The government internal auditor's role in implementing SAS 82

David Sinason, *William Hillison*, *Carl Pacini*. **Journal of Public Budgeting, Accounting & Financial Management**. Boca Raton: Winter 2001.Vol. 13, Iss. 4; pg. 512, 24 pgs

Subjects:	Studies, Statements on auditing standards -- SAS 82, Auditing standards, Internal auditors, Governmental accounting, Fraud
Classification Codes	9190, 9130, 4130, 9550
Locations:	United States, US
Author(s):	David Sinason, William Hillison, Carl Pacini
Document types:	Feature
Publication title:	Journal of Public Budgeting, Accounting & Financial Management. Boca Raton: Winter 2001. Vol. 13, Iss. 4; pg. 512, 24 pgs
Source type:	Periodical
ISSN/ISBN:	10963367
ProQuest document ID:	98222130
Text Word Count	6445
Document URL:	http://proquest.umi.com/pqdweb?did=98222130&sid=2&Fmt=4&clientId=8631&RQT=309&VName=PQD

Abstract (Document Summary)

In the past years the incidence of fraud has increased dramatically and has cost government organizations billions of dollars. In response to this situation, Statement on Auditing Standards No. 82 was issued. This statement emphasizes the auditor's responsibilities with respect to fraud and should induce government managers to implement proactive measures to deter and detect fraud. The involvement of the internal auditors is instrumental in any fraud prevention program. In addition, the independent auditors will review details of the internal auditor's work for information concerning fraud prevention. This paper examines the nature of fraud and how the internal auditors can improve fraud prevention and detection in government entities.

Full Text (6445 words)

[Headnote]
Abstract. In the past years the incidence of fraud has increased dramatically and has cost government organizations billions of dollars. In response to this situation, Statement on Auditing Standards No. 82 was issued. This statement emphasizes the auditor's responsibilities with respect to fraud and should induce government managers to implement proactive measures to deter and detect fraud. The involvement of the internal auditors is instrumental in any fraud prevention program. In addition, the independent auditors will review details of the internal auditor's work for information concerning fraud prevention. This paper examines the nature of fraud and how the internal auditors can improve fraud prevention and detection in government entities.

INTRODUCTION

During a six month period in 1998, the thirteen fraud cases (Appendix 11) could be found in selected prominent newspapers throughout the country. A survey performed by Welch, Holmes, and Strawser (1997a) identified losses due to fraud in the federal government in excess of $157 million (208 cases). These losses were reported on 2,475 surveys returned to the authors by members of the Association of Certified Fraud Examiners (ACFE). This represents a return of 30% of the surveys that were originally sent. It is easy to conclude that the amount of fraud identified would have been higher had more surveys been returned, and, therefore, the $157 million amount is only a fraction of the actual fraud in the federal government.

These examples illustrate that fraud can occur at all levels of government and present itself in many different profiles. At the same time, constituents are asking for more accountability from agencies and governmental units regarding the use and safeguarding of assets and the protection of the public trust. External auditors are not in the best position to detect or prevent fraudulent activities. Even with guidance provided by recent changes in audit standards relating to fraud detection, external auditors lack the day-to-day involvement necessary to detect fraud

and typically are not empowered to establish fraud prevention and deterrence programs. This raises the question of who in an organization is in the best position to detect and prevent fraud? It can be argued that managers are in the best position to evaluate the risks of fraud and take steps to prevent it. The increased accountability demanded by the public and the increased scrutiny provided by the external auditors will make the prevention and detection of fraud a prime issue for the government manager. The government manager must rely heavily on the internal auditor who is in an optimum position to understand the organization's policies and procedures and observe the execution of these policies and procedures on a daily basis. Therefore, now more than ever, it is imperative that the internal auditor take a more proactive role to preventing and detecting fraud in all types of government organizations.

This article focuses on the changing roles and responsibilities of the internal auditor as one of government's main lines of defense against fraud. In the discussion that follows, the authors identify 1) the assistance that internal auditors can provide external auditors in implementing fraudrelated audit standards, 2) the fraud risks and signals that internal auditors should recognize, and 3) the proactive steps internal auditors can take to prevent, deter, detect, and report fraud.

OPPORTUNITY FOR GOVERNMENT INTERNAL AUDITORS PRESENTED BY SAS 82

In general, the public has been very critical of independent auditors for their failure to find fraud in both the public and private sectors. In the public sector, auditors have been defendants in major lawsuits involving Orange County, California, as well as numerous medicare and medicaid frauds. The criticism is due, in part, to the difference between what the public expects from independent auditors and what external auditors regard as their professional responsibilities (the "expectation gap"). The expectation gap entails a public perception that auditors have not played an adequate role in reporting fraud and other illegal client acts. In response to this criticism, the American Institute of Certified Public Accountants (AICPA) issued Statement on Auditing Standard (SAS) No. 82, Consideration of Fraud in a Financial Statement Audit, which took effect on December 15, 1997.

According to the AICPA, SAS No. 82 clarifies, but does not increase the external auditor's responsibility to detect fraud. The external auditor's responsibility is still framed by the key concepts of reasonable assurance and materiality and requires an assessment of the risk of material misstatements in the planning phases of an external audit. SAS No. 82, however, emphasizes that the assessment of the risk of material misstatement is a cumulative and ongoing process. Given the attention SAS No. 82 has received and the significant litigation exposure of CPAs, it seems that external auditors will give a high priority to compliance with all aspects'of SAS No. 82. The responsibilities of external auditors (with respect to public companies) have also been increased by the recently enacted Private Securities Litigation Reform Act.'

It should be noted that SAS No. 82 does not conflict in any way with Government Auditing Standards. Generally Accepted Government Auditing Standard (GAGAS) 4.3 states that SASs are incorporated into the GAGAS. In addition, GAGAS 4.14 states:

Auditors are responsible for being aware of the characteristics and types of potentially material irregularities that could be associated with the area being audited so they can plan the audit to provide reasonable assurance of detecting material irregularities.

This statement is in conceptual agreement with SAS No. 82 and the government independent auditor can be expected to incorporate guidance from SAS No. 82 into future external audits.

Additionally, the implementation of SAS No. 82 gives new meaning to the importance of the role and responsibility of internal auditors in the deterrence, detection, investigation, and reporting of fraud as outlined in Statement on Internal Auditing Standard (SIAS) No. 3. The standard indicates clearly that deterrence of fraud is the responsibility of management, but it is well established that internal auditors are responsible for examining and evaluating the adequacy and effectiveness of management's actions. With regard to detection of fraud, government internal auditors should have sufficient knowledge of fraud to identify indicators that fraud might have been committed. Internal auditors also must conduct tests directed toward identification of other indicators of fraud if significant control weaknesses are present.

Scope of the Fraud Problem

According to the 1996 Report to the Nation on Occupational Fraud and Abuse (Association of Certified Fraud Examiner, 1996) produced by the Association of Certified Fraud Examiners (ACFE), fraud and abuse cost U.S. organizations more than $400 billion annually. It is estimated that the average organization loses about six percent of its total annual revenue to fraud and abuse committed by its own employees. While this study focused on the

private sector, it is reasonable to believe that similar problems exist in government organizations and private-sector companies doing work for government entities. Indeed, Frauds in construction and healthcare have been uncovered in public projects, public hospitals, and government healthcare assistance programs.

Asset misappropriation accounted for more than four out of five fraud offenses. This category of offense is most often perpetrated by employees rather than management. Welch, Holmes and Strawser (1997a) noted that individuals in management positions account for 14.9% of fraud cases reported in their survey. The median loss of these cases was $97,000. Nonmanagement employees accounted for 36.5% of the reported frauds with a median loss of $45,000. Noted fraud expert Joseph T. Wells has classified asset misappropriation into several distinct scheme types as depicted in Exhibit 1. Fraudulent disbursements, those that involve false payments by the victim firm, make up 67 percent of cash fraud schemes and 48 percent of all fraud cases. It is clear that these frauds are not limited to the private sector.

Given the frequency of offenses involving asset misappropriation, internal auditors must play a key role in satisfying their responsibilities to the organization as well as assisting external auditors with satisfying the requirements of SAS No. 82. A focused effort by internal auditors on the prevention, deterrence, and detection of financial statement misstatements arising from asset misappropriation is consistent with their broad mission-- which requires safeguarding the entity's assets and preserving the public trust. In carrying out their mission, government internal auditors should be aware of the risks and warning signs of fraud.

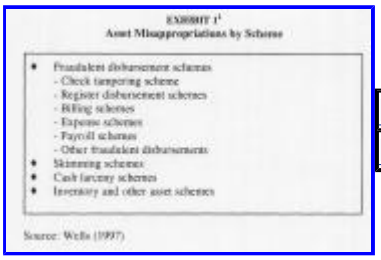
EXHIBIT 1[1]
Asset Misappropriations by Scheme

- Fraudulent disbursement schemes
  - Check tampering scheme
  - Register disbursement schemes
  - Billing schemes
  - Expense schemes
  - Payroll schemes
  - Other fraudulent disbursements
- Skimming schemes
- Cash larceny schemes
- Inventory and other asset schemes

Source: Wells (1997)

Enlarge 200%
Enlarge 400%

EXHIBIT 12

The Fraud Risk Model

Exhibit 2 portrays the fraud risk model developed by the ACFE. The model highlights the three characteristics of employee fraud: pressure, opportunity, and rationalization (attitude). The three circles representing the characteristics of fraud overlap such that when all three factors are present, the risk of fraud is the highest. This high risk is portrayed by the center area of the intersecting circles. Each characteristic depicted in the model is described below.

Pressure. An employee's actual or perceived need for assets can create the desire to commit fraud. It is important to note that the pressure need only be perceived to motivate the commission of fraud. In the publication Fraud.: Bringing Light to the Dark Side of Business, Albrecht, Wernz and Williams note that 95 percent of all fraud cases involve either financial or vice-related pressures. These pressures result from the fraudster having an immediate need for cash or assets. Very few perpetrators have been known to save or hoard stolen assets or resources. Assets are generally spent quickly, usually with visible changes in employee lifestyle. Thus, it is vital for internal auditors to know and understand the entity's employees and the pressures that prevail and to review key employees within the organization for issues related to pressures and employee lifestyle.

Enlarge 200%
Enlarge 400%

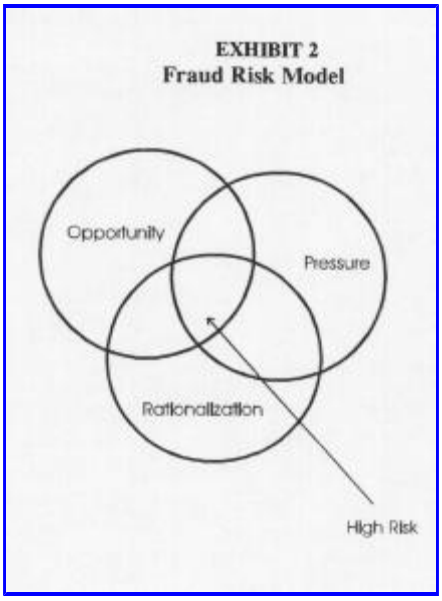

EXHIBIT 2

Certain employee situations are consistent with actual or perceived pressure. Financial or vice-related pressure may be caused by:

- Greed or preoccupation with being successful;

- Economic hard times associated with high personal debt;

- Decreasing earnings, rising costs or downsizing by the employer;

- Expensive habits such as gambling or the use of drugs or alcohol;

- Illicit sexual relationships;

- Living beyond one's means;

- Poor credit or inability to obtain credit;

- Work-related pressures such as low-pay failure to receive a promotion, unfair treatment; and

- Spouse or family-imposed pressures.

This list is not exhaustive but contains pressures fraud researchers have associated with employee fraud.

Traditionally government internal auditors have not been responsible for employee issues that induce pressures associated with fraud. However, by helping to establish employee assistance programs for those employees confronting drug, gambling, and family problems and/or economic hardship, the auditor increases the likelihood that employees will seek problem solutions rather than resort to fraud. The recommendation and review of employee assistance programs is a new issue for internal auditors. However, if only one in ten potential fraud perpetrators chooses counseling instead of fraud, these programs will pay for themselves. This makes employee assistance programs a key issue of internal control.

Opportunity. Opportunity relates to the ability of an employee to perpetrate and conceal a fraud. Opportunity is often promoted by a lack of proper internal controls or the lack of enforcement of those controls. According to Welch, Homes and Strawser (1997b: 42), a lax attitude toward controls is

.... the most frequently reported problem in every scheme, and apparently sends a strong signal to perpetrators regarding opportunities for fraudulent activities... Organizational leadership, in effect, often seemed to signal to perpetrators that an environment conducive to fraud existed, for example, when a lack of interest in enforcing rules

was perceived to exist.

While internal auditors cannot regulate the pressure attribute, they can help mitigate the opportunity to commit fraud. The following are typical failures in control that increase opportunity risk:

- Lack of established policies or controls related to investment risk;

- A lack of job screening procedures when hiring employees with access to assets susceptible to misappropriation;

- A lack of mandatory vacations for employees in key control functions;

- Lack of segregation of duties;

- Lack of an audit trail;

- Ineffective supervision;

- Lack of transaction authorizations;

- Poor accounting records;

- Lack of physical controls;

- Failure to discipline perpetrators;

- Lack of controls over access to information;

- Breakdown of procedures (for example, inappropriate computer access, ineffective physical inventories);

- An ineffective or nonexistent means of communicating and supporting the entity's accountability for public resources and ethics, especially regarding conflicts of interest and codes of conduct; and

- Significant pressure to obtain additional funding necessary to stay viable and maintain levels of service considering the financial position of the entity.

Asset misappropriation can occur not only by allowing access to physical assets, but also by giving employees the ability to initiate and/or approve certain transactions. Fraud cases exist where an employee, who had no physical access to inventory, still committed a theft by initiating shipping documents to have the assets delivered to himself or someone in collusion with him. Employees attempting to circumvent controls may try to conceal their acts by working unusual hours and/or not taking vacations or days off.

Government internal auditors evaluate controls to determine if the controls are adequate and encourage enforcement of those controls that are in place to remove perceived opportunities. Where controls are lacking or ineffective, the government internal auditors should inform management and recommend remedial action. Actions appropriate for internal auditors to reduce the likelihood of employee fraud are discussed subsequently.

Radonalizaton. Individuals who commit fraud must justify their actions as being consistent with their own personal code of ethics. Levels of ethical principles vary greatly among individuals, however, internal auditors should assume that anyone is capable ofjustifying the commission of fraud. Internal auditors should exercise "professional skepticism" particularly since fraud is typically committed by "those we trust." This is often a function of the fact that those who are trusted are placed in positions where fraud may be committed (i.e., trusted individuals are given responsibility to manage and control assets).

Certain employee attitudes or rationalizations are often associated with acts of fraud:

- Feeling of being underpaid;

-Belief of being overworked;

- Feeling that "everybody else is doing it;"

- Belief that rank has its privileges;

- Low self-esteem or morale;

- A desire to seek revenge;

- It Is only a loan and will be paid back; and

- Nobody will get hurt.

Rationalization is a factor often viewed as out of the control of management and internal auditors. After all, how does one keep a person from justifying his or her own actions? Yet, if fraud prevention is routinely discussed with employees as part of an on-going fraud prevention program, the subject of rationalization can be approached. Employees can be reminded often that no justification exists for illegal activities. The internal auditors should review and monitor an on-going program that maintains an ethical foundation for the organizations employees. These may require only five minutes at weekly or monthly department meetings. If only a small percentage of potential fraud schemes is discouraged, the cost of such a program can be justified.

Typical Fraud Targets

Risk of misappropriation of assets is related to specific assets owned by the entity. Eight of the nine asset misappropriation schemes in Exhibit 3 involve cash with billing schemes that result in the highest median losses -- $250,000. The other scheme category entails inventory and other assets. Misappropriation of inventory and other assets encompass a median loss of $100,000 per incident. These statistics indicate that internal auditors should focus their efforts on the prevention, deterrence, and detection of fraud involving cash, but other "non-balance sheet " assets may also be at risk.

"Non-balance sheet" assets which may be at risk of misappropriation include:

- Employee time (for example, assigning subordinates to do non-work related activities);

- Telephone usage;

- Intellectual property (such as computer software);

- Competitive information (such as contractor/vendor bids);

- Data files;

- Computer time and resources; and

- Vehicle usage.

The government internal auditor should be acutely aware of both the common types or acts of fraud and related signals of fraud. The type or act of fraud is what actually causes a loss for the victim. It is what the perpetrator attempts to conceal. A fraud symptom is a signal or sign of fraud. However, the presence of a signal does not necessarily mean that fraud exists. The internal auditor should be alert and take appropriate steps to investigate these signals to ensure that fraud does not exist. Exhibit 4 identifies many common types or acts of government fraud. Exhibit 5 lists a number of signals (symptoms) typically associated with government fraud.

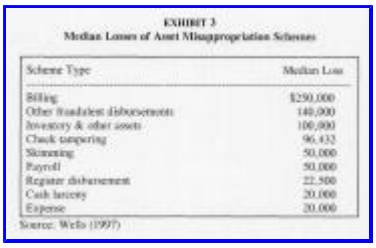

EXHIBIT 3
Median Losses of Asset Misappropriation Schemes

Scheme Type	Median Loss
Billing	$250,000
Other fraudulent disbursements	140,000
Inventory & other assets	100,000
Check tampering	96,432
Skimming	50,000
Payroll	50,000
Register disbursement	22,500
Cash larceny	20,000
Expense	20,000

Source: Wells (1997)

EXHIBIT 3

WHAT ELSE CAN GOVERNMENT INTERNAL AUDITORS DO TO ADDRESS THE FRAUD PROBLEM?

Government internal auditors occupy a special position within the government entity to assist in the prevention, deterrence, and detection of fraud. In addition to considering the common types and signals of fraud, the following are some key steps that can be taken by government internal auditors to combat fraud. These steps are summarized in Exhibit 6, "Government Internal Auditor's Fraud Checklist.'

Steps to Sharpen the Internal Auditor's Focus on Fraud

An increased focus placed by internal auditors on preventing fraud may serve to deter some employees from engaging in fraudulent ctivities. Internal auditors, working with management, should aggressively pursue possible fraudulent conduct instead of waiting for situations to be brought to the forefront. A proactive stance on preventing and detecting fraud should increase employee perception of the likelihood of detection. Several steps are outlined below.

1. Create and Maintain a Fraud Policy. The ACFE urges every organization to create and maintain a fraud policy for guiding employees. A government fraud policy should be separate and distinct from an entity's corporate code of conduct or ethics policy. An outline of a fraud policy that can be used to create a detailed fraud policy is provided in Appendix 2. Such a fraud policy should be clearly communicated to employees. Various avenues of communication include use in orientation of new hires, annual employee training seminars, and annual performance evaluations. Written acknowledgment by each employee that the policy has been read and understood should be required.

2. Consult a Certfied Fraud Examiner. Another step internal auditors may take to emphasize fraud prevention and deterrence is to consult a certified fraud examiner (CFE) in appropriate situations. A CFE has the training and expertise to evaluate the risk of fraud within most types of organization. Areas of high vulnerability can be pinpointed by a CFE for remedial action before any significant losses are incurred by an organization. CFEs are also available to investigate and resolve alleged fraudulent activities. The activities of CFEs are aimed specifically at preventing and detecting fraud. Many internal audit organizations may designate an employee for training in preparation for the CFE exam, if they do not have a CFE within the organization.

EXHIBIT 4
Common Types or Acts of Government Fraud

1. Voiding receipts.
2. Not issuing receipts to certain customers.
3. Dismissing citations after citizens pay fines.
4. Cash theft by under-recording collections.
5. Theft of daily deposits.
6. Theft of funds from discretionary "agency" bank accounts (e.g. vending machine operations).
7. Stealing tools, supplies, and other assets (supply fraud).
8. Theft of property and/or cash from police custody (originally seized as evidence).
9. Forging checks received.
10. Altering credit card receipts.
11. Setting up fictitious employees (ghost employees) on the payroll records and taking their paychecks.
12. Manipulating payroll records to divert wages, payroll taxes, or paychecks.
13. Embezzling payroll withholding.
14. Overstating hours worked or working unauthorized overtime.
15. Charging personal purchases to a governmental entity through misuse of purchase orders or entity credit cards.
16. Overloading expense accounts or diverting advances to personal use.
17. Paying false invoices obtained through collusion with suppliers.
18. Bid submissions and bid rigging schemes, including
    - premature opening of bids
    - altering bids
    - unjustifiable extensions of bid opening dates
    - controlled bid opening
    - falsifying bid logs and documents
    - bid rotation
    - bid suppression
    - complementary or "shadow" bidding
    - phantom bids
19. Defensive pricing schemes, including
    - use of vendors other than the proposed vendor
    - not disclosing vendor discounts
    - changing make/buy decisions
    - inflating costs by channeling work under contract through a shell company
20. Product substitution schemes, including
    - delivery of inferior material
    - falsification of test results
    - delivery of counterfeit products
    - placing inspection tags on uninspected goods
21. Receiving bribes and kickbacks for licenses or permits.

Enlarge 200%
Enlarge 400%

EXHIBIT 5
Signals of Fraud

1. Unexpected or unexplained reductions in revenue
2. Frequent voids in the receipt ledger
3. Out-of-sequence receipts
4. Daily deposit includes mostly or entirely checks (most government entity deposits include both checks and cash).
5. Unexpected or unexplained reductions in revenue.
6. Discrepancies between departmental revenue records and entity's general ledger.
7. Unexpectedly low levels of cash in the deposit or departmental collections.
8. Unusual or increasing time lags between deposits.
9. Questions from organization sponsors about how much money is left in their account.
10. Petty cash fund discrepancies (for example, cash shortages, insufficient disbursement documentation, checks from the fund custodian or coworkers, and frequent or unusual reimbursements of the fund).
11. No clear reconciliation or validation of prenumbered receipts or parking tickets.
12. Missing or poorly prepared bank reconciliations
13. Frequent or unusual purchases of supplies
14. Large or unusual budget variances in individual line items (e.g. police department maintenance)
15. Missing safeguard controls (e.g. unlocked repair facilities and unlocked supply areas).
16. Complaints from vendors or citizens about unfair treatment compared to others
17. Missing documentation.
18. Alterations of documents.
19. Employees on the payroll who do not sign up for benefits
20. Duplicate payments
21. Second endorsements on checks
22. Stale items on bank reconciliations
23. Failure of certain employees to take a vacation.
24. Significant increase or decrease in account balances
25. Unreasonable expenses or reimbursements
26. Products or services purchased in excess of needs
27. Product compliance certificate missing.
28. High percentage of product returns to vendor for noncompliance with specifications.

Enlarge 200%
Enlarge 400%

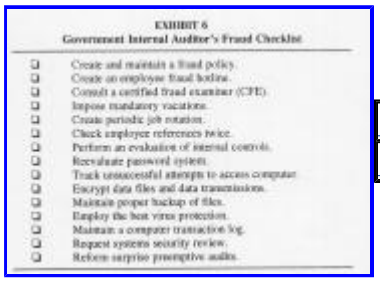

EXHIBIT 6
Government Internal Auditor's Fraud Checklist

- ❑ Create and maintain a fraud policy.
- ❑ Create an employee fraud hotline.
- ❑ Consult a certified fraud examiner (CFE).
- ❑ Impose mandatory vacations.
- ❑ Create periodic job rotation.
- ❑ Check employee references twice.
- ❑ Perform an evaluation of internal controls.
- ❑ Reevaluate password system.
- ❑ Track unsuccessful attempts to access computer.
- ❑ Encrypt data files and data transmissions.
- ❑ Maintain proper backup of files.
- ❑ Employ the best virus protection.
- ❑ Maintain a computer transaction log.
- ❑ Request systems security review.
- ❑ Reform surprise preemptive audits.

Enlarge 200%
Enlarge 400%

3. Assist with the Implementation and Operation of a Fraud Hodine. According to the Report to the Nation on Occupational Fraud and Abuse (Association of Certified Fraud Examiners, 1996), an employee fraud hotline is the single most cost effective means for detecting occupational fraud and abuse. Employees often observe the occurrence or commission of fraud but have no way to report it anonymously. The use of a telephone hotline offers an employee an opportunity to report potential fraud without fear of reprisal. Hotlines may be supported in-house or provided by a third party. An example of a third-party hotline is a subscription service offered by the ACFE. A toll-free telephone number links to the ACFE hotline facilities. Announcements and signs can promote the use of the hotline at the government unit. The results of all calls are provided to the client within one business day. The cost of the service is based on the number of employees.

4. Enforcement of Internal Controls. In the late 1980s, the National Commission on Fraudulent Financial Reporting (also known as The Treadway Commission) stated that a breakdown in internal controls led to the perpetration of fraud in 45 percent of the alleged fraud cases reviewed by the SEC. KPMG Peat Marwick reported in its 1994 Fraud Survey that poor internal controls led to almost 60 percent of the frauds that occurred. Welch, Holmes, and Strawser (1997a) indicate that internal control weaknesses were reported approximately 85 percent of the fraud cases reported. These three reports highlight the important role that an internal audit staff can play in implementing, monitoring, and enforcing a strong internal control system. Numerous steps can be taken by government internal auditors to enhance both the reliability and effectiveness of an entity's internal control system.

Traditional application of internal controls include the segregation of duties and responsibilities among the functions of authorization, recording, custody, and proper supervision. This is the "first line of defense" and deserves periodic evaluation by internal auditors.

Certain employee fraud schemes require constant attention by the fraudster to prevent detection. Two inexpensive means to strengthen internal control suggested by the ACFE are enforcement of mandatory vacations and periodic job rotation. An example of a mandatory vacation policy is the one used by all FDIC-insured banks. The policy requires all officers to take two consecutive weeks of vacation per year. In some cases, it is critical that vacation periods include times) when an employee's presence, for fraud purposes, is crucial. For example, it may be imperative to a fraud scheme that an employee is present to conduct a month end balance and/or reconciliation. An employee with such a responsibility should be required to include a month end as part of a vacation period or that the job duties be carried out by another employee on a surprise basis as part of a job rotation program.

Job rotation programs should be designed so that the rotated employee has little or no access to the documents, journals, data files, programs, etc., that he or she worked with on the previous job. The requirement of mandatory vacations and the adoption of job rotation plans deter fraud as well as allow existent fraud schemes to surface.

Another internal control that helps prevent fraud is checking employment references. An employee with a history of perpetration of fraud schemes may move from one organization to another. When employee references are not checked a dishonest person may be hired. A dishonest employee can defraud anunsuspecting organization of thousands of dollars and move on to a new job before the fraud is discovered. Resumes should be scrutinized and information verified to determine that prospective employees graduated from the schools listed and has the

experience requested. Also, an organization should not rely on the telephone numbers listed on the resume for prior employers, as they may be false. Employer phone numbers should be obtained by the organization independently. An additional technique that may be used is for employers to do a second check of employee references six months after an employee starts work. The reason for a dishonest employee's recent dismissal from a previous job may not have had time to become part of the employee's record during the initial search.

In this information age, any increased focus on internal controls by internal auditors should include consideration of those that relate to an entity's computer system. Government investigators recently viewed the computer networks of the U.S. Department of State and the Federal Aviation Administration as "wide open and vulnerable to attack. " In fact, .white-hat hackers" not only easily penetrated the State Department system, but the State Department's internal mangers could not even detect that an intrusion into their system had occurred (Dido, 1998). Many different types of fraudulent schemes involve tampering with computer programs, data files, and equipment. The internal auditor's focus here is on controls that may have been overlooked or those that deserve additional consideration. More traditional controls, such as physical controls over equipment and files, are assumed to be employed and are typically considered in auditing texts.

Telecommuting and the growth of the Internet have led generally to an increase in the number of dial-in ports to computer networks increasing the exposure to computer fraud. Internal auditors should assure that only legitimate users have access to the computer network and associated data. Currently, the most effective and efficient method of controlling access is still the password. Proper password use, however, is mandatory if control is to be maintained. Ideally, passwords should be randomly generated by the computer system and contain a combination of letters, numbers, and special characters. Employees should be prohibited from sharing their passwords with other users. Password security requires that they be changed periodically; but how often depends on the risks. Employees should not be permitted to display their passwords in any location where they may be viewed by unauthorized individuals. An organization's operating system should keep track of unsuccessful attempts to gain access and limit attempts before the user is automatically "signed off. " Technology is advancing to create new forms of password protection using biological features of the user such as voice prints, fingerprints, retina patterns, and digital signatures. These are likely to become cost-effective in the very near future. Internal auditors who keep abreast of technology enhancements will be in prime position to take advantage of these controls.

Data stored in files and transmitted over communications lines are subject to invasion by unauthorized employees or other parties. For example, in some cases employees may be able to circumvent password protection and gain access to files. One control that addresses this problem is encryption. It involves the encoding of data to hide their real meaning. A key is used to encode and then decode the encrypted data. Security software is available to perform this function. Disadvantages to data encoding are the cost of the hardware and software and inherent delays in execution time from additional processing. However, most currently designed database and communication software packages incorporate the ability to encrypt the data and likely make the control costeffective. Organizations should be taking advantage of these control features where available.

Data files and systems should be protected from sabotage by disgruntled employees and outsiders, disaster recovery and reconstruction require proper backup procedures. Basically, this requires systematic duplication and storage policies for data files. Internal auditors should assure proper virus protection, although this type of sabotage is not typically a threat from employees. The firm should purchase and use the most effective virus protection software available. The benefits likely far outweigh the costs.

One control that deserves special attention is the creation and use of a console log. Internal auditors should address the ability of the computer operating system to maintain a secure log of every transaction or entry into the system. The user identification, time of entry, and transaction or entry should be captured. With the improvements in computer storage technology, this has become a cost effective control, A console log proves useful to an internal auditor to test for combinations of users and transactions (for example, file accesses and changes by certain employees), as well as to provide support for subsequent allegations of fraud. It also serves as a deterrent in the sense that employees know that a record of all activity is being maintained.

Also, an auditor or fraud specialist with computer security skills should perform a periodic review of system or network security controls. Information as to which security controls have been established could be collected through a preliminary survey. Inquiry procedures can be applied to gain an understanding of the reason for including or not including particular controls, as well as the effectiveness of the controls. Such a review will also reveal what additional steps, if any, internal auditors can take to reduce the likelihood of computer fraud.

As an overall consideration, surprise preemptive fraud audits should be a weapon in the arsenal of the internal audit staff. Such audits should be conducted by seasoned internal auditors. One key reason is that the audit trail often is nonexistent or incomplete. A surprise audit, however, gives fraud perpetrators less time to alter, destroy, or hide records and other evidence. Another reason for using experienced internal auditors is that it is likely that members of a fraud audit team will be interviewing many people, including those implicated. Internal auditors must have well-developed skills in discovery and testimonial interviews. Also, working papers are likely to be introduced as evidence and to be thoroughly examined. Impeccable working papers are more apt to be generated by an experienced internal auditor.

Given that one of the biggest exposures government entities face is new technology, internal auditors must keep pace with computer developments and understand those developments. One important challenge for internal auditors is the examination of new technology applications for control and security issues. The audit environment is becoming paperless and internal auditors must adapt to this new environment. Through proper training, internal auditors can curtail the unnecessary exposures facing entities today.

Those Challenge?

Much attention has been paid to the role of the independent auditor in detecting fraud, however, internal auditors are in the best position to

Much attention has been paid to the role of the independent auditor in detecting fraud, however, internal auditors are in the best position to prevent, deter, and detect fraud. Those internal to an entity should be more familiar with the policies and procedures of the organization and, therefore, be better able to identify when violations have occurred. In addition, the internal auditor needs to be aware of the situations and circumstances that increase the risk of employee fraud. The internal auditor must also take on the role of educator, providing information and training to management regarding fraud and fraud symptoms.

The tasks of auditors, both internal and external are becoming more difficult. All three fraud attributes--pressure, opportunity and rationalization--appear to be moving in a direction that increases the risk to the entity. Financial demands seem to be at the forefront for many employee frauds. In many government entities, where raises are slow to occur and may not meet increases in the cost of living, the risk of employee fraud may be greater. Changing technology provides previously unrecognized fraud opportunities for employees, while a decrease in middle management may allow more employees to work with minimum supervision or without proper control procedures. Finally, a perceived deterioration in ethics may have created an acceptance of less than honest behavior by some employees.

The potential for employee fraud demands a sharpened focus by internal auditors and the use of effective, common sense steps, to help reduce the occurrence of fraud and its attendant losses.

[Footnote]
NOTES

[Footnote]
1. Passage of Title II of the Private Securities Litigation Reform Act of 1995 (adopted as Section I OA of the Securities Exchange Act of 1943) requires external auditors to take specific actions when an illegal act is identified during the audit. These actions include 1) determining whether it is likely that an illegal act has occurred; and 2) if it is likely, determining the possible effect of the illegal act on financial statements. The auditor must inform management and the audit committee of any illegal act and, ensure that timely and appropriate action has taken place, including notification of the SEC.

[Reference]
REFERENCES

[Reference]
Albrecht, W. S., ET et al. (1998), Guide to Fraud Investigation, Volume 2, Fort Worth, TX: Practitioners Publication Company.
Albrecht, W. S., Wernz, G. W., and Williams, T. L. (1995), Fraud: Bringing Light to the Dark Side of Business, Burr Ridge, IL: Irwin Professional Publishing.
Association of Certified Fraud Examiners (1996), Report to the Nation on Occupational Fraud and Abuse, Austin, TX:

Author.
DiDio, L. (1998, May 25), "Federal Agencies Fail Security Test," Computerworld, 32(21): 16.
KPMG Peat Marwick (1998), 1998 Fraud Survey, New York: Author.

[Reference]
Welch, S., Holmes, S., and Srawser, J. W. (1997a), "Fraud in the Federal Government Part I - The Perpetrators and the Victims," Government Accountants Journal, 46(1): 24-27
Welch, S., Holmes, S., and Srawser, J. W. (1997b), "Fraud in the Federal Government Part II - Characteristics of the Schemes -- Detection and Resolution of the Cases," Government Accountants Journal, 46(2): 38-45.
Wells, J. T. (1997), Occupational Fraud and Abuse, Austin, TX: Obsidian Publishing.
Wells, J. T. , et al. (1994), Fraud Examiners Manual, Revised Second Ed., Austin, TX: Association of Certified Fraud Examiners.

[Author Affiliation]
David Sinason, William Hillison and Carl Pacini*

[Author Affiliation]
* David Sinason, Ph.D., is an Associate Professor, Department of Accountancy, Northern Illinois University at Dekalb. His teaching and research interests are in fraud auditing, audit management, and internal audit. William Hillison, Ph.D., is the Arthur Andersen Professor of Accounting, Department of Accounting, Florida State University. His teaching and research interests are in auditing and systems. Carl Pacini, Ph.D., is an Assistant Professor, College of Business, Florida Gulf Coast University. His teaching and research interests are in auditing, accountant liability, forensic accounting, and risk management and insurance.

[Appendix]
APPENDIX 1
Reported Fraud cases in Selected Prominent Newspapers, 1998

[Appendix]
The Los Angles Times (March 18, 1998): Los Angeles County awarded a contract to build a child-care center and low-income housing project to a federal prison inmate, whose company then bilked the county out of $690,000 in cash and $900,000 in costs for unfinished construction. The Washington Post (April 1, 1998): Eight D.C. Water and Sewer Authority workers were indicted by a federal grand jury for allegedly with collecting thousands of dollars for doctoring permits and doing illegal private work on city time with city supplies.

[Appendix]
The Boston Globe (April 2, 1998): The coordinator of a state-subsidized home for elderly men misused $25,000, spending it on clothing, cosmetics, toys, pet food, and sports tickets.
The Los Angles Times (April 8, 1998): Admitting that she spent money from federal contracts on everything from personal vacations to window shades for her home, one of the nation's most prominent minority contractors pleaded guilty in Los Angles federal court to misusing government funds.
The Los Angles Times (April 24, 1998): The Baldwin Park City Council hired as its interim city manager a man who was convicted of a $3 million land fraud scheme and was removed from a professional association of city managers. Council members say that no one ran a background check and he did not include his criminal history on his resume.

[Appendix]
The Chicago Tribune (May 9, 1998): A women on trial for ghostpayrolling charges testified that her ex-boyfriend placed her on the City of Chicago payroll in a do-nothing job without her knowledge and forged her signature on more than $43,000 worth of paychecks.
New York Times (June 30, 1998): Ninety people, including 14 New York City workers, created false identities for as many as 50 nonexistent children to defraud the welfare system.
The Chicago Tribune (July 7, 1998): Will County State's Attorney filed suit accusing a former Bolingbrook insurance broker of cheating the county out of more than $400,000.
The Houston Chronicle (July 15, 1998): The grand jury begins hearing testimony regarding a former basketball star and allegations that he falsified time sheets filed with the city when he oversaw the Houston Parks and Recreation Department's Youth Sports Program. On several occasions, the star charged the city for overtime on days he was out-oftown working for the Houston Rockets basketball team.

[Appendix]
The Chicago Tribune (July 21, 1998): A judge ordered an individual to serve 5'/2 years in prison and repay $12.3 million dollars for bribes he accepted in exchange for helping Management Services of Illinois (MSI) defraud millions of dollars from the Department of Public Aid.
The Wall Street Journal (July 31, 1998): An employee of the Drug Enforcement Administration (DEA) for 21 years, stole more than $6

[Appendix]
million dollars between 1990 and 1996. The employee set up his own company and had the DEA repeatedly send checks although no services were provided. The employee alone verified services rendered and authorized payments. The DEA acknowledges that the handling of funds violated the agency's own safeguards.

The Boston Globe (August 12, 1998): Modern Continental agreed to pay a total of $500,000 to federal and state authorities and set up a program to train employees in business ethics. The agreement was a settlement of a 16-count indictment that includes extortion, corruption, and mail fraud. The Chicago Sun-Times (September 4, 1998): Three current and former employees of the Illinois' Secretary of State's office were arrested for taking payoffs from customers attempting to improperly obtain commercial driver's licenses. Sources in the investigation said the problem is pervasive and extends to other secretary of state facilities, with more arrests expected.

[Appendix]
APPENDIX 2
Outline of a Sample Fraud Policy

[Appendix]
Background

[Appendix]
This section sets forth the importance of fraud policy in the prevention and detection of fraud.
Scope of Policy

[Appendix]
This section states that the policy applies to employees, consultants, vendors, contractors, and any party doing business with the organization. Policy

[Appendix]
In this section, management acknowledges its responsibility for the detection and prevention of fraud. Fraud is defined, and an explanation of how reported fraud cases are managed is provided.
Actions Constituting Fraud

[Appendix]
This section contains an outline of specific behaviors or activities that are considered by management to be fraud. The list should include items such as forgery of financial instruments; misappropriation of funds, securities,

[Appendix]
supplies, or other assets; profiteering as a result of inside information; bribery; and other illegal activities.
Investigation Responsibilities

[Appendix]
The organizational unit responsible for the investigation of possible occurrences of fraud is named, and the overall responsibilities of the unit are outlined.
Confidentiality

[Appendix]
The importance of confidentiality in conducting fraud investigations is set forth in this section.
Authorization for Investigating Suspected Fraud
The authority to conduct internal fraud investigations and the activities that are permitted to conduct such investigations are outlined. Reporting Procedures

[Appendix]
This section states that an employee who suspects fraudulent activity should contact the unit responsible for investigations. Anonymity of the reporting employee should be preserved. The policy should state that a reporting employee should not discuss the alleged fraud with any other person, including the suspected individual.
The use of a hotline for reporting suspected fraud cases may encourage more employee involvement.
Termination and Other Sanctions

[Appendix]
This section sets forth the appropriate procedures to be followed if an investigation results in a recommendation to terminate or prosecute an individual.
Administration and Approval

[Appendix]
Approval of the fraud policy by senior management should clearly be indicated in the policy. Also, the policy should state who is responsible for the administration, interpretation, and revision of the policy.

[Appendix]
Source: Wells, J. T. , et al. (1994), Fraud Examiner's Manual, Revised Second Ed., Volume 1, Austin, TX: Association of Certified Fraud Examiners.