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

Preventing and Detecting Fraud in Not-For-Profit Organizations

AN OVERVIEW OF FRAUD IN THE UNITED STATES

2024 Report 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* 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 2024 report was based on 1921 fraud cases that were reported by the Certified Fraud Examiners (CFE) who investigated them. The latest report focused on these areas: the cost of occupational fraud, how it is committed, who commits it, and how it can be prevented and detected.

Based on the 2024 study, the following conclusions were reached:

- It was estimated that 5% of revenues will be lost as a result of fraud.

- About 89% of occupational frauds involve asset misappropriations. Asset theft schemes – check and payment tampering, billing, and theft of noncash assets – present the greatest overall risk to organizations, based on the combination of frequency and potential loss. The second most frequent category of fraud was corruption, e.g., schemes involving bribery or conflicts of interest, at 48%

- The study reported on education and religious, charitable and social services organizations when it considered the not-for-profit industry. Methods of asset fraud found in educational institutions in the 2024 study: corruption, 43%; billing, 36%; skimming, 19%; expense reimbursements, 17%; noncash, 16%; cash on hand, 13%; check and payment tampering, 10%; cash larceny, 9%; payroll, 7% and register disbursements, 6%[1]. Corruption was identified as a particularly high-risk area in educational institutions.

- Methods of asset fraud found in religious, charitable and social services organizations in the 2024 study: corruption, 45%; billing, 36%; expense reimbursements, 29%; cash on hand, 24%; cash larceny and check and payment tampering each at 17%; non-cash theft, 10%; payroll, 7%; and register disbursements, 2%.[1] Here again corruption was identified as a particular risk in this category of the not-for-profit industry.

  [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 were committed by operations, 14%, followed by accounting and sales departments at 12% each. While about 87% of the fraudsters were first-time offenders and 7% were charged but not convicted, the study found that the longer one stays at an organization, the greater their level of responsibility [and trust level] and the greater loss to fraud.

The median tenure of the perpetrator in the study was 1-5 years with the largest losses attributed to those more than ten years of employment with the organization.

- 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. Other potential indicators included unusually close relationship with a vendor, control issues, defensiveness, wheeler dealer attitude and divorce/family problems.. At least one red flag was exhibited in 84% of the cases. Fraudsters living beyond their means has consistently be the most common behavioral red flag since ACFE began tracking the data in 2008.

- The most common methods for detecting fraud in organizations was by a tip from an employee, (52%); customer, (21%); anonymous source, (15%); or vendor, (11%). Other common methods include internal audit, management review, document examination, account reconciliation, followed by accident, external audit and in that order. The typical scheme lasted 12 months before discovery.

- The implementation of anti-fraud controls appears to have a measurable impact on the organization's exposure to loss. Some of the most commonly used controls were:
    - Code of conduct 85%
    - External audit of financial statements 84%
    - Internal audit department 80%
    - Management review 72%
    - Hotline 71%
    - Independent audit committee 68%
    - Fraud training for employees 63%
    - Formal fraud risk assessments 48%
    - Proactive data analysis 45%
    - Surprise audits 42%

- Overall, surprise audits proved to be the most effective in fraud loss at 63%, although used in only 42% of the cases reported. Smaller organizations with fewer resources are particularly vulnerable to fraud but several controls-such as a code of conduct, management review procedures and fraud training for employees-can be implemented at nominal cost.

- Smaller organizations failed to implement the following controls which are low cost but are often effective: hotline, 50%; anti-fraud policy, 50%; fraud awareness training for managers/executives and for employees, 50%; and code of conduct, 40%. Nonprofit organizations were found to have the lowest implementation rate of fraud awareness training. The 2024 study found that nonprofit organizations that provided awareness training uncovered frauds more than 2.5X times faster than organizations that did not.

- The lack of adequate internal controls was most commonly cited as the factor that allowed the fraud to occur. The some of the internal control weaknesses that contributed to fraud were as follows.

  - Lack of internal controls 32%
  - Override of existing internal controls 19%
  - Lack of management review 18%
  - Lack of competent personnel in oversight roles 9%
  - Poor tone at the top 8%
  - Lack of employee fraud education 3%

Other Relevant Highlights from the 2024 ACFE Report

The median loss caused by fraud in the study was $145,000. The median loss for religious, charitable or social services organizations was $85,000 and $50,000 for educational institutions.

Approximately 57% of the organizations conducted background checks before the fraudster was hired. The background checks included employment history 47%; criminal checks, 43%; reference checks, 30%; education verification, 30%; credit checks, 20% and drug screening, 13%. The study found that background checks revealed red flags in 16% of the cases. The study also found that 5% of the perpetrators had been convicted of a prior fraud-related offense and 7% were fired for fraud-related conduct by a previous employer. The study also found that 18% of the schemes had two co-conspirators (median loss - $135,000) and 36% had three or more co-conspirators (median loss - $329,000).

Fraud in Heartland Churches

The ACFE study reported on education and religious, charitable and social services organizations when it considered the not-for-profit industry. One segment of the religious organizations, churches, was the focus of a study conducted by Keller & Owens, LLC. At that time over 12,500 churches in Kansas and Missouri were invited to participate in an anonymous on-line survey about whether they had experienced financial fraud. Here are some of the findings:

- Slightly more than two-thirds of the churches that were victims of fraud reported average Sunday worship attendance of less than 250 congregants.
- Fifty percent of fraud victims reported annual average budgeted revenue of $250,000 or less.
- Nearly 60% of churches that experienced fraud reported having only 1 or 2 persons assisting in the accounting/finance areas underscoring the importance of the internal control principle of adequate segregation of duties.
- The survey found that estimated losses ranged from less than $1,000 to a high of approximately $400,000 with a median loss of $40,000.
- The survey found that poor or non-existent oversight or inadequate internal controls provided the fraudster with the most frequent opportunities to commit fraud.

- Respondents to the survey reported that asset misappropriation was the most common type of fraud they had experienced.
- Seventy percent of the respondents reporting incidents of fraud identified "red flags" that might have given observers reason for concern, such as defensiveness, living beyond means or refusing to take vacations and let others do their tasks.
- Sixty-five percent of the churches reported having no fraud gave strong oversight, good segregation of duties and sound internal controls as the reasons for no financial fraud.

Estimated Impact on the Not-For-Profit Industry

Generally available data for 2024, found that there were more than 1.5 million not-for-profit organizations in the U.S. generating an estimated $592 billion in revenue. The ACFE estimates that organizations lose about 5% of annual revenue to fraud. That means that as much as $30 billion dollars is lost to fraud in not-for-profit organizations. Of the 1,921 cases studied, 10 percent of those involved a not-for-profit organization, with a weighted average loss of approximately $76,000 per incident.

Looking again at the religious organization segment of the not-for-profit sector, church fraud is "big business." According to a recent article from the Center for the Study of Global Christianity which reports that there was more than $62 billion in church-related financial fraud during the 2023 (the latest data reported). This compares to $55 billion churches spent on missions during the same period. An article in *Christianity Today* states that financial fraud is expected to cost Christian ministries $170 billion by 2050.

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).

- Leaders of the Minnesota nonprofit, Feeding Our Future, were convicted for stealing over $240 million from federal nutrition funds to buy luxury homes, cars, and fund lavish travel, involving bribery and money laundering.

- Cancer Fund of America Network was accused of collecting over $187 million in donations, most of which was not used to help cancer patients but was instead funneled to the founders and their families for lavish personal expenses.

- In 2025, a Missouri couple was accused of stealing $7 million in federal funds intended for a program that provided meals for low-income children. The couple faked records to claim they had served more than 2million meals, using the money to finance a lavish lifestyle that included a $1.4 million home.

- In 2025, federal authorities arrested the leaders of a special needs trust, who allegedly embezzled $100 million over 15 years from disabled people and their families.

- 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 local church senior pastor stole tens of thousands using false expense reports and supporting documents.

- 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.

- The teaching pastor of a large metropolitan church persuaded two widows to give their insurance settlements to the church through him. He pocketed the funds.

- 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.

- A former school official pleaded guilty to fraud charges in the misuse of more than $325,000 in grant money meant to improve the teaching of science and mathematics.

- Three persons associated with a university athletic association plead guilty to selling complimentary tickets for personal benefit and gain.

- An individual not associated with a United Way chapter through the use of identity theft initiated a wire transfer of $800,000 to a personal bank account.

- The senior financial officer diverted millions of dollars from a social services organization by arranging for payments of fictitious invoices for non-existent services from a fictitious vendor.

- An employee of a nursing home embezzled approximately $10,000 by writing checks to himself.

- An investment manager of a university foundation diverted funds into an entity that was determined to be a “Ponzi scheme”.

- A program manager of a senior services organization issued checks approximating $90,000 to a fictitious subcontractor for alleged home repairs and moving services for families in the caregiver program.

- A veterans’ foundation found that the office manager had been approving for payment invoices from vendors that included significant overcharges which were refunded by the vendor and kept by the employee.

- An organization serving orphans reported that an employee diverted about $175,000 in donations received in the mail. The employee opened the mail alone.

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, directors and volunteers. External frauds are committed by persons outside of the organization, such as vendors, sub-recipients, grant applicants, hackers and program participants.

Internal frauds can be broken down into three separate categories: asset misappropriations, corruption 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 (see Appendix J for a sample internal audit checklist):

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 or receives payment for tuition, meals, fees or merchandise sales, 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 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

- Altered payee schemes – involves changing the payee designation on the check to the fraudster or accomplice after it was correctly written and recorded.

- 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. One way employees commit credit card schemes is to "double dip", i.e., use the organization's credit card to make a purchase and then submits the documentation for the expenditure for reimbursement on their expense report.

- Electronic funds (wire) transfers – employee transfers funds to personal or fictitious vendor accounts.

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

- Forged endorsement schemes – consists of forging the manual or stamped endorsement of an intended payee of an organization check.

- Forged maker schemes – involves forging an authorized signature, manually or by facsimile, on an organization check.

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 – expense reimbursement schemes commonly used are mischaracterized expenses, overstated expenses, fictitious expenditures and multiple reimbursements. Examples of mischaracterized expenses include claiming personal travel as a business trip, claiming unauthorized spousal travel expenses, listing dinner with a friend as business development, purchasing supplies and equipment for the organization and taking them for personal use and so on. An employee can overstate expenses by altering receipts or other supporting documents and submitting a photocopy of the receipt. Altered receipts from other persons can be submitted as this employee's expense. Photocopies of altered receipts can be submitted multiple times for reimbursement.

Other asset misappropriations:

- Property and equipment schemes – outright theft of an asset. This includes the theft of supplies, tools, computers, and intellectual property including proprietary information such as trade secrets and works made for hire. The latter includes creative works such as those that can be copyrighted: 1) music, 2) sound recordings, 3) literary works [includes sermons], 4) drama, 5) audio-visual (videos/films), 6) choreography, 7) visual images and 8) architecture covered by Section 201(b) of the Copyright Act of 1976.

- Personal use of organization's assets and other resources (corruption) – use of organization's computers, software, printers and vehicles 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.

Corruption (see Appendix K for steps to root out corruption):

Corruption is the wrongful use of influence to procure a benefit for the fraudster or another person contrary to the duty or rights of others. The 2024 ACFE study reported that the second most frequent category of fraud overall was corruption and the most frequent category in nonprofits. An overview of available resources states that corruption in US nonprofits is due to common vulnerabilities like weak internal financial controls, lack of oversight (especially with volunteers/boards focused on missions), poorly trained volunteers, trusting environments and insufficient resources in IT/auditing. Nonprofit corruption in the US involves various schemes, from embezzlement (stealing, faking payroll, misusing credit cards) and fraudulent fundraising (deceptive campaigns) to vendor schemes (fake invoices) and political influence (using donations to sway lawmakers) among others. Some examples -

- Diversion of funds for personal use – see multiple examples on pages 6-8.

- Conflict of interest - a facilities manager who purchased supplies at inflated prices from a company in which he has an undisclosed ownership interest.

- Invoice kickbacks – business manager receives a kickback (cash or goods) from a vendor who inflated prices, overbilled or delivered goods of lesser quality than ordered.

- Bid rigging – executive director did not seek competitive bids or accept the lowest, qualified bid but awarded the contract to a personal friend, relative or business in which he has an undisclosed ownership interest or received some personal benefit.

External fraud, while not as common as internal frauds, externally initiated 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.

- Cybercrimes – malicious activity such as online identity theft, hacking, phishing, loss of intellectual property, loss of property and an increasing variety of fraudulent actions.

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 or administrative 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 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.

- Fraudulent statement of compliance with requirements of funding sources.

- Misclassifying restricted donations to mislead donors or charity watchdogs.

- Holding records open beyond the period end 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 to understate expenses.

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

As the 2024 ACFE 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.

Rationalization

Those involved in a fraud 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.

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 Appendices A and C for a sample antifraud policies.

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.

According to the publication, *Managing the Business Risk of Fraud: A Practical Guide (the Guide)*, the governing board should, among other things:

- Understand fraud risks for their organization and how to evaluate them.
- Maintain oversight of the fraud risk assessment process by making it a periodic agenda item when general risks to the organization are considered.
- Monitor management's reports on fraud risks, policies and control activities including obtaining assurance that the controls are effective.
- Oversee the internal controls established by management.

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. According to the *Guide*, management must -

- Set the tone at the top for the rest of the organization.
- Implement adequate internal controls, including documenting fraud risk management policies and procedures and evaluating their effectiveness.
- Report to the governing body on what actions have been taken to manage fraud risks and regularly report to the board on the effectiveness of the fraud risk management program.

All employees, regardless of their position, have a responsibility to protect against fraud. The *Guide* suggests that all employees, including management, should:

- Have a basic understanding of fraud and be aware of the red flags through periodic training provided by management or outside experts.
- Understand their role within the internal control framework.
- Read and understand relevant policies and procedures such as the antifraud policy, code of conduct, conflict of interest policy and whistleblower policy.

- Participate in the process of designing and implementing antifraud controls and in monitoring activities.
- Report suspicions or incidences of fraud to the appropriate designated party.

Appendices D and E 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. The *Managing the Business Risk of Fraud: A Practical Guide (the Guide)* suggests that organizations engage in "brainstorming" to anticipate the behavior of a potential fraudster. See Appendices F and G for examples of potential fraud assessment procedures. The *Guide* suggests that a fraud risk assessment generally includes three elements:

- Identify fraud risks by considering all types of fraud schemes and scenarios inherent to the organization.
- Assess the likelihood and significance of the fraud risks identified based on history, interviews and research into possible fraud schemes.
- Respond to the inherent fraud risks that are reasonably possible and potentially significant including a cost-benefit analysis of those risks.

The following illustrates a framework adapted from the *Guide* that can be used to document the organization's fraud risk assessment.

Identified Fraud Risks & Schemes	Likelihood & Significance[1]	People &/or Department	Existing Controls Residual Assessment[2]	Anti-fraud Required Risks	Action	Status
Misappropriation:						
Unauthorized credit card use	RP/C	Facilities	Tested and assessed as D	Action needed	Increased oversight	Dept head to implement
Reporting:						
Fraudulent journal entries	RP/M	Accounting	Tested and assessed as SD	Action required	Mgmt review & approve all	Audit committee follow-up
Corruption:						
Conflict of Interest	R/C	Management	Tested by Audit Committee - deemed adequate	Risk of override	Retest annually	No change
Other risks:						

[1]-Assessing the likelihood and significance of a potential fraud risk is subjective and varies by organization. The likelihood assessment may be based on previous occurrences, industry experience, strength of internal controls, etc. Organizations often use these categories: R – remote, RP – reasonably possible and P – probable.

The significance assessment is based on management's estimate of the financial, reputational and legal impact as designated as I – immaterial, C – consequential and M – material.

[2]-Professional standards generally categorize identified internal control weaknesses as D – a control deficiency, SD – a significant deficiency or MW – a material weakness. A control deficiency is a deficiency in the design or operation that does not allow management, employees or volunteers, in the normal course of performing their functions, to prevent, or detect and correct financial errors or omissions on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness yet important enough to merit attention by those charged with governance. A material weakness is a deficiency, or combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement in the entity's financial statements, reports or records will not be prevented, or detected and corrected on a timely basis.

Appendices F and G are a fraud risk checklists for use by the board/audit committee and management in identifying and measuring risks. Appendix J provides the organization with steps to take to audit areas of risk.

Financial and Non-Financial Systems and Controls

As noted earlier, the 2024 ACFE study found that the lack of adequate internal controls was most commonly cited as the factor that allowed the fraud to occur. The study found the lack of adequate internal controls resulted in 32% of the losses, followed by override of existing controls at 19% of losses.

Internal control is a process, effected by an entity's board of directors, management and other personnel designed to provide reasonable assurance regarding the achievement of objectives relating to 1) operations, 2) reporting and 3) compliance. An internal control process or system includes certain key controls that are the most important in achieving particular control objectives and principles and whose failure might not prevent, or detect on a timely basis, other control failures that would be material to the entity's objectives.

One of the basic key control concepts of sound internal financial controls is segregation of duties. This is the policy and practice of dividing incompatible duties among different people and systems so that no one person can authorize transactions, record those transactions in the financial records and exercise custody of the related assets. Coverage of the basics of this and other key controls can be found in Appendix H. This appendix is a tool that an organization may use to identify the existence of typical key controls and to assess the strength of its financial internal process.

An organization should periodically assess barriers to internal controls that might exist. For example, unwarranted trust may be exhibited in the hiring and monitoring of accounting personnel. Also management sometimes allocates insufficient resources to personnel and systems for the accounting function in favor of program activities.

Management should implement both financial and non-financial systems and controls to detect and prevent fraud.
Among the general financial control concepts 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 and trend analyses – compare number of donors with contributions, compare number of employees with payroll expense, explain significant variances in trends and budget to actual differences.

- Review all general ledger adjustments, the related support and the accuracy of the postings.

- Institute job rotation and mandatory vacations.

- Conduct surprise audits.

Cybersecurity is an area of special concern in today's high-tech environment. Nonprofits have both a financial risk and reputational risk. Nonprofits handle reams of valuable information on a regular basis, from donor social security numbers, donor contact information, banking information, payroll data, and much more. According to some cybersecurity experts, what are some of the top cybersecurity threats to nonprofits?

- Unsecured software – out-of-date software. Optimal Networks, an IT consultant, says that "the older the operating system, computers and network, the more susceptible an organization is to data breaches. Open-source software, though less expensive, is often extremely vulnerable to attacks." To prevent phishing (described below), computers and mobile devices should be armed with up-to-date spam filters, antivirus and anti-spyware software and a firewall.

- Weak or unenforced password policy – allowing members, vendors and others access to private information requires a comprehensive password policy. Passwords should be shared on a "need-to-know" basis, complex (at least 12 characters – numbers, letters and symbols) and changed regularly (at least quarterly).

- Employees – without regular and comprehensive training, employees are susceptible to some sort of social engineering technique such as phishing or scanning social media that contains sensitive information. Phishing has various forms but in general occurs when the sender dupes an individual or organization into providing sensitive information by falsely claiming to be from an actual business, bank, ISP or other entity or plants crime ware onto PCs to steal information directly. Employees must be instructed to never open an e-mail and to completely delete unsolicited e-mails from financial institutions, investment firms, government agencies and others with which they do not have an established relationship. They should also be advised to review their personal social media such a Facebook to ensure that it doesn't contain data that can be used to track back to the entity's computer network and to "think twice" before posting anything onto a web-based portal of any kind.

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

- Pre-screen potential employees, including criminal and financial background checks. Consider periodic post-employment checks for employees who handle significant assets.
- Communicate often with current employees so you will know when they are feeling operational or personal pressures that could impact their work and integrity.
- Communicate the consequences of committing fraud.
- Set a good example by following the rules.
- Provide and monitor a confidential hotline.
- Conduct anti-fraud training for managers and employees.
- Implement an anti-fraud policy.

Appendix L provides an outline for basic anti-fraud training. Appendices A and C are examples of anti-fraud policies the organization might use.

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 4% 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 material weaknesses or 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 2016 ACFE Fraud Study found that nearly 17% of reported fraud was discovered by internal audit." The results of this process are secondly only to an internal or external "tip" in disclosing fraud. 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 J 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 anti-fraud 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, the BBB Giving Wise Alliance and Charity Navigator 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.
- Develop a plan to investigate the matter, engaging professional investigators if needed.
- Preserve the documents or other evidence (electronic and hardcopy) that may be needed in proving the fraud, maintaining a chain of custody in the event legal action results.
- Repair the breach in internal controls, policies and procedures that made the fraud possible.
- Determine what action is appropriate against the suspect, if the allegation proves to be true.
- In certain cases, inform law enforcement or appropriate government authorities.
- Develop and implement a plan of communication with key stakeholders to mitigate any reputational damage.

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

The 2024 ACFE Study reported the following actions taken against the perpetrators:

- The matter was referred to law enforcement 57% of the time primarily when the median loss was $250,000 or more.

- The top reasons for declining to refer the matter to law enforcement were sufficient internal discipline (49%), fear of bad publicity (34%), private settlement (24%) and too costly (21%).

- Prosecution resulted in 72% guilty pleas or convictions with 14% of the cases rejected by legal authorities.

- Only 27% of the matters resulted in a civil suit filed by the victim organization, generally when the median loss was $300,000 million or more. The victim organization received a judgment in 37% of the cases with another 37% of the cases ending in a settlement.

- Judgments were rendered in favor of the perpetrator in 20% of the civil suits reported.

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 X 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 X 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

POTENTIAL FRAUD RISK ASSESSMENT PROCEDURES FOR USE AT GOVERNING BODY LEVEL

Introduction:

While the governing board has oversight responsibilities for the whole not-for-profit organization, it may want to focus on management (includes financial staff, department heads, administrators, et al) and other employees/volunteers with significant authority and responsibility. Personnel at this level, while not perpetrating the greatest number of frauds, usually cause the greatest harm. Even in a not-for-profit organization with reasonable internal controls and common values, persons at this level have the ability and sometimes do override those controls. In a paper published by the American Institute of CPAs entitled, *Management Override of Internal Controls: The Achilles' Heel of Fraud Prevention*, the following six key actions the governing body should consider were identified:

1. Maintaining skepticism.
2. Strengthening understanding of the not-for-profit organization and its activities.
3. Brainstorming to identify fraud risks.
4. Using the code of conduct to assess the financial reporting culture.
5. Ensuring the not-for-profit organization has a vigorous whistleblower program, (the number one method for catching fraud at the management level).
6. Developing a broad information and feedback network (beyond senior management).

Even with the best procedures in place, the lack of active and purposeful oversight by the governing body is a sign of negligence and a prescription for failure.

Purpose:

To protect the not-for-profit organization's assets, personnel and reputation from fraudulent activities and the effects thereof.

General:

Ensure that at least annually the following policies are current, formalized in not-for-profit organization documents and communicated to all board members, administrators, employees and volunteers:

1. Institutional antifraud & code of conduct policies[1] [location and latest update]
2. Whistle-blower policy[1] [location and latest update]
3. Conflict of interest policy[1] [location and latest update]
4. Annual signed conflict of interest disclosure statement[1] from each board member, administrator and key volunteer (who handles not-for-profit organization resources or makes commitments on its behalf). [On file with ……] [Accounted for by a member of the governing body].

Fraud Risk Assessment Procedures[2]:

1. Obtain management's written fraud risk assessment documents for the period and review. Consider communicating with management to discuss any significant risks identified and actions taken.
2. Obtain management's written assessment of financial controls, identified control deficiencies, compensating factors, and actions taken to correct or mitigate those deficiencies. Consider communicating with management to discuss any significant matters identified and actions taken.
3. Communicate with external auditors:
    a. Prior to the annual audit to discuss fraud risks including management override of controls, request audit scope modifications, if any, and other matters of relevance to the audit;
    b. At the conclusion of the annual audit to discuss the auditors' findings re: fraud, internal controls and other matters relevant to the audit and the not-for-profit organization.
4. Obtain written response from management re: comments and recommendations from external auditors re: fraud, internal controls or related matters.
5. Communicate with management to discuss the following issues:
    a. New accounting principles or tax positions during the period;
    b. Significant changes in computer software and inherent controls, including Internet or e-commerce;
    c. Significant or complex transactions;
    d. Non-routine transactions and process for handling them;
    e. Other recent developments that could have a material impact on the entity's financial statements.
    f. The estimates used in preparing the financial statements, how they are calculated, and how accurate they were looking back to prior year(s).
    g. Any related party transactions and the substance behind them.
    h. Quality of the entity's financial and accounting personnel resources and the ongoing relevant training they are receiving.
    i. New hires in positions with access to financial resources, accounting and IT systems, or ability to commit resources and whether background checks, including criminal checks were performed.
    j. Insurance coverage re: employee/volunteer dishonesty including amount and deductible.
    k. Other matters of relevance or concern
6. Exercising a reasonable level of skepticism, brainstorm about the potential for fraudulent financial reporting with special emphasis on management and considering[3]:
    a. Information that indicates of the presence of ***incentives or pressures*** for management to intentionally misstate the financial statements, reports to regulatory agencies, reports to funders or others.

Fraud Risk Assessment Procedures[2]: (continued):

   b. Information that indicates ***opportunities*** for management to intentionally misstate the financial statements, reports to regulatory agencies, reports to funders or others.
   c. Information that indicates management ***attitudes/rationalizations*** may justify intentional misstatement of the financial statements, reports to regulatory agencies, reports to funders or others.

7. Exercising a reasonable level of skepticism, brainstorm about the potential for misappropriation of assets with special emphasis on management and considering[3]:
   a. Information that indicates of the presence of ***incentives or pressures*** for management, employees or volunteers to misappropriate assets.
   b. Information that indicates ***opportunities*** for management, employees or volunteers to misappropriate assets.
   c. Information that indicates ***attitudes/rationalizations*** on the part of management, employees or volunteers to engage in or justify misappropriation of assets.
8. Perform regular financial oversight including regular review of financial reports, budgets, variance reports, performance measures, benchmarks, etc.
9. Document the process, results and conclusions of steps 1-8 in minutes or Memoranda.

Notes:

[1] Sample policies are found elsewhere in this booklet. Additional copies of this booklet *Preventing and Detecting Fraud in Not-For-Profit Organizations*, can be obtained at www.kellerowens.com in the Not-For-Profit Industry Division section under Download KO+ Publications.

[2] The fraud risk assessments procedures should be performed at least annually but may be spread over a series of meetings during the period.

[3] Detailed considerations are found in Appendix G.

[4] The steps enumerated above or in Appendix G are not intended to be complete and should be amplified by the not-for-profit organization.

APPENDIX G

POTENTIAL FRAUD RISK ASSESSMENT FACTORS

Fraud risk factors are events or conditions that indicate the presence of:

- ***incentives or pressures*** for employee or volunteer, employees, or vendors to commit fraud,
- ***opportunities* to** commit fraud, usually combined with a belief that the fraud will go undetected, and/or
- ***attitudes/rationalizations*** on the part of employee or volunteer, employees, or vendors to justify committing fraud.

Consider whether information about the organization, its personnel, and its operations indicates the presence of one or more fraud risk factors. (Consider both the financial statements and the federal award programs, if any.)

The risk factors presented for consideration are classified into:

- factors related to ***fraudulent financial reporting***, and
- factors related to ***misappropriation of assets***.

Note that factors related to fraudulent financial reporting, such as employee or volunteer dominance without compensating controls, or ineffective oversight of financial reporting, may also be present when misappropriation occurs.

Consider each item; however, the factors listed are only examples and may spark awareness of additional relevant risk factors.

A. Fraudulent Financial Reporting

Factors which increase the risk of financial statement misstatement due to fraudulent financial reporting:

1. Incentives/Pressures

Consider whether information about the entity, its operations, and its industry indicates the presence of ***incentives or pressures*** for employee or volunteer to intentionally misstate the financial statements. Consider risk factors such as:

a. Indications that the financial stability or operating results of the organization may be threatened by economic, industry, or operating conditions, such as:

(1) The organization is experiencing a high degree of competition or market saturation and declining margins:

(a) There is intense competition for a limited pool of resources, such as contributions and grants, thereby pressuring employee or volunteer to manipulate financial reports to attract those contributions and grants.

(b) There is increasing competition from other nonprofit (or for-profit) organizations for clients, members, students, patients, or other program participants.

(2) The organization is experiencing high vulnerability to rapid changes such as changes in technology, interest rates, or demand for the organization's services.

(3) Economic or political events are causing, or may cause, significant decreases in revenue (contributions -including gifts-in-kind, grants, dues, fees, sales, investment return).

(4) Threat of a major source of funding (contributions or dues) being terminated or significantly reduced.

(5) Difficulty in generating cash flows from activities; pressure to obtain more grants or contributions for programs or to cover expenditures.

(6) Shortfalls in unrestricted revenues that may create incentives to use restricted amounts to cover.

(7) Significant revenues are based on formulas tied to the organization's budgeted or actual revenues or expenses that create incentives to alter financial reports to maximize these revenues.

(8) Claims of unusually rapid growth in contributions or service fees, especially when compared to historical trends or similar nonprofit organizations.

(9) The financial results are significantly better or worse than those of similar organizations, or compared to prior periods or to budgets, for no apparent reason.

(10) Threat of imminent bankruptcy or foreclosure.

(11) The organization is subject to new accounting, statutory or regulatory requirements that could impair the organization's operating results or financial stability.

(12) The organization has been the subject of recent significant adverse publicity.

(13) There is suspicion of asset misappropriation, and employee or volunteer may be trying to cover up the effects.

c. Indications of pressure on employee or volunteer to meet requirements or expectations of third parties, such as:

(1) Employee or volunteer has committed to significant creditors, major funders, members, or others to achieve unduly aggressive or unrealistic forecasts.

(2) Donors, grantors, other contributors, or lenders have imposed significant restrictions or conditions based on reported financial statement amounts.

(3) High dependence on debt financing, financing agreements have debt covenants that are difficult to meet, or there is a marginal ability to meet debt repayment terms.

(4) Unusual focus by external financial statement users (such as contributors, members, rating agencies, and media) on reported amounts such as revenue or the change in unrestricted net assets, or on maintaining favorable ratios between programs, employee or volunteer and general, and fund-raising expenses.

(5) Perceived or real adverse consequences on a significant pending transaction (such as a pending financing arrangement, large contribution, or grant) if poor financial results are reported.

(6) Pressure to charge unallowable or questionable costs to government or other grants.

(7) Unusual pressures to meet budgetary targets:

(a) To avoid expense budget overruns, or to offset overruns in one budget category or grant against under-expenditures in another category or grant.

(b) To appear to attain budgeted revenue amounts, especially if matching grants are involved.

(8) Pressure to avoid or minimize balances in:

(a) Unrestricted net assets, because of the potential perceived effect of such balances on fund-raising.

(b) Programs for which surpluses would have to be returned to the funding source.

(9) There is a mix of fixed price, units of service, and cost-reimbursement programs funded by third parties, which could create incentives to shift costs or manipulate accounting transactions.

(10) The organization is involved in certain activities, which if disclosed to the public or to members, may, in the opinion of employee or volunteer, adversely affect contributions or other revenue.

c. Indications that employee or volunteer's personal financial situation may be threatened by the organization's financial performance, such as:

(1) A significant portion of employee or volunteer's compensation depends on bonuses, or other incentives, which depend on the organization meeting performance goals (for example, fund-raising or membership targets, program accomplishments, budget numbers, financial position, cash flow, or other financial or operating goals).

(2) The organization is experiencing a weak or deteriorating financial condition, and board members or employee or volunteer have loaned money to, or personally guaranteed debts of, the organization.

d. Employee or volunteer over-reacts to pressure to meet or exceed financial targets, such as targets for fund-raising efforts or individual programs. This may involve practices, such as:

(1) Use of controversial or aggressive accounting policies or reporting methods.

(2) Inappropriate bookkeeping, resulting in a need for the auditors to propose large numbers of adjustments.

(3) Reluctance to record adjustments proposed by the auditors.

e. Significant interest by employee or volunteer in minimizing taxes (such as unrelated business income or foundation excise taxes) through inappropriate means (including inappropriate allocation of costs between for-profit and tax-exempt subsidiaries or aggressively interpreting the definition of the organization's exempt purpose to include taxable sales).

f. Significant interest in 'managing' reported contribution revenue or unrestricted net assets:

(1) To make the organization look more 'needy' to potential contributors (minimize), or

(2) To meet matching requirements of other contributions (maximize).

h. Other: (add as appropriate)

2. Opportunities

Consider whether information about the organization, its operations, or its industry indicates ***opportunities*** for employee or volunteer to intentionally misstate the financial statements. Consider risk factors such as:

a. The organization:

(1) Engages in significant related-party transactions not in the ordinary course of business (including transactions with related entities that are unaudited or audited by another firm, or with different fiscal years).

(2) Has financial statement data based on significant estimates involving unusually subjective judgments or uncertainties that are difficult to corroborate, or that could significantly change in the near term in a manner that may be financially disruptive to the organization.

(3) Has significant, unusual, or complex transactions (particularly close to year-end) that are difficult to assess for substance over form (such as grants or split-interest agreements with complex provisions).

(4) Has diverse programs with multiple funding sources and complex compliance requirements (such as provisions of donor restrictions, statutes, or grant, trust, or contractual agreements).

(5) *(See factor A-1. b. (9) above.)*

(6) Has operations in foreign jurisdictions with differing accounting principles, business environments, and cultures.

(7) Has bank or investment accounts, or subsidiary or branch operations, in tax-haven jurisdictions for which there does not appear to be a clear business justification.

b. There is ineffective monitoring of employees or volunteers as a result of circumstances such as:

(1) Employee or volunteer is dominated by a single individual (such as the board chair, executive director, development director, a program director, or a large funder or dues-paying member) or a small group, without compensating controls such as effective oversight by the board of directors or an audit committee.

(2) Ineffective board-level oversight over financial reporting and internal control. Financial information provided to the board is delayed, incomplete, of questionable validity, or difficult to understand.

(3) Employee or volunteer with oversight responsibilities lack appropriate background and experience in nonprofit operations and the organization's programs, or they appear to lack a commitment to diligently fulfilling their duties.

(4) Employees or volunteers, their close family members, businesses under their control, or major resource providers (donors or members) have business relationships with the organization without prior knowledge and approval by the full governing board.

c. Conditions that indicate a complex or unstable organizational structure, such as:

(1) It is difficult to determine whether the organization controls, or is controlled by, a related party.

(2) An overly complex organizational structure involving unusual legal entities, lines of managerial authority, or contractual arrangements that do not appear to have an organizational purpose.

(3) High turnover in employees or volunteers.

(4) Major subrecipient or subcontract relationships, especially without a clear program or organizational purpose.

(5) Multiple and/or distant locations with inadequate employee or volunteer oversight.

d. There are deficiencies in internal controls due to circumstances such as:

(1) Employee or volunteer fails to implement and adequately monitor internal controls over the financial reporting process.

(2) There have been high turnover rates, and the organization continues to rely on ineffective accounting or information technology (IT) personnel (employees, contractors, or volunteers).

(3) Organization continues to use ineffective or poorly documented accounting systems, especially those with significant known deficiencies in internal control.

e. Other:(add as appropriate)

3. Attitudes/Rationalizations

Consider whether information about the entity, its operations, and its industry appears to indicate employee or volunteer ***attitudes/rationalizations*** that might justify intentional financial statement misstatement. Consider risk factors such as:

a. Organization fails to effectively define, communicate, implement, support, and enforce strong positive organizational values or ethics, including strong "whistleblower' policies and procedures, or they communicate inappropriate values or ethics.

b. The organization as a whole or leadership of the organization has a poor reputation in the community.

c. A history of assertions that the organization, employee or volunteer, have committed fraud, or violations of laws and regulations or grant terms, or have engaged in inappropriate or unethical fundraising practices.

d. *Non*financial employee or volunteer excessively participate in (or demonstrate an excessive preoccupation with) the determination of significant judgments and estimates or selection of accounting principles (such as accounting for contributions and other revenue, or allocation of costs).

e. Excessive interest by employee or volunteer in manipulating the organization's trends in contribution revenue, the change in net assets, or expense allocations by using unusually aggressive accounting practices.

f. Employee or volunteer frequently attempts to justify marginal or inappropriate accounting on the basis of materiality.

g. An attitude that it is acceptable to overcharge grants, since “funders have lots of money anyway.”

h. *(See factor A-1. f above.)*

i. Employee or volunteer fails to promptly correct known reportable conditions in internal control.

j. Employee or volunteer frequently and inappropriately overrides the organization's control policies and procedures.

k. Employee or volunteer and others display significant disregard for accounting rules and regulatory requirements.

l. Other (add as appropriate).

B. Misappropriation of Assets

Factors which increase the risk of financial statement misstatements arising from asset misappropriation:

1. Incentives/Pressures

Consider whether information about the entity and its operations appears to indicate the presence of ***incentives or pressures*** for employees, or volunteers to misappropriate assets. Consider risk factors such as:

a. Personal obligations (such as arising from addictions or abuse related to gambling, alcohol, drugs, or other behavior, or from a family or medical situation) create financial pressure on employee or volunteer, employees, or volunteers.

b. Indications of adverse or strained relationships between the organization and its employees or volunteers with access to assets susceptible to misappropriation, such as: (See also Factor 3. f below)

(1) Known or anticipated future employee or volunteer layoffs.

(2) Unfavorable recent or anticipated changes in employee compensation or benefits, or volunteer rewards.

c. Other: (add as appropriate)

2. Opportunities

Consider whether information about the entity, its operations, and its industry indicates ***opportunities*** for employees, or volunteers to misappropriate assets. Consider risk factors such as:

a. Indications of higher susceptibility of assets to misappropriation (including unauthorized disbursements or unauthorized trading in securities), such as: The organization

(1) Maintains or processes large amounts of cash, or assets easily convertible to cash (e.g., bearer bonds, collectibles).

(2) Receives numerous small-dollar contributions for which donors receive no or only routine acknowledgment, and/or contributions said to be from 'anonymous' donors.

(3) Receives cash and other contributed assets in numerous departments (e.g., development, programs, accounting, administration), or in numerous locations, especially locations such as conferences not under strong controls.

2. Opportunities (continued)

(4) Uses a complex fee structure, and/or bases fees on 'ability to pay,' making it difficult for employee or volunteer to ascertain that proper charges have been made and collected for all services rendered.

(5) Has inventory and/or fixed assets easily susceptible to misappropriation (e.g., due to small size, high value, high demand, portability, marketability, lack of ownership identification).

(6) Has significant amounts of assets, such as cars, computers, etc. susceptible to personal, nonofficial use.

(7) Is susceptible to unauthorized disbursements (such as vendor, payroll, or sub recipient disbursements) being made in material amounts, especially in cash.

(8) Engages in an activity, such as unsupervised securities trading, that could cause assets held by custodians to be susceptible to misappropriation through engaging in unauthorized transactions.

b. Indications of possible deficiencies in internal controls over assets susceptible to misappropriation, such as:

(1) Weak segregation of duties, not mitigated by factors such as effective employee or volunteer or other oversight.

(2) Inadequate screening procedures when hiring employees, or recruiting volunteers.

(3) Lack of timely and adequate documentation, recordkeeping, and/or reconciliation procedures over assets susceptible to misappropriation (e.g., cash and noncash contributions, cash collections from pledges).

(4) Ineffective physical safeguards over assets susceptible to misappropriation (e.g., cash donations not secured, inventory or collection items not stored in a secured area, computers not secured, cash or investments kept in unlocked drawers, pre-signed checks available, or unprotected passwords).

(5) Lack of employee or volunteer oversight of assets susceptible to misappropriation (e.g., inadequate supervision of remote locations or failure to develop adequate controls over contributions and grants because scarce resources are assigned to program activities rather than internal control).

(6) Lack of appropriate systems for authorizing and approving transactions (e.g., in purchasing, travel and entertainment, or payroll disbursements), especially involving charges to restricted funds.

2. Opportunities (continued)

(7) Regular budget variance analysis not performed mad reviewed on a timely basis.

(8) Employees or volunteers with oversight responsibilities lack necessary background and experience in nonprofit operations and program activities, or lack commitment to fulfilling their duties.

(9) Significant financial functions performed by volunteers not under strong employee or volunteer oversight and review.

(10) Vacations for personnel in key control functions not mandatory, or those persons' duties not performed by others while they are absent.

(11) Employee or volunteer has a weak understanding of IT that could enable IT personnel to perpetrate fraud.

(12) Computer security not regularly assessed by a qualified professional.

(13) Inadequate controls over access to electronic records, including controls over mad review of computer event logs (e.g., audit trail functionality of accounting software not used or can be bypassed by users).

c. Other: (add as appropriate)

3. Attitudes/Rationalizations

Consider whether information about the entity, its operations, and its industry indicates ***attitudes/rationalizations*** on the part of employees, or volunteers to engage in or justify misappropriation of assets. Consider risk factors such as:

a. Inadequate acceptance of the importance of adequately monitoring and safeguarding assets; attitude that the organization has plenty of money' and 'this little bit won't be missed.'

b. Belief that a 'temporary loan' which will be repaid 'soon' does not constitute misappropriation of assets.

c. Attitude that internal controls are more of a 'nuisance' than a benefit; every dollar spent on 'overhead' is a dollar that did not go to help achieve the organization's goals.

d. Attitude that any action which appears to 'further the cause' is acceptable, even when laws, regulations, controls, or organizational policies are thereby violated (e.g., providing benefits to ineligible recipients or for less than standard rates, excess lobbying or political activity, not 'wasting time' by keeping required records, etc.).

3. Attitudes/Rationalizations (continued)

e. Disregard for internal controls designed to prevent or detect misappropriation, for example, by ignoring or overriding controls or failing to correct known deficiencies in controls.

f. Dissatisfaction with the organization or with other personnel.

g. Indications of strained relationships between the organization and other employees or volunteers, such as:

(1) Failure to receive promotions or other expected rewards, or proper recognition for volunteer efforts.

(2) A perception that 'insiders' are being unjustly rewarded.

h. Other employees or volunteers, have observed unusual changes in behavior or lifestyle that may indicate assets have been misappropriated to support this behavior or lifestyle.

i. Other: (add as appropriate)

APPENDIX H

ASSESSING YOUR ORGANIZATION'S FINANCIAL INTERNAL CONTROLS

Please check the box (es) below that you would consider to be key controls. There could be multiple key controls in each section. Use as your definition of a key control the following:

KEY CONTROLS – These are controls that are some of the most important in achieving particular control objectives and principles and whose failure might prevent, or detect on a timely basis, other control failures that would be material to the entity's objectives.

1. Indicate each of the following factors that describe the overall control environment or "tone at the top" in your organization.

a) The governing board sets a clear tone of financial integrity and accountability for the organization. ☐
b) The governing board (or a finance or audit committee appointed by the board) play an active role monitoring the financial activities of the organization. ☐
c) Majority of the governing board are elected by members. ☐
d) The elected board members have limited terms on the board as specified by organization by-laws or other official documents. ☐
e) The governing board (or a finance/audit committee appointed by the board) includes at least one person who's knowledgeable in the accounting and tax requirements of non-profits. ☐
f) All board members are required to complete a conflict-of-interest statement before joining the board and annually thereafter. ☐
g) The board has adopted a written formal code of conduct and communicates that code to all employees and volunteers. ☐
h) The board has adopted and communicated a whistle-blower policy to all employees and volunteers. ☐
i) Nepotism on the board is not permitted. ☐

2. Indicate each of the skills that represent finance & accounting personnel resources (through board members, finance committee members, staff members, volunteers, consultants, et al) in your organization.

a) Ability to prepare formal financial statements with required footnotes for internal and 3rd party users. ☐
b) Adequate knowledge of accounting principles currently or potentially applicable to the organization. ☐
c) Ability to recognize and accurately correct current or potential weaknesses in the design and/or operation of internal controls. ☐

d) Ability to prepare accurate and timely internal financial data to operate the organization. ☐
e) Adequate knowledge of federal, state and local tax rules and regulations the absence of which could negatively impact the organization's tax status or its tax liability. ☐
f) Receives regular training on accounting, tax and compliance matters significant to the organization. ☐

3. Indicate <u>each</u> of the general internal control procedures for cash in use at your organization.

a) Written procedures for handling cash contributions (checks and currency) and other cash are in use. ☐
b) Employees and volunteers handling cash are covered by dishonesty insurance or bond. ☐
c) The same person who receives cash or disburses cash is prohibited from posting to the books and records of the organization. ☐
d) Bank statements are originally received and opened for review by someone other than the person who reconciles that bank statement. ☐
Bank accounts are reconciled on a timely basis. ☐
e) Bank reconciliations are reviewed and approved by someone other than the person who prepares the reconciliation. ☐
f) Organization debit and credit card statements and supporting documents are reviewed on a timely basis and approved by an authorized member of management, finance committee, officer or the governing board. ☐
g) Persons with cash handling and recording duties are required to take time off (vacations, etc.) during which time someone else performs their duties. ☐
h) Cash revenues and non-payroll expenses are regularly compared to budget and variances investigated and documented. ☐

4. Indicate <u>each</u> of the internal control procedures for cash receipts in use at your organization.

a) Persons receiving cash are encouraged to use pre-numbered receipt books. ☐
b) Handling of cash receipts is always controlled by at least two unrelated people. ☐
c) All checks received are restrictively endorsed as soon as possible. ☐
d) All funds are safeguarded in the organization and quickly bank deposited after receipt. ☐
e) Someone other than a money counter or the general ledger bookkeeper records the contributions in individual donor records and reconciles donor records to the general ledger revenue accounts at least monthly. ☐
f) Contribution statements are sent to donors one or more times per year with instructions to initially report errors or irregularities to someone other than the person who records donations in the records. ☐

5. Indicate <u>each</u> of the internal control procedures for cash disbursements in use at your organization.

a) All cash disbursements, except petty cash, are made by serially pre-numbered check or approved bank transfers (such as direct deposit payroll). ☐
b) All check are pre-numbered, used in sequence and accounted for (including voids). ☐
c) All voided checks are properly mutilated (such as signature option removed) and retained. ☐
d) Bank check stock is only available to the person responsible for preparing the check. ☐
e) Check or electronic funds transfers are supported by vendor invoices or check requests approved by someone other than the person preparing the check or performing the transfer. ☐
f) All supporting documentation accompanying checks or wire transfers are properly canceled at the time of signature or transfer to prevent duplicate payment. ☐
g) Persons authorized to sign checks or approve electronic funds transfers are prohibited from recording the transactions in the books and records of the organization. ☐
h) Checks are not pre-signed or made out to cash bearer. ☐
i) Dollar limits are used for one-signature checks. ☐
j) Custody of the checks after signature and before mailing is handled by an employee independent of recording the checks in the books and records of the organization. ☐

6. Indicate <u>each</u> of the internal control procedures for cash disbursements in use at your organization.

a) Appropriate checks, including reference, criminal and credit checks, are required for all employees and volunteers who handle the organization's financial resources, records and reports. ☐
b) All employees and volunteers who handle organization financial resources, records and reports are required to complete a conflict of interest statement initially and annually thereafter. ☐
c) All employees and volunteers who handle organization financial resources, records and reports are provided with a board approved code of conduct and required to read and sign it. ☐
d) Personnel files are restricted and maintained for all employees (pastoral and non-pastoral, if a church) and, where applicable, include such documents as employment application and investigations, (pastoral licenses or ordination certificates, if a church), approval for deductions and changed in pay, benefits and position, W-4 form, immigration documentation, specimen signatures, performance reviews and termination data. ☐
e) Time cards or other records are kept, signed by the employee and reviewed and approved by their supervisor. ☐
f) Persons preparing the payroll are independent of other payroll duties (such as timekeeping, distribution of checks, etc.) and do not have access to other payroll data or cash. ☐

g) Payroll is subject to review and approval before payment by a responsible official or another person who is independent of payroll preparation and timekeeping. ☐
h) Unclaimed checks and unclaimed W-2 forms are returned and held by an employee
i) who is not part of the payroll function. ☐
j) The total wages on W-2 forms are returned and held by an employee who is not part of the payroll function. ☐
k) Payroll, other compensation, benefits and taxes are compared to budgeted amounts and significant variances are investigated and documented. ☐

7. Indicate <u>each</u> of the internal control procedures for <u>payroll</u> processed <u>by an outside service organization.</u>

a) Time records submitted for processing are complete and accurate and appropriate control totals are maintained for subsequent reconciliation to payroll registers. ☐
b) All other payroll information provided to the service organization (pay rates, withholdings, etc.) is authorized and all authorized information is communicated. ☐
c) Paychecks and payroll registers produced by the service organization are reviewed, reconciled to control totals and approved prior to distribution of the checks. ☐
d) A current copy of the auditor's report on the controls utilized by the outside service organization to process the payroll and related reports and returns has been obtained and reviewed by the organization's management. ☐

8. Indicate <u>each</u> of the internal control procedures for purchasing in use at your organization.

a) Written purchasing procedures provide clear, approved guidelines for requesting purchasing authority, making purchases and recording purchases. ☐
b) Purchase orders approved by authorized persons are used for purchases that exceed established limits. ☐
c) Purchases are compared to approved budget limits before the purchases are made. ☐
d) Open accounts established with vendors can only be used by authorized persons, for specified types of items and up to established limits. ☐
e) Written procedures provide clear, approved guidelines for the use of the organization's credit and debit cards. ☐
f) Vendors statements and invoices as well as credit card statements are carefully and promptly reviewed by appropriate authorized persons for improper or personal expenses. ☐
g) Employee business expenses are reported and documented in accordance with IRS guidelines. ☐

9. Indicate <u>each</u> of the internal control procedures for IT (information technology) in use in your organization.

a) The organization has an IT planning and risk management process in place to support its financial reporting process. ☐
b) Regular data backup and off-site storage are practices of the organization. ☐
c) The organization has written and tested disaster recovery plans. ☐

d) Physical security and access to program and data are appropriately controlled to prevent unauthorized use, disclosure, modification, damage or loss of data. ☐
e) User access rights through passwords are granted on a need-to-know, need-to-do basis. ☐
f) Passwords are controlled and changed on a regular basis. ☐
g) Access to software programs and data bases and financial records by the same person is prohibited. ☐
h) Appropriate controls and safeguards are present if remote access and processing of financial records occurs. ☐

GRADING INTERNAL CONTROLS – Each box checked has a value. Using the table below determine the value of each checked box.

3 – Overarching key control	1a, 1b, 1e
2 – Key control	1h, 2b, 2c, 2e, 3c, 3d, 3f, 4b, 4e, 5b, 5d, 5e, 5g, 5j, 6a, 6f, 6g, 6j, 7a, 7b, 7c, 8f, 9b, 9f
1 – Standard control	All others

SCORING GUIDE – Aggregate the values determined from the previous section and score your organization's financial internal controls.

96-100	Superior
81-95	Above average
66-80	Average
50-65	Below average
49 and below	Represents significant risk

NOTE – The financial internal controls listed above are based on general practice and may not represent controls for every not-for-profit organization. The grading guide used is based upon the judgment of professionals with decades of experience servicing the not-for-profit industry. The scoring guide may not represent every organization's circumstances or risk tolerance.

APPENDIX I

THE ASSOCIATION OF CERTIFIED FRAUD EXAMINERS' FRAUD PREVENTION CHECKUP

(Reprinted with permission)

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 5% 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 damage 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	
For example, some 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 "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.	**RESULTS**

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. 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	**RESULTS**

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., 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.	**RESULTS**

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*** • 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.	**RESULTS**

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 J

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 K

SAMPLE STEPS TO ROOT OUT CORRUPTION

Identifying and combatting corruption in non-profit organizations requires constant attention and aggressive action. Listed below are some of the areas contributing to the risk of corruption and actions to take to minimize that risk:

1. Inadequate governing board composition and oversight; poor "tone at the top".

    a. The majority of the board should consist of independent members with varied skills and backgrounds. At least one member should have an accounting or finance background with a solid knowledge of non-profit accounting, reporting and tax rules and regulations.
    b. Before joining the board and annually thereafter all board members should complete a comprehensive conflict of interest statement (see Appendix E for a sample conflict of interest policy).
    c. The board should have term limits and staggered terms and a clear and detailed job description describing the role and responsibilities of a board member.
    d. There should be annual performance evaluations of members and committees with emphasis on areas of special interest such as finance, fundraising, human resources and purchasing.

    Leadership must show through its words and actions that dishonest or unethical behavior will not be tolerated by anyone, even if it benefits the organization. (See Appendix D for a sample code of conduct).

2. Weak, ignored or overridden financial controls.
    a. Internal accounting controls should split approval, custody, recording, reconciliation and reporting responsibilities; no one person should control a transaction from inception to end. (See Appendix H to assess the organization's financial controls).
    b. Multi-signatures should be required for payments over a specified amount; payment or EFTs approvals should always be accompanied with supporting documents such as approved requisitions, purchase orders, invoices and other appropriate support and follow budget limits. Credit cards should have strict limits and all purchases should be supported by receipts and reconciled monthly.
    c. Board or finance committee should approve all major contracts or related party transactions.
    d. Particular attention should be given to handling cash including collection or payments in cash at events, programs or services. (See Appendix J for an internal audit checklist re: cash).
    e. There should be an approved budget and variance reporting. Major changes to the budget (including reallocations) should be approved by the governing body. The organization should regularly publish and the board and/or finance committee review budget vs actual results with a clear explanation of variances.

f. The organization should consider a periodic internal audit by qualified members of the finance committee or an annual external audit by a CPA firm with significant experience serving nonprofits. Publish audited financial statements and management letter responses.
g. The organization should have sufficient IT resources, including qualified personnel, up-to-date software, and policies and procedures to protect information assets, including access controls (passwords, biometrics, MFA), security measures (firewalls, antivirus, encryption, patching), operational controls (backups, monitoring, incident response) and application-specific checks (data validations, input authorization).
h. The organization should theft, embezzlement and cyber security insurance.

3. Lack of clear funding raising policies and practices.

    a. The organization should have written and monitored fundraising practices that include planning, ethical practices and strong donor engagement.
    b. The policies should prohibit deceptive campaigns, high-pressure emotional manipulation, failing to personalize asks, ignoring data, failing to thank donors, relying on a single method or misleading donors with inaccurate claims.
    c. Prohibit board members, management, employees or volunteers from personally collecting cash donations.
    d. The organization must provide the donor with documentation of the donation as required by the IRS.
    e. If the donor specifying the use of the donation, the organization must honor the donor's restriction.
    f. The organization should not use donations for political influence to sway lawmakers.

4. Lack of or weak procurement and contracting policies and procedures.

    a. The organization should require written solicitations (RFPs/RFQs) for goods and services above established thresholds, with at least three bids, where practical.
    b. Objective evaluation matrices should be used and records kept of decision rational and bidder selection.
    c. There should be mandatory disclosure and independent review of contracts involving board members, staff or close associates, including family.
    d. Invoice kickbacks, bid rigging, and similar practices must be forbidden resulting in severe consequences if found. Investigate unexplained vendor concentration and frequent sole-source awards.

5. Lack or weak human resource practices and volunteer management.

    a. There should be an anti-nepotism policy that defines limits on hiring or supervising relatives and requiring disclosure and alternative supervision arrangements if exceptions apply.

    b. The organization should publicly post openings, conduct formal interviews, often involving at least one independent interviewer, two if possible, for both employees and volunteers.
    c. Periodic documented performance appraisals, remediated training when appropriate, a publicized grievance policy and communication of whistleblower protections.
    d. Both employees and volunteers should read and sign the Code of Conduct (See Appendix D) and the Conflict of Interest Policy (See Appendix E).
    e. Volunteers should have written description of role and responsibilities and properly trained, supervised and evaluated.
    f. Both employees and volunteers should receive periodic antifraud training (See Appendix L).
    g. Investigate unusual staff turnover and sudden resignations of key personnel; conduct exit interviews.
    h. Enforce sanctions consistently (dismissal, contact termination, legal action) and publish summary outcomes to reinforce deterrence.

APPENDIX L

OUTLINE FOR ANTI-FRAUD STAFF TRAINING

The following outline is intended for use in providing basic anti-fraud training to management, staff and volunteers who have direct or indirect access to the organization's assets. Training should occur at least annually. The outline should be modified based on conditions and risks of the specific organization. Accordingly, the outline primarily refers to sections of this booklet from which basic material can be drawn.

- Review and discuss the following:
  - What is occupational fraud? Page 1
  - What types of fraud are committed against not-for-profit organizations? Pages 7 – 10
  - What types of fraud are committed by not-for-profit organizations that we must avoid? Pages 10 – 11

- Review and discuss who perpetrates fraud and three elements present in every fraud Page 11

- Discuss some of the common red flags to watch for:
  - Living beyond ones means
  - Excess pressure for success
  - Addiction problems, including gambling
  - Divorce or family problems such as sickness of spouse or child
  - Other financial difficulties
  - Complaints of inadequate compensation or recognition
  - Control issues, unwilling to share duties
  - Unwilling to take vacation
  - Irritability, defensiveness
  - Unusually close relationship with vendor
  - Wheeler-dealer attitude
  - Past employment or legal problems

- Discuss cybercrime risks Page 17

- Discuss corruption Page 10 & 69 – 71

- Discuss what to do if fraud is discovered or suspected Page 17 – 21

- Review and discuss the following policies, obtaining sign-offs where required:
  - Organization anti-fraud policy Page 30 – 31
  - Code of conduct statement Page 32 – 34
  - Conflict of interest policy Page 35 – 36
  - Whistle-blower guidelines (in antifraud policy) Page 37 – 38, 65 – 71

APPENDIX M

OTHER USEFUL RESOURCES

Websites 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/antifraud/
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
Committee of Sponsoring Organizations – www.coso.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
Wiley Online Library – www.onlinelibrary.wiley.com

Printed resources

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. *2024 Report to the Nation, Occupational Fraud and Abuse*. Austin, TX: ACFE, 2016.

Association of Certified Fraud Examiners & Grant Thornton. *Anti-fraud Playbook*. Austin, TX

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.

Committee on Sponsoring Organizations. *COSO-Fraud-Risk-Management-Guide-Executive-Summary.pdf*

Dawson, Steve. *Internal Control/Antifraud Program Design for Small Business*. John Wiley & Sons.

Frederick & Lipman. *Whistleblowers: Incentives, Disincentives and Protection Strategies*. John Wiley & Sons. 2012

ISACA. *State of Cybersecurity Implications for 2016*. An ISACA and RSA Conference Survey.

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

Lang, Andrew & Cicciardella, Tammy. *Preventing Fraud: How to Safeguard your Organization*: Board Source.

Nonprofit Risk Management Center. *A Violation of Trust: Fraud Risk in Nonprofit Organizations.* Nonprofitrisk.org.

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.

US cybersecurity: Progress stalled. Key findings from the 2015 US State of Cybercrime Survey. PwC.

Vona, Leonard W. *Fraud Risk Assessment: Building a Fraud Audit Program*. John Wiley & Sons. 2008

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

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

KELLER & OWENS, LLC

Who We Are

Keller & Owens, LLC was founded in 1980 with the needs of clients in mind. The founders believed individuals, commercial and not-for-profit organizations wanted and deserved the opportunity to obtain high quality, timely, broadly-based services from trained and experienced professionals at a reasonable cost. They were convinced that these attributes combined with close, personal services of management level personnel would mean success for clients and the firm. As a result, Keller & Owens, LLC has become one of the larger independent local firms in the greater Kansas City metro area specializing in serving churches.

Keller & Owens, LLC is a full service public accounting firm providing accounting, auditing, consulting and tax services to our clients. The firm specializes in services to not-for-profit organizations and has one of the largest not-for-profit client bases in the city. The firm consists of eight management level personnel, including two owners, and twenty-eight full and part-time professional and clerical personnel. Most of our professionals are CPAs and average about 10 years of experience in public accounting and business.

For more information about Keller & Owens, LLC visit our website at www.kellerowens.com.

Financial Fraud Deterrence Services

Our team of professionals, led by Certified Fraud Examiners, is available to provide the following services:

- Train your governing body on the risks of financial fraud in nonprofits and how to combat it.
- Train your employees on how to identify financial fraud and steps to take if it's detected.
- Review your internal policies covering such areas as conflict of interest, code of conduct, whistleblower and others with recommendations for improvements.
- Work with you to document your anti-fraud internal accounting controls and make recommendations for improvements.
- Work with you to develop tailored fraud risk assessment tools for use by the governing body and by management.
- Assist you in developing an internal audit program to help detect fraud and provide other important financial oversight for the nonprofit organization.