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

Carolyn A. Strand*, Kathryn A.S. Lancaster* and Jerry Thorne*

1Seattle Pacific University, Seattle, WA USA 
2Cal Poly State University, San Luis Obispo, CA USA 
3North 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 rate of assets. Norman Inkster, President of KPMG, believes that many factors in current business environments, and sophisticated technology – can create an example, when a company downsizes, layers of management are eliminated. This usually results in more responsibilities for fewer employees. However, if the auditor does not take these into consideration when assessing the detection of misappropriation of assets, the incidence of fraud will increase.

SAS No. 82, paragraph 20, notes that the auditor should consider employee dissatisfaction or adverse relationships with the workforce, (2) employees who are known to be dissatisfied, or (3) employees with access to assets. Accounting researchers have examined the topic of perspectives and have employed a variety of methodologies to better understand and explain this problem. Th misstatements arising from fraudulent financial reporting by SEC Enforcement Releases for the period 1990-1997. Recently, the Committee of Sponsoring Organizations (COSO) sponsored a study on fraud (Beasley et al. 1993; Johnson et al. 1993; Matsumura and Tu 1977). Seidman (1990) noted that not many studies have been conducted on this topic is that more individuals to commit fraud – that is, the
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 deterreable 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 system within a corporation. After a review of whistleblowing may be used as an effective it suggested that this represents a rational approach whereas good communication systems have been long-term. This study found that, across industries, over theft and in terms of the deterrent effect of

Another form of deterrence is the presence of controls. Matsumura and Tucker (1992) noted that the internal audit function in charitable organizations is particularly significant in cases involving the misappropriation of assets. The authors also found that when proper segregation of duties was lacking, the probability of fraud was often used to the advantage of the perpetrator.

Barton et al. (1996) suggest that not-for-profit charitable organizations are particularly susceptible to fraud. First, the operating environment is different than for-profit organizations. Internal controls normally found in for-profits are not always present in not-for-profits. The lack of internal controls allows them to be used in fraudulent activity. Typically, a single individual who has a dominant personality can use the internal controls (internal controls) to the advantage of the perpetrator. With a typically all-volunteer board of directors, it is difficult to detect instances of fraud.

Several researchers and forensic accountants have identified fraudulent disbursement of funds as the most frequent form of fraud (Robertson 1997; Thornhill and Thorne 1997). An accountant, not-for-profit, notes that purchasing fraud is common, involving the entry of false or fraudulent disbursement of funds (Robertson 1997; Thornhill and Thorne 1997).
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 of commonly used schemes, and a summar­ detection. Seidman claims that the outside their financial stresses all require careful and is an attempt by the employee to resolve vari- (1996) suggests that management style is fre- include management not listening to employ­quate pay, employee beliefs that they are the ignoring outstanding employee achievement. 1, which is also referred to as the deterrence lived threat of sanctions influences personal ity of contexts. Hollinger and Clark (1983) the deterrence doctrine. Randomly selected were asked to self-report their involvement results indicate that the magnitude of employ­ and severity of organizational sanctions, rable as their older counterparts, especially h severity of punishment. 1orm of the deterrence doctrine in an account- game theory. The game involved one deci- within this context, the researchers investigat- reputation. The results indicate that increasing the audit fee resulted in less fraud; and 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; Weisbom 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 more than forty-five days; trust in key executives (overlooking controls); and, (4) poor accounting procedures. Pincus (1989) utilized a field experiment involving 137 mid-level auditors. The author identified a red flag questionnaire to assess the risk of materially misstated financial statements. The subjects were 137 mid-level auditors divided into two groups, one of which assessed a hypothetical case where fraud had occurred and the other half assessed a case where the fraud had not occurred. The results indicate that the auditors who assessed the case where fraud had occurred were more likely to identify red flags that would increase the likelihood that the results of the audit situation.

Based on SAS No. 53 (superseded by SAS No. 99), the authors used a survey to study auditors' experience with material misstatements. The subjects were partners of KPMG who had one or more material misstatements. The descriptions of some warning signs of fraud described an irregularity with which (s)he was involved. Over half of the irregularities described were present in a large proportion of the research, the authors found that "...where one management fraud exists, an error to occur" (p. 25).

Heiman-Hoffman et al. (1996) utilized a questionnaire to identify some warning signs of fraud. Special warning signals as to their relative importance. The auditors who participated in this study are from the largest accounting firms. Those who respond to the red flags are the most important red flag. Overall, the authors concluded that a weak control environment is an indication of some warning signs of fraud. Special warning signals as to their relative importance.
C.A. Strand, K.A.S. Lancaster and J. Thorne

Corporate Training Assessment Technique

Strand (1996) suggests that the persons who authorized computer users, who have assets while the fraudulent activity is in an event that is normally witnessed first-hand, and sometimes difficult even to have committed" (p.26). Too frequently the Lindner (1996) believe, however, that "red signaling the likelihood of fraud. Further, positioned to identify and assess any red

ational indicators that suggest the auditor more than one red flag is present, the auditor Albrecht et al. (1980) conducted an are to identify the individual and organizationally auditors to detect fraud. These authors was problematic, and concluded that the following fraud is: (1) improper actions resulting in errors and is harmful to shareholders or creditors of the consumer public (such as false bribes, kickbacks, violations of regulatory : internal control system.

37 red flags for fraud that were divided into nal to commit fraud on behalf of the compan (2) factors that motivate individuals to com- internalization of assets). A number of studies or 's list (Albrecht and Romney 1986; Pincus Heiman-Hoffman et al. 1996; Weisborn and Weisborn and the annual KPMG Fraud Surveys).

The predictive ability of the 87 red flags suggest that only about one-third of the 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 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 company's stock. The results indicate that insiders in companies with fraudulent financial statements did in fact reduce their net position in the company’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 Related to Fraud

<table>
<thead>
<tr>
<th>Risk Factors Relating to Susc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Large amounts of cash on hand</td>
</tr>
<tr>
<td>b. Inventory characteristics such as expiration dates</td>
</tr>
<tr>
<td>c. Easily convertible assets</td>
</tr>
<tr>
<td>d. Fixed asset characteristics, such as poor physical safeguards</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk Factors Relating to Cont.</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Lack of management oversight</td>
</tr>
<tr>
<td>b. No screening procedures for employees</td>
</tr>
<tr>
<td>c. Lack of appropriate segregation of duties</td>
</tr>
<tr>
<td>d. Lack of appropriate authorization for transactions</td>
</tr>
<tr>
<td>e. Poor physical safeguards over assets</td>
</tr>
<tr>
<td>f. Lack of documentation for transactions</td>
</tr>
<tr>
<td>g. Lack of mandatory vacations</td>
</tr>
</tbody>
</table>

Source: Statement on Auditing Standards 99

Corporate training assessment techniques the instructor has taught and what the employee misbehavior. According to Cottell and Harwood (1998), feedback so that instructors may change and improve student learning. Further, Angell et al. (1998) describe assessment methods on a regular basis provide become more self-assessing, more self-directed.

Further, training (educational) assessment Cross 1993). Rebele et al. (1998) described as follows. Because effective teaching partial to assessing teaching effectiveness, I
red flags that were validated in Albrecht and well-known and relatively infamous cases of fraud in the text. Contemporary Auditing: Issues and Study suggest that dishonest or unethical detecting management fraud, followed by: (3) domination of the company's assets; (4) inadequate internal controls or failure to enforce

An association between financial statement fraud identified as a "red flag" in SAS No. 82 or in prior detecting should be an important risk factor for auditors to regulators who are monitoring insider hypothesized that during the period of fraud-detractors in the company will strategically reduce results indicate that insiders in companies with reduce their net position in the entity's stock

(b) factors) believed to be associated with mis-statement. This Statement identifies two categories of assets to misappropriation, and (b) specific to the nature of an entity's assets and the controls the latter pertains to the lack of controls over the disposition of assets (AICPA 1997, para. 18). Table 1 factors derived from SAS No. 82.

Table 1 Risk Factors Relating to Misappropriation of Assets

<table>
<thead>
<tr>
<th>a. Risk Factors Relating to Susceptibility of Assets to Misappropriation:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Large amounts of cash on hand</td>
</tr>
<tr>
<td>• Inventory characteristics such as small size, high demand, high value</td>
</tr>
<tr>
<td>• Easily convertible assets</td>
</tr>
<tr>
<td>• Fixed asset characteristics, such as small size, marketability</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>b. Risk Factors Relating to Controls:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Lack of management oversight</td>
</tr>
<tr>
<td>• No screening procedures for employees with access to vulnerable assets</td>
</tr>
<tr>
<td>• Lack of appropriate segregation of duties</td>
</tr>
<tr>
<td>• Lack of appropriate authorization and approval of transactions</td>
</tr>
<tr>
<td>• Poor physical safeguards over cash, investments, inventory, or fixed assets</td>
</tr>
<tr>
<td>• Lack of documentation for transactions</td>
</tr>
<tr>
<td>• Lack of mandatory vacations for employees</td>
</tr>
</tbody>
</table>

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 exposure to expert performance in a going-concern task, which suggests expertise by prolonged practice (Spires 1991).

**SUGGESTIONS AND CONCLUSIONS**

The *Springer Junction* case in the Appendix of assets that may be used to help employees are frequently associated with employee fraud-specific CTATs throughout a training course, as well. Any actual instance of fraud may be taken from the journal. Next, the instructor would select the scenario. Perhaps the instructor might use the CTAT to determine whether the employees are well-educated.

The annual fraud surveys conducted by KPMG misbehavior is a growing concern to the business and is relevant for corporate training if employees are familiar with their work environment. Employees may gain expertise that are commonly associated with the risk factors that are included in SAS No. 82. Similarly, trainers should provide to employees to increase the efficiency of learning.

**REFERENCES**


C.A. Strand, K.A.S. Lancaster and J. Thorne

CORPORATE TRAINING ASSESSMENT TECHNIQUE

203

Encourage both trainers and employees to engage in training, as they promote learning of the subject matter and company awareness (Beard 1993). CTATs should be more likely to provide corporate trainers with feedback on how well the employees are learning.

Instructional training that incorporates actual instances of misappropriation of assets may be used to help employees practice the recognition of common clues that are frequently associated with employee fraud. CTATs should be constructed from an actual instance of misappropriation of assets by a governmental employee creating fictitious financial statements. Additional cases or scenarios may be developed that focus on employee fraud and unethical business practices that are commonly present in actual instances of misappropriation. A single case may be used as a stand-alone CTAT, or it may be modified to incorporate risk factors associated with the misappropriation of assets. Any actual instance of fraud may be taken from a newspaper, news journal, or business journal. Surveys of these studies have repeatedly received high ratings (Choo 1996, Anger and Pennington 1991, Donner and Calderon 1994, Mills 1995). In other research, case studies have been used to study decision-making and judgment abilities (Anthony 1974; Donner and Pennington 1991). The intent of these instructional tools is for employees to gain expertise in the area of red flags and their relationship to fraud. Bonner and Pennington's (1991) results suggest that training and decision making are related. The timing of this instruction appears to be critical for the effectiveness of this method of instructional training. 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


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


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

259-276.
CORPORATE TRAINING ASSESSMENT TECHNIQUE


---

**EDWARDS**

**APPENDIX**

**Department of Finance**

**City of Springer Junction**

**Instructions for Trainees:** The case mate Organizational Chart for a governmental office. The listing of departmental personnel, along with the Background Information and Organizational Chart that is contained in the Scenario. Using these pi questions that follow the scenario. Each question each question to the best of your ability. There is no situation.

**BACKGROUND INFORMATION:**

Stan Wandell was pleased. He recently accepted the position of Finance Department and identified a number of day-to-day concerns he had about the Department.

First, he plans to streamline procedures in the Internal Auditing. He also wants to improve the way that internal auditors can be provided quickly when needed by citizens' confidence in the Department. Stan is concerned about employee turnover. Five of the seven employees have left within the past year. Stan has been told that the prior employer turned over. Five of the seven employees have left within the past year. Stan has been told that the prior employer turned over. Five of the seven employees have left within the past year. Stan has been told that the prior employer turned over. Five of the seven employees have left within the past year. Stan has been told that the prior employer turned over.

Stan noted that the City does not have an internal audit department. Quigley & Matherson, CPAs has been the Independent...