The Bookkeeper's Guide to Internal Controls

The American Institute of Professional Bookkeepers

Suite 500
6001 Montrose Road
Rockville, Maryland 20852

A significant portion of this part of the report is by Professor David P. Kirch, CPA, Ph.D., University of Ohio.

Introduction
Internal controls are a major area of accounting. This report is designed only as a quick guide to offer basic, practical steps for preventing loss.

By reducing or eliminating employee or customer criminal acts, you directly increase your company's or client's profits, let owners know that you are looking out for their best interests, and help to protect yourself if there are losses.

Many firms assume that the outside auditor "takes care of" internal controls. But auditors focus on technical accounting requirements, not on the key to fraud, theft and other crime: human behavior.

Freelancers can offer to review internal controls at no charge as a marketing tool, which signals the importance of such internal controls and of uncovering problems for which the solutions generate fees.

Be prepared for skepticism, even distrust. And if you charge for it, clients may see the controls as a waste of time or suspect that you are selling an unneeded service.

Reviewing internal controls
Because controls are an art rather than a science, they are not going to uncover every system flaw or solve every problem. Some firms may not have enough employees to implement certain controls.

The simplest way to uncover missing controls is to ask about company accounting procedures: "What happens when . . .?" Start with revenues, go on to expenses, and so on.

Instead of writing each answer, it may be more effective to draw a picture of the system —which employee performs what functions. Ask yourself about that area (expenses, generation of revenues, etc.):

1. How might undetected errors or theft occur at this point in the process?
2. How likely is the theft or error to occur?
3. How material are the amounts involved?

The key factors to list are susceptible processes or areas. Where appropriate, play devil's advocate. For example, do you have new owners? New owners who are honest may assume that employees are, too. Bring a healthy skepticism to this based on experience. Reinforce recommendations with horror stories.

Spouses are important
A spouse not involved in the business can still help with internal controls. For instance, have monthly bank statements sent directly to the owner's home so the spouse can review the checks. Consider using the owner's address for all tax-related correspondence.

Checks used to pay employment taxes are a favorite target for thieves because many are made out to the bank. Therefore, the owner, spouse or outside bookkeeper **must** review the endorsement on every payroll tax check every month.

Employees who see the bank statement will know someone else is reviewing it, but will not know how closely or what is being reviewed and are likely to assume that there are ore controls than there actually are.

A spouse who hears the owner discuss daily business operations will pick up internal control problems that the owner does not.

A spouse working at the firm presents special problems. Normal controls may be relaxed or ignored because of the owner-spouse relationship.

If a spouse retires, the relaxed controls are inadvertently passed on to the employee replacing the spouse, providing an easy way to steal.

Bottom line: For purposes of internal controls, ignore the fact that an employee is a spouse.

Have the spouse at the first meeting where internal controls are discussed. Spouses tend to be much less trusting of employees than owners are, especially when workers are the same sex as the spouse.

Part 1: Preventing theft by employees

Hiring procedures

The first step in stopping employee dishonesty is to hire competent, honest workers. Careful screening and a practical skepticism can be a big help. For example, all applicants should be told that your firm checks employer and credit (where applicable) references and finds out whether applicants have a police record. Consider using psychological and polygraph (lie detector) tests. These steps can uncover or discourage high-risk candidates.

Before taking these steps, consult a labor lawyer.

Encouraging employee honesty

Commitment to internal controls must be supported by company integrity—how it treats customers and suppliers. There should be a code of ethics that includes prompt return of overshipments and overpayments and prohibits putting employees in a position where they are required to cheat or lie.

Management must set a tone of integrity by uniformly and consistently applying, and enforcing, standards of honesty and ethical conduct, written and unwritten, to employees, managers, and owner-employees. Uneven enforcement by rank, salary or status is worse than having no standards because employees will soon disregard them.

Company policies that discourage theft

To prevent fraud and embezzlement, assign a different employee to carry out each of the following duties: invoicing, receivables, purchasing, payables, offering discounts and customer credits.

The following policies have proven effective for firms of every size. Some apply to all industries, some only to one, such as retailers:

- Any employee caught stealing will be terminated and turned over to local law enforcement officials. (*Check with a labor lawyer before implementing.*)
- All items must be priced by machine or rubber stamp, not by hand, including items marked down.
- Restrict price setting/marking to authorized personnel.
- Have someone other than the original salesperson inspect and approve returns and refunds.
- Refunds, over-rings and voids must identify the salesperson.
- Tell employees that those with a high volume of refunds will have their refunds reviewed.
- Announce that there will be random checks of supporting documents for refunds. Check for similar names, addresses and phone numbers popping up.
- Have random phone checks of payees to verify that they received payment and for the correct amount.
- Number receiving reports and shipping orders sequentially to prevent payment of phony invoices or destruction of shipping or receiving records.
- Require that receiving reports be made upon receipt of merchandise.
- Announce that lunchboxes and toolboxes, packages and bags may be inspected without notice by a supervisor or guard when employees leave the premises. *Check with your labor lawyer on state privacy laws.*
- Do not permit lunch boxes or bags at work stations. Use only if practical, and consult a labor lawyer before implementing.

You can create your own preventive measures, such as the restaurant that had pocketless uniforms.

A small retailer eliminated shrinkage simply by requiring employees to record all inventory *and* equipment (vacuum cleaners, etc.) *and* items to be discarded, such as old or spoiled inventory.

Spotting employee fraud or embezzlement
If you see any of the following signs of trouble, alert management immediately:

- Ghost employees on payroll, or phony overtime pay.
- A second endorsement on an employee's paycheck.
- A different endorsement on an employee's paycheck from the one you normally see.
- Different termination dates on personnel records v. payroll records.
- An employee not there when paychecks are delivered.
- No timecards for an employee.
- A timecard filled out in a supervisor's handwriting.
- A different-looking signature on a timecard.
- Unemployment claims from someone on the payroll.
- An unexplained rise in salary expense or paid absences.
- Company checks outstanding for too long.
- Too many checks with second endorsements.
- Checking accounts not being reconciled regularly.
- Employee checks (especially postdated ones) found in the cash drawer during the cash count.
- A spike in employee complaints about W-2 errors.
- High turnover in a particular department.
- A department's requests for more staff unrelated to an increase in workload or other causes.
- A big, inexplicable increase in sales returns.
- Unusual bad-debt writeoffs; unusually slow collections.
- A noticeable, unexplained decline in cash sales or disproportionate increases in credit sales.
- Unusual drops in revenue or increases in expenses.
- Missing sales or purchase documentation.
- Unusual shortages or overages in cash-drawer counts—usually accompanied by piles of paper clips, toothpicks or similar items next to the cash register, indicating that a thief is compiling unrung sales.
- Bank deposits with checks for amounts that do not appear on the cash register tape or in other records.
- An unusual increase in voids or refunds, especially refunds with common names and addresses.
- Deposits in transit are growing or are slow in reaching the bank.
- Collection of past-due or written-off accounts becomes unusually lax.
- An increase in past-due accounts, customer complaints about prior payments not being credited to their account, excessive late charges, or increases in the number of late charges being written off.
- The general ledger trial balance does not balance, or computer journal entries in subsidiary accounts do not equal control-account totals.

  For example, A/R is $100,000, but total subsidiary A/R accounts come to $96,000.

  Possible cause: An employee kept or "borrowed" $4,000 by crediting an A/R subsidiary account. Savvy hackers can do this on even sophisticated accounting software.
- Shortages in, or unusual adjustments to, inventory.

  Examples: Purchase of excess goods, excessive freight costs, purchases with shipping addresses that are not your firm's, shipments that are short or include items not used by your firm, duplicate invoices, invoices not on preprinted forms or letterheads, a vendor address that is actually an employee's address, excessive prices charged for inventory, suspicious inventory ratios.

continued

- Employees make entries or adjustments to their own accounts.
- Orders are entered late in the sales reporting period by a rep, then canceled.
- Discounts are unusually large.
- Payees have common addresses.
- Files contain copies of invoices, not originals.
- There are too many company checking accounts. (An employee may be using them for kiting.)
- Excessive or unjustified cash transactions.
- Assets are sold but they are still on the premises.
- Assets are sold for less than their fair market value.
- Dramatic, unexplained changes in financial ratios.
- The same employee controls assets and their accounting records (lack of segregation of duties).

Employee behavior that bears watching
Signs that may predict or indicate employee theft include:

- An employee living beyond his or her means.
- Problem gambling, speculating in the stock market or other markets, alcohol or drug problems.
- Illicit sexual relationships.
- Regular calls from creditors.

Make no accusations. Instead, management should contact your labor lawyer, bonding company, the police or a private security firm.

Part 2: Preventing theft by outsiders

Preventing losses from bad checks
Losses from bad checks are easier to prevent than other kinds of theft—you can reject a check—but this requires effective policies. Use those of the following guidelines that are appropriate to your business:

- Refuse checks from out-of-town banks. If impractical, require positive identification and customer's local and out-of-town addresses and phone numbers.
- Do not accept second-party checks or, if you do, at least refuse any check more than 30 days old.
- Accept checks only for the amount of the purchase.
- Verify that numerical and written amounts agree.
- Setting a dollar limit on sales that can be accepted without a supervisor's approval offers only limited protection. Most bad checks are for $25-$35, because fraud-sters know that clerks are less cautious about small checks.
- Require employees to get a supervisor's approval for checks with low numbers or no number. Most new accounts start with check #101. As a rule, very low-numbered checks have a higher return rate.
- Request at least two current IDs for checks; at least one with a photo. An employee who is suspicious about an ID should try to verify the address and phone number.
- Compare the signature on identification documents with the one on the check.
- Do not accept as identification Social Security cards, business cards, birth certificates, library cards, organizational membership cards, unsigned credit cards, bank books, work permits, insurance cards, voter registration cards, learner's permits, or letters.

Physical deterrents that discourage theft
Good locks and keys are a proven way to prevent theft, but only if used properly.

- ✓ **Use the right locks, properly installed**. Security experts recommend pin-tumbler cylinder locks with at least five pins, which are hard to pick. Double-cylinder deadbolt locks can't be opened with a credit card or by breaking the glass and reaching in for the handle. Double locks prevent "break-outs" by individuals hiding on the premises until everyone has left. Burglars favor rear doors; further protect these with burglar bars.

- ✓ **Keep padlocks locked,** regardless of how inconvenient it is to repeatedly lock a door or gate during the day. It prevents employees and outsiders from switching padlocks, then returning to burglarize the firm. Keep keys in a secure place (not hanging on a nail by the door or in the top drawer of the secretary's desk).

- ✓ **Apply strict security measures to keys**. Locks are useless unless the keys are protected. Keep a record of who has each key at all times. Unauthorized duplication of a key should result in immediate termination. If an employee loses a key, or terminates without returning one, locks should be rekeyed. Periodically inventory issued keys to make sure none have been lost or stolen. To minimize losses when a key is lost or stolen, never tag keys with your firm's address or the location of the locks they fit.

- ✓ **Put safes in well-lit areas** that are easy to see from the street. Keep safes closed when not being used, even during working hours. Bolt all safes to the floor or wall, regardless of their weight.

- ✓ **Keep trash cans away from storage sites**. Conduct random inspections to see if company assets are intentionally discarded for later retrieval.

- ✓ **If you use outside security guards, rotate them** to prevent fraternization with employees.

- ✓ **Change safe combinations often.** Keep combinations off the premises and give them only to trusted individuals.
  - ➢ During nonworking hours, put all cash in the safe, lock it, and leave cash register drawers open.
  - ➢ Deposit cash in the bank at least daily —more often if cash accumulates.
  - ➢ Balance cash registers an hour or two before closing and lock cash in the safe, or make a night deposit. Keep on hand only the minimum cash required.

- ✓ **To discourage theft by truckers**, consider installing fences between bays and using closed-circuit television cameras at loading docks. Have the receiving supervisor's office where the docks are easy to see.
  - ➢ Do not permit trucks near loading docks except to load/unload, and restrict drivers to a designated area.
  - ➢ Whenever possible, have employees rather than another company's drivers load or unload trucks.

- ✓ **If your firm is in a high-crime area**, consider heavy window screens, burglar-resistant glass windows or bars, watch-dogs on premises when you are closed. or hiring a private security patrol.

Improving your building's security
If your firm does not own the building, discuss with other renters how to get the landlord to implement the following recommendations.

A building should be well lit outside on all sides, ideally with floodlights (mercury or metallic vapor lamps)—and inside, especially at night so that passers-by or the police can see suspicious activity—and should have a burglar alarm. The best, but most expensive, is a silent, central-station alarm connected to the police or a security firm. If this is too expensive, install a loud alarm bell or siren.

Also, consider using radar motion detectors, invisible photo beams, or ultrasonic sound or vibration detectors. All can be hooked up to automatic dialers that call the police and a designated company official.

Protection against robbery

Have *two* employees open and close, one to observe outside. If the person closing does not appear on time, the observer calls the police.

The observer must carry a cell phone that has the police phone number and your firm's address. When under stress about a possible robbery, it's easy to forget the address of a place where you go each day

Make sure employees are prepared. Instruct them to cooperate with a robber, to stay calm and make mental notes about him —height, build, hair and eye color, complexion, voice, clothing, identifying characteristics— but to never try to play hero. Some firms mark doorframes at different heights as a fast way to estimate a thief's height. If there is a robbery, no one should discuss the robbery until the police have interviewed employees.

For retailers: preventing shoplifting

Anyone may be a shoplifter, but professionals are different from amateurs.

Who shoplifts. Amateurs include youths (half of all shoplifters), impulse shoplifters, kleptomaniacs, alcoholics, vagrants and drug addicts. Professional shoplifters focus on items that can quickly be resold, such as stereos, TVs and small appliances.

Youths and pros often work in groups. One distracts employees by asking for help or arguing with them or creating a scene (fighting among themselves or pretending to faint), while the others steal. They may come at lunch hour, just after opening or before closing, when fewer employees are there.

How to spot shoplifting. Police departments offer training on shoplifting prevention and detection. Offer this to your employees. Signs of shoplifting include:

- walking in short, unnatural steps in order to conceal merchandise between their legs;
- quick, nervous glances to see where other people are before attempting to shoplift;
- carrying bulky packages, knitting bags, shopping bags, pocketbooks, folded newspapers and magazines, umbrellas, arm slings; and
- wearing oversized coats and capes (which may have hidden pockets).

Employees may also want to keep an eye on baby carriages and gift-wrapped boxes that may be hinged and used to conceal stolen merchandise.

How to discourage it. Have all areas of the store well lit. Place convex mirrors high on walls so that employees can watch any shopper. Consider closed-circuit TV Keep small high-priced items behind a counter or in locked display cases. To discourage shoplifters from using unlocked exits that are not for customer use, put noise alarms on them.

What to do about it. The best deterrent to shoplifting is prosecution of all offenders, regardless of whether they are amateurs or professionals. Apprehension of shoplifters is covered by state law. Make sure employees are familiar with basic legal requirements so that your company avoids lawsuits over "false accusation" or "false arrest." The Small Business Administration recommends detaining a suspected shoplifter only when the following four criteria have been met:

1. the shoplifter is actually observed taking or concealing merchandise; and
2. the item can be identified as the company's; and
3. the employee can testify that the goods were taken with the intent to steal; and
4. the merchandise was not paid for.

Employees asked to apprehend shoplifters should do so outside the store—and they should never make accusations.

Instead, they can inquire, "Did you forget to pay for the item(s)?" Ask the police if they believe it is advisable to prosecute.

Just calling the police discourages other shoplifters. Wrongly calling the police, however, can create devastating PR. Check with a lawyer and local police before implementing.

Part 3: Liability of employee bookkeepers

By A. Reinstein, D.B.A., CPA, Chair, Dept. of Accounting, School of Business Administration, Wayne State U.; A. Spalding, J.D., CPA, Asst. Professor, Business Law, Wayne State U.

Liability for disclosure to third parties. Financial data can be disclosed or "leaked" in many ways: in correspondence, through the financial statements or even on the phone.

What to do: Avoid public statements. Be secretive about company matters. Never respond to phone inquiries or distribute corporate information to outsiders.

Liability for withheld taxes

Although the employer is responsible for withholding federal and state taxes, the employee to whom withholding is delegated could be held personally liable for monies withheld but not paid. This personal liability can be imposed on the person "responsible" for paying the taxes, including in certain cases, the bookkeeper or the payroll clerk.

IRC §6672(a), the 100% penalty, is used to recover employer payroll taxes from those responsible for withholding and paying them. Even when check-signing authority does *not* involve payroll or payroll taxes, it can trigger personal liability if that person pays creditors. The IRS and other tax agencies deem funds used to pay creditors as having "come from" payroll taxes withheld and therefore "belong" to the IRS or tax agency.

If the IRS thinks it cannot recover unpaid payroll taxes from the employer, it may sue the employee before—or instead of—going after the firm, because anyone responsible for withholding and paying taxes is as liable as the employer. Here are ways to protect yourself:

- **Don't be the only signatory on checks**. The authority to sign checks is the authority to disburse funds and can trigger personal liability if withheld taxes are not paid. You are protected if your firm requires all checks to have a second signature from a supervisor or corporate officer *after* you sign them.

  Note: If you must sign paychecks temporarily (an owner is away) or permanently, your only protection may be to have your employer give someone else "final authority."

- **Hold checks until funds are available**. Liability for payroll taxes is not incurred until paychecks are mailed or delivered to employees. If funds are available for "net pay" but not for payroll taxes, you can protect yourself by not delivering signed paychecks until funds for the entire gross pay are available. This is easier to do if one checking account is used exclusively for payroll, since only payroll and payroll taxes would be paid from it.

- **Be indemnified**. Are you required to sign and release paychecks even if you can't verify that there are sufficient funds?

  - If you work in a closely held corporation, protect yourself by asking for a signed indemnification agreement from the owners that personally guarantees payment of payroll taxes, even if this means that the owner would reimburse you for amounts you might personally have to pay the IRS. This protects you and lets the owners operate without signing every paycheck. Make sure your lawyer reviews it before you sign.

- **Check federal and state laws**. Laws covering your company may cover its employees. For example, even a closely held corporation that raises capital by issuing promissory notes or debentures (bonds without security) or by selling stock may come under securities laws—and so may its employees.

- **Accept professional responsibility**. If something raises a question in your mind about accounting practices, ask about it. For instance, if another employee is taking out cash without the proper documentation, it is entirely proper to ask about it. Ignoring a questionable practice does not protect you and may result in your being blamed for it.

- **Install internal controls**. For example, writing and disbursing checks and balancing the checkbook should be done by two different people. This helps prevent fraud, embezzlement, and similar problems and may protect you if funds are missing. Suggest that your firm ask its CPA for guidance.

Liability for pensions and retirement plans. Pension and retirement plans (e.g., 401(k), money purchase plans) are trusts: legal documents that include specific instructions for collecting, managing and distributing money and other assets. Retirement plans generally cover the collection and investment of both contributions and payment of benefits. Pensions come under ERISA and other tax and labor laws.

You can be held personally liable for pension-related work if you are a "fiduciary" —a person responsible for the management of trust assets. Pension plans have a trustee named in the plan documents, and the trustee is a fiduciary of the plan. But the trustee is often not the only fiduciary. Some plans name an "Administrator" as well as a trustee, and the administrator can be treated as a fiduciary.

Under ERISA, a fiduciary is not only a person named as a trustee or an administrator in the plan document, but also someone who is otherwise given power to control or manage the trust assets. Other persons, including employees of the sponsoring company, are considered fiduciaries to the extent that they:

1. exercise any discretionary authority or discretionary control with respect to management of the plan, or exercise any authority or control with respect to management or disposition of its assets;

2. render investment advice for a fee or for other compensation, direct or indirect, with respect to any money or other property of such plan; or have any authority or responsibility to do so; or

3. have any discretionary authority or discretionary responsibility in the administration of such a plan.

Under the law, a fiduciary has a duty to act loyally and prudently, to manage and diversify plan investments properly, to implement plan document instructions, and make sure that the plan follows various laws on prohibited transactions and preparation of reports. A fiduciary who fails to meet these responsibilities may be required to personally reimburse any losses as the result of such a breach and to restore lost profit.

What to do:

- **Know how to protect yourself**. Generally, if you only assist with the paperwork and accounting—including Forms 5500 and W2-P, and plan and loan documents—you are not considered a fiduciary to a retirement plan. But. you may be considered a fiduciary if you:
  - exercise either discretionary authority or discretionary control in the management of the plan;
  - exercise either authority or control in the management or disposition of the plan's assets;
  - render investment advice for a fee, either directly or indirectly; or
  - have any discretionary authority or discretionary responsibility in the administration of the plan. In other words, as long as all of the investment, loan, distribution and benefits decisions are made by someone else (such as a named trustee other than you), you almost always escape personal liability.

- **Follow pension plans and laws to the letter**. Even if limited authority has been delegated to you, you generally will not incur personal liability if you carry out your responsibilities according to the plan documents. Ask your firm's CPA or lawyer or benefits consultant to explain how various laws affect your fiduciary responsibilities, reporting requirements and prohibited transactions.

Liability for fraud

As noted above, employees worry about the information they give to government agencies and third parties (banks, creditors, vendors, pension plan participants).

Note: The solutions offered here presume that no one in the firm is intentionally trying to defraud anyone. But sometimes employees see fraud and do not know what to do.

Caution: If you ever face criminal prosecution, the courts will not accept, "I was only doing what I was told."

Most federal and state tax authorities can enforce a variety of anti-fraud laws.

"Conspiracy" laws permit prosecution of anyone who knows of and participates in a criminal activity. Even banks can sue employees under state credit fraud statutes.

The IRS can prosecute anyone under IRC tax fraud provisions. Not only does tax law include criminal and civil penalties for filing a false return, it contains a provision implicating anyone who *aids in* preparing or submitting a false return. Employees can be and are prosecuted under this provision.

For example, if employees are treated as independent contractors and their compensation is not included on the 941, the bookkeeper who completes the 941 and submits it to the IRS could be questioned.

What to do:

- **When in doubt, ask**. Even the strangest or most suspicious looking transactions are almost always legitimate. But, if you don't understand them, be safe—ask for an explanation.
- **If you are sure, consult an attorney**. But if, after discussing the matter with management and/or a member of the board, you are convinced that a crime is being committed, speak to your attorney before taking action. Although many state laws protect whistle-blowers, ask an attorney.

Although these guidelines are no guarantee against being named in a lawsuit, defending yourself will be much easier. In many cases, your attorney will be able to persuade the court to drop your name from the suit, and your employer will reimburse legal expenses. And, the judge may even require the plaintiff to pay your legal costs.

Copyright ©2017 by The American Institute of Professional Bookkeepers (AIPB). All rights reserved under International and Pan-American Copyright Convention. No part of this report may be reproduced in any form or by any means, electronic or mechanical, including photocopying, without written permission from the publisher: AIPB, 6001 Montrose Rd., Suite 500, Rockville, MD 20852. Published in the U.S.A.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

– From a Declaration of Principles jointly adopted by a Committee of the American Bar Assn. and a Committee of Publishers.