

POTENTIAL FRAUD RISK ASSESSMENT PROCEDURES
AT THE EMPLOYEE BENEFIT PLAN SPONSOR LEVEL

INTRODUCTION:

While the governing board of a plan sponsor has oversight responsibilities for the whole organization, it may want to delegate its plan oversight responsibility to an audit committee or top managers who have no direct involvement in the plan's management. This oversight team should focus on administrators and other employees/volunteers with significant authority and responsibility in the operation of the plan as well as third party administrators, investment managers and other third party service providers. Even for a plan with reasonable internal controls and ethical 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 or surrogate should consider were identified:

1. Maintaining skepticism.
2. Strengthening understanding of the church and its activities.
3. Brainstorming to identify fraud risks.
4. Using the code of conduct to assess the financial reporting culture.
5. Ensuring an 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 or its surrogate is a sign of negligence and a prescription for failure.

PURPOSE:

To protect the plan's assets, and participants, administrative personnel and plan sponsor from fraudulent activities and the plan sponsor's reputation from the effects from fraudulent activities.

GENERAL:

Ensure that at least annually the following policies are current, formalized in plan documents and communicated to all board members, administrators, employees and volunteers:

1. Institutional antifraud & code of conduct policies¹ [location and latest update]
2. Whistle-blower policy¹ [location and latest update]
3. Conflict of interest policy¹ [location and latest update]
4. Annual signed conflict of interest disclosure statement¹ from each board member, administrator and key volunteer (who handles church resources or makes commitments on its behalf). [On file with] [Accounted for by a member of the governing body].
5. Document retention and other significant policies as determined by the governing body [location and latest update]

POTENTIAL FRAUD RISK ASSESSMENT PROCEDURES
AT THE EMPLOYEE BENEFIT PLAN SPONSOR LEVEL

FRAUD RISK ASSESSMENT PROCEDURES - GENERAL

1. Obtain and read a copy of the latest Type 2 SOC 1 service organization audit report from the third party administrator, investment manager(s) or other service provider(s). Note any internal control deficiencies that could affect your plan and determine if they have been corrected. Identify the Client Control Considerations in each report.
2. Obtain internal plan administration staff's written assessment of financial controls (including the Client Control Considerations), identified control deficiencies, compensating factors, and actions taken to correct or mitigate those deficiencies. Consider communicating with internal plan administration staff to discuss any significant matters identified and actions taken.
3. Communicate with internal plan administration staff 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 plan'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, such as policy and procedure for locating former participants.
4. Communicate with external auditors 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.
5. Communicate with external auditors 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 plan.
6. Obtain written response from management re: comments and recommendations from external auditors re: fraud, internal controls or related matters.

FRAUD RISK ASSESSMENT PROCEDURES – SPECIFIC:²

1. Obtain and review the latest list of *Department of Labor Criminal Enforcement Cases* and *AICPA Employee Benefit Plan Fraud Examples*³.

POTENTIAL FRAUD RISK ASSESSMENT PROCEDURES
AT THE EMPLOYEE BENEFIT PLAN SPONSOR LEVEL

FRAUD RISK ASSESSMENT PROCEDURES – SPECIFIC:² (Continued)

2. Exercising a reasonable level of skepticism, brainstorm about the potential for fraudulent financial reporting and misappropriation of assets using some or all of the AICPA *Fraud Risk Factors Specific to Employee Benefit Plans*,^{3,4}.
3. Document any risk factors identified that should be avoided, reduced or transferred and indicate the action taken (or to be taken, who is responsible and when it is to be completed). Communicate to the governing board as appropriate.
4. Perform regular financial oversight including regular review of financial reports, budgets, variance reports, performance measures, benchmarks, etc.
5. Document the process, results and conclusions of steps 1-4 above in minutes or a memoranda.

Notes:

¹Sample policies are found in the booklet, *Preventing and Detecting Fraud in Not-For-Profit Organizations*, at www.kellerowens.com. The document is in the Not-For-Profit Industry Division section under Download KO+ Publications.

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

³These documents and other relevant documents from the AICPA *Effective Monitoring of Outsourced Plan Recordkeeping and Reporting* and *The Importance of Internal Control in Financial Reporting and Safeguarding Plan Assets* can be found at www.kellerowens.com in the Employee Benefit Plan Services under Employee Benefit Plan Downloadable Publications.

⁴The steps enumerated above or in of the AICPA *Fraud Risk Factors Specific to Employee Benefit Plans* are not intended to be complete and should be modified by as appropriate.