PREVENTING AND DETECTING FRAUD IN

NOT-FOR-PROFIT ORGANIZATIONS

UPDATED EDITION

Keller & Owens, LLC

Certified Public Accountants

Preventing and Detecting Fraud in Not-For-Profit Organizations

Table of Contents

Page

I. An Overview of Fraud in the United States
- A. Recent reports on occupational fraud and abuse....1
- B. Estimated impact on the not-for-profit industry 2
- C. Some recent cases in the news....2

II. Fraud and Perpetrators
- A. A definition of fraud 3
- B. Frauds committed against not-for-profit organizations 3
- C. Frauds committed by not-for-profit organizations....5
- D. Perpetrators and the fraud triangle....6

III. A Comprehensive Approach to Controlling Fraud
- A. Setting the tone at the top....7
- B. Assessing fraud risks and responses 7
- C. Financial and non-financial systems and controls 7

IV. The Antifraud Team
- A. The audit committee 9
- B. The external auditors....10
- C. The internal audit process 11
- D. Certified fraud examiners 12
- E. Other members of the antifraud team 12

V. When Fraud is Discovered....13

VI. Appendices
- A. Sample Board Antifraud Policy....15
- B. Sample Audit Committee Charter....17
- C. Sample Organization Antifraud Policy....22
- D. Sample Code of Conduct Statement 24
- E. Sample Conflict of Interest Policy....27
- F. Sample Fraud Prevention Checkup....29
- G. Sample Internal Audit Checklist – Cash....38
- H. Other Useful Resources 42

Preventing and Detecting Fraud in Not-For-Profit Organizations

AN OVERVIEW OF FRAUD IN THE UNITED STATES

Recent Reports on Occupational Fraud and Abuse

In 1996, The Association of Certified Fraud Examiners (ACFE) published its first *Report to the Nation on Occupational Fraud and Abuse*. In 2002 and every two years thereafter, this report was updated and the study was expanded to provide the most detailed view yet of how occupational fraud affects organizations. The 2008 report was based on 959 fraud cases that were reported by the Certified Fraud Examiners (CFE) who investigated them. The latest report focused on five areas: the cost of occupational fraud, how it was committed, detection of fraud schemes, victim organizations, and the perpetrators.

Based on the 2008 study, the following conclusions were reached:

- It was estimated that 7% (5% in 2006) of revenues will be lost as a result of fraud.
- About 89% of occupational frauds involve asset misappropriations. Cash is the targeted asset 83.7% of the time. These are down slightly from the 2006 study.
- Methods of asset fraud found in not-for-profits in the 2006 study: unauthorized benefit, 29.3%; expense reimbursements, 28.6%; billing, 28.6%; check tampering, 24.5%; skimming, 24.5%; cash larceny, 17.7%; non-cash theft, 14.3%; payroll, 12.9%; and fraudulent statements & wire transfers, 5.4% each.[1] Similar data was not provided in 2008.

  [1] The sum of these percentages exceeds 100% because several cases involved multiple schemes.

- The dollar impact of fraud increases by level of responsibility while the frequency of fraud follows the opposite order. Most frauds are committed by the accounting department or upper management. About 81% of the fraudsters were first-time offenders.
- Perpetrators often display behavioral traits that serve as indicators of risk. The most commonly cited red flags were perpetrators living beyond their means or experiencing financial difficulties at the time of their frauds.
- The most common methods for detecting fraud in non-profits is by a tip from an employee, customer, vendor or anonymous source followed by accident, internal audit, internal controls and external audit, in that order. The typical scheme lasted 2 years before discovery.
- The implementation of anti-fraud controls appears to have a measureable impact on the organization's exposure to loss. The lack of adequate internal controls was most commonly cited as the factor that allowed the fraud to occur.

Estimated Impact on the Not-For-Profit Industry

If the total losses in the 2008 ACFE study are applied to the 2008 U.S Gross Domestic Product, it can be assumed that $994 billion is lost to fraud. Of the 959 cases studied, 14.3 percent of those involved a not-for-profit organization, with a median loss of $109,000 per incident. The report did not estimate what percentage of the $994 billion is associated with not-for-profits, however, since not-for-profits typically account for about 8.5% of the gross domestic product, it can be assumed that as much as $84 billion dollars is lost to fraud in not-for-profit organizations.

Some Recent Cases in the News

The Enron and WorldCom frauds were highly publicized, but represent only a few of many cases involving fraud and abuse. Recent news reports bring to the forefront that fraud can occur anywhere by anyone (even in your local area).

- A former employee of the Wisconsin Conference of a large denomination was sentenced to two years in prison for embezzling more than $158,000.
- The former finance secretary at an area church has been charged with stealing more than $100,000 during a 2 year period.
- A local church pastor was sentenced to probation for stealing $44,000 in church funds to cover a gambling debt.
- The president of a national convention looted millions from the organization to finance a lifestyle of waterfront homes, expensive cars and jewelry.
- A metropolitan church dean resigned and agreed to repay more than $100,000 in church money that he improperly spent over six years.
- A former treasurer of a suburban church was sentenced to seven years in prison for stealing nearly $200,000.
- Fictitious invoices resulted in an organization losing approximately a half a million dollars because of loose internal controls.
- A manager persuaded employees not to follow the internal controls set up and had a $40,000 check written to a fake company he set up. He was subsequently prosecuted for fraud.
- A temporary bank account which was unused for 10 years was left open. A director deposited several checks from donors into the account for his personal use. He was the only one who knew the account existed. He was only caught because he felt guilty and told a staff member about the account.

Fraud is a significant potential problem for all organizations.

FRAUD AND PERPETRATORS

A Definition of Fraud

The ACFE defines occupational fraud as "The use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets."

Frauds Committed Against Not-For-Profit Organizations

There are two broad categories of frauds that are perpetrated against not-for-profit organizations - internal and external. Internal frauds are committed by persons inside of the organization such as employees, officers and directors. External frauds are committed by persons outside of the organization, such as vendors, sub-recipients, grant applicants and program participants.

Internal frauds can be broken down into two separate categories: asset misappropriations and fraudulent financial reporting. Asset misappropriations are the most common and can involve any of the following (among many others): revenue and cash receipts schemes, purchasing and cash disbursement schemes, payroll and employee expense reporting schemes and non-cash asset misappropriations.

Asset misappropriations:

Revenue and cash receipts schemes

- Skimming – theft of cash before the funds have been recorded on the books. Skimming can be perpetrated by someone who either initially collects or opens incoming mail, the person who initially logs in cash receipts, prepares the deposit or takes the deposit to the bank, or door-to-door solicitors of charitable contributions. Checks can also be skimmed. The perpetrator opens up a bank account in the organization's name with themselves as a signer and simply deposits and withdraws the checks.

- Theft of donated merchandise – donated merchandise can be just as susceptible to theft as cash. While it may be a little harder for the perpetrator to carry the merchandise out, most organizations have poor controls or recordkeeping over donated items.

Purchasing and cash disbursement schemes

- Credit card abuse – perpetrators either use organization issued cards for personal use, or more damaging for the organization is the use of credit card numbers of donors.

- Fictitious vendor schemes – perpetrators set up a company and submit fake invoices to the organization for payment.

Payroll and employee expense reporting schemes

- Ghost employees – whereby either terminated employees are left on the payroll system, or fake employees are set up in payroll. Payroll checks are issued for non-existent employees and the checks are cashed by the perpetrator.

- Overstatement of hours worked – A recent survey found that 16 percent of the 617 workers surveyed reported witnessing the claiming of extra hours worked by other employees.

- Fictitious expenditures – submission of fictitious expenditures for reimbursement has become a significant problem especially with the evolution of desktop publishing. The effort involved in creating a bogus invoice for reimbursement can be rather minimal.

Other asset misappropriations

- Property and equipment schemes – outright theft of an asset.

- Personal use of organization's assets and other resources (corruption) – use of organization's computers, software, and printers for personal projects. Personal long-distance telephone calls. Utilizing the organization's Internet access and e-mail for personal use. Photocopying personal documents on the organization's copy machine.

While not as common as internal frauds, external frauds can occur in organizations and be just as detrimental. Common examples of external fraud are:

- Fraudulent billings by vendors – charging for goods or services not delivered or inflating prices, phony extra charges.

- Fraud committed by service organizations to whom organizations outsource important internal functions – using funds for other purposes before remitting, charging for false transactions, receiving kickbacks from other vendors for subcontracting services.

- Fraud by sub recipients – reporting fraudulent data or program costs to the not-for-profit that made the award from the original grant.

- Financial assistance fraud – students who falsely receive financial aid or others who fraudulently apply for or use grant funds.

Frauds Committed By Not-For-Profit Organizations

The preceding examples are types of frauds committed against not-for-profit organizations; however, not-for-profit organizations also can and do commit frauds. Fundraising is a particularly sensitive area that can be ripe for fraud. Fraudulent fundraising practices include:

- Charging fund-raising costs to programs to improve expense ratios scrutinized by donors, potential donors and charity watchdogs.
- Misrepresenting the portion of donations that will be used in charitable programs.
- Misrepresenting the extent of a charitable contribution deduction to which a contributor is entitled, such as in some car donation programs.
- Failing to comply with donor-imposed restrictions pertaining to the use of a gift.
- Other fraudulent practices by not-for-profit organizations could include knowingly failing to comply with Internal Revenue requirements related to housing allowances or compensation reporting, knowingly misclassifying employees or using them as volunteers to avoid paying overtime, or using or selling donor data collected under false pretenses.

Fraudulent Financial Reporting:

Fraudulent financial reporting is intentionally making false assertions relating to financial statements, false statements re: compliance with specific requirements of funding sources, charging of unallowable costs to grants and other false statements to government agencies. Fraudulent financial reporting is most often committed by management and includes such misrepresentations as:

- Failing to disclose significant related party transactions.
- Failing to disclose noncompliance with debt requirements or lack of waiver of noncompliance from lender.
- Misclassifying restricted donations to mislead donors or charity watchdogs.
- Holding records open beyond the period end in order to inflate revenues.
- Misclassifying expenses to mislead donors and others regarding the funds used for programs.

- Failing to correctly value receivables, inventory, donated assets, and liabilities under split-interest or gift annuity obligations.

- Failing to report trade payables in the correct period in order to understate expenses.

- Failing to correctly report obligations for deferred compensation or retirement benefits.

As a 2003 KPMG Fraud Survey reported, fraudulent financial reporting often costs the organization and society as a whole much more than theft of assets.

Perpetrator and the Fraud Triangle

Though some perpetrators are perpetual criminals who continue their actions because they aren't prosecuted or there are inadequate background checks by employers, most frauds are committed by trusted employees or ordinary persons who never thought they would engage in fraud.

There are three elements present in every fraud which are commonly known as the fraud triangle: perceived pressures, rationalization and perceived opportunity.

Perceived pressures/incentive

Management or other employees may have an incentive or be under pressure, which provides a motivation to commit fraud. The individual could feel financial pressures for themselves or others, have a drug, gambling or spending addiction, believe that they are "underpaid", that the funds are just borrowed or the incentive may be nothing more than the fact that the perpetrator wants to see if they could get away with fraud.

Opportunity

Circumstances exist – for example, the absence of controls, ineffective controls, or the ability of management to override controls – that provide an opportunity for fraud to be perpetrated.

Rationalization

Those involved in a fraud are able to rationalize a fraudulent act as being consistent with their personal code of ethics. Some individuals possess an attitude, character or set of ethical values that allows them to knowingly and intentionally commit a dishonest act.

Everyone experiences pressures and rationalizes, thus combining just the right level of pressure and rationalization with the perceived opportunity is what allows a person to commit fraud. Therefore, an organization should follow several steps to lessen the chance of fraud.

A COMPREHENSIVE APPROACH TO CONTROLLING FRAUD

Fraud is a significant potential problem for all organizations. The AICPA and a consortium of professional associations issued *Management Antifraud Programs and Controls, Guidance to Help Prevent and Detect Fraud*. In its preface, the document stated "that some organizations have significantly lower levels of misappropriation of assets and are less susceptible to fraudulent reporting than other organizations because they take proactive steps to prevent or detect fraud. It is only those organizations that seriously consider fraud risks and take proactive steps to create the right kind of climate to reduce its occurrence that have success in preventing fraud." The foundation for a comprehensive approach to controlling fraud rests on an antifraud policy set by the board of directors. See Appendix A for a sample antifraud policy.

Setting the Tone at the Top

For starters, management, including directors and officers need to "set the tone at the top" for ethical behavior in an organization. Management must show employees through its words and actions that dishonest or unethical behavior will not be tolerated, even if the result of the action benefits the organization. Additionally, it should be evident that all employees will be treated equally, regardless of their position. Appendices C and D are a sample Code of Conduct statement and a sample Conflict of Interest policy, respectively.

Assessing Fraud Risks and Responses

Organizations should be proactive in reducing fraud opportunities by (1) identifying and measuring fraud risks, (2) taking steps to mitigate identified risks, and (3) implementing and monitoring appropriate preventative and detective internal controls and other deterrent measures. Appendix E is a fraud risk checklist for use by the audit committee and management in identifying and measuring risks. Appendix F provides the organization with steps to take to audit areas of risk.

Financial and Non-Financial Systems and Controls

Management should implement both financial and non-financial systems and controls to detect and prevent fraud.

Among the financial controls management can implement include:

- Reconcile accounts – reconcile bank accounts as well as fundraising assets such as raffle tickets and cash receipts. A person who doesn't authorize transactions or have custody of the assets should perform the reconciliations.

- Perform ratio analysis – compare number of donors with contributions, compare number of employees with payroll expense.

- Review all general ledger adjustments.

- Institute job rotation and mandatory vacations.
- Conduct surprise audits.

The organization should consider using the following non-financial controls, among others:

- Pre-screen potential employees.
- Communicate often with current employees so you will know when they are feeling pressured.
- Communicate the consequences of committing fraud.
- Set a good example by following the rules.
- Provide a hotline.
- Conduct anti-fraud training for managers and employees.
- Implement an anti-fraud policy.

THE ANTIFRAUD TEAM

The Audit Committee

The audit committee is the board's primary direct representation on the antifraud team. A sample audit committee charter describing its general duties and responsibilities is found in Appendix B. The audit committee's antifraud role is one of both oversight and participation. The audit committee should constantly challenge management to enforce the antifraud policies of the board. It should regularly evaluate management's identification of fraud risks and their responses to those risks, including of the adequacy of the organization's internal financial controls. It should support and assess management's creation of a culture with a "zero tolerance" for fraud. The audit committee should also assess the risk of fraud by management and develop appropriate responses to those risks.

Among other things, the audit committee should:

- Remain alert to factors that might indicate management fraud, including changes in life-style.
- Consider periodically reviewing management travel and other expenses.
- Carefully review unusual and complex financial transactions.
- Consider periodically reviewing significant nonstandard journal entries, especially those near year-end.
- Monitor compliance with the organization's general code of conduct and conflict-of-interest policies.
- Identify and assess the propriety of related party relationships and transactions at all levels.
- Monitor the adequacy of the organization's information management system and other physical security measures required to protect the entity from fraud and abuse.
- Ensure that every employee or volunteer is aware that the committee is the contact point for reporting suspected fraud or abuse and that the "whistleblower" will be protected.
- Take the lead in investigating suspected fraud and abuse, including communicating appropriate matters to legal counsel and governmental authorities.
- Review the adequacy of insurance coverage associated with fraud and abuse.

- Communicate with external auditors regarding the audit committee's assessment of fraud risks, the entity's responses to those risks and any suspected or actual fraud and abuse reported to it during the year.

- Oversee the internal audit function or perform certain internal audit functions if needed.

In fulfilling its responsibilities, the audit committee should carefully document its actions and periodically report to the full board.

The External Auditors

The most recent study by the Association of Certified Fraud Examiners reported that less than 10% of the frauds included in the study were discovered as a result of an audit by an independent CPA firm. Despite the belief of many organizations and the users of their financial statements, the standard financial statement audit is not designed and should not be relied upon to detect fraud. Most fraud is discovered by others within an organization or reported by outside parties who become aware of inappropriate situations. Preventing and detecting fraud is the responsibility of the organization.

However, the accounting profession has taken steps to help the organization with its responsibility to prevent and detect fraud. The American Institute of Certified Public Accountants has promulgated professional standards designed to provide guidance to auditors in the area of fraud detection during the course of a normal audit. These standards require auditors to set aside time for assessing fraud risks, and planning and implementing procedures to improve the likelihood that the auditors will detect material misappropriation of assets or material misstatements of financial statements due to fraud. In addition, the external auditors should be expected to communicate the following matters to the organization, usually through its audit committee:

- Unusual accounting principles used or reporting practices followed.

- The basis for estimates used in the organization's financial statements and the reasonableness of those estimates.

- Significant audit adjustments that management needs to make in order to make the organization's financial statements fairly stated in all material respects.

- Unrecorded differences found in the audit that were notable, but not material to the financial statements individually or in the aggregate.

- Any fraud, regardless of size, that was discovered or suspected during the course of the audit.

- Illegal acts or instances of material noncompliance with laws or regulations.

- Weaknesses (known as significant deficiencies) in the design or operation of the organization's internal financial controls that if undetected could adversely affect the organization's ability to record, process, summarize and report financial data consistent with the assertions of management in the financial statements.

- Any disagreements with management or difficulties encountered during the audit.

While the primary responsibility for fraud prevention and detection remains with the board and management, the external auditors can be a significant part of the organization's antifraud team.

The Internal Audit Process

The 2003 Fraud Survey published by KPMG, the international accounting and consulting firm, found that "almost two thirds [of organizations surveyed] reported discovery [of fraud] by internal audit." The results of this and similar studies suggest that while an internal audit process doesn't prevent misappropriation of assets or misrepresentation of financial statements from happening, it does 1) increase the probability of detecting fraud and 2) detect fraud earlier, resulting in smaller losses.

The internal audit process is similar to that of the external audit with at least one important difference. The external audit is designed to obtain reasonable assurance that the organization's financial statements are free of material misstatement. As a result, the external audit generally focuses on larger transactions. However, the internal auditor can examine 100% of the activity in an area. This is what makes the internal audit process so valuable. Besides looking at detailed transactions, the internal auditor can assist the audit committee with many of its tasks.

While some organizations are able to afford an internal audit staff to help detect fraud and assess the efficiencies of operations, funding constraints prevent most from using this antifraud resource. However, given some useful tools and diligent volunteers almost all organizations can realize the antifraud (and operational) benefits of the internal audit process. The Sample Internal Audit Checklist for Cash found in Appendix F can be a starting point.

The internal audit process should be under the direction of and report exclusively to the audit committee so that they can convey any concerns about management's commitment to the organization's code of conduct, management's success in establishing and enforcing strong internal controls as well as report suspicions or allegations of fraud involving senior management.

Certified Fraud Examiners

A certified fraud examiner may assist the audit committee with aspects of the oversight process and/or with the direct fraud investigation. They can provide extensive knowledge and experience and more objective insight into management's analysis of fraud risk and its implementation of antifraud policies and controls. The certified fraud examiner can also conduct examinations to resolve allegations or suspicions of fraud and act as expert witnesses in any legal proceedings.

Other Members of the Antifraud Team

Both charity watchdogs and government agencies can also be a part of the fraud prevention and detection team. Organizations such as the Evangelical Council for Financial Accountability and the BBB Giving Wise Alliance set standards for charitable accountability. These oversight organizations periodically evaluate charitable organizations through onsite visits or analytical procedures to ensure that donors and potential donors have a higher level of confidence as they dispense their charitable dollars.

Government agencies also aid in the accountability process. For example, the Internal Revenue Service reviews the annual information returns of many not-for-profit organizations for such things as reasonable relationships between donations and fund-raising costs. When no fund-raising expenses or unusual relationships are found and the organization is found to be filing inaccurate returns, significant penalties may be assessed. Many other federal, state and local government agencies conduct onsite examinations of organizations within their jurisdiction. The threat of economic loss, legal sanctions or discovery of wrongdoing can be a significant deterrent to fraud.

WHEN FRAUD IS DISCOVERED

Fraud can be suspected or discovered by many sources, such as employees, internal auditors, vendors and others. If fraud is discovered or there is a reasonable basis to believe that improprieties have occurred, the audit committee should be notified immediately and is responsible for ensuring that an investigation is conducted. If necessary, external auditors, internal auditors or certified fraud examiners may need to be engaged to assist the audit committee with the investigation. The audit committee should also consider the following actions, among others:

- Consult legal counsel on the prudent steps to take in order to protect the rights of the accused and ensure the rights of the organization.
- Inform the organization's insurance carrier of the suspected or discovered fraud loss in accordance with the terms of the insurance policy.
- Preserve the documents or other evidence that may be needed in proving the fraud.
- Repair the breach in internal controls, policies and procedures that made the fraud possible.
- In certain cases, inform law enforcement or appropriate government authorities.

The appropriate handling of such situations can minimize the harm done to the organization, the people involved and public impact of the experience.

The 2006 ACFE study reported the following actions taken against the perpetrators:

- The matter was referred to law enforcement 70.6% of the time primarily when the median loss was $200,000 or more.
- Prosecution resulted in 88.3% guilty pleas or convictions with 11.7% of the cases rejected by legal authorities.
- Only 23.5% of the matters resulted in a civil suit filed by the victim organization, generally when the median loss was $1.2 million or more. The victim organization received a judgment in nearly 60% of the cases with another 38.5% of the cases ending in a settlement.
- Judgments were rendered in favor of the perpetrator in 2% of the civil suits reported.

Similar data was not provided in the 2008 study.

APPENDICES

APPENDIX A

SAMPLE BOARD ANTIFRAUD POLICY

The following is a sample policy for boards of directors (or their equivalent) that documents the organization's underlying policies for preventing and detecting fraud. This sample should be reviewed and adapted to the specific needs of the organization.

General Statement

The organization and its board, management, employees and volunteers must, at all times, comply with all ethical principles and policies of the organization and all laws and regulations governing the activities of the organization. The board accepts its responsibility to undertake all appropriate actions to prevent and detect fraud against the organization or that may be perpetrated by anyone associated with the organization.

Fundamental Concepts

The board or board committee, with the assistance of management when appropriate, is charged with the responsibility for the following:

- Creating, demonstrating and maintaining a culture of honesty and high ethics by setting the "tone at the top". This includes preparing a code of conduct that expresses "zero tolerance" for unethical behavior and communicating it to all employees and volunteers of the organization. Management should also train employees regularly regarding the organization's values and code of conduct and document their understanding and compliance therewith at least annually.

- Regularly accessing fraud risks (including management fraud) and related risks that may occur within the organization. This includes establishing and monitoring appropriate policies, procedures and controls designed to mitigate or eliminate the risk of fraud and abuse. The assistance of external consultants may be warranted. A report regarding such fraud risks and actions taken must be made to the board at least annually.

- Creating, implementing and monitoring a strong system of controls, including continually seeking ways to increase security in the organization's computer, recordkeeping and payment systems.

- Training employees and volunteers to be alert to warning signs of fraud and unethical behavior and providing a system for reporting such matters. Reporting irregularities by creating a system for employees and volunteers to anonymously report (to the designated board representative or the board, if management is involved) illegal or unethical actions they have witnessed or suspect. This system should promote a transparency with the external auditors.

- Conducting regular (at least annually) audits of the organization's financial records including evaluating the organization's antifraud policies and procedures, internal controls systems and other relevant matters. This audit can be done by members of the audit committee, the internal audit staff, external auditors or other qualified consultants. The results of such audits are to be communicated to the board and other authorized parties.

Summary

The board of directors and management are responsible for preventing and detecting fraud and abuse within the organization. The board (or board committee) and management are charged with establishing, implementing and monitoring policies and procedures that address the fundamental responsibilities noted above.

APPENDIX B

SAMPLE AUDIT COMMITTEE CHARTER

The following sample charter reflects some of the best practices currently in use. Since no sample charter encompasses all activities that might be appropriate to a particular audit committee, this charter must be tailored to the organization's needs and governing rules. The charter should be reviewed annually for adequacy.

Purpose

The audit committee's charge is to assist the board of directors in fulfilling its oversight responsibilities for the financial reporting process. This includes risk assessment and management through the system of internal control over financial reporting, the audit process, and the organization's process for monitoring compliance with laws and regulations and its code of conduct.

Authority

The audit committee has authority to conduct or authorize investigation into any matters within its scope of responsibility with complete and unrestricted access to all books, records, documents, facilities and personnel of the organization. It is empowered to:

- Retain outside counsel, accountants or others to advise the committee or assist in the conduct of its responsibilities.

- Seek any information it requires from employees – all of whom are directed to cooperate with the committee's requests – or from external parties.

- Meet with company officers, external auditors or outside counsel, as necessary.

Membership

The audit committee will be a standing committee and consist of at least three members of the board of directors. The board or its nominating committee will appoint committee members and the committee chair.

Each committee member will be both independent from management and the organization and financially literate. At least one member shall have expertise in financial accounting and reporting for not-for-profit organizations.

Meetings

The committee will meet at least once a year, with authority to convene additional meetings, as circumstance require. All committee members are expected to attend each meeting, in person or via tele-conference or video-conference. The committee will invite members of management, auditors or others to attend meetings and provide pertinent information, as necessary. It will hold private meetings with auditors and executive sessions. Meeting agendas will be prepared and provided in advance to members, along with appropriate briefing materials. Minutes will be prepared.

Responsibilities

The committee will carry out the following responsibilities:

Financial Statements

- Review significant accounting and reporting issues, including complex or unusual transactions and highly judgmental areas; and review recent professional and regulatory pronouncements and understand their impact on the financial statements.

- Review with management and the external auditors the results of the audit, including any difficulties encountered.

- Review the annual financial statements, and consider whether they are complete, consistent with information known to committee members, and reflect appropriate accounting principles.

- Review other sections of the annual report and related regulatory filings before release and consider the accuracy and completeness of the information.

- Review with management and the external auditors all matters required to be communicated to the committee under generally accepted auditing standards.

- Understand how management develops interim financial information, and the nature and extent of internal and external auditor involvement.

- Review interim financial reports with management and the external auditors, before filing with regulators, and consider whether they are complete and consistent with the information known to committee members.

Internal Controls

- Consider the effectiveness of the organization's internal controls over annual and interim financial reporting, including information technology security and control.

- Understand the scope of internal and external auditors' review of internal controls over financial reporting, and obtain reports on significant findings and recommendations, together with management's responses.

Internal Audit

- Review with management and the internal audit director the charter, plans, activities, staffing and organizational structure of the internal audit function.

- Ensure there are no unreasonable restrictions or limitations, and review and concur in the appointment, replacement or dismissal of the internal audit director.

- Review the effectiveness of the internal audit function, including compliance with The Institute of Internal Auditors' *Standards for the Professional Practice of Internal Auditing.*

- On a regular basis, meet separately with the director of internal audit to discuss any matters that the committee or internal audit believes should be discussed privately.

External Audit

- Review the external auditors' proposed audit scope and approach, including coordination of audit effort with internal audit.

- Review and confirm the independence of the external auditors by obtaining statements from the auditors on relationships between the auditors and the company, including non-audit services.

- Review the performance of the external auditors, and exercise final approval on the appointment or discharge of the auditors.

- Meet separately with the external auditors to discuss any matters that the committee or auditors believe should be discussed privately, such as difficulties encountered during the audit.

- Review and discuss the findings and recommendations of the external auditor included in the management letter and Schedule of Findings and Questioned Costs, if an OMB Circular A-133 audit is required.

Compliance

- Review the effectiveness of the system for monitoring compliance with laws and regulations and the results of management's investigation and follow-up (including disciplinary action) of any instances of noncompliance.

- Determine that all required tax and information returns are filed with federal, state and local government agencies on a proper and timely basis.

- Review the findings of any examinations by regulatory agencies and any auditor observations.

- Review the process for communicating the code of conduct to organization personnel, and for monitoring compliance therewith.

- Obtain regular updates from management and organization legal counsel regarding compliance matters.

Fraud detection and prevention

- Remain alert to factors that might indicate management fraud, including changes in life-style.

- Consider periodically reviewing management travel and other expenses.

- Carefully review unusual and complex financial transactions.

- Consider periodically reviewing significant nonstandard journal entries, especially those near year-end.

- Monitor compliance with the organization's general code of conduct and conflict-of-interest policies.

- Identify and assess the propriety of related party relationships and transactions at all levels.

- Monitor the adequacy of the organization's information management system and other physical security measures required to protect the entity from fraud and abuse.

- Ensure that every employee or volunteer is aware that the committee is the contact point for reporting suspected fraud or abuse and that the "whistle blower" will be protected.

- Take the lead in investigating suspected fraud and abuse, including communicating appropriate matters to legal counsel and governmental authorities.

- Review the adequacy of insurance coverage associated with fraud and abuse.

- Communicate with external auditors regarding the audit committee's assessment of fraud risks, the entity's responses to those risks and any suspected or actual fraud and abuse reported to it during the year.

Reporting Responsibilities

- Regularly report to the board of directors about committee activities, issues and related recommendations.

- Provide an open avenue of communication between internal audit, the external auditors and the board of directors.

- Review any other reports the organization issues that relate to committee responsibilities.

Other Responsibilities

- Perform other activities related to this charge as requested by the board of directors.

- Institute and oversee special investigations, as needed, regarding significant matters brought to its attention within the scope of its charter.

- Review and assess the adequacy of the committee charter annually, requesting board approval for proposed changes.

- Evaluate the committee's and individual members' performance on a regular basis.

APPENDIX C

SAMPLE ORGANIZATION ANTIFRAUD POLICY

The following is a sample policy for the organization that implements the board's fundamental concepts for preventing and detecting fraud. This sample should be reviewed and adapted to the specific needs of the organization.

General Statement

Management is responsible for establishing the cultural environment, training employees and volunteers, assessing fraud risks, implementing internal controls and monitoring activities designed to prevent and detect misappropriation of organization's assets and intentional material misrepresentation of organization's financial or other data or other actions constituting fraud. It is management's responsibility to communicate this policy to all board members, employees and volunteers and their responsibility to comply with this policy.

Actions Constituting Fraud

It is the organization's policy that there is zero tolerance for actions constituting fraud. These actions include but are not limited to:

- Theft of cash, securities, merchandise, equipment, supplies or other assets.
- Unauthorized use of organization employees, property, credit cards, cell phones or other resources.
- Submission of personal or fictitious employee expenses for reimbursement or fictitious or inflated vendor invoices or payroll records for payment.
- Receiving kickbacks or other unauthorized personal benefits from vendors or others.
- Forgery or fraudulent alteration of any check, bank draft, statement, billing, record, form, report, return or other financial document.
- Intentional material misclassification or misrepresentation of revenues, expenses, costs or other data in financial statements, reports, regulatory returns, applications or other communications.
- Intentional failure to disclose material related party transactions, noncompliance with lender requirements or donor/grantor restrictions or other required disclosure matters.
- Intentional improper use or disclosure of confidential donor, client/customer, employee or organization proprietary information.
- Any other illegal or unethical activity.

The policy applies to fraud or suspected fraud by board members, employees, volunteers, vendors, contractors, consultants and others doing business with the organization.

Reporting Responsibilities and Safeguards

It is the responsibility of every director, employee or volunteer to report, preferably in writing, discovered or suspected unethical or fraudulent activity immediately to the Executive Director and the Chairman of the Board.

No reporting party who in good faith reports such a matter will suffer harassment, retaliation or other adverse consequences. Any director or employee who harasses or retaliates against the party who reported such a matter in good faith is subject to discipline up to and including termination of employment. Additionally, no director, employee or volunteer will be adversely affected because they refuse to carry out a directive which constitutes fraud or is a violation of state or federal law.

Any allegation that proves to have been made maliciously or knowingly to be false will be viewed as a serious disciplinary offense.

Confidentiality

Discovered or suspected matters can be reported anonymously or on a confidential basis. Anonymous allegations will be investigated, but consideration will be given to seriousness of the issue, its credibility and the likelihood of confirming the allegation from other reliable sources. In the case of allegations made on a confidential basis, every effort will be made to keep the identity of the reporting party secret, consistent with the need to conduct an adequate and fair investigation.

Allegations will not be discussed with anyone other than those who have a legitimate need to know. It is important to protect the rights of the persons accused, to avoid damaging their reputation should they be found innocent and to protect the organization from potential liability.

Investigation Procedures

The Executive Director, Chairman of the Board or their delegate will investigate all allegations on a timely basis. The investigation may include but is not limited to examining, copying and/or removing all or a portion of the contents of files, desks, cabinets and other facilities of the organization without prior knowledge or consent of any individual who may use or have custody of such items or facilities when it is within the scope of the investigation.

The reporting party must not attempt to personally conduct investigations, interviews or interrogations related to the alleged fraudulent activity.

Resolution Procedures

The results of the investigation will be reported to the Board of Directors. Actions taken against the perpetrator of alleged fraud will be determined by the Board in consultation with legal counsel.

APPENDIX D

SAMPLE CODE OF CONDUCT STATEMENT

The following is a sample code of conduct with emphasis on topics that have anti-fraud implications which should be reviewed and adapted to the specific needs of the organization.

Organization-Wide Code of Conduct

The organization and its employees and volunteers must, at all times, comply with all principles and policies of the organization and applicable laws and regulations. The organization does not condone or promote the activities of employees or volunteers who achieve results through violation of law or unethical dealings. This includes any payments for illegal acts, indirect contributions, rebates, bribery or misrepresentation of any financial or other data.

All conduct should be well above the minimum standards required by the underlying philosophy of the organization or required by law. Accordingly, employees and volunteers must ensure that their actions cannot be interpreted as being, in any way, in contravention of the ethical principles or laws and regulations governing the organization's operations.

Employees uncertain about the application or interpretation of any governing principles or legal requirements should refer the matter to their superior or the audit committee.

Employee/Volunteer Conduct

The organization expects its employees and volunteers to conduct themselves in a professional manner at all times. The organization has clearly defined prohibited conduct, including use of intoxicants, gambling, sexual harassment, pornography, accepting unapproved financial gains, improper use of organization's assets or time, as well as the reporting responsibilities and the potential consequences of such activities in Section 2 of the organization's Personnel Manual. Those policies and procedures are incorporated in full in this code of conduct.

Conflicts of Interest

The organization has clearly defined possible conflicts of interest, immediate reporting obligations and annual conflict-of-interest statement requirements in Section 2 of the organization's Personnel Manual. Those policies and procedures are incorporated in full in this code of conduct.

Handling Organization Resources and Records

Organization resources have been provided by donors, customers, government funding agencies and others in trust for the exempt purposes of the organization. The resources and other assets of the organization are for organization purposes only and not for personal benefit of employees or volunteers. This includes the personal use of the organization's facilities, materials, personnel, influence, equipment (including computers) and other resources.

Employees and volunteers who have access to the organization's resources and records in any capacity must follow the prescribed procedures as detailed in the Financial Policies and Procedures Manual. The organization has established and implemented a comprehensive system of internal controls. It is the responsibility of every employee and volunteer to understand and work within that system.

The organization uses records of many types to manage its activities and to meet the organization's financial and legal responsibilities. Accurate and complete records are a must. The employees and volunteers responsible for accounting and reporting must fully record all assets and liabilities and fully disclose all matters required by accounting principles, government regulations and ethical practices.

Employees and volunteers must not engage in any false recordkeeping or reporting of any kind, whether external or internal, including:

- False attendance or enrollment reports, client service or unit delivery counts, or donor lists or similar non-financial reports.

- Misleading donor or grantor solicitations, false advertising, deceptive marketing practices, and other misrepresentations.

- False expense reports, deceptive attendance, enrollment or client/unit delivery, production reports, false revenue or expense classification or other financial misrepresentations.

When handling financial and personal information about donors, customers, employees, volunteers and others with whom the organization has dealings, the following principles must be observed[1]:

- Collect, use and retain only the personal information necessary for the organization's activities. Whenever possible, obtain only any relevant information directly from the person concerned. Use only reputable sources to supplement this information.

- Retain information only as long as necessary or as required by law. Protect the physical security of this information.

- Limit internal access to personal information to those with legitimate purpose for seeking and using that information for the purposes it was originally obtained.

The organization imposes strict standards to prevent fraud and dishonesty. If employees or volunteers discover or become aware of any information that would cause them to suspect fraudulent activity, they must report such activity to the audit committee. The employee or volunteer reporting such activity can be assured that their communication will be kept in the strictest confidence and, as protected by law, will not result in any form of retribution. Employees or volunteers who are proven to have engaged in fraud or dishonest activity will be prosecuted to the full extent of the law.

Each board member, officer, manager, employee and volunteer is required to sign the following statement. The statement must be kept on file and updated annually.

To the Audit Committee

I have read and understand the organization's code of conduct and related documents and represent that I understand my obligations and that I have not engaged in any activities that would be prohibited under these policies. In addition, I represent that any activities that would be considered to be prohibited by these policies have been fully and completely reported to you.

Name_____ Date_____

[1] Adapted from the AICPA's *CPA Handbook of Fraud and Commercial Crime Prevention*.

APPENDIX E

SAMPLE CONFLICT OF INTEREST POLICY

Fairness in decision-making is more likely to occur in an impartial environment. Conflicts of interest and related-party transactions are two forms of subjective activity that can result in improper results. The following policy is communicated to board members, management, employees and volunteers upon joining the organization and annually thereafter.

Conflicts of Interest

The potential for a conflict of interest arises in situations in which a person has a responsibility to promote the organization's best interest, but has a direct or indirect personal competing interest at the same time. If the personal competing interest is exercised over a fiduciary interest, the conflict is realized. Conflicts of interest or the appearance thereof should be avoided. Examples of conflict of interest may include, but are not limited to the following situations in which a director, employee or volunteer of the organization:

- Receives a gift from a vendor if the organization's representative is responsible for initiating or approving purchases from that vendor.

- Approves or authorizes the organization to provide financial or other assistance to persons related to the director, employees or volunteer.

- Transacts a contract, sale, lease or purchase for the organization and receives direct or indirect personal benefit from the purchaser, lessor or vendor. Transactions with officials of the organization are adequately controlled and disclosed in the records, and such transactions occur only in the normal course of business and are approved by the board.

- Uses the organization's facilities, assets, employees or other resources for personal benefit.

Related-Party Transactions

Related-party transactions are transactions that occur between two or more parties that have interlinking relationships. These transactions should be disclosed to the governing board. Transactions should be evaluated to ensure they are made on a sound economic basis. Some related-party transactions are clearly to the advantage of the organization and should be pursued. Other related-party transactions are conflicts of interest and should be avoided.

Transactions with related parties should be undertaken only in the following situations:

- The audited financial statements of the organization fully disclose material related-party transactions.
- Related parties are excluded from the discussion and approval of related-party transactions.
- Competitive bids or comparable valuations exist.
- The organization's board approves the transaction as being in the best interest of the institution.

Each board member, the executive director (or equivalent), members of senior management, employees or certain volunteers with purchasing and/or hiring authority or responsibilities are required to sign the following statement. The statement must be kept on file and updated annually.

To the Board (or Board Committee)

I have read and understand the organization's conflict of interest policy and represent that I have not engaged in any activities that would be prohibited under that policy. In addition, I represent that any activities that would be considered to be related-party transactions have been fully and completely reported to you.

Name_____ Date_____

APPENDIX F

THE ASSOCIATION OF CERTIFIED FRAUD EXAMINERS' FRAUD PREVENTION CHECKUP

HOW TAKING THE CHECKUP CAN HELP

It could save your company or other entity from disaster. Fraud can be a catastrophic risk. If you don't proactively identify and manage your fraud risks, they could put you out of business almost overnight. Even if you survive a major fraud, it can damage your reputation so badly that you can no longer succeed independently. It could pinpoint opportunities to save you a lot of money. Fraud is an expensive drain on an entity's financial resources. In today's globally competitive environment, no one can afford to throw away the 7% of revenues that represents the largely hidden cost of fraud. Those businesses that have identified their most significant fraud costs (such as insurance and credit card companies) have made great strides in attacking and reducing those costs. If an entity isn't identifying and tackling its fraud costs, it is vulnerable to competitors who lower their costs by doing so. Fraud is now a common risk that shouldn't be ignored. The incidence of fraud is now so common that its occurrence is no longer remarkable, only its scale. Any entity that fails to protect itself appropriately from fraud should expect to become a victim of fraud, or rather, should expect to discover that it is a victim of fraud.

- It's the least expensive way to find out the entity's vulnerability to fraud. Most entities score very poorly in initial fraud prevention checkups because they don't have appropriate anti-fraud controls in place. By finding this out early, they have a chance to fix the problem before becoming a victim of a major fraud. It's like finding out you have seriously high blood pressure. It may be bad news, but not finding out can be a lot worse.

- It's a great opportunity for an entity to establish a relationship with a Certified Fraud Examiner whom they can call on when fraud questions arise. Since the risk of fraud can be reduced but is rarely eliminated, it's likely that the entity will experience fraud in the future and will need a CFE's assistance.

- Strong fraud prevention processes could help increase the confidence investors, regulators, audit committee members and the general public have in the integrity of the entity’s financial reports. They could help to attract and retain capital.

THE ASSOCIATION OF CERTIFIED FRAUD EXAMINERS' FRAUD PREVENTION CHECKUP

BEFORE YOU TAKE THE CHECKUP

- Let your entity's general counsel or outside legal counsel know you plan to take the test. They may want to have you use the test under their direction, to protect your entity's legal rights.
- Don't take the test if you plan to ignore the results. If it shows you have poor fraud prevention processes, you need to fix them. Failing to act could cause legal problems.

WHO SHOULD PERFORM THE CHECKUP?

- The fraud prevention checkup should ideally be a collaboration between objective, independent fraud specialists (such as Certified Fraud Examiners) and people within the entity who have extensive knowledge about its operations. To locate a Certified Fraud Examiner in your area, see www.CFEnet.com or call (800) 245-3321.

- Internal auditors bring extensive knowledge and a valuable perspective to such an evaluation. At the same time, the perspective of an independent and objective outsider is also important, as is the deep knowledge and experience of fraud that full-time fraud specialists provide.

- It is helpful to interview senior members of management as part of the evaluation process. But it is also valuable to interview employees at other levels of the entity, since they may sometimes provide a "reality check" that challenges the rosier view management might present, e.g., about management's commitment to ethical business practices.

HOW MANY POINTS SHOULD WE AWARD FOR EACH ANSWER?

- The number of points available is given at the bottom of each question. You can award zero points if your entity has not implemented the recommended processes for that area. You can give the maximum number of points if you have implemented those processes and have had them tested in the past year and found them to be operating effectively. Award no more than half the available points if the recommended process is in place but has not been tested in the past year.

- The purpose of the checkup is to identify major gaps in your fraud prevention processes, as indicated by low point scores in particular areas. Even if you score 80 points out of 100, the missing 20 could be crucial fraud prevention measures that leave you exposed to major fraud. So there is no passing grade other than 100 points.

THE ACFE FRAUD PREVENTION CHECKUP

	RESULTS
ENTITY:_____ **DATE OF CHECKUP:_____** ***1. Fraud risk oversight*** • To what extent has the entity established a process for oversight of fraud risks by the board of directors or others charged with governance (e.g., an audit committee)? • Score: From 0 (process not in place) to 20 points (process fully implemented, tested within the past year and working effectively). ***2. Fraud risk ownership*** • To what extent has the entity created "ownership" of fraud risks by identifying a member of senior management as having responsibility for managing all fraud risks within the entity and by explicitly communicating to business unit managers that they are responsible for managing fraud risks within their part of the entity? • Score: From 0 (process not in place) to 10 points (process fully implemented, tested within the past year and working effectively). ***3. Fraud risk assessment*** • To what extent has the entity implemented an ongoing process for regular identification of the significant fraud risks to which the entity is exposed? • Score: From 0 (process not in place) to 10 points (process fully implemented, tested within the past	

year and working effectively).	

THE ACFE FRAUD PREVENTION CHECKUP

	RESULTS
4. Fraud risk tolerance and risk management policy • To what extent has the entity identified and had approved by the board of directors its tolerance for different types of fraud risks? For example, some fraud risks may constitute a tolerable cost of doing business, while others may pose a catastrophic risk of financial or reputational downage to the entity. The entity will likely have a different tolerance for these risks. • To what extent has the entity identified and had approved by the board of directors a policy on how the entity will manage its fraud risks? Such a policy should identify the risk owner responsible for managing fraud risks, what risks will be rejected (e.g., by declining certain business opportunities), what risks will be transferred to others through insurance or by contract, and what steps will be taken to manage the fraud risks that are retained. • Score: From 0 (process not in place) to 10 points (process fully implemented, tested within the past year and working effectively). ***5. Process level anti-fraud controls/re-engineering*** • To what extent has the entity implemented measures, where possible, to eliminate or reduce through process re-engineering each of the significant fraud risks identified in its risk assessment? Basic controls include segregation of duties relating to authorization, custody of assets and recording or reporting of transactions. In some cases it may be more cost-effective to re-engineer business processes to reduce fraud risks	

rather than layer on additional controls over existing processes. For example, some	

THE ACFE FRAUD PREVENTION CHECKUP

fraud risks relating to receipt of funds can be eliminated or greatly reduced by centralizing that function or outsourcing it to a bank's lockbox processing facility, where stronger controls can be more affordable. • To what extent has the entity implemented measures at the process level designed to prevent, deter and detect each of the significant fraud risks identified in its risk assessment? For example, the risk of sales representatives falsifying sales to earn sales commissions can be reduced through effective monitoring by their sales manager, with approval required for sales above a certain threshold. • Score: From 0 (process not in place) to 10 points (process fully implemented, tested within the past year and working effectively). ***6. Environment level anti-fraud controls*** • Major frauds usually involve senior members of management who are able to override process-level controls through their high level of authority. Preventing major frauds therefore requires a very strong emphasis on creating a workplace environment that promotes ethical behavior, deters wrongdoing and encourages all employees to communicate any known or suspected wrongdoing to the appropriate person. Senior managers may be unable to perpetrate certain fraud schemes if employees decline to aid and abet them in committing a crime. Although	**RESULTS**

"soft" controls to promote appropriate workplace behavior are more difficult to implement and evaluate than traditional "hard" controls, they appear to be the best defense against fraud involving senior management.	

THE ACFE FRAUD PREVENTION CHECKUP	
• To what extent has the entity implemented a process to promote ethical behavior, deter wrongdoing and facilitate two-way communication on difficult issues? Such a process typically includes: - o Having a senior member of management who is responsible for the entity's processes to promote ethical behavior, deter wrongdoing and communicate appropriately on difficult issues. In large public companies, this may be a full- time position as ethics officer or compliance officer. In smaller companies, this will be an additional responsibility held by an existing member of management. o A code of conduct for employees at all levels, based on the entity's core values, which gives clear guidance on what behavior and actions are permitted and which ones are prohibited. The code should identify how employees should seek additional advice when faced with uncertain ethical decisions and how they should communicate concerns about known or potential wrongdoing affecting the entity. o Training for all personnel upon hiring and regularly thereafter concerning the code of conduct, seeking advice and communicating potential wrongdoing.	**RESULTS**

Communication systems to enable employees to seek advice where necessary prior to making difficult ethical decisions and to express concern about known or potential wrongdoing affecting the entity. Advice systems may include an ethics or compliance telephone help line or e-mail to an ethics or compliance office/officer. The same or similar systems may be used to enable	
THE ACFE FRAUD PREVENTION CHECKUP	
employees (and sometimes vendors, customers and others) to communicate concerns about known or potential wrongdoing affecting the entity. Provision should be made to enable such communications to be made anonymously, though strenuous efforts should be made to create an environment in which callers feel sufficiently confident to express their concerns openly. Open communication makes it easier for the entity to resolve the issues raised, but protecting callers from retribution is an important concern. • A process for promptly investigating where appropriate and resolving expressions of concern regarding known or potential wrongdoing, then communicating the resolution to those who expressed the concern. The entity should have a plan that sets out what actions will be taken and by whom to investigate and resolve different types of concerns. Some issues will be best addressed by human resources personnel, some by general counsel, some by internal auditors and some may require investigation by fraud specialists. Having a pre-arranged plan will greatly speed and ease the response and will ensure appropriate persons are notified where significant potential issues are involved (e.g.,	**RESULTS**

legal counsel, board of directors, audit committee, independent auditors, regulators, etc.) • Monitoring of compliance with the code of conduct and participation in the related training. Monitoring may include requiring at least annual confirmation of compliance and auditing of such confirmations to test their completeness and accuracy.	

THE ACFE FRAUD PREVENTION CHECKUP	
• Regular measurement of the extent to which the entity's ethics/compliance and fraud prevention entity goals are being achieved. Such measurement typically includes surveys of a statistically meaningful sample of employees. Surveys of employees' attitudes towards the entity's ethics/compliance activities and the extent to which employees believe management acts in accordance with the code of conduct provide invaluable insight into how well those items are functioning. • Incorporation of ethics/compliance and fraud prevention goals into the performance measures against which managers are evaluated and which are used to determine performance related compensation. • Score: From 0 (process not in place) to 30 points (process fully implemented, tested within the past year and working effectively). ***7. Proactive fraud detection***	**RESULTS**

• To what extent has the entity established a process to detect, investigate and resolve potentially significant fraud? Such a process should typically include proactive fraud detection tests that are specifically designed to detect the significant potential frauds identified in the entity's fraud risk assessment. Other measures can include audit "hooks" embedded in the entity's transaction processing systems that can flag suspicious transactions for investigation and/or approval prior to completion of processing. Leading edge fraud detection methods include computerized e-mail monitoring (where legally permitted) to identify use of certain phrases that might indicate planned or ongoing wrongdoing.	

THE ACFE FRAUD PREVENTION CHECKUP

	RESULTS
• Score: From 0 (process not in place) to 10 points (process fully implemented, tested within the past year and working effectively). TOTAL SCORE (Out of a possible 100 points): **Interpreting the Entity's Score** A brief fraud prevention checkup provides a broad idea of the entity's performance with respect to fraud prevention. The scoring necessarily involves broad judgments, while more extensive evaluations would have greater measurement data to draw upon. Therefore the important information to take from the checkup is the identification of particular areas for improvement in the entity's fraud prevention processes. The precise numerical score is less important and is only presented to help communicate an overall impression. The desirable score for an entity of any size is 100 points, since the recommended processes are scalable to the size of the entity. Most entities should expect to fall significantly short of 100 points in an initial fraud prevention checkup. That is not currently considered to be a material weakness in internal controls that represents a reportable condition under securities regulations. However, significant gaps in fraud prevention measures should be closed promptly in order to reduce fraud losses and reduce the risk of future disaster.	

APPENDIX G

SAMPLE INTERNAL AUDIT CHECKLIST - CASH

The following sample internal audit antifraud checklist reflects a few indicators or risks of fraud (or error) in the area of cash receipts and disbursements and some possible audit procedures used to pursue common fraud schemes. Since no sample checklist can encompass all possibilities or responses, the user must tailor the following to the organization's particular situation.

Misappropriation of assets:		
Possible fraud scheme	Risk/Indicator	Audit procedure
• Theft of all receipts or shorting the deposit (skimming[1])	• Missing transaction record • Inventory shortage • Cash receipts or deposit totals differ from expected patterns • Unusual journal entries or unusual items on the bank reconciliation • Unusual behavior of potential suspects • Inadequate segregation of duties	• Compare bank deposits to cash receipts records • Reconcile inventory to sales • Review existing bank reconciliations • Prepare 4-column bank reconciliation • Examine documents supporting entries, slow-to-clear or reconciling items • Written confirmation to prior donors • Send bank statement to independent party • Donor statements prepared and mailed by independent party
• Lapping[2]	• Donor complaints • Different dates between deposits and entries to donor records • Differences between deposit slip names and amounts of credits to donor accounts • Unauthorized write-off of pledges or promises to give • Unusual journal entries • Inadequate segregation of duties	• Direct interview or written confirmation of amounts with donor • Trace deposits with special attention to details of each deposit • Prepare 4-column bank reconciliation • Examine documents supporting entries • Ratio analysis • Assignment rotation and mandatory vacations

Misappropriation of assets:		
Possible fraud scheme	Risk/Indicator	Audit procedure
• Unauthorized general check or credit card disbursements	• Unusual behavior of potential suspects • Theft of checks, missing checks or checks out of sequence • Altered checks[4] • Missing voided or cancelled checks • Unusual payees (such as cash or unapproved vendors) • Unusual endorsements on checks[4] • Stale checks on bank reconciliations • Unlimited access to unused checks or check printing machines • Missing or unusual supporting documents • Copies rather than original supporting documents • Difference between payee on check and check register • Unusual or duplicate amounts of travel, entertainment or other employee expenses • Inadequate segregation of duties • Unusual behavior of potential suspects	• Inventory unused checks • Review check register for extended period and account for un-sequenced checks • Obtain check duplicate from bank • Compare to vendor list; contact payee • Review cancelled checks for same payee and endorsement • Examine supporting documents • Contact credit card company for support or vendor name • Contact vendor for duplicate document or proof of transaction • Obtain cut-off bank statements • Review bank reconciliations • Prepare 4-column bank reconciliation • Review journal entries • Contact travel agent or travel company • Re-compute mileage, contact vendor • Conduct interviews • Use positive pay bank controls

Misappropriation of assets:		
Possible fraud scheme	Risk/Indicator	Audit procedure
• Unauthorized payroll or payroll related disbursements	• Theft of checks, missing payroll checks or checks out of sequence • Checks to employees with incomplete or no personnel records • Duplicate paychecks or entries on payroll records • Employee complaints about improper pay or withholdings • Employee complaints about excess compensation on Form W-2 • Unusual payees or endorsements on checks • Uncontrolled unclaimed payroll checks • Unauthorized electronic funds transfers • Unusual or unexpected fluctuations from budget in payroll expense or hours • Unapproved timesheets or time cards • IRS notices about failure to make timely deposits • Late tax deposits • Unusual endorsements on tax deposits • Inadequate segregation of duties • Unusual behavior of potential suspects	• Inventory unused checks • Review check register for extended period and account for un-sequenced checks • Obtain check duplicate from bank • Verify existence of employee • Distribute or observe distribution of payroll checks on a surprise basis • Review payroll register • Review personnel files • Review payroll checks • Perform social security number review • Compare authorized pay rates to pay rates on payroll records • Review payroll withholding tax returns filed • Ratio analysis • Investigate variances from budget

Misrepresentation of financial statements:		
Possible fraud scheme	Risk/Indicator	Audit procedure
• Improper cash cut-off at end of reporting period	• Holding receipts records open after period end date • Recording disbursements in subsequent reporting period • Improper accounting for held checks • Multiple cash transfers among bank accounts at end of period (kiting[3]) • Minimum cash balances required by grants or debt agreements • Inadequate segregation of duties • Unusual behavior of potential suspects	• Inspect deposits and cancelled checks for dates cleared bank noting any unusual patterns • Examine receipts and disbursement registers and related supporting documents for proper period • Examine undeposited receipts and unpaid invoices for proper period • Prepare and review interbank transfer schedule to determine transfer recorded in same period

Notes:
1 - Skimming is removal of cash received prior to entry in an accounting system leaving no audit trail.
2 - Lapping is continuously recording receipts from one source in the account of another to cover theft from that account.
3 - Kiting is transferring funds among bank accounts and not recording the transfers in the same period.
4 - Altered checks could include forged maker, fictitious payee, altered payee or amount, forged endorsement, dual endorsement and many others.

APPENDIX H

OTHER USEFUL RESOURCES

Web sites with information directly related to prevention or detection of fraud or addressing issues related to fraud.

American Institute of Certified Public Accountants – www.aicpa.org
American Institute of Philanthropy – www.charitywatch.org
Association of Certified Fraud Examiners – www.cfenet.com
Association of Fundraising Professionals – www.afpnet.org
BBB Wise Giving Alliance – www.give.org
BoardSource – www.boardsource.org
Charity Navigator – www.charitynavigator.org
EthicsLine – www.ethicsline.com
Evangelical Council for Financial Accountability – www.ecfa.org
FraudNet – www.fraudnet@gao.gov
General Accounting Office – www.gao.gov
GuideStar – www.guidestar.org
IGNet – www.ignet.gov
Information Systems Audit and Control Association – www.isaca.org
The Institute of Internal Auditors – www.theiia.org
Internal Revenue Service – www.irs.gov
Management Assistance Program for Nonprofits – www.mapnp.org
National Association of College and University Business Officers – www.nacubo.org
National Association of State Charity Officials – www.nasconet.org
National White Collar Crime Center – www.nw3c.org
Nonprofit Risk Management Center – www.nonprofitrisk.org
Society for Human Resource Management – www.shrm,org
Wall Watchers' Ministry Watch – www.ministrywatch.com

Printed resources

American Institute of Certified Public Accountants. *Statement on Auditing Standards No. 99, Consideration of Fraud in a Financial Statement Audit*. New York: AICPA, October 2002

American Institute of Certified Public Accountants. *Management Antifraud Programs and Controls, Guidance to Help Prevent and Deter Fraud*. New York: AICPA, October 2002

American Institute of Certified Public Accountants. *The AICPA Audit Committee Toolkit*. New York: AICPA, December 2003

Association of Certified Fraud Examiners. *2008 Report to the Nation, Occupational Fraud and Abuse*. Austin, TX: ACFE, 2008.

Association of Certified Fraud Examiners. *How Fraud Hurts You and Your Organization*. Austin, TX: ACFE, 2002.

Burke, Frank M., and Guy, Dan M. *Audit Committees: A Guide for Directors, Management, and Consultants,* Second Edition. New York: Aspen Publishers, Inc., 2002.

KPMG. *Fraud Survey 2003*. KPMG, 2003.

Kurtz, Daniel L. *Managing Conflicts of Interest*. Washington, DC: BoardSource, 2001.

Thompson-PPC. *Guide to Fraud Detection*. Fort Worth, TX: PPC, 2004

Thompson-PPC. *Guide to Internal Control and Fraud Prevention*. Fort Worth, TX: PPC, 2004

Romney, Marshall B. *Fraud-Related Internal Controls*. Austin, TX: Association of Certified Fraud Examiners.

Wells, Joseph T. *Occupational Fraud and Abuse*. Austin, TX: Obsidian Publishing Company, 1997.

Zack, Gerard M. *Accounting & Audit Issues of Nonprofit Organizations*. Rockville, MD: Nonprofit Resource Center and Williams Young, LLC, 1992-2002.

Zack, Gerard M. *Fraud and Abuse in Nonprofit Organizations: A Guide to Prevention and Detection*. Rockville, MD: Nonprofit Resource Center and Williams Young, LLC, 1992-2002.