Fraud: A Growing Crisis PART 1

This article is the first in a series of articles about fraud in the church. Statistics cited in this article are derived from the 2018 Global Study on Occupational Fraud and Abuse *published by the Association of Certified Fraud Examiners.*

by Rodney Smith, CPA, CFE

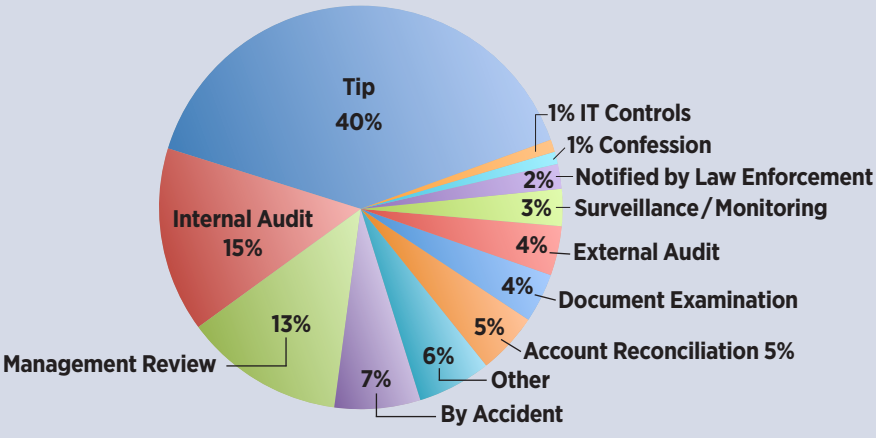
WHEN I INTERVIEW CHURCH ADMINISTRATORS AND ASK THEM ABOUT THEIR FRAUD PREVENTION MEASURES, THE ANSWER I MOST OFTEN GET GOES SOMETHING LIKE THIS:

"Well, we have our financial statements audited every year, and we feel like we have all the necessary checks and balances in place. We try to hire trustworthy people."

By far, the majority of church embezzlement cases, with which I am personally familiar, are perpetrated by staff who are also members of the victimized church – they profess to be followers of Christ. More specifically, it is usually someone directly involved with core accounting functions of the church or one of its auxiliary ministries. Oftentimes, a respected and trusted individual with a long tenure of service to the church is the perpetrator.

This is difficult to imagine by those that have not been victimized, but it is important to understand that efforts to prevent financial shenanigans in the church are tantamount to protecting church staff from unwarranted accusations of impropriety. With this perspective in mind, let us examine the anatomy of a fraud case.

METHOD OF INITIAL DETECTION OF FRAUD



HOW IS FRAUD DETECTED?

The most common way frauds are discovered is by a tip – 40% of them. Internal audit efforts and management review (oversight functions) run a distance second and third place. Many people are surprised to learn that external audits only account for detecting 4% of fraud cases.

CPAs are required to plan financial statement audit procedures based upon assessed risk that the financial statements could be materially misstated due to fraud or error. Remember, the primary purpose of a financial statement audit is not to search for fraud, but instead, to determine whether the financial statements are prepared according to the customary accounting rules dictated by the accounting standards setters. This is not to say that external audits are ineffective in deterring fraud, but only that they cannot be very well relied upon to detect fraud.

When I ask church leaders why they have a financial statement audit, the three most common answers are

1. our lender requires it,
2. accountability, and
3. "we want to make sure we are doing everything right."

I am ready to help with the first two requirements, but no CPA firm can promise to satisfy the everything right standard. If they could, the church would not want to pay that rather large fee! In summary, church leaders should be realistic about the benefits of a financial statement audit, instead of expecting miracles from the auditors.

HOW DOES FRAUD HAPPEN IN THE CHURCH?

A partial list of explanations for church fraud is listed below:

- Internal controls are not designed with proper segregation of duties, or they are not functioning as designed.
- There is complacency among senior church leadership with respect to enforcement of policies (of any kind, not just financial and accounting).
- Trust is the primary "internal control."
- Certain unique fraud risks present in churches are not recognized and properly mitigated.
- The perception that an annual external financial statement audit is a major fraud deterrent can lead to a false sense of security.
- Automation has evolved and continues to evolve rapidly, which renders some internal controls ineffective, while at the same time presenting new risks that go unrecognized.
- The church's accounting and financial reporting system is unnecessarily complex, convoluted, inaccurate and / or incomplete – often held together with duct tape and bailing wire.

There are generally three elements that exist in an organization's office environment that affect the risk of fraud. These elements form the three sides of what is known as the Fraud Triangle and are fundamental considerations for anyone that is interested in mitigating the risks of fraud or cleaning up the mess afterward:

THE FRAUD TRIANGLE

For example, when people are under financial pressure, or just acting evil (under devil pressure), they will rationalize their way into exploiting a vulnerability – an opportunity to steal from their employer. However, they normally do not see it as stealing due to rationalizing their behavior. What we see as theft is seen by a fraudster as borrowing, taking what they truly deserve, or in the case of a church, providing themselves with some benevolence.

THE BENEVOLENCE FACTOR

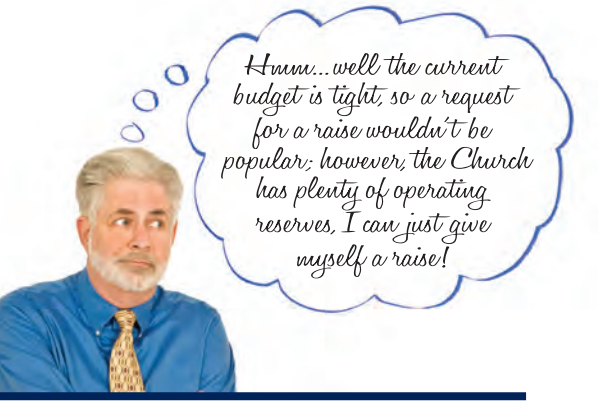
Although many secular employers have established employee assistance programs in the last few decades, the church has been aiding needy people for over two thousand years. Benevolence ministries can take on many forms in the current day local church, but even if the program is primarily outsourced to a ministry partner, it is woven into

Oftentimes, a **respected and trusted individual** with a long tenure of service to the church is the perpetrator.

the culture, so church staffs observe the benevolence process play out in their daily lives. Church embezzlers often rationalize their behavior as providing themselves with a benevolence award. They are just merely circumventing the application process for the sake of efficiency, since they would surely be approved!

THE VOLUNTEER FACTOR

Church staff often begin serving in the church as volunteers then are later hired in a part-time role and paid a fixed amount, regardless of the number of hours worked each week, while continuing to volunteer in similar or other roles. Initially, the rate of pay is not necessarily a motivating factor – possibly they are only looking to supplement their overall household income. As they demonstrate competence, along with an eagerness to serve, they tend to absorb more duties without an increase in pay. The line between employee and volunteer duties becomes blurry or maybe even disappears. (This creates another problem, for sure, but that is an employment law matter beyond the scope of this article.) As time goes on, ministry staff turns over, and possibly a few disagreements with ministry leaders occur. The person can reach a point where he feels undervalued. The remedy? An increase in pay! The rationalization:



THE BUDGET FACTOR

Did someone say budget? Churches with slow-growing, "flat," or declining revenues are often very budget-conscious; yet, it is not uncommon for them to have fairly low turnover among non-ministerial employees. These staff people are often employed by a church for more than a decade or two – receiving regular pay increases along the way – even though their job duties may not have changed much. Out of loyalty, the churches are reluctant to replace these workers for a less expensive alternative (whether via outsourcing or an equally competent person that is willing to work for less), but when one of these devoted soldiers does voluntarily leave the service of the church, their duties are commonly redistributed among the remaining employees. The collective increase in pay, however, to those absorbing those duties is much less than the overall compensation saved due to the departed employee. While the finance committee celebrates the budget victory, they may have compromised the established segregation of duties and be totally unaware they have left the fox to guard the chicken coop.

Regarding the aforementioned Fraud Triangle, my observation is that churches, as compared to the secular world, are much more overexposed to opportunity due to inadequate internal controls. Even though trust is not an internal control, church employees are generally considered more trustworthy than the general public, so church leaders themselves rationalize their reliance on trust. Churches can rock along for twenty or thirty years with major vulnerabilities without adverse consequences, but the moment the financial pressure becomes unbearable, even followers of Christ can succumb to the temptation and rationalize their own decision to raid the vault.

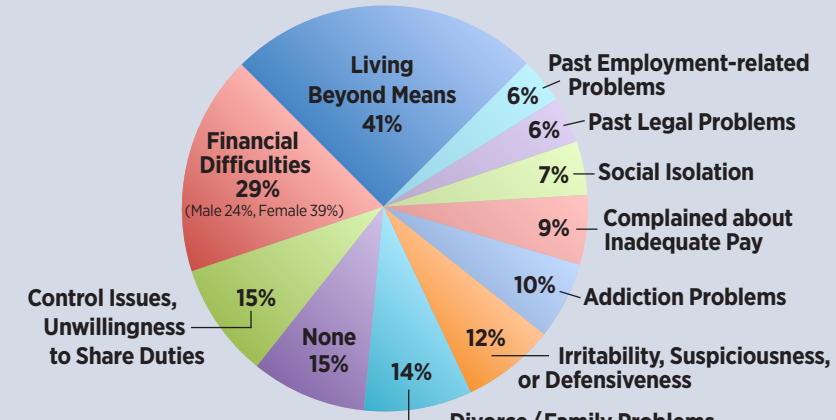
THE RED FLAGS

In the aftermath of church embezzlements, victims obviously suffer through a range of emotions, including shock, embarrassment, frustration, anger, and sadness. In the midst of all these feelings, a nagging question begs for an answer: How did we not see this coming? In other words, what were the behavioral red flags flown by the fraudster?

The chart presented on the following page is not church-specific. The red flags are all labeled as behavioral, but many seem to be more circumstantial. From my experience, a church fraudster's flagpole is most likely flying a banner of financial pressure due to a major life change – huge medical bills for a loved one, divorce or other strife in the family, spouse losing a job, poor credit rating and all that entails, etc. Although it is common for church fraudsters to live beyond their means, it may not be so obvious, because they would usually be careful to hide extravagances, or they may be a member of a relatively low-income household just trying to lead an "ordinary" middle-class life.

Behavioral red flags for a church embezzler could definitely include the unwillingness to share duties; this and the others listed in the chart are probably

HOW OFTEN FRAUDSTERS EXHIBITED BEHAVIORAL RED FLAGS



Percentages exceed 100% because an embezzler may exhibit more than one red flag.

no more or less common than all those red flags present in the full study.

I recommend that churches recognize and acknowledge those fraud risks that are unique to the church and explain to their staff that any changes in internal control are intended to protect them as well as the church.

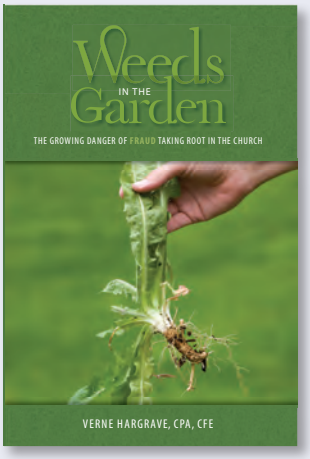
Future articles will focus on other aspects of church fraud risks and fraud prevention measures. It is best practice to develop a comprehensive anti-fraud program based upon a church's unique control environment, but some anti-fraud maneuvers would be common to most any church as seen in the chart below.

4 EASY ANTI-FRAUD MANEUVERS

1	Have bank reconciliations prepared by someone not involved in accounting and financial reporting functions, preferably someone outside the business office.
2	Church credit card activity should be reviewed by someone without a church-issued card.
3	Accounting personnel should be denied administrative login rights to accounting software, payroll software, online giving, and banking portals.
4	Utilize serially numbered tamper-evident deposit bags when offering collections are temporarily stored before preparing the bank deposit or processing the remote capture.

EDITOR'S NOTE

For additional information on fraud see *Weeds in the Garden* in the TCN Resource Center.
http://thechurchnetwork.com/resources



Author

Rodney Smith is audit partner with PSK, LLP. He can be reached at rodney.smith@pskcpa.com.

My observation is that churches are much more overexposed to opportunity due to **inadequate internal controls.**

Fraud: A Growing Crisis PART 2

This article is the second in a series of articles about fraud in the church. (The first article was published in the Fall 2018 issue of this magazine.) Statistics cited in this article are derived from the 2018 Global Study on Occupational Fraud and Abuse *published by the Association of Certified Fraud Examiners.*

by Rodney Smith, CPA, CFE

IN THE FIRST ARTICLE IN THIS SERIES, I WROTE ABOUT SOME COMMON METHODS OF FRAUD DETECTION AND FRAUD RISKS THAT ARE SOMEWHAT UNIQUE TO THE CHURCH. ADDITIONALLY, BEHAVIORAL RED FLAGS WERE IDENTIFIED ALONG WITH SOME EASY ANTI-FRAUD MANEUVERS.

In Part 2 of the series, I will revisit or expand upon some of these topics and also provide additional food for thought based upon my experience as fraud examiner and a church financial statement auditor.

When I interview church leaders and ask them about their most common (administrative) frustrations, two concerns typically appear at top of the list: monthly financial statements and credit card management. I believe it is no coincidence that these two matters are common elements contributing to fraud risk.

By far the majority of church embezzlement cases, with which I am personally familiar, are perpetrated by staff directly involved with core accounting functions of the church. These fraudsters typically had a long tenure of service to the church, but it is highly unlikely they had a prior conviction. However, it is likely that news of a church embezzlement can cause a crisis of confidence among the church members and scar the reputation of the church in its community.

If these possibilities do not provide enough motivation to implement fraud prevention measures, just know that the majority of fraud victims recover nothing from the fraudster.

I consider it important to emphasize that protecting church staff from unwarranted accusations of impropriety is just as important as protecting against misappropriation of assets. With this perspective in mind, let us once again consider the anatomy of a fraud case.

HOW DOES FRAUD HAPPEN IN THE CHURCH?

A partial list of explanations for church fraud is listed below:

- Internal controls are designed with monitoring and supervision as key aspects of fraud prevention, yet those functions are neglected by church management.

- There is complacency among senior church leadership with respect to enforcement of expense reimbursement and credit card use policies.
- Trust is relied upon as internal control.
- Certain common fraud risks present in churches are not recognized and properly mitigated.
- The church's accounting and financial reporting system is prone to error, inadequate and/or incomplete – often providing a smokescreen for the fraudster's dirty work.
- Advances in technology create new fraud risks that are surprising to church leaders.

To revisit our prelude to fraud from Part 1 of the series, remember there are generally three elements that exist in an organization's office environment that affect the risk of fraud. These elements form the three sides of what is known as the Fraud Triangle and are fundamental considerations for anyone that is interested in mitigating the risks of fraud, or preventing it from recurring:

THE FRAUD TRIANGLE

Constant financial pressure over an extended period of time can cause an individual to rationalize their way into exploiting a vulnerability – an opportunity to steal from their employer. What we see as theft is often seen by a fraudster as borrowing, taking what they truly deserve, or in the case of a church, providing themselves with a benevolence award. Rationalizing behavior is a complex matter, but in the case of church embezzlement, it is fueled by pressure and opportunity.

A CASE STUDY

The competence factor.

Although not unique to the church business office, poorly designed and inaccurate financial reporting is a common phenomenon in faith-based organizations, and churches in particular. Some churches employ accounting professionals, but more often I encounter church bookkeepers that are intelligent, conscientious, and disciplined individuals that exhibit a tremendous work ethic and servant attitude. Sadly, they know very little, if anything, about accounting. Training for these workers is generally focused on what to do, not why it is being done or how it impacts the world around them.

Bookkeepers lacking proper skills will often follow the same procedures for months and years, with very little supervision. When circumstances change, they likely fail to adapt, resulting in accounting errors – possibly intentional – that go unnoticed or are just tolerated. Then church decision-makers regularly rely on flawed information based upon outdated or invalid assumptions, until a financial statement user with respectable accounting knowledge starts to ask questions.

The neglect factor.

At the hub of any accounting and financial reporting system is the general ledger chart of accounts – a nerdy accounting term appreciated by so few, but incredibly important to so many. In other words, the chart of accounts is the order of listing balance sheet elements, such as assets and liabilities and the groupings of income and expense accounts into departments or other meaningful categories. When subject to the whims of those lacking appreciation for its design, or with changes in personnel, mismanagement of the chart of accounts can cause financial reports to deteriorate in usefulness as various cash and investment accounts, properties, loans, restricted funds and ministry activities come and go.

In summary, financial reporting that was initially useful for decision makers is increasingly met with skepticism as the information becomes more convoluted, confusing or obviously full of errors.

The alternative factor.

What do you get when a bookkeeper lacking accounting skills regularly provides financial reports to decision makers that are not useful? An alternative reporting system.

By far the **majority of chuch embezzlement cases**... are perpetuated by staff directly involved with core accounting functions of the church.

Frustrated finance committee members resort to giving the church business office what is essentially a list of demands, i.e., "We need to know cash in / cash out, bank balance, loan balance, budget vs actual, etc…"

Now, data that is partly derived from the church's accounting system can be combined with other sources of data to populate reports that are "disconnected" from the general ledger chart of accounts. The alternative soon becomes the "new normal" as the decision makers become comfortable with the reporting system they designed. Yet, it forms a smokescreen for the clever fraudster.

Regarding the aforementioned Fraud Triangle, my observation is that churches, as compared to the secular world, are much more overexposed to opportunity due to flawed internal controls. Church employees are generally considered more trustworthy than the general public, so church leaders themselves rationalize their reliance on trust. Churches can be exposed to major vulnerabilities without adverse consequences for decades, but the moment the financial pressure becomes unbearable, even the most loyal and tenured worker can succumb to the temptation and rationalize their decision to crack the safe.

The smokescreen.

The bookkeeper that lacks accounting skills, but is otherwise intelligent and resourceful, is now the beneficiary of an alternative financial reporting system that serves as a smokescreen for the newly disconnected general ledger.

What can happen behind this smokescreen? Some real-world examples for your consumption:

- Budget vs actual reports are exported from the general ledger to a spreadsheet. Amounts are edited to compensate for fraudulent transactions in the general ledger, or those fraudulent transactions are never even recorded in the general ledger.

- The Finance Committee only expresses an interest in budget vs actual activity (translated as cash in / cash out), and they are not interested in the balance sheet or statement of financial position – a snapshot in time. The bookkeeper stops sending balance sheet reports, and then begins recording fraudulent transactions in balance sheet accounts. (But…the bank reconciliations still balance….maybe…)

- Since fraudulent transactions could cause cash balances to be understated, the clever bookkeeper creates a designated fund (another balance sheet account), and records fake transfers to cash.

The sideshow.

Let us not forget about the other major frustration of church business administrators: Church-issued credit cards. (As you might imagine, an entire article could be devoted to the pitfalls and drawbacks of managing the users of church-issued credit cards.) Obtaining supporting documentation for credit card purchases is enough of a struggle.

PRO TIP

With changes in technology and banking customs, churches can suffer a false sense of security by requiring two signatures on a check. It is best to be more thorough on the expenditure approval process – no less than two approvals, so that the signature on the check is anticlimactic. There are many instances where requiring two signatures is an ineffective control because of potential circumvention:

- When one of the authorized check signers will be unavailable, they will sign several blank checks as a matter of convenience.

- Automated and electronic transactions, which require different types of approvals than manual signatures, are becoming increasingly more cost efficient, and therefore, more popular.

- Payees often use remote capture to deposit checks, so the checks clear the bank before the bank could even consider whether two signatures were present.

- Many banks will not honor the request for two signatures because monitoring the control is too cost prohibitive.

Church employees are generally considered **more trustworthy than the general public**, so church leaders themselves rationalize their reliance on trust.

Preventing credit card abuse or detecting credit card fraud can be more challenging when there is inadequate checks and balances over credit card purchases. The typical credit card sideshow develops when the sneaky bookkeeper has access to a church-issued credit card, but also has management responsibilities over the church's credit card accounts. The script for the sideshow:

- **Act 1** – Develop the alternative financial reporting system to serve as a smokescreen.
- **Act 2** – Bookkeeper obtains a church-issued credit card. (Undetected by other church staff because the bookkeeper is the only person with access to the master account statement / online portal.)
- **Act 3** – Personal credit card purchases are recorded…

  Scene 1 – To balance sheet accounts (Not detected because oversight body does not receive a balance sheet report.)

  Scene 2 – To budget accounts that would otherwise have a favorable variance or unfavorable variances that are tolerable and will not be questioned. (Over time, the oversight body might even begin budgeting for fraudulent transactions.)

  Scene 3 – Does not matter where; maybe not at all, because the reports are not connected to the general ledger and are falsified.

We do not want to automatically assume that sloppy accounting or alternative reporting systems are an indication of fraud – just an increased risk of such. Weak accounting practices are sometimes used to play a "shell game," but just as often they are just evidence of neglect or incompetence.

FRAUD PREVENTION

I recommend that churches recognize and acknowledge those fraud risks that are common in the church, and explain to their staff that any changes in internal control are intended to protect them as well as the church.

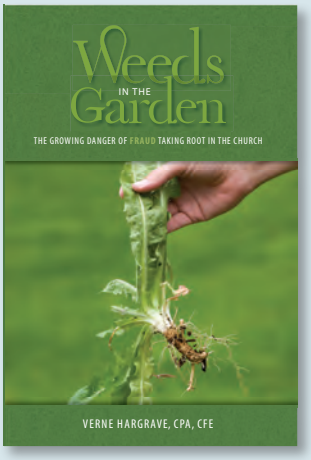
It is best practice to develop a comprehensive anti-fraud program based upon a church's unique control environment, but some anti-fraud maneuvers would be common to most any church:

4 EASY ANTI-FRAUD MANEUVERS

1	Send activity reports (budget vs actual; restricted funds) AND a balance sheet to your financial oversight body as a matter of routine.
2	Require two signatures for expenditure approval as opposed to two signatures on a check.
3	Financial reports should be generated directly from the general ledger, and/or reconciled back to the general ledger by someone other than the preparer.
4	A person other than those involved in the core accounting processes should have supervisory responsibilities for church-issued credit cards.

EDITOR'S NOTE

For additional information on fraud see *Weeds in the Garden* in the TCN Resource Center. http://thechurchnetwork.com/resources



Author

Rodney Smith is audit partner with PSK, LLP. He can be reached at rodney.smith@pskcpa.com.

Fraud: A Growing Crisis PART 3

This article is the last in a series of articles about fraud in the church. (The first article was published in the Fall 2018 issue of this magazine, and the second in the Spring 2019 issue.)

by Rodney Smith, CPA, CFE

IN PREVIOUS ARTICLES, WE OBSERVED THAT TIPS, MANAGEMENT OVERSIGHT, AND INTERNAL AUDIT EFFORTS ARE THE MOST COMMON METHODS OF FRAUD DETECTION; HOWEVER, WE ALSO OUTLINED SOME EASILY IMPLEMENTED ANTI-FRAUD MANEUVERS.

By far, sound internal controls are the best component of an anti-fraud culture. Even though there is always a chance for collusion, there is no substitute for common-sense checks and balances.

In this article, we will share a more advanced technique for fraud prevention, particularly, how to organize and execute a Fraud Risk Assessment (FRA), with The Fraud Triangle as a backdrop.

The stories of the victims are scary enough, but they only provide motivation for reducing fraud risk. The thought of instituting a comprehensive fraud risk prevention program can be overwhelming, even to the most capable church business leader.

THE FRAUD TRIANGLE

Occasionally, a church administrator will ask me if I can share a sample fraud policy, and my customary smarty-pants response is, "Yes. I'm opposed to it." If they do not hang up the phone, then I explain that fraud prevention is not a policy that is adopted and filed away. Fraud prevention is a way of life. Also, each church has its own unique culture and control environment, and as an auditor, I must remain objective and independent. I cannot be directly involved in development of my clients' internal controls.

To borrow a slogan from The Church Network, when it comes to fraud prevention, my advice to a church business administrator is Don't Go It Alone. In fact, the executive primarily responsible for a church's business affairs should NOT spearhead a fraud risk assessment, and certainly not a member of the accounting staff. Standing committees typically already have plenty to do, so if you want to perform an FRA, then utilizing a special task force is best practice.

Knowing that the word "committee" is a dirty word in many churches these days, you will need to form an ad hoc team. Call it the Fraud-buster Task Force (FTF), or something clever so people will be eager to participate.

The FTF Coordinator will play the key role, so this person must be carefully selected – one with the requisite technical and leadership skills to execute an efficient and effective initiative.

Regarding formation of the FTF, the last thing I recommend is scanning the church member roster to identify all the accounting professionals that can serve. I mean no disrespect to my CPA buddies, but the FTF should be composed of people from a range of adult age groups and varied industries or professions. Here is a partial list of workers that are generally good candidates to serve on an FTF:

Truck Driver
Banker or Mortgage Lender
Warehouse Manager
Sales Representative
Auditor (not necessarily a CPA)
Small Business Owner or Retailer
Purchasing Agent
Government Bureaucrat
Software Developer
Police Officer or Detective
Insurance Claims Adjuster
Social Worker

Ideally, there would be six, nine, or twelve people on the team, PLUS the coordinator. Depending on the complexity of the organization, the coordinator can divide the team into groups of three or four and dole out assignments, if desired or deemed necessary to balance the workload.

Choose FTF members that work in high fraud-risk industries and those that are trained to understand human behavior, must follow strict regulations or tight controls, or regularly tolerate a lot of "red tape." For example, warehouse managers are trained to prevent inventory shrinkage, but the purchasing agents they work with are tempted to accept bribes or kickbacks from suppliers. Social workers and police detectives work with folks on a regular basis that exhibit ethical standards driven more by survival instincts than societal norms. Bankers and software developers are accustomed to changes in technology and the necessary controls that accompany them. As explained later in the article, brainstorming and role-playing are methods utilized to assess fraud risks. The sales representative may be best to play the role of the pressurized, rationalized, opportunistic fraudster, because in my three-plus decades of experience as an accounting and auditing professional, I have learned that if there is a way around a system, the sales rep will find it!

There are many resources readily available to help identify the actual internal control weaknesses or other environmental factors that would be considered a fraud risk. (Even without much coaching, a properly assembled FTF will have little trouble identifying the potential leaks in the church's cash flow.)

This article is not intended to detail all of the accounting processes to evaluate for the following reasons: First, that level of detail would turn this article into an absolute snoozer. Second, administrators that intend to conduct a fraud risk assessment (but still have not) procrastinate, not because they do not know what to do. Instead, they often perceive it as a monumental task, and they just do not know how to get started.

So, here it is, step by step:

1) Pray (repeat as necessary).
2) Sell the idea to the church governing body responsible for financial oversight.
3) Identify the candidates for FTF Coordinator.
4) Explain to these candidates that the project should take no more than 20 hours of time for the Coordinator, and no more than 8 hours of time for each member of the FTF. Total timeline, start to finish, is seven weeks. (I like seven. It is a biblical number, right?)
5) If one of the candidates accepts, say a prayer of thanksgiving and proceed. If not, then pray a prayer of supplication and go back to Step 3.

> In American society, we have meeting after meeting after meeting, and then we meet to determine why we have so many meetings, with the hopes of finding a way to reduce the number of meetings and the length of said meetings. Speaking as a person that has the attention span of a gnat, meetings should last no longer than an hour, and with today's technology, there is no requirement that everyone be physically present in the same location. If meetings last more than an hour, then we are either not working enough between meetings, or we are not honoring the time limits listed for each item on the agenda (hint…hint).

6) Recruit FTF members, explaining to them that they would need to participate in three meetings that are 1 hour each, and then they would have some homework assignments with a similar time commitment in advance of each meeting.
7) Calendar three meetings with about two weeks in between.
8) Execute the Fraud Risk Assessment and report to the governing body.

The coordinator's first action related to the FRA will be to request the written accounting policies and procedures from the church business office along with the most recent financial statements. If the current procedures are incomplete or nonexistent, then the business office personnel must outline the processes they follow as an alternative. They will only have two or four weeks to produce the information, and they should not be allowed to ask for an extension of time, because that would delay the entire process. This may seem like an unreasonable position, but if this is the reality of the situation, then the church is exceptionally vulnerable, and there needs to be a "come to Jesus meeting…" with the business manager.

It is also important to note that no member of the church staff should be a

member of the FTF; however, there should be a liaison that is available to answer questions and provide clarification throughout the process. This liaison should be dismissed from any FTF meetings while any brainstorming or other discussions are conducted.

Before the initiative is launched, the coordinator and everyone else involved, must understand the objective of the FRA:

1) Identify fraud risks.
2) Determine whether or not they are adequately mitigated.
3) Report findings to the Church's financial oversight body.

There are many ways a Fraud-buster Task Force can conduct its affairs. I offer the following template:

FTF Homework Assignment 1 – *sent by coordinator via email*

- Explain objectives of the FRA.
- Remind members of the date and time of each meeting, and the commitment they have made to be prepared for each one.
- Send recent financial statements of the church, and ask the FTF to be prepared to brainstorm about areas where the church might be at risk of fraud, particularly embezzlement or misappropriation of assets.

FTF Meeting 1 – *meet via video conference, in person, or a combination of the two. Screen sharing / video projector in the meeting space is a must. Adhere to an agenda that has time limits for each matter. Exchange all documentation during the draft in a common format, so it can be easily edited. Avoid, retyping handwritten information. If everyone brings a computer to the meeting, it can save a lot of time. Copy, Cut, Paste and Edit are your friends.*

- Document the brainstorming session on possible vulnerabilities to fraud, based simply upon reading the church's financial statements.
- Divide the team into groups of three or four and assign areas to investigate further.

FTF Homework Assignment 2 – *sent via email immediately after Meeting 1*

- Current policies and procedures that were requested from staff at the beginning of the FRA should now be sent to FTF members. (Do not send before first meeting because you do not want the initial brainstorming session to be influenced by this information.)
- The FTF sub-groups should determine the current policies and procedures that would mitigate the fraud risks identified in Meeting 1, and then also determine which fraud risks do not appear to be adequately addressed.
- Phone calls with or interviews of church staff could be conducted to clarify the actual procedures performed.

FTF Meeting 2

- Discuss findings from homework assignments of each group.
- Conduct role playing or additional brainstorming exercises, as necessary.
- Outline major elements of the report.

FTF Homework Assignment 3 – *Coordinator drafts report and distributes in advance of Meeting 3*

- Read draft report and be prepared to offer and discuss edits at the final meeting.
- Remember it is NOT the role of the FTF to write (or re-write) policies and procedures. Instead, the FTF should simply report its findings to the governing body. (For example, if there is no written credit card use policy, or there is one that is not enforced, simply say so in the report.)

FTF Meeting 3

- Live edit of the report in order to produce final draft during the meeting.
- Each FTF member should have a chance to affirm content.

PRO TIP

Following the Enron scandal of the 1990's, the Sarbanes-Oxley Act mandated that all types of organizations adopt a Whistle-blower Policy. In other words, when an employee becomes aware of or suspects improper behavior, they should not suffer retribution for reporting allegations. However, if the improper activity involves a supervisor or another closely connected worker, reporting can be very awkward. For this and many other reasons, it is best for a church to appoint a Compliance Officer – typically a volunteer lay leader. Allegations can be reported to this person, even anonymously, and held in confidence, to the extent allowed by law. Whether the allegations are found to be true or false, there would be no repercussions to the person reporting them.

- If there is any disagreement over final report content, it should be documented in the report, so that the oversight body is aware.
- Findings do not have to be absolutely conclusive, or based upon unanimous consent of the FTF; the oversight body can draw its own conclusions.

Once the Fraud Risk Assessment report is sent to the oversight body, the FTF can be thanked, acknowledged for their efforts, and disbanded. It would now be up to the oversight body to coordinate changes in controls with the church staff. Forward the FRA to the church's audit firm, and then be prepared to share management's responses to that report.

Author

Rodney Smith is a CPA with PSK, LLP. He can be reached at rodney.smith@pskcpa.com.