No. 82 offers several examples of potenti
that are known to the workforce, (2) employees
propriation who are known to be dissatisfied, o
lifestyle of employees with access to assets sus

Accounting researchers have examined the topic
ety of perspectives and have employed a variety
better understand and explain this problem. Th
misstatements arising from fraudulent financial
from misappropriation of assets (Heiman-Hoffn
1994; Johnson et al. 1993; Matsumura and Tu
1977). Recently, the Committee of Sponsoring
(COSO) sponsored a study on fraud (Beasley et
alleged fraudulent financial reporting by SEC
Auditing Enforcement Releases for the period
pany and management characteristics that coul

Seidman (1990) noted that not many studies ha
explanation for so few studies on this topic is th
more individuals to commit fraud – that is, the

ɔr employees can decrease the entity's lia-
nd penalties (Clarke 1998; Linares 1999).
riation of assets, an important skill for all
factors that are frequently associated with
ıy corporate executives, managers, fraud
ırporate fraud is a growing problem, this
g.

ıdulent activities are discovered through
ıd, or by internal auditors. However, cor-
G fraud surveys indicate that they are less
ctivities. In the 1993 study, 96 percent of
cated they were knowledgeable about the
ı. That number dropped to 84 percent in
ne, approximately 75 percent of the man-
ajor problem for business and about two-
fraud will increase.

to train employees on the topic of misap-
that result from employee misbehavior.
ɪt of economic crime in 1990 was at least
ıe vis-à-vis eight dollars to internal crime,
ı some type of fraud. However, it is diffi-
as fraud while the activity is in progress.

ıte training assessment technique (CTAT)
the topic of fraud. This CTAT was devel-
essing risk that may arise from misappro-
ɔf SAS No. 82, Consideration of Fraud in

e next section provides a literature review
ets and red flags; section three discusses
ng section offers suggestions and conclu-
l as a corporate training assessment tech-
e instructor in an evaluation of the effec-
ıppropriation of assets.

MISAPPROPRIATION OF ASSETS AND RED FLAGS

Misappropriation of Assets

KPMG's annual fraud surveys indicate that the most common type of fraud is misappropriation of assets. Norman Inkster, President of KPMG Investigation and Security in Toronto, believes that many factors in current business environments – such as downsizing, de-layering, and sophisticated technology – can create opportunities for fraud (Gauthier 1995). For example, when a company downsizes, layers of management oversight and control are eliminated. This usually results in more responsibility for fewer managers. In such instances, managers might have more opportunities to override internal controls, which would make the detection of misappropriation of assets more difficult.

SAS No. 82, paragraph 20, notes that the auditor is not required to plan the audit to detect employee dissatisfaction or adverse relationships that may exist between the entity and its employees. However, if the auditor does become aware of such problems, then the auditor should take these into consideration when assessing the risk of misappropriation of assets. SAS No. 82 offers several examples of potential problems: (1) anticipated future layoffs that are known to the workforce, (2) employees with access to assets susceptible to misappropriation who are known to be dissatisfied, or (3) known unusual changes in behavior or lifestyle of employees with access to assets susceptible to misappropriation.

Accounting researchers have examined the topic of fraud and fraudulent activity from a variety of perspectives and have employed a variety of research methodologies in an attempt to better understand and explain this problem. The majority of these studies have focused on misstatements arising from fraudulent financial reporting rather than misstatements arising from misappropriation of assets (Heiman-Hoffman et al. 1996; Ponemon 1994; Hooks et al. 1994; Johnson et al. 1993; Matsumura and Tucker 1992; Uecker et al. 1981; Baron et al. 1977). Recently, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) sponsored a study on fraud (Beasley et al. 1999). This study examines instances of alleged fraudulent financial reporting by SEC registrants reported in SEC Accounting and Auditing Enforcement Releases for the period 1987-1997. The report identifies key company and management characteristics that could help auditors recognize warning signs.

Seidman (1990) noted that not many studies have been reported on the topic of fraud. His explanation for so few studies on this topic is that such public information might encourage more individuals to commit fraud – that is, the information might teach others how to com-

mit fraud. Hollinger and Clark (1983) note that although relatively few researchers have empirically examined employee theft, several theoretical models have been developed to explain this problem of employee misbehavior: (1) external financial pressures, (2) workplace inequities, and (3) general moral laxity.

Seidman's (1990) study of fraud, an example of the first paradigm, used a survey instrument to gain insights pertaining to more than 500 cases of fraud. Seidman was able to develop a profile for the typical perpetrator, a description of commonly used schemes, and a summary of the methods used by perpetrators to avoid detection. Seidman claims that the outside activities of employees, their lifestyles, and their financial stresses all require careful and continuous scrutiny.

The second paradigm explains employee theft as an attempt by the employee to resolve various (perceived) workplace inequities. Fowler (1996) suggests that management style is frequently at fault in these situations, which can include management not listening to employee suggestions, employee perceptions of inadequate pay, employee beliefs that they are the subject of unfair treatment, and management ignoring outstanding employee achievement.

A number of studies examine the third category, which is also referred to as the deterrence doctrine. This theory assumes that the perceived threat of sanctions influences personal behavior, and has been investigated within a variety of contexts. Hollinger and Clark (1983) examined misappropriation of assets based on the deterrence doctrine. Randomly selected employees from three different industry sectors were asked to self-report their involvement in a number of property theft activities. The results indicate that the magnitude of employee theft is related to both the perceived certainty and severity of organizational sanctions. However, younger employees are not as deterrable as their older counterparts, especially under conditions of both high certainty and high severity of punishment.

Matsumura and Tucker (1992) investigated a form of the deterrence doctrine in an accounting setting by developing an experiment using game theory. The game involved one decision by the manager and two by the auditor. Within this context, the researchers investigated the effects of penalties, lawsuits, and loss of reputation. The results indicate that increasing the auditor's penalty decreased fraud; increasing the audit fee resulted in less fraud; and increased testing decreased fraud.

In other studies, researchers have found additional factors that may serve as a deterrent to fraud. Hooks et al. (1994) investigated the deterrent effect of a good communication sys-

tem within a corporation. After a review of
tle-blowing may be used as an effective ir
suggested that this represents a rational a
cealment whereas good communication fo
examined the deterrent effect of pre-empl
This study found that, across industries, o
theft and in terms of the deterrent effect of

Another form of deterrence is the presence
al. (1996) noted that the internal audit func
a wide variety of accounts in sustaining
cases involving the misappropriation of as
ing on the victims of the fraud, the characte
used, and the methods of detection. The re
trol environment) toward existing controls
authors also found that when proper sepa
lacked sufficient competence, and when en
(internal controls), the probability of frau
were often used to the advantage of the pe

Barton et al. (1996) suggest that not-for-
charitable organizations) are particularly su
of reasons. First, the operating environme
internal controls normally found in for-pro
the boards of directors of not-for-profits oft
insulates them from fraudulent activity. Th
a single individual who has a dominant pers
with a typically all-volunteer board of dire
(1996) report on such an instance in their
director misused over $244,000. The autho
for-profit entity was the lack of a strong in

Several researchers and forensic accounta
fraudulent disbursement of funds) is the n
propriate assets (Robertson 1997; Thornhill
accountant, notes that purchasing fraud fi
which involves the entry of false or fraudule

at although relatively few researchers have
theoretical models have been developed to
(1) external financial pressures, (2) work-

the first paradigm, used a survey instrument
es of fraud. Seidman was able to develop a
of commonly used schemes, and a summa-
detection. Seidman claims that the outside
eir financial stresses all require careful and

s an attempt by the employee to resolve var-
1996) suggests that management style is fre-
nclude management not listening to employ-
quate pay, employee beliefs that they are the
noring outstanding employee achievement.

y, which is also referred to as the deterrence
ved threat of sanctions influences personal
iety of contexts. Hollinger and Clark (1983)
the deterrence doctrine. Randomly selected
were asked to self-report their involvement
sults indicate that the magnitude of employ-
ity and severity of organizational sanctions.
rable as their older counterparts, especially
h severity of punishment.

rm of the deterrence doctrine in an account-
game theory. The game involved one deci-
ithin this context, the researchers investigat-
reputation. The results indicate that increas-
asing the audit fee resulted in less fraud; and

onal factors that may serve as a deterrent to
terrent effect of a good communication sys-

tem within a corporation. After a review of the relevant literature, they concluded that whistle-blowing may be used as an effective internal control mechanism to deter fraud. They suggested that this represents a rational approach to deterrence since fraud involves concealment whereas good communication fosters an open environment. Parilla et al. (1988) examined the deterrent effect of pre-employment screening and the threat of punishment. This study found that, across industries, organizations vary in terms of victimization from theft and in terms of the deterrent effect of controls to reduce organizational theft.

Another form of deterrence is the presence of internal auditors in an organization. Welch et al. (1996) noted that the internal audit function restricts the ability of perpetrators to access a wide variety of accounts in sustaining a fraud. These authors analyzed 2,573 reported cases involving the misappropriation of assets in both the public and private sectors, focusing on the victims of the fraud, the characteristics of the perpetrators, the schemes that were used, and the methods of detection. The results indicate that poor company attitudes (control environment) toward existing controls helped the perpetrators commit the fraud. These authors also found that when proper separation of duties was lacking, when employees lacked sufficient competence, and when employees were able to manipulate documentation (internal controls), the probability of fraud increased significantly. Weak internal controls were often used to the advantage of the perpetrator.

Barton et al. (1996) suggest that not-for-profit entities (such as volunteer, religious, and charitable organizations) are particularly susceptible to an occurrence of fraud for a number of reasons. First, the operating environment of a not-for-profit usually does not have the internal controls normally found in for-profit entities. Second, the management team and the boards of directors of not-for-profits often believe that their charitable mission somehow insulates them from fraudulent activity. Third, not-for-profit entities are often managed by a single individual who has a dominant personality. When a dominant manager is combined with a typically all-volunteer board of directors, the results can be disastrous. Barton et al. (1996) report on such an instance in their case study of a not-for-profit entity where the director misused over $244,000. The authors note that the most serious problem for this not-for-profit entity was the lack of a strong internal control structure.

Several researchers and forensic accountants have concluded that purchasing fraud (i.e., fraudulent disbursement of funds) is the most prevalent method employees use to misappropriate assets (Robertson 1997; Thornhill 1996; Levy 1985). Thornhill (1996), a forensic accountant, notes that purchasing fraud fits into the broad category of input tampering, which involves the entry of false or fraudulent data into a computer and can include data that

have been altered, forged, or counterfeited. Thornhill (1996) suggests that the persons who most often perpetrate a purchasing fraud are trusted, authorized computer users, who have either neutralized or avoided any controls that are in place.

Red Flags

It is difficult to detect the misappropriation of assets while the fraudulent activity is in progress. As Albrecht (1996) points out, it is not an event that is normally witnessed first-hand. Rather, it is "...a crime shrouded in ambiguity, and is sometimes difficult even to determine whether or not a crime has actually been committed" (p.26). Too frequently the scheme is discovered by accident. Green and Calderon (1996) believe, however, that "red flags" can create crucial pieces of evidence in signaling the likelihood of fraud. Further, they argue that the internal auditors are optimally positioned to identify and assess any red flags that are present.

According to Uretsky (1980), red flags are situational indicators that suggest the auditor should be more watchful than normal. When more than one red flag is present, the auditor should move from professional skepticism to suspicion. Albrecht et al. (1980) conducted an extensive review of existing fraud-related literature to identify the individual and organizational factors (red flags) that might be used by auditors to detect fraud. These authors acknowledged that a single definition of fraud was problematic, and concluded that the following definition was preferable for their study. Fraud is: (1) improper actions resulting in a material misstatement of the financial statements and is harmful to shareholders or creditors; (2) improper actions resulting in the defrauding of the consumer public (such as false advertising); (3) embezzlement and defalcations perpetrated by employees against their employers; or (4) other improper actions such as bribes, kickbacks, violations of regulatory agency rules, and failure to maintain an adequate internal control system.

Albrecht et al.'s (1980) study resulted in a list of 87 red flags for fraud that were divided into two categories: (1) factors that motivate individuals to commit fraud on behalf of the company (e.g., fraudulent financial statements), and (2) factors that motivate individuals to commit fraud against the company (e.g., misappropriation of assets). A number of studies or surveys have examined or added to Albrecht et al.'s list (Albrecht and Romney 1986; Pincus 1989; Loebbecke et al. 1989; Beasley 1996; Heiman-Hoffman et al. 1996; Weisborn and Norris 1997; Summers and Sweeney 1998; and the annual KPMG Fraud Surveys).

Albrecht and Romney (1986) empirically analyzed the predictive ability of the 87 red flags identified in Albrecht et al.'s (1980) study. Results suggest that only about one-third of the

87 red flags were significant predictors of
misstated. Several of the red flags that
require executives to take vacations of m
trust in key executives (overlooking contr
enforce controls; and, (4) poor accounting

Pincus (1989) utilized a field experiment
naire. The author identified a red flags que
auditors assess the risk of materially m
engagements. The subjects were 137 mid
age of 18 months experience being in cha
half of the auditors assessed a case where
ed due to fraud and the other half assesse
The results indicate that the auditors who
risk assessment considered a more compr
cators than did those subjects who did not
thetical case, and acknowledged that usi
should increase the likelihood that the resu
al audit situation.

Based on SAS No. 53 (superseded by SA
vey to study auditors' experience with ma
partners of KPMG who had one or more
material defalcation or material misstat
described an irregularity with which (s)he
were present in a large proportion of the
research, the authors found that "...where
that would allow either management fraud
an error to occur" (p. 25).

Heiman-Hoffman et al. (1996) utilized a s
ion of some warning signals of fraud. Spe
tial warning signs as to their relative imp
The auditors who participated in this study
largest accounting firms. Those who resp
to be the most important red flag. Overal
that a weak control environment is an im
activities by management.

87 red flags were significant predictors of fraud where financial statements were materially misstated. Several of the red flags that were significant predictors were: (1) failure to require executives to take vacations of more than one or two days at a time; (2) too much trust in key executives (overlooking controls); (3) inadequate internal controls or failure to enforce controls; and, (4) poor accounting records.

Pincus (1989) utilized a field experiment to examine the efficacy of a red flags questionnaire. The author identified a red flags questionnaire as an audit tool that is designed to help auditors assess the risk of materially misstated financial statements on ordinary audit engagements. The subjects were 137 mid-level auditors in a large CPA firm, with an average of 18 months experience being in charge of fieldwork for their clients. Approximately half of the auditors assessed a case where the financial statements were materially misstated due to fraud and the other half assessed a parallel case with no material misstatements. The results indicate that the auditors who used a red flags questionnaire to aid them in fraud risk assessment considered a more comprehensive and uniform set of potential fraud indicators than did those subjects who did not use a questionnaire. The author utilized a hypothetical case, and acknowledged that using a fraud case developed from a real situation should increase the likelihood that the results of the experiment would generalize to an actual audit situation.

Based on SAS No. 53 (superseded by SAS No. 82), Loebbecke et al. (1989) utilized a survey to study auditors' experience with material irregularities. The subjects were 165 audit partners of KPMG who had one or more experiences with a material irregularity (either a material defalcation or material misstatement of financial statements). Each subject described an irregularity with which (s)he had experience. The results indicate that red flags were present in a large proportion of the cases of material management fraud. As in prior research, the authors found that "...where controls are weak, a significant condition exists that would allow either management fraud (misstated financial statements), a defalcation, or an error to occur" (p. 25).

Heiman-Hoffman et al. (1996) utilized a survey to query 130 auditors regarding their opinion of some warning signals of fraud. Specifically, the auditors were asked to rank 30 potential warning signs as to their relative importance in spotting fraudulent financial reporting. The auditors who participated in this study were from several offices of one of the (then) six largest accounting firms. Those who responded to the survey considered client dishonesty to be the most important red flag. Overall, the results are consistent with prior research in that a weak control environment is an important indicator of fraudulent financial reporting activities by management.

Weisborn and Norris' (1997) study used the 87 red flags that were validated in Albrecht and Romney's (1986) study and applied them to 30 well-known and relatively infamous cases of fraudulent financial reporting that were included in the text, *Contemporary Auditing: Issues and Cases* by Knapp (1986). The results of this study suggest that dishonest or unethical management is the most important red flag for detecting management fraud, followed by: (2) too much trust in key executives (overriding controls); (3) domination of the company by one or two strong individuals; and (4) inadequate internal controls or failure to enforce controls.

Summers and Sweeney (1998) focused on the association between financial statement fraud and a specific risk factor that was not identified as a "red flag" in SAS No. 82 or in prior research. These authors claim that insider trading should be an important risk factor for auditors who are attempting to detect fraud and to regulators who are monitoring insider trading. Specifically, Summers and Sweeney hypothesized that during the period of fraudulent financial reporting by entity officials, insiders in the company will strategically reduce their net position in the entity's stock. The results indicate that insiders in companies with fraudulent financial statements did in fact reduce their net position in the entity's stock through a high level of stock sales activity.

SAS No. 82 provides examples of red flags (risk factors) believed to be associated with misstatements arising from misappropriation of assets. This Statement identifies two categories of risk factors: (a) the general susceptibility of assets to misappropriation, and (b) specific control weaknesses. The initial category pertains to the nature of an entity's assets and the degree to which they are subject to theft, while the latter pertains to the lack of controls designed to prevent or detect the misappropriation of assets (AICPA 1997, para. 18). Table 1 provides a list of the two groups of risk factors derived from SAS No. 82.

TRAINING AND ASSESSMENT TECHNIQUES

A number of instructional cases, which describe employee fraud and unethical management practices, have been developed to train employees in the detection of risk factors that are frequently associated with the misappropriation of assets. Training materials and professional standards now include more detailed information on the subject of fraud and the auditor's responsibility, as well as management's responsibility, with respect to the detection of fraud. The next logical step should be to assess employee training on this topic – did the employees learn what you taught them? In particular, can employees recognize risk factors when they are embedded in an actual instance of misappropriation of assets?

Table 1 Risk Factors Re

a. Risk Factors Relating to Susc
- Large amounts of cash on ha
- Inventory characteristics suc
- Easily convertible assets
- Fixed asset characteristics, su

b. Risk Factors Relating to Cont
- Lack of management oversig
- No screening procedures for
- Lack of appropriate segregati
- Lack of appropriate authoriza
- Poor physical safeguards ove
- Lack of documentation for tr
- Lack of mandatory vacations

Source: Statement on Auditing Stan

Corporate training assessment technique the instructor has taught and what the e that a gap does exist, that employees do the expectation is that the instructor wou ensure that the learning objectives are lecture format, the instructor might cho these methods to help employees recog employee misbehavior.

According to Cottell and Harwood (19 feedback so that instructors may chang improve student learning. Further, Ang techniques on a regular basis provide become more self-assessing, more self-d

Further, training (educational) assessme Cross 1993). Rebele et al. (1998) descri as follows. Because effective teaching p tial to assessing teaching effectiveness.

red flags that were validated in Albrecht and
well-known and relatively infamous cases of
d in the text, *Contemporary Auditing: Issues*
is study suggest that dishonest or unethical
detecting management fraud, followed by:
g controls); (3) domination of the company
equate internal controls or failure to enforce

ssociation between financial statement fraud
d as a "red flag" in SAS No. 82 or in prior
ding should be an important risk factor for
d to regulators who are monitoring insider
ypothesized that during the period of fraud-
ders in the company will strategically reduce
ults indicate that insiders in companies with
luce their net position in the entity's stock

factors) believed to be associated with mis-
ets. This Statement identifies two categories
assets to misappropriation, and (b) specific
ns to the nature of an entity's assets and the
le the latter pertains to the lack of controls
ion of assets (AICPA 1997, para. 18). Table
rs derived from SAS No. 82.

QUES

employee fraud and unethical management
es in the detection of risk factors that are fre-
assets. Training materials and professional
on on the subject of fraud and the auditor's
ibility, with respect to the detection of fraud.
yee training on this topic – did the employ-
can employees recognize risk factors when
appropriation of assets?

Table 1 Risk Factors Relating to Misappropriation of Assets

a. Risk Factors Relating to Susceptibility of Assets to Misappropriation:
- Large amounts of cash on hand
- Inventory characteristics such as small size, high demand, high value
- Easily convertible assets
- Fixed asset characteristics, such as small size, marketability

b. Risk Factors Relating to Controls:
- Lack of management oversight
- No screening procedures for employees with access to vulnerable assets
- Lack of appropriate segregation of duties
- Lack of appropriate authorization and approval of transactions
- Poor physical safeguards over cash, investments, inventory, or fixed assets
- Lack of documentation for transactions
- Lack of mandatory vacations for employees

Source: Statement on Auditing Standards No. 82 (AICPA 1997).

Corporate training assessment techniques (CTATs) are used to assess the gap between what the instructor has taught and what the employees have learned. If the instructor discovers that a gap does exist, that employees do not recognize these risk factors (or only a few), then the expectation is that the instructor would adjust the training methodology that was used to ensure that the learning objectives are met. For example, if the training was delivered via lecture format, the instructor might choose cases, instructional videos, or a combination of these methods to help employees recognize a wider variety of the risk factors that signal employee misbehavior.

According to Cottell and Harwood (1998), assessment can provide important and timely feedback so that instructors may change course coverage and/or teaching approaches to improve student learning. Further, Angelo and Cross (1993) believe that using assessment techniques on a regular basis provide students (employees) the necessary feedback to become more self-assessing, more self-directed, and more effective learners.

Further, training (educational) assessment may improve the quality of learning (Angelo and Cross 1993). Rebele et al. (1998) describe the underlying premise of assessment techniques as follows. Because effective teaching produces learning, an evaluation of learning is essential to assessing teaching effectiveness. In general, corporate training assessment techniques

(CTATs) have two characteristics: (1) they encourage both trainers and employees to engage in a constructive discussion of learning, and (2) they promote learning of the subject matter while providing feedback on teaching effectiveness (Beard 1993). CTATs should be anonymous exercises so that employees will be more likely to provide corporate trainers with unbiased feedback on what, how much, and how well the employees are learning.

The *Springer Junction* case (see Appendix) is constructed from an actual instance of misappropriation of assets that was the result of a governmental employee creating fictitious invoices. This case may be used to reinforce and assess employee learning subsequent to training on internal controls and fraud, as well as any instructional training that incorporates fraud awareness, and the risk factors that are typically present in actual instances of misappropriation of assets. The instructor may use the case as a stand-alone CTAT, or it may be used in conjunction with other instructional cases that focus on employee fraud and unethical management practices (Dwyer 1998, Green and Calderon 1994, Mills 1995). Surveys of corporate training directors indicate that case studies have repeatedly received high ratings for developing problem-solving skills (Kaupins 1997). In other research, case studies have been shown to help develop critical thinking and judgment abilities (Anthony 1974; Subotnik 1987; Campbell and Lewis 1991). The intent of these instructional tools is for employees to build their recognition skills of risk factors associated with the misappropriation of assets, and for instructors to assess the effectiveness of this method of instructional delivery as it pertains to learning about fraud risk factors.

Such instruction and reinforcement should help employees gain expertise in the area of red flags and employee misbehavior. For example, Bonner and Pennington's (1991) results suggest that instruction is important for learning and for good task performance by experts. Bonner (1990) noted that task-specific knowledge aided experienced professionals in making better decisions. Based on these results, Bonner suggested that training and decision aids could be useful in improving performance. The timing of this instruction appears to be important, also, based on Bonner et al.'s (1997) finding that instruction prior to experiencing an event is instrumental to improved learning. Johnson et al. (1993) conclude that to successfully detect fraud one must not only continually acquire new knowledge, but also learn how to use what they already know.

Bonner and Walker (1994) studied the effectiveness of various combinations of instruction and experience (practice and feedback) in producing this knowledge. Their results suggest that combinations of instruction and no experience, or instruction and practice without feedback do not produce knowledge. However, practice with explanatory feedback was helpful.

Choo's (1996) results show that repeated e
expertise in a going-concern task, which su
expertise by prolonged practice (Spires 199

SUGGESTIONS AND CONCLUSIONS

The *Springer Junction* case in the Appendi
of assets that may be used to help employee
are frequently associated with employee fra
cific CTATs throughout a training course, a
lar. Any actual instance of fraud may be tak
journal. Next, the instructor would select th
the scenario. Perhaps the instructor might r
CTAT to determine whether the employees
setting.

The annual fraud surveys conducted by KP
ee misconduct is a growing concern to the b
is relevant for corporate training if employe
their work environment. Employees may g
risk factors that are commonly associated w
included in SAS No. 82. Similarly, trainers
provided to employees to increase the effica

REFERENCES

Albrecht, W. 1996. Employee fraud. *The Inter*

_____ and M. Romney. 1986. Red-flagging
Accounting 3: 323-334.

_____, D. Charrington, I. Payne, A. Roe, and M.
tion of fraud. In *Management Fraud: De*
Willingham. New York, NY: Petrocelli Bo

American Institute of Certified Public Account
Financial Statement Audit. *Statement on*
Institute of Certified Public Accountants, In

Angelo, T. and K. Cross. 1993. *Classroom*
Teachers. San Francisco, CA: Jossey-Bass

Anthony, R. 1974. The case method in acco
Prospects, edited by J. Edwards. Sarasota,

ırage both trainers and employees to engage
they promote learning of the subject matter
veness (Beard 1993). CTATs should be
e more likely to provide corporate trainers
d how well the employees are learning.

nstructed from an actual instance of misap-
governmental employee creating fictitious
nd assess employee learning subsequent to
s any instructional training that incorporates
ically present in actual instances of misap-
e case as a stand-alone CTAT, or it may be
es that focus on employee fraud and unethi-
and Calderon 1994, Mills 1995). Surveys
e studies have repeatedly received high rat-
pins 1997). In other research, case studies
ing and judgment abilities (Anthony 1974;
ne intent of these instructional tools is for
k factors associated with the misappropria-
ffectiveness of this method of instructional
k factors.

employees gain expertise in the area of red
Bonner and Pennington's (1991) results sug-
nd for good task performance by experts.
ge aided experienced professionals in mak-
onner suggested that training and decision
The timing of this instruction appears to be
finding that instruction prior to experienc-
ng. Johnson et al. (1993) conclude that to
ntinually acquire new knowledge, but also

ness of various combinations of instruction
cing this knowledge. Their results suggest
ce, or instruction and practice without feed-
tice with explanatory feedback was helpful.

Choo's (1996) results show that repeated exposure may be an alternative proxy for audit expertise in a going-concern task, which supports earlier findings that novice auditors gain expertise by prolonged practice (Spires 1991).

SUGGESTIONS AND CONCLUSIONS

The *Springer Junction* case in the Appendix represents an actual case of misappropriation of assets that may be used to help employees practice the recognition of common clues that are frequently associated with employee fraud. If a trainer wishes to use several fraud-specific CTATs throughout a training course, additional cases may be developed that are similar. Any actual instance of fraud may be taken from a newspaper, news journal, or business journal. Next, the instructor would select three risk factors from SAS No. 82 to include in the scenario. Perhaps the instructor might repeat a risk factor or two that was used in this CTAT to determine whether the employees could recognize that risk factor(s) in a different setting.

The annual fraud surveys conducted by KPMG continue to document the fact that employee misconduct is a growing concern to the business community, which implies that the topic is relevant for corporate training if employees are to be properly prepared for this threat in their work environment. Employees may greatly benefit from periodic instruction on the risk factors that are commonly associated with the misappropriation of assets, such as those included in SAS No. 82. Similarly, trainers should routinely assess the training that is being provided to employees to increase the efficacy of such instruction.

REFERENCES

Albrecht, W. 1996. Employee fraud. *The Internal Auditor* 53(October): 26-37.

_____ and M. Romney. 1986. Red-flagging management fraud: A validation. *Advances in Accounting* 3: 323-334.

_____, D. Charrington, I. Payne, A. Roe, and M. Romney. 1980. Auditor involvement in the detection of fraud. In *Management Fraud: Detection and Deterrence*, edited by R. Elliott and J. Willingham. New York, NY: Petrocelli Books, Inc.

American Institute of Certified Public Accountants (AICPA). 1997. Consideration of Fraud in a Financial Statement Audit. *Statement on Auditing Standards* No. 82. New York: American Institute of Certified Public Accountants, Inc.

Angelo, T. and K. Cross. 1993. *Classroom Assessment Techniques: A Handbook for College Teachers*. San Francisco, CA: Jossey-Bass Publishers.

Anthony, R. 1974. The case method in accounting. In *Accounting Education: Problems and Prospects*, edited by J. Edwards. Sarasota, FL: AAA.

Armour, S. 1999. Training takes front seat at offices. *USA Today* (January 19): B6.

Baron, C., D. Johnson, D. Searfoss, and C. Smith. 1977. Uncovering corporate irregularities: Are we closing the expectation gap? *Journal of Accountancy* 163 (10): 56-66.

Barton, T., W. Shenkir, and J. McEldowney. 1996. The case of Dr. Grayson: Fraud and abuse at a not for profit. *The CPA Journal* 66(2): 46-50.

Beard, V. 1993. Classroom assessment techniques (CATs): Tools for improving accounting education. *Journal of Accounting Education* 11: 293-300.

Beasley, M., J. Carcello, and D. Hermanson. 1999. COSO's new fraud study: What it means for CPAs. *Journal of Accountancy* 187 (5): 12-14.

Beasley, M. 1996. An empirical analysis of the relation between the board of director composition and financial statement fraud. *The Accounting Review* 71(4): 443-465.

Bonner, S. 1990. Experience effects in auditing: The role of task-specific knowledge. *The Accounting Review* 65(1): 72-92.

_____, and N. Pennington. 1991. Cognitive processes and knowledge as determinants of auditor expertise. *Journal of Accounting Literature* 10: 1-50.

_____, and P. Walker. 1994. The effects of instruction and experience on the acquisition of auditing knowledge. *The Accounting Review* 69 (1): 157-178.

_____, R. Libby, and M. Nelson. 1997. Audit category knowledge as a precondition to learning from experience. Accounting, Organizations, and Society 22(5): 387-410.

Calhoun, C. and A. Luizzo. 1992. Team partners in fraud detection. *The CPA Journal* 62(10): 32-36.

Campbell, J. and W. Lewis. 1991. Using cases in accounting classes. *Issues in Accounting Education* 6(2): 276-283.

Choo, F. 1996. Auditors' knowledge content and judgment performance: A cognitive script approach. Accounting, Organizations, and Society 21(4): 339-359.

Clarke, R. 1998. Investing in human assets. Healthcare Financial Management 52(11): 16.

Cottell, P. and E. Harwood. 1998. Using classroom assessment technique to improve student learning in accounting classes. *Issues in Accounting Education* 13(3): 551-563.

Dwyer, P. 1998. Embezzlement at the University of California: An instructional case in employee fraud. *Issues in Accounting Education* 13(4): 975-984.

Fowler, B. 1996. Are embezzlers at work? Supervision 57(February): 6-9.

Gauthier, Y. 1995. Forever fraud. Internal Auditor 52(October): 26-29.

Gautschi, T. 1998. Develop your intellectual capital. *Design News* 53(14): 170.

Green, B. and T. Calderon. 1994. Using real-world cases to illustrate the power of analytical procedures. *Journal of Accounting Education* 12(3): 245-268.

_____. 1996. Information privity and the internal auditor's assessment of fraud risk factors. *Internal Auditing* 11(4): 4-15.

Heiman-Hoffman, V., K. Morgan, and J. Patto reporting. *Journal of Accountancy* 182(4)

Hollinger, R. and J. Clark. 1983. Deterrence in ity, and employee theft. Social Forces 62(

Hooks, K., S. Kaplan, and J. Schultz. 1994. E and detection. *Auditing: A Journal of Pra*

Johnson, P., S. Grazioli, and K. Jamal. 1993. nition. Accounting, Organizations, and So

Jurinski J. and E. Lippman. 1999. Preventing

Kaupins, G. 1997. Trainer opinions of popul *for Business* 73(1): 5-8.

Knapp, M. 1986. *Contemporary Auditing:* Company.

KPMG. 1998, 1995, 1994, 1993. Fraud Surve

Levy, M. 1985. Financial fraud: Schemes and

Linares, M. 1999. A watchful eye. Strategic F

Loebbecke, J., M. Eining, and J. Willingham. ties: Frequency, nature, and detectability. 28.

Matsumura, E. and R. Tucker. 1992. Fraud d *Review* 67(4): 753-782.

Mills, P. 1995. Milianaw University: An instr *Accounting Education* 10(2): 377-387.

Parilla, P., R. Hollinger, and J. Clark. 1988. Or employee theft. *Social Science Quarterly*

Pincus, K. 1989. The efficacy of a red flags Accounting, Organizations, and Society 1

Ponemon, L. 1994. Whistle-blowing as an in tional considerations. *Auditing: A Journal*

Rebele, J., B. Apostolou, F. Buckless, J. Hassel cation literature review (1991-1997), part I faculty issues. *Journal of Accounting Edu*

Robertson, J. 1997. Fraud Examination for M

Seidman, J. 1990. A case study of employee f 28-35.

Spires, E. 1991. Auditors' evaluation of test- 259-276.

es. *USA Today* (January 19): B6.
1977. Uncovering corporate irregularities: Are
countancy 163 (10): 56-66.
The case of Dr. Grayson: Fraud and abuse at a
.
(CATs): Tools for improving accounting
11: 293-300.
9. COSO's new fraud study: What it means for
4.
lation between the board of director composition
Review 71(4): 443-465.
g: The role of task-specific knowledge. *The*
esses and knowledge as determinants of auditor
0: 1-50.
tion and experience on the acquisition of auditing
57-178.
gory knowledge as a precondition to learning from
ociety 22(5): 387-410.
n fraud detection. *The CPA Journal* 62(10): 32-
s in accounting classes. *Issues in Accounting*
and judgment performance: A cognitive script
ciety 21(4): 339-359.
hcare Financial Management 52(11): 16.
n assessment technique to improve student
unting Education 13(3): 551-563.
of California: An instructional case in employee
975-984.
vision 57(February): 6-9.
r 52(October): 26-29.
al. *Design News* 53(14): 170.
d cases to illustrate the power of analytical proce-
): 245-268.
uditor's assessment of fraud risk factors. *Internal*

Heiman-Hoffman, V., K. Morgan, and J. Patton. 1996. The warning signs of fraudulent financial reporting. *Journal of Accountancy* 182(4): 75-77.

Hollinger, R. and J. Clark. 1983. Deterrence in the workplace: Perceived certainty, perceived severity, and employee theft. Social Forces 62(2): 398-418.

Hooks, K., S. Kaplan, and J. Schultz. 1994. Enhancing communication to assist in fraud prevention and detection. *Auditing: A Journal of Practice & Theory* 13(2): 86-117.

Johnson, P., S. Grazioli, and K. Jamal. 1993. Fraud detection: Intentionality and deception in cognition. Accounting, Organizations, and Society 18(5): 467-488.

Jurinski J. and E. Lippman. 1999. Preventing fraud. *Strategic Finance* (April): 64-67.

Kaupins, G. 1997. Trainer opinions of popular corporate training methods. *Journal of Education for Business* 73(1): 5-8.

Knapp, M. 1986. *Contemporary Auditing: Issues and Cases.* St. Paul, MN: West Publishing Company.

KPMG. 1998, 1995, 1994, 1993. Fraud Survey Results. New York, NY: KPMG.

Levy, M. 1985. Financial fraud: Schemes and indicia. *Journal of Accountancy* 160(8): 78-87.

Linares, M. 1999. A watchful eye. Strategic Finance (April): 69-71.

Loebbecke, J., M. Eining, and J. Willingham. 1989. Auditors' experience with material irregularities: Frequency, nature, and detectability. *Auditing: A Journal of Practice & Theory* 9(1): 1-28.

Matsumura, E. and R. Tucker. 1992. Fraud detection: A theoretical foundation. *The Accounting Review* 67(4): 753-782.

Mills, P. 1995. Milianaw University: An instructional case in internal control and ethics. *Issues in Accounting Education* 10(2): 377-387.

Parilla, P., R. Hollinger, and J. Clark. 1988. Organizational control of deviant behavior: The case of employee theft. *Social Science Quarterly* 69(2): 261-280.

Pincus, K. 1989. The efficacy of a red flags questionnaire for assessing the possibility of fraud. Accounting, Organizations, and Society 14(1): 153-163.

Ponemon, L. 1994. Whistle-blowing as an internal control mechanism: Individual and organizational considerations. *Auditing: A Journal of Practice & Theory* 13(2): 118-130.

Rebele, J., B. Apostolou, F. Buckless, J. Hassell, L. Paquette, and D. Stout. 1998. Accounting education literature review (1991-1997), part II: Students, educational technology, assessment, and faculty issues. *Journal of Accounting Education* 16(2): 179-245.

Robertson, J. 1997. Fraud Examination for Managers and Auditors. Austin, TX: Viesca Books.

Seidman, J. 1990. A case study of employee fraud (reprint of 1939 article). *The CPA Journal* (1): 28-35.

Spires, E. 1991. Auditors' evaluation of test-of-control strength. *The Accounting Review* 66(2): 259-276.

Subotnik, D. 1987. What accounting can learn from legal education. *Issues in Accounting Education* 2(2): 313-324.

Summers, S. and J. Sweeney. 1998. Fraudulently misstated financial statements and insider trading: An empirical analysis. *The Accounting Review* 73(1): 131-146.

Thornhill, W. 1996. Input tampering. *Internal Auditing* 12 (Summer): 46-50.

Uecker, W., A. Brief, and W. Kinney. 1981. Perception of the internal and external auditor as a deterrent to corporate irregularities. *The Accounting Review* 61(3): 465-478.

Uretsky, M. 1980. An interdisciplinary approach to the study of management fraud. In *Management Fraud: Detection and Deterrence*, edited by R. Elliott and J. Willingham. New York, NY: Petrocelli Books, Inc.

Weisenborn, D. and D. Norris. 1997. Red flags of management fraud. *National Public Accountant* 42(March/April): 29-33.

Welch, S., S. Holmes, and R. Strawser. 1996. The inhibiting effect of internal auditors on fraud. *Internal Auditing* 12(Fall): 23-32.

Wexley, K. and G. Latham. 1991. *Developing and Training Human Resources in Organizations*. 2nd Edition. New York, NY: HarperCollins Publishers, Inc.

APPENDIX

Department of Finance City of Springer Junction

Instructions for Trainees: The case mate
Organizational Chart for a governmental office. T
listing of departmental personnel, along with thei
the Background Information and Organizational (
that is contained in the Scenario. Using these pi
questions that follow the scenario. Each questior
each question to the best of your ability. There ar
situation.

BACKGROUND INFORMATION:

Stan Wandell was pleased. He recently accept
Junction, a city with a population just over 60,0
past several decades, and collected over $80 mi
fiscal year.

Stan's picture has already appeared on the fro
Junction newspaper. In the interview for that fe
of the Finance Department and identified a nu
However, Stan noted that initially he planned t
day-to-day concerns he had about the Departme

First, he plans to streamline procedures in the I
are rarely used. He also wants to improve the e
can be provided quickly when needed by citiz
siders' confidence in the Department. Stan is pa
employee turnover. Five of the seven employee
less than a year. Stan has been told that the prior
oriented, and that this may have caused Departr

Stan noted that the City does not have an inter
Quigley & Matherson, CPAs has been the Ind