

Fraud Safeguards Only as Effective as Employee Follow-Through

By Diane C.O. Gilson, CPA, CIA, President, Info Plus⁽⁺⁾ AccountingSM PC

Re-printed from Nation's Building News, December 20, 2004

This is the eleventh in a series of articles on preventing fraud from affecting your business.

A system of controls designed to safeguard your company's financial assets is only as effective as the people who use it. It's important to set aside time to explain the importance of controls to your employees and get their buy-in about using fraud-prevention measures.

Employees who are used to a more casual work environment with few — or loosely enforced — controls sometimes resist new systems. They may think the new procedures are annoying, cumbersome or seem to slow down operations.

To allay their concerns, explain to your team that:

- You are taking specific steps designed to improve overall company operations.
- All responsible companies with an interest in protecting their assets and their employees' livelihoods and reputations follow standard, typical controls like those you are putting in place
- You have invested considerable time in designing these new processes.
- You understand that they may initially feel strange or unusual to employees; however, you expect everyone to adhere to the new procedures.
- You are serious about implementing these changes. They will become effective on *(fill in the date)*.
- You will begin spot-checking performance on *(date)*. If necessary, you will begin enforcing the "penalty" provisions at that time.
(Note: Penalty provisions will be discussed in an upcoming "Protecting Yourself From Fraud" article.)
- You will evaluate employees' suggestions for improvements or modifications after they've used the new controls for six weeks.

Be sure to follow up on that last bullet point. You may get some outstanding ideas or suggestions to implement. Whether you use their input or not, thank everyone who contributed ideas.

Monitoring Your Control System

After you've designed, documented and implemented your new control system, you need to make sure it is operating as designed. It is not enough to merely ask and/or obtain verbal assurance that someone has correctly performed a control procedure. You need to implement specific, ongoing monitoring and testing processes.

Also, if you don't test your system, team members will realize that the new procedures and controls are not being monitored — and compliance will drop dramatically.

Auditors use formal checklists, sampling procedures and mathematical models to measure the adequacy of various control systems. That level of testing is probably far beyond what you need, but steal a page from the auditor's toolkit and be prepared to periodically monitor — and sporadically test — your control system.

When designing your system, keep in mind the following questions to ensure that you are creating it with a testing procedure in mind:

- Is there another existing control that supplements or can act as a check or balance of this control? If so, how much can you rely on it?
- What objective proof will you need to determine that employees are following this control procedure? For example, can you:
 - **Review** the security system alarm log (instead of asking, "Do we always set the alarm at night?").
 - **Verify** that the file cabinet that holds your checks is locked each night as you leave (instead of asking, "Do we always keep all of our blank checks locked up?").
 - **Observe** the desk of an employee who has just left in a hurry to pick up a sick child at school to make sure all critical documents were placed in a locked drawer for safekeeping and that the drawer key was not left lying on the desk (instead of asking, "What do you do with critical documents and keys when you leave the office?").
 - **Check** several transactions and the ending balance on a bank statement against the detailed reconciliation prepared by your bookkeeper (instead of asking, "How are you doing on the reconciliations?").

These checks and observations are necessary because employees, when asked directly, tend to want to impress you with answers you want to hear.

Conversely, if an employee is doing something dishonest, that employee is even more likely to give you skillfully crafted, reassuring answers.

- If you need to check or test this control, how often should you do so?
 - The investigative process may need to happen more frequently immediately after implementation (until team members get used to the new control procedures and understand that you are serious about enforcing them). Later, you may be able to stretch out intervals between checkups.
 - Higher-risk areas should be checked more frequently than lower-risk areas.
- How will you work this into your schedule and remember that it needs to be done? (e.g., Do you need to schedule this step into your daily calendar?)
 - Don't underestimate what you can fold into your daily routine just by knowing what you know needs to happen and by being more observant.

For example, when walking through the office or searching for a client file, take a few extra moments to look carefully around. You might notice that checks to be mailed to vendors are sitting unattended on someone's desk (while your employee is out to lunch). Or you might see a box of blank checks sitting on an open shelf in a storeroom or in an employee's unlocked desk drawer. In these situations, the employee who has been entrusted with safeguarding your negotiable instruments is not properly following control procedures.

- When scheduling checkups, remember that the element of quiet surprise can be very revealing. Like the state trooper waiting around the bend with a radar gun who is not out to cause problems, but will take appropriate action when it comes to violators:

Don't —

- Announce your checkup intentions in advance to your employees.
- Put your monitoring activities on an in-office calendar that can be viewed by others.
- Perform checkups in a predictable manner. (“Yeah, the boss comes by every Tuesday around 1 o'clock to check on product deliveries and paperwork, so we'd better get the ruined materials and beer cans cleaned up before she shows up.”)

Do —

- Be calm and quiet, ask questions and obtain clarification.
- Think through in advance how you will respond to the (inevitable) disappointments or violations you'll probably encounter.
- Resist the urge and make changes, modifications and decisions on-the-spot when you find a violation. Make them only after gathering and fully considering all of the facts.
- For minor violations, be prepared to document your findings, clarify your expectations and issue a documented warning.
- If you suspect a major problem, don't sweep it under the rug. Give it your immediate attention.

Modifying Your Control System

As you monitor your results, be prepared to modify your control system. Some controls may not be that effective, and you may discover some underlying problems or hurdles, such as:

- Employees who are unclear about the procedures or the reasons for them
- Procedures that are too time-consuming
- Procedures that involve too many steps
- Procedures that cost more to implement than you originally anticipated
- Procedures that conflict with other company goals
- Procedures that are forgotten or overridden when other circumstances or stressors come into play
- Other justifiable reasons to resist specific procedures

Instead of simply discarding the control because it is encountering some turbulence, see if you can resolve the underlying problem. If your first attempt produces less than desirable results and you're stumped about what to do next, use feedback from your team members and professional advisors to see if the control can be modified or even re-invented.

Keep focusing on the asset you are trying to protect and on the risk you want to avoid or minimize. If the asset is worth protecting, you need a control.

Logic, creativity and perseverance will provide you with a smoothly functioning set of controls. You will eventually wonder how you ever functioned without these specialized procedures.

In addition, when you walk into someone else's business, you will begin to notice the difference between your *controlled* operations and their *out-of-control* operations. You will then know that you have moved your business one giant step closer to safety and financial security.