Internal Controls in Accounts Payable

Mary S. Schaeffer
Internal Controls in Accounts Payable

Mary S. Schaeffer
Course Information

Course Title: Internal Controls in Accounts Payable

Learning Objectives:
- Identify really bad accounts payable practices that weaken controls
- Pinpoint problems likely to occur if strong controls are not used in accounts payable
- Delineate problems created when segregation of duties are not set up correctly
- Demonstrate the interaction between fraud and internal controls
- Reveal internal control practices every organization should use to deter fraud
- Identify weak control practices that don't curtail duplicate payments
- Show how poor controls make duplicate payments more likely
- Pinpoint places where internal controls most commonly breakdown in the accounts payable function
- Locate places where purchase orders cause control problems
- Identify common purchase order problems and solutions to fix them
- Establish how best invoice control practices improve processing
- Recognize invoice automation control issues as they arise
- Be aware of how control issues can fall apart in the accounts payable function in the month end and year end close
- Implement the proper controls around the check production process
- Demonstrate why signature stamps represent a poor control and can cause your organization big problems
- Identify poor controls related to check request forms
- Identify controls that should be incorporated into every corporate procurement program
- Reveal best fraud control strategies for your p-card program
- Demonstrate why daily bank reconciliations are so important even if electronic payments are not being made
- Show how a good policy and procedures manual can strengthen internal controls

Subject Area: Accounting

Prerequisites: None

Program Level: Overview

Program Content: Strong internal controls are key to any effective accounts payable function. Without such controls, fraud is easier to commit, duplicate payments increase and the function is not cost-effective. This course presents
information the professional can use to identify control problems and implement strong controls. Industry expert Mary Schaeffer shows auditors, controllers, and managers where control issues are likely to occur, how to strengthen controls, and best practices for a control effective accounts payable function. The text includes not only examples of strong controls but it also examines common and not so common ways controls are inadvertently weakened.

**Advance Preparation:** None

**Recommended CPE Credit:** 5 hours
**Table of Contents**

**Introduction**................................................................. xi

**Chapter 1 – The Basics of Internal Controls: Theory **........... 1

- Learning Objectives .......................................................... 1
- Introduction ............................................................................. 1
- Segregation of Duties ......................................................... 1
- Reasonable Hiring and Background Checks .......................... 1
- Strong Controls Throughout the Accounts Payable Process ... 2
- Eliminate Really Bad Accounts Payable Practices ............... 3
- Paper Trails ........................................................................... 4
- Monitoring Reports .............................................................. 4
- Training .................................................................................. 5
- Review Questions ............................................................... 6
- Review Answers ................................................................. 7

**Chapter 2 – The Basics of Internal Controls: In Practice **......... 8

- Learning Objectives .......................................................... 8
- Introduction ............................................................................. 8
- Ten Problems Created by Inappropriate Segregation of Duties ... 8
- Dissecting the Procure-to-Pay Process ................................. 8
- Where Controls Break Down .................................................. 9
- Concluding Thoughts .......................................................... 11
- Often-Overlooked Practices that Make Accounts Payable Less Efficient
  - Than It Could Be............................................................... 11
- Segregation of Duties Problems ............................................. 14
- Review Questions ............................................................... 15
- Review Answers ................................................................. 16

**Chapter 3 – Fraud Prevention Controls and Practices **............ 17

- Learning Objectives .......................................................... 17
- Introduction ............................................................................. 17
- ACFE’s Biannual Report ....................................................... 17
- Fraudulent Disbursements .................................................... 18
- Uncovering Fraud ................................................................. 18
- Who Commits Fraud ............................................................ 19
- Dealing with Employee Fraud .............................................. 19
- The Ugly Issue: Employee Fraud Prevention ....................... 20
  - The Big Problem ............................................................. 20
  - Overriding Fraud Prevention/Detection Guidelines ............. 20
  - What Else ........................................................................... 21
  - If You Suspect Fraud.......................................................... 22

- Vendor Fraud ....................................................................... 23
- Small Dollar Invoice Fraud .................................................. 23
- W-9 ..................................................................................... 24
- Check Fraud ........................................................................ 25
Internal controls are crucial in accounts payable because, as Willy Sutton says about banks, “it’s where the money is.” Poor controls can lead to duplicate payments and fraud – both of which make an immediate and ugly impact on any organization’s bottom line. Despite what many think, strengthening internal controls does not make the accounts payable department less efficient. In fact, just the opposite happens.

For when controls are tightened, second invoices don’t get through, eliminating the need for double work. What’s more, payments get made on time, eliminating many of those “where’s-my-money” calls. This translates into more satisfied vendors meaning they are apt to be more understanding the next time there is a legitimate problem.

In this course we focus on the procure-to-pay portion of the accounts payable function, starting with an exploration of the theoretical basics before moving into the hands-on practical aspects of the function.
Chapter 1
The Basics of Internal Controls: Theory

Learning Objectives

- Identify really bad accounts payable practices that weaken controls
- Pinpoint problems likely to occur if strong controls are not used in accounts payable

Introduction

In this section we take a look at practices that will help accounts payable departments strengthen and improve controls.

Segregation of Duties

In order to perpetrate a fraud through accounts payable it is frequently necessary to have access to more than one function. For example, a person would have to have access to the check stock and the facsimile signer. Thus one of the easiest ways to prevent fraud is to assign responsibilities in such a manner to minimize this risk. Depending on the size of the department, it may be necessary to work with another group to achieve this goal.

Alternatively, close scrutiny on a regular basis of any person with multiple conflicting responsibilities is recommended. Companies sometimes get lulled into a false sense of security because the particular employee with multiple conflicting responsibilities has been with them a long time. This is a mistake, as most frauds are committed by long-time trusted employees.

Reasonable Hiring and Background Checks

Because the employees in accounts payable are sometimes viewed as clerks, not much consideration goes into the hiring or background checking process. This can be a huge mistake as the employees in the department regularly come in contact with or have access to the organization’s lifeblood – its money.
Chapter 1 – The Basics of Internal Controls: Theory

Should a fraud occur on your watch and it is perpetrated by someone on the accounts payable staff, the manager should be able to demonstrate that reasonable care was exercised in hiring that person. This is not to say that reference checks will necessarily uncover a potential thief but they will cover the bases for the manager who made the unfortunate decision to hire the individual. Often just a few phone calls will uncover enough information to raise a red flag.

The phone calls may not uncover a potential thief, even if the person providing the reference has knowledge of prior wrongdoings. The reason for this is that many companies refuse to provide references, only verifying that the individual had worked for them for a particular period. Fear of lawsuits due to unfavorable references has forced many to set a corporate policy of just providing the equivalent of name, rank, and serial number. This is unfortunate because often employees who deserve sterling references are hung out to dry because of these policies.

**Strong Controls Throughout the Accounts Payable Process**

Two problems that have plagued accounts payable departments everywhere are fraud and duplicate payments. The two are often mentioned in the same breath because the controls to prevent the latter also help with the former. Although this is starting to change, many organizations often looked at their accounts payable operations as a bunch of clerks who pay the bills – and how hard can that be? The answer is not too hard if you don’t care about:

- Timely payments and vendor relations
- Check fraud
- Duplicate payments
- State audits for unclaimed property
- State sales and use tax audits
- B-Notices for incorrect 1099s
- Penalties for incorrect 1099 reporting
- Payment of independent contractors’ taxes because of failure to obtain proper 1099 information
- Employee phony invoicing schemes
- Censure by the IRS for inappropriate reporting of non-resident alien income
- Inaccurate or incomplete accruals
- Inaccurate financial statements
- Failure of a Sarbanes-Oxley audit
Chapter 1 – The Basics of Internal Controls: Theory

These are just a few of the areas that a company can run into trouble with if proper policies and controls are not fully integrated into an organization’s accounts payable function.

Establish the appropriate controls throughout the function even if it means that the comfortable routines of a few people will be disturbed. In the long run it will benefit your organization.

Eliminate Really Bad Accounts Payable Practices

More organizations than you would suspect employ what are generally considered really bad practices in some parts of their process. Many of these are inherited practices (we always did it that way) and others are a result of corporate culture (boys will be boys). Whatever the reason, Sarbanes-Oxley has shined its light on these dirty little secrets and at least some of the organizations that tolerated these practices are finally letting go of them. Before listing them, we have to salute the accounts payable professionals who seized the opportunity presented by Sarbanes-Oxley and use the Act as ammunition to get rid of the practices. Here are just a few of them:

- Petty cash box
- Not enforcing the T&E policy equitably across the board
- Questionable Travel and Entertainment reimbursement practices
- Not using positive pay
- Not using a duplicate payment audit firm because the company “never” makes duplicate payments (since these firms almost always work on a contingency basis, why not verify that claim)
- Allowing frequent rush checks to cover employee sloppiness
- Not mandating the use of a corporate T&E card
- Not requiring a W-9 before a payment is made to a vendor
- Ignoring the unclaimed property laws

You can probably identify more in your own organization. Very few groups are immune from employing one or two bad practices somewhere across their financial spectrum. Once you’ve identified them, try and root them out. If you need help, both your internal and external auditors are likely to be in your corner so get their support.
Paper Trails

Now more than ever it is crucial that a trail – be it paper or electronic – be established and easily verifiable. Timely documentation and a record retention policy that assures a clear audit trail are two good first steps toward complying with Sarbanes-Oxley as well as proof to state and federal auditors should your organization come under scrutiny by the authorities for not complying with one of their programs.

A verifiable audit trail ties into the concept of strong internal controls. Review your processes to ensure that the audit trail is there. Some companies find that they need to review their indexing procedures to get an acceptable audit trail.

Monitoring Reports

Establishing effective controls, unfortunately, is not a one-shot project; it is an ongoing process. To ensure that the controls remain effective and function appropriately they need to be reviewed on a periodic basis. Additionally, and equally important, reports need to be designed to ensure that the controls function as they should. They are also part of the control process. These reports can be best designed by figuring out where the potential weaknesses are in the process.

For example, one of the most common ways for an employee to commit check fraud is for the employee to simply change the mailing address of a vendor in the master vendor file. Then, once the check has been mailed, the employee with access to the master vendor file goes back into the system and changes the address back to the correct address. It often takes months for it to come to light that the check went to the wrong vendor and an even longer time to track down where the check did go. If the employee is smart, they will have covered their tracks by that time.

How can you uncover this little scheme? A report of all changes to the master vendor file should be run each week (or month) and the report reviewed by someone at a fairly senior level not related to the process. By looking at all the changes, this little scheme would be uncovered. The problem with this approach is that few executives at senior levels want to wade through the minutia of the changes made to the master vendor file.

Review your own processes and find the applicable weak spots and then design your own reports. Depending on your processes you may need a few or many such reports. For example, if inactive vendors are infrequently (or heaven forbid, never) deactivated in the master vendor file, you’ll need to review any activity in formerly inactive accounts. A
Chapter 1 – The Basics of Internal Controls: Theory

shrewd employee might use one of these accounts, along with some address changes to the master vendor file, to submit a phony invoice, get it approved, and then maneuver your organization’s money into his or her bank account. By the way, if management is dragging its heels at deactivating inactive vendors, you might point this scheme out to them.

Training

In many organizations the accounts payable group gets short shrift when it comes to continuing education. This is unfortunate and to be perfectly honest, not really fair. The organization relies on its accounts payable staff to:

- Keep the organization compliant with all regulatory issues
- Keep up to date on each year’s changes to the 1099 filing requirements
- Know what’s going on with regard to unclaimed property legislation
- Be able to recommend and employ the best practices for the payables process, including all sorts of technological advances
- Help prevent check fraud by implementing the latest controls available as well as knowing about all regulatory changes
- Establish routines that minimize duplicate payments
- Integrate the sales and use tax calculations from as many as 10,000 taxing authorities into their daily routines
- Spot phony invoices when they are submitted
- Tactfully deal with belligerent and often uncooperative vendors
- Skillfully handle angry employees who need T&E reimbursements despite the fact that their boss has still not approved their expense report

For a variety of reasons, many organizations do not allocate anything for training the hard-working accounts payable professionals who staff their organizations. This is a crime. Currently there are several organizations that provide training in all these areas. They offer onsite conferences where your professional staff can network with other professionals and learn from the best. For organizations that do not wish to send their staff a distance, there are several groups that offer one-day local seminars.

And, if the staff can’t leave the office, the Internet now brings the learning right into your office. And, of course, there are books and newsletters to help keep your staff up-to-date.
Chapter 1 – The Basics of Internal Controls: Theory

Review Questions

1. If inadequate attention is paid to the invoice processing function, which of the following is not likely to occur?
   A. Check fraud
   B. Timely payments
   C. B-Notices
   D. Inaccurate accruals

2. Which of the following does not demonstrate poor controls in the accounts payable process?
   A. Petty cash box
   B. Not requiring a W-9 before making a payment
   C. Use of positive pay
   D. Ignoring unclaimed property laws
Review Answers

1. A. Incorrect. Poor internal controls in the check function unfortunately do allow fraud to occur with greater ease.
   B. Correct. Timely payments are the reward for doing everything right in accounts payable. However, if you have poor controls it is not likely you’ll be able to achieve that goal.
   C. Incorrect. Another negative consequence of poor controls is an increase in B-Notices.
   D. Incorrect. If you don’t have controls in place, the likelihood of accurate accruals is small.

2. A. Incorrect. Petty cash boxes are high on the list of policies that make accounts payable inefficient and signal poor controls.
   B. Incorrect. Not requiring a W-9 before making a payment is one way to guarantee lots of extra work at year-end. Not getting W-9s will also allow payments to slip through to questionable vendors.
   C. Correct. Use of positive pay is one of the best controls any organization can use to guard against check fraud.
   D. Incorrect. Ignoring unclaimed property laws demonstrates poor controls in the accounts payable process.
Chapter 2
The Basics of Internal Controls: In Practice

Learning Objectives

- Delineate problems created when segregation of duties are not set up correctly
- Identify real-life issues that arise due to poor internal controls

Introduction

Let’s take a look at what can go wrong when internal controls are not properly implemented. We’ll start with a look at segregation of duties and potential conflicts you might not have expected.

Ten Problems Created by Inappropriate Segregation of Duties

One of the principles related to strong internal controls is the appropriate segregation or separation of duties. When it comes to the procure-to-pay cycle, this means that no one person should have the ability to perform more than one piece of the transaction. By restricting this access it becomes more difficult for an employee to defraud the organization. Typically, collusion makes a fraud easier to commit. With the same person handling two or more legs of a transaction, the collusion is a done deal. What follows is a look at the different pieces of the procure-to-pay function. This is followed by identifying ten situations ripe with conflict of interest and weakened internal controls.

Dissecting the Procure-to-Pay Process

Typically there are three distinct departments involved in the procure-to-pay operation of any company. They are the purchasing department, the receiving department and the accounts payable department. Rarely do the responsibilities handled in one department overlap into a second. However, organizations with smaller accounts payable or purchasing functions may sometimes find themselves stretched to assign tasks in such a way that there are no segregation of duties issues.
Chapter 2 – The Basics of Internal Controls: In Practice

Before we look at some of the potential problems that might arise if duties aren’t separated appropriately, let’s take a look at the different steps along the procure-to-pay trail. Most companies have different parties handling each of the following:

1. Ordering goods
2. Approving purchases
3. Receiving ordered materials
4. Approving invoices for payment
5. Processing invoices
6. Handling preprinted check stock
7. Signing checks/releasing ACH payments
8. Setting up vendors/changing vendor information in the Master vendor file
9. Handling unclaimed property reporting
10. Reviewing and reconciling financial records including bank reconciliations

Where Controls Break Down

When two or more legs of the transaction are handled by the same person, there can be a problem. Now, for example, if an organization had one individual ordering goods and doing the unclaimed property reporting, there wouldn’t be much of an issue. The problem is the skillset needed to do those two tasks are so disparate that no organization would have the same person performing them. The problem occurs with tasks that are in the same chain. Let’s take a look at what can go wrong when certain responsibilities are handled by the same individual.

Potential Conflict #1: If the same person orders goods and then approves the purchases, there is no control and no checks and balances. Of course, the person who ordered the goods might have to review the purchase to ensure that what is on the invoice is what was ordered and not something entirely different.

Potential Conflict #2: If the same individual orders and receives purchases, there is no control over whether the goods were actually ordered in the first place. All an employee who wanted to defraud the company would have to do would be to send an invoice and claim it had been received. Alternatively, low-quality goods could be ordered while the invoice might reflect the price of much higher priced materials.
Potential Conflict #3: If the same person received goods and approved invoices for payment there would be no controls over the pricing or quality.

Potential Conflict #4: If the same individual approved purchases and set up vendors in the master vendor file, it would be very easy to set up a phony vendor and submit a fraudulent invoice for goods that do not go through the company’s receiving channel.

Potential conflict: #5: If the same individual could approve invoices and process invoices, there would be no controls in place to ensure the invoice was legitimate to start with. The crook would submit and approve a phony invoice and then the processor would run it through, allegedly verifying it.

Potential conflict #6: By allowing the same person to process invoices and set up vendors in the master vendor file you open the door to someone setting up a phony vendor in the master vendor file and then processing an invoice against it as though it had been approved by a purchaser.

Potential conflict #7: Permitting one person to both process invoices and sign checks or release ACH payments, you are removing the checks and balances put in place to prevent an employee from processing a phony invoice or sending payment to the wrong address.

Potential conflict #8: If one individual can approve invoices and set up vendors in the master vendor file, they can set up a phony vendor, submit a phony invoice and then approve it for payment. When the approved invoice shows up in accounts payable, the processor won’t realize they are handling a fraudulent invoice and it will fly through your process – especially if it is for a non-PO item.

Potential conflict #9: If the same person handles preprinted check stock and signs checks, they are effectively set up with a blank company check.

Potential conflict #10: If the same person reconciles the bank account statements and handles unclaimed property reporting, they will know which checks haven’t cleared. This will enable them to easily adjust the records so when the unclaimed property is turned over to the state, it is
reported in their name instead of the rightful owner’s name. The company’s records will balance and unless the rightful owner comes forward (unlikely) the employee will claim the money that did not belong to them and no one will be the wiser.

**Concluding Thoughts**

Inappropriate segregation of duties is one sign of weak internal controls. We’ve uncovered ten of them above but you can probably come up with a lot more. Now, some organizations just don’t have enough people working in accounts payable and purchasing to implement all the separations discussed above. They have two options.

1) Enlist employees in other departments to handle some of the responsibilities discussed. It is not uncommon to find master vendor file, bank reconciliations and/or unclaimed property handled in another department so the appropriate segregation of duties is maintained.

2) If help is not available from other departments, it is sometimes necessary to add additional steps in the process to make up for the weakened controls. This might be the president or CFO reviewing all checks before they are released in a smaller company.

The important issue is that an organization recognizes where their potential weaknesses are and create additional reviews around them.

**Often-Overlooked Practices that Make Accounts Payable Less Efficient Than It Could Be**

You’ve heard the old adage, work smarter not harder. Sometimes we’ve been doing things a certain way for so long in accounts payable, it never occurs to us to try another approach. That’s where the smarter issue comes in. Sure, it’s possible to improve productivity if you spend a lot of money, but that’s not what we’re talking about. Let’s take a look at some practices that would make any accounts payable department function a little more efficiently – and won’t require special budget allocations to do so.

1. Start accepting invoices both by e-mail and fax. For many years, companies refused to do this because they were concerned about du-
Duplicate payments. But now, we know that it is possible to have original-looking documents that are actually copies so not paying from a copy does not provide the protection it once did. By accepting invoices by email and fax you speed up the mail time, making it easier to earn early payment discounts. What’s more, if you are scanning invoices, an emailed invoice removes the need to scan.

2. Get rid of petty cash boxes, if you still have them. Anecdotal evidence suggests that approximately one-quarter of all organizations still have petty cash boxes. They are huge time wasters, are rarely in balance, and may tempt employees with financial issues. By eliminating petty cash boxes you will make the accounts payable function more efficient and you’ll strengthen internal controls. And as an added benefit, your staff will probably be thrilled not having to deal with the sometimes questionable reimbursement requests.

3. Return invoices addressed inappropriately/addressed to no one to the vendor with a polite letter explaining that in order to process invoices efficiently it is imperative that every invoice contain the name of the requisitioner or a purchase order number. Without one of these vital pieces of information, your staff will waste time trying to figure out who ordered the item. You’ll also eliminate those fraudulent invoices sent by crooks hoping to entice you to pay.

4. Develop and use strong coding standards for invoices and data entry in the master vendor file. Put it in writing and insist everyone use it. This simple approach will eliminate a good portion of potential duplicate payments. Don’t assume everyone would use the same abbreviations as you would. They won’t. And, by putting it in writing and giving a copy to every processor, they can refer to it if they have any questions.

5. Eliminate as many paper checks as you can. This can be done by moving small dollar items to p-cards and trying to pay as many vendors as possible using ACH. Paper checks are incredibly inefficient; they require a lot of manual handling, get lost in the mail and are expensive, to boot. On the other hand, electronic payments require no manual handling, are less expensive than paper checks and have very few or no unclaimed property issues.

6. Don’t play favorites with employees from other departments (or for that matter from your own). Don’t make exceptions against policy
Chapter 2 – The Basics of Internal Controls: In Practice

based on how much you like a person. For example, if you always do
rush checks for Jane in accounting, other employees will expect
similar treatment. If you don’t extend them the same courtesy there’s
bound to be a lot of complaining and grumbling and accounts payable’s image will take a hit. What’s more, eventually other groups will
figure out who your favorites are and those people will be recruited
to come down and ask for exceptions for the rest of their department.
Often, when accounts payable plays favorites, it is thought that no
one knows. But, like all other gossip in an organization, it spreads
faster than anyone might imagine.

7. Don’t entertain special requests from vendors to pay them faster than
the payment terms agreed to in their contracts. More than occasionally,
a vendor will call and ask/demand to be paid more quickly than
agreed-upon terms. Sometimes they’ll claim someone in purchasing
promised this. Other times, especially when they have gotten to
know the processor handling their account well, they’ll simply ask
for a special favor trying to convince the processor to enter an early
due date. While you want your processors to have good relations
with your vendors, these relations need to be arm’s-length and not
result in inappropriate actions. This is the first step down that slip-
ppery path of fraud due to collusion. While a processor putting some-
thing in for payment earlier than it should be paid is not a guarantee
that fraud will occur in the future, it is a poor practice and should not
be tolerated. Preventing this type of familiarity is another reason for
regularly rotating processors.

As you can see, none of the above recommendations require budget
allocations. All can be implemented without spending any money. Okay,
the not accepting invoices without the name of the requisitioner or a
purchase order number does require a postage stamp and an envelope.
But you can use a form letter and you don’t need budget approval for
postage stamps.

These are just a few examples of strategies any organization can im-
plement in their accounts payable department to make it a little more
efficient. And, we’re certain, if you put your mind to it, you can identify
a handful of other practices that will improve departmental productivity
without incurring a huge expense.
Segregation of Duties Problems

One of the more basic ways that fraud occurs in any organization is when the appropriate checks and balances are not in place. In accounts payable this is an important component of strong internal controls. There are certain functions that need to be segregated. For example, a person who can enter an invoice for payment should not also be able to set up a new vendor in the master vendor file or make changes to that file.

As a general rule of thumb, no employee, regardless of title or rank, should be able to handle two functions such that they would be in a position to defraud the organization through a manipulation of those responsibilities. So for example, authorized check signers should not be able to issue and/or print checks.

While a lot of this may seem like common sense, it can cause problems in small departments. In some instances it will not be possible to segregate duties appropriately without involving employees from another department. And that is what should be considered.

Even departments that can adequately segregate duties sometimes run into trouble when employees take vacation or are unexpectedly absent. Thus, it is a good idea to perhaps work with another group in smaller organizations.

And, finally, even where it appears there is adequate staff to segregate duties, there can be problems. If there is just enough staff, problems can arise when:

- There is a natural disaster
- The backup staff is out in combination with a planned absence
- One or more employees leave the company
- Planned staff reductions occur (because management rarely thinks about the effects on the segregation of duties when reductions are mandated)
Chapter 2 – The Basics of Internal Controls: In Practice

Review Questions

1. Which of the following is not a potential conflict of the segregation of duties principle?
   A. Having the same person who orders goods also approve invoices
   B. Having the same person issue 1099 Forms and print checks
   C. Having the same person who approves invoices also set up vendors in the master vendor file
   D. Having the same person who approves invoices also process invoices

2. Which of the following is no longer considered a bad practice?
   A. Petty cash boxes
   B. Playing favorites with employees making rush check requests
   C. Handling special requests from vendors
   D. Accepting invoices by fax and e-mail
Review Answers

1. A. Incorrect. By letting the same person who orders goods also approve invoices, an organization makes it very easy for an employee with the dual responsibilities to commit fraud.
   B. Correct. Having the same person issue 1099 Forms and print checks is not a potential conflict of the segregation of duties principle.
   C. Incorrect. Letting the same person who approves invoices also set up vendors in the master vendor file makes it easy for that individual to set up a phony vendor in the master vendor file and then submit a phony invoice for payment.
   D. Incorrect. By letting the same person who approves invoices also process invoices, the organization greatly weakens controls in the invoice processing function.

2. A. Incorrect. Petty cash boxes continue to be a poor practice, wasting time of an employee that could be better spent on a more value-add task.
   B. Incorrect. Playing favorites with employees making rush check requests is a terrible practice that not only weakens controls but is also likely to make for poor relations with those not getting the favored treatment.
   C. Incorrect. Handling special requests from vendors is not the place of accounts payable. Any special requests should be directed to management or purchasing.
   D. Correct. Accepting invoices by fax and e-mail was once considered a poor practice but is now a recommended best practice. This is because it is not possible to distinguish a copy from the original and so organizations have to rely on other techniques to guard against duplicate invoices.
Chapter 3
Fraud Prevention Controls and Practices

Learning Objectives

- Demonstrate the interaction between fraud and poor internal controls
- Reveal internal control practices every organization should use to deter fraud

Introduction

Rarely does a fraud occur in the corporate world when it does not signal a serious breakdown in internal controls, that someone was asleep at the switch. Alternatively, it could mean that the controls didn’t break down, they were so weak to start with that the only surprise is that fraud didn’t occur sooner. Thanks to the Association of Certified Fraud Examiners (ACFE), we have some statistics on corporate fraud. The ACFE refers to this type of fraud as occupational fraud. It is also called employee fraud. By providing an overview of what actually goes on in the corporate world, executives will be able to identify potential similar situations in their own organizations.

ACFE’s Biannual Report

The ACFE calls its report, the Report to the Nation. It is produced every two years. Cash misappropriations have always accounted for a large number of the frauds studied. These fell into three categories:

1. **Fraudulent Disbursements**, in which the perpetrator causes his organization to disburse funds through some trick or device. Common examples include submitting false invoices or forging company checks

2. **Skimming**, in which cash is stolen from an organization before it is recorded on the organization’s books and records

3. **Cash Larceny**, in which cash is stolen from an organization after it has been recorded on the organization’s books and records
Chapter 3 – Fraud Prevention Controls and Practices

The definitions of the types of fraud used above came directly from the Report.

**Fraudulent Disbursements**

The type of fraud that is most frequently related to accounts payable is fraudulent disbursements. Approximately three-quarters of frauds in the study involved some form of fraudulent disbursement. It is instructive to know how these schemes were further broken down.

The following information is from the Report.

- **Billing Schemes**, in which a fraudster causes the victim organization to issue a payment by submitting invoices for fictitious goods or services, inflated invoices, or invoices for personal purchases.
- **Check Tampering**, in which the perpetrator converts an organization’s funds by forging or altering a check on one of the organization’s bank accounts, or steals a check the organization has legitimately issued to another payee.
- **Expense Reimbursement Schemes**, in which an employee makes a claim for reimbursement of fictitious or inflated business expenses.
- **Payroll Schemes**, in which an employee causes the victim organization to issue a payment by making false claims for compensation.
- **Register Disbursement Schemes**, in which an employee makes false entries on a cash register to conceal the fraudulent removal of currency.

**Uncovering Fraud**

Most companies would like to believe that their own internal processes are strong enough to catch a disbursement fraud before the money goes out the door. Unfortunately that is not always the case. In fact, of the frauds that were uncovered after the fact, internal controls were not a key factor in detecting the fraud. And, when it comes to large cases, that is, those over a million dollars, the internal controls fell down on the job big time.

What is truly frustrating is that uncovering these crimes is often a matter of luck, or rather bad luck on the part of the crook. In a typical report, over one-third of all cases were discovered not because of any grand work on the part of company executives but rather because of a tip.
When you combine this with the significant number of cases that are discovered by accident, the matter gets more disheartening.

**Who Commits Fraud**

The traditional response to the question of who commits fraud against their companies was a long-term trusted male employee. This fact comes through every time the ACFE does this study.

Other factors likely to increase a crook’s proclivity for fraud include longer tenures with the company and gender, with more frauds committed by males than females.

**Dealing with Employee Fraud**

What the ACFE data demonstrates is that there is a need for strong internal controls. Here are some things that can be done to make it difficult for those few employees who would actually defraud their employers.

- **Establish an anonymous hotline.** There are two good reasons to do this. First, it is required by Sarbanes-Oxley. But there’s an even better reason. In reviewing the data above, an extremely high percent of the fraud discoveries came from tips. Make it easy and anonymous for employees to come forward.

- **Make sure that you have the appropriate segregation of duties.** While this will not prevent fraud, it will make it more difficult for potential crooks. With proper segregation of duties certain frauds become impossible to commit without collusion. Unfortunately, this just reduces the incidence of these crimes because occasionally, employees do get together to defraud their employers.

- **Insist that employees take their vacation time.** This is often when an ongoing employee fraud comes to light. Be suspicious of the employee who goes several years without ever taking a day off. The following will be hard to do if your firm only offers two weeks of vacation. Some banks require that employees take at least two consecutive weeks off. It is believed that all frauds will be discovered within that timeframe. If it is reasonable to make this a requirement, do so. And, if it is not, consider rotating employees off their normal assignments for cross-training purposes.

- **Put SIC-code limitations on p-cards.** This needs to be done with care and will prevent employees from making certain unauthorized purchases. However, be aware that the SIC code assignment is not perfect and you could end up creating a few problems.
Chapter 3 – Fraud Prevention Controls and Practices

- **Have a thorough investigation process before hiring a new employee.** Check references and verify former employment. While this will not completely prevent fraud, it will help when it comes to filing a claim in case of a loss. By being able to prove that you took reasonable care in your hiring practices you will have less trouble with the insurance company when filing the claim.

These issues all address your internal control structure.

**The Ugly Issue: Employee Fraud Prevention**

No one likes to admit it but occasionally an employee will steal from their employer. What’s even more disheartening is that year after year, the statistics demonstrate that the people most likely to steal from their employers are long-term trusted employees. Now before a few of our readers are offended by that allegation, let me point out that the thieves among us are few and far between. The problem is identifying the crook is not easy. They look like every other long-term trusted employee. Let’s take a look at some tactics every organization should employ to avoid an employee-theft disaster.

**The Big Problem**

The reason that organizations with strong internal controls are at such high risk is simple. Their employees know where the weaknesses are and know how to exploit them. What’s more, some organizations have great segregation of duties controls set up and then they negate the whole thing by giving one or two “trusted employees” access to everything. Often this works fine, but occasionally it does not.

The other misconception that makes it easy for in-house fraudsters is the sense of complacency some organizations have. They think “it would never happen here” or “we’re too big or too small.” More than one executive has had to eat his or her our-employees-would-never-steal-from-us words.

**Overriding Fraud Prevention/Detection Guidelines**

Ideally, your goal should be to deter all potential frauds. By this I mean the controls and monitoring you have in place are so stringent that no one even attempts to steal from your organization. The only problem is there is no way to measure frauds that were deterred so you never really know if you were effective on this front.
Chapter 3 – Fraud Prevention Controls and Practices

If you haven’t deterred a fraud and someone is bold enough to try, your next goal should be to prevent it. By this we mean catch the fraud before the money leaves your bank account. And, finally, if the money does get away, you want to have processes in place to identify the fraud and hopefully recover the funds. If you can’t recover the funds, at least you can put a stop to the fraud, if it is ongoing. Many employee frauds are continuing.

The following three principal guidelines will help you structure a framework that will serve to both deter and prevent fraud in your organization.

- Establish a strong internal control framework covering all facets of the payment function. This includes purchasing and receiving and of course, travel and entertainment reimbursements.
- Take segregation of duties seriously and make sure one person cannot do more than one part of the procure-to-pay process. Regularly review the scope of your employees’ access to ensure nothing has gone awry.
- Create a policy of zero tolerance when it comes to any type of fraud or abuse. The policy should come from the highest level executive in the organization along with a letter stating the organization intends to abide by it across all spectrums.

What Else
There are a number of other tactics savvy organizations use, although you’d be amazed to discover the number of businesses that ignore these principles. What follows is a look at three simple steps any organization can use to both prevent and detect fraud.

1) Mandatory Vacations. Anyone associated with any part of the payment function should be required to take five consecutive days off and someone else should perform their job function. The theory behind this approach is that in five days an ongoing fraud will unravel. Too often we hear staffers complain that their organization won’t allow them to take their vacation because everyone is overworked. This is just asking for trouble. Not only has the organization ignored the five-consecutive vacation tactic, there’s a good chance they have an unhappy employee.

2) Job Rotation. This strategy is a little harder to implement if you have a smaller department. And, to be blunt, there are certain
functions that cannot be rotated. Asking the corporate head of tax to switch positions with the company’s top lawyer is just not going to work. However, if you have more than three or four processors, rotating the suppliers they cover every six months or a year is very feasible. This makes collusion more difficult. What’s more, you get the added benefit of having more than one person knowledgeable about different accounts. If you do take this step, and we recommend that you do, it is imperative that you have a strict coding standard and the associates handling your invoices all process exactly the same.

3) **Surprise Audits.** First and foremost, we’re talking about surprise audits of the petty cash box, if you still have one. We recommend the elimination of the petty cash box as a best practice. But, assuming you have one, surprise audits are one way to detect and prevent games in that arena. But, that is not the only auditing you should be doing. Periodically audit your processors to ensure they are sticking to your rigid guidelines for handling invoices.

**If You Suspect Fraud**

The first thing to remember if you suspect fraud is that you could be wrong. Not everything is as it appears. So, before accusing do a little research and gather your facts. For if you accuse someone and you are wrong, you will never have the trust of that person again. What’s more, the organization’s relationship with that person will be strained for some time.

The second reason you don’t want to accuse someone before you have all the facts is that you may alert them, giving them time to either destroy needed evidence or flee. So, if you don’t accuse the person, what should you do?

For starters, immediately share your concerns privately with your boss. He or she will probably want to involve HR and do further research. HR may even bring in a fraud expert to help with the matter. Follow the guidance given by HR on this matter. It is something you really should not address on your own.

Employee fraud is something most of us would prefer happened to the other guy. Unfortunately, we cannot afford to take that view. By bulletproofing your processes you will go a long way towards making sure it doesn’t happen on your watch. But, if it does, then prepare to act appropriately.
Vendor Fraud

Fraudulent invoices are a serious issue for corporate America. New vendors should be verified. Have a process in place before a vendor is entered into the master vendor file. A form should be filled out and a W-9 obtained. The form should have all relevant data about the vendor. Ideally it should be submitted by one person and approved by a second. When it arrives in accounts payable (or wherever the master vendor file function resides) some additional verification should be done.

When verifying the information provided by the vendor, do not use that data. For example, instead of using the phone number on the application (it’s just too easy to provide an incorrect number) get on the Internet and find the number. Check out the address as well. Is it the same? If not, is there a good reason? For example, a company may have a “Pay To” address that is actually its lockbox.

The problem of fraudulent invoices for low-dollar items is one that continues to plague organizations everywhere. Crooks know that if they send a small-dollar invoice (say less than $100) many organizations will simply pay it rather than spend time getting it approved and doing a three-way match. In cases where best practices related to the master vendor file are not strictly followed, some processors will even set the company sending the fraudulent invoice up in the master vendor file.

Once a fraudulent invoice has been paid it is likely the vendor will send another and another. Strong internal controls, the employment of best practices and rigid coding guidelines are the best protection against this type of fraud.

Small Dollar Invoice Fraud

If you work in an organization of any size, you are probably bombarded with invoices for copier toner, yellow pages ads, and a variety of other items never ordered by anyone in your organization. Invariably, you will find that these invoices are for common items at highly inflated prices. Sometimes the goods will even be delivered to your organization and they will be of extremely low quality. This of course makes it a little more difficult because when accounts payable goes to do the three-way match, there is a receiving document. Of course, they can never figure out who ordered the goods. Unfortunately, in the case of toner and copier paper, the goods sometimes get mixed in with the company’s supplies and used … and paid for.
Chapter 3 – Fraud Prevention Controls and Practices

The control issue here is to have some sort of a tracking system for identifying who ordered goods when invoices come into accounts payable without a PO number. Some companies take the aggressive step of returning such invoices to the supplier. They have a policy that states that all invoices must either have a valid PO number or the name of the person who ordered the goods. Others take an even harsher stance. They insist on a PO number and demand that the supplier go back to the person who ordered the item and obtain one. While these practices work well in getting rid of fraudulent invoices, they do not make for good vendor relations.

From a practical standpoint it might seem that it would be reasonable to occasionally pay for these goods rather than invest a lot in setting up controls to avoid paying for them. The problem with that philosophy is that once you pay once, you go on the sucker list and will continue to get billed for inferior products not ordered.

W-9

Some accounts payable departments have trouble getting W-9s from their independent contractors. Because of heightened IRS scrutiny and fines for Form 1099 errors, requiring a W-9 from every vendor should be a no-brainer. However, in some cases there still is reluctance on the part of purchasing to ask suppliers for these documents. It is a control issue for three reasons:

1. It is needed in order to correctly report income and the company could be liable for the taxes owed by the contractor if it is not reported correctly.
2. You are not in compliance with Sarbanes-Oxley if W-9s (it’s the law) are not obtained and 1099s not issued in an appropriate manner.
3. By getting the W-9 and verifying the TIN (tax identification number)/name match you are confirming that the vendor is a legitimate entity.

Note: While you’ve confirmed that the vendor is legitimate, it does not mean necessarily that the invoices it sends your firm are legitimate. That should be addressed in your invoice processing standards and procedures.

From a control point, every company should have a No TIN, No Payment policy. If a vendor refuses to provide the TIN, simply withhold the appropriate taxes and pay it, if management insists. This will not win
Check Fraud

Check fraud is a huge problem in the United States. Even as more organizations move toward electronic payments, check fraud continues as the type of payment fraud most commonly attempted. If good controls are used along the entire check processing cycle, you will have diminished, but not eliminated, the potential for check fraud. To be perfectly honest, it is unlikely that the threat will ever be completely eradicated. It is an ongoing battle. Every time the corporate world comes up with a solution to a particular form of check fraud, the thieves move on and come up with another variation.

From both a protection standpoint and control issue, positive pay is considered to now be an essential tool in the fight against check fraud. While the number of companies using the many varieties of positive pay is growing, there are still a number who have refused to make the move. That is not wise.

Inactive bank accounts should be closed and any remaining check stock destroyed. This is not likely to be a favorite task among your staff. When we say destroyed, we are not talking about just throwing the checks in the garbage. They should be shredded. This is another reason why companies are moving to laser check stock. There is no check stock to shred when accounts are closed.

While there is some fraud associated with electronic payments, it is, at least at this point, much less common than check fraud. Thus, a move to the electronic world can help in this regard.

Segregation of duties should be strictly adhered to when allocating responsibilities for the various functions in the check production cycle. Each person should have their own password and user ID for any systems used. It is considered a weak control to allow employees to share passwords and it will get your organization in trouble during your Sarbanes-Oxley audit.

Six Practices that Enable Internal Check Fraud

Certain sloppy practices, especially when it comes to checks, actually make it easier for employees to commit check fraud. Allowing these practices to continue is effectively enabling the fraudsters who might be lurking in your corridors. And these are all things you can change without spending a cent. So what are these easy-to-fix processes?
Chapter 3 – Fraud Prevention Controls and Practices

**Practice #1** Allowing checks to be returned to the person who requested them. Without a doubt, this is the biggest enabler of them all. And this is a practice that is permitted in many, many organizations. While we concede there are rare occasions when the checks need to be returned, they are few and far between. We recommend that any organization that allows the return of checks develop a form to be included with the check. The form should be filled out by the person requesting the return and it should be signed by a very senior executive. It should contain a place for the person to enter the reason the check must be returned and not mailed. The form works in two ways to deter fraud. First, few employees will want to get it signed unless the check really must be returned. And, second, a crook will think twice (hopefully) about documenting the request if he or she intends to steal the check. Few thieves want to draw attention to themselves.

**Practice #2** Permitting rush or ASAP checks in all but the most urgent circumstances. When the data is analyzed, rush checks represent a disproportionate share of both fraudulent checks and duplicate payments. The reason is simple. Crooked vendors know if they call an organization’s accounts payable department and threaten to put the company on credit hold, the chance of a rush manual check being issued is high. So that is exactly what they do. Even if the call is legitimate, the chances are a second or third invoice has been issued before the vendor got desperate enough to call and demand a rush check. Inevitably, the original invoice eventually makes its way into accounts payable and sometimes gets paid. Part of the reason for this is the manual process sometimes results in records not being updated or entered correctly.

**Practice #3** Lack of appropriate segregation of duties. Whenever an employee is authorized to perform two tasks that serve as checks and balances to each other, it increases the risk of fraud. So, making someone a check signer and giving them access to check stock or the ability to approve an invoice increases the ease with which they could commit check fraud, if they wanted to. Thus, especially when it comes to an organization’s money, appropriate segregation of duties is crucial.

**Practice #4** Giving high level executives access to everything. In some ways, this is a subset of the issue discussed above. There are organizations that go out of their way to set up the appropriate segregation of duties and then give either a high level executive or the accounts payable manager access to everything. This completely negates everything else done. When questioned about it, inevitably the response is that the per-
son in question is a trusted employee. Well, guess who commits most internal fraud? Long-term trusted employees!

**Practice #5** Making all high-level executives authorized signers. In some organizations all vice presidents are put on bank accounts as signers, even if they never sign and check signing is not part of their job. As in the discussion above, this can negate the segregation of duties the organization strove to set up.

**Practice #6** Poor master vendor file practices. So many organizations ignore their master vendor file not realizing they are providing the perfect hiding place for employees looking for ways to defraud them. This is especially true when the file is never cleansed and vendors not used in over 12 or 14 months deactivated. It is easy to put this task off when other issues are pressing. But don’t; you are only asking for trouble by leaving inactive vendors in the file. Use of strict coding standards also helps. When was the last time your master vendor file was cleansed?

As we said at the beginning, these practices are fixable at virtually every organization – and the fix doesn’t cost a red cent. How many of these practices still exist in your organization?

**Demand Draft Fraud**

This little known payment device was designed to accommodate legitimate telemarketers who receive authorization from consumers to take money out of the consumer’s checking account. This payment alternative is very similar to writing a check – except that it requires no signature. In place of the authorized signature on the check the words “signature not required, your depositor has authorized this payment to payee” or similar wording is used. Since the check processing areas at banks are completely automated, the signature line is virtually never checked.

In the telemarketer example this is a creative payment approach that enables the transaction to proceed smoothly. Demand drafts are also sometimes referred to as remotely created checks. You can see there is potential for check fraud in this arrangement but then anytime a check is used for payment, there is also the possibility for abuse. Once the thief has the account number and the name of the account owner, check fraud is merely a matter of conscience, opportunity, and a few dollars for technology.
Chapter 3 – Fraud Prevention Controls and Practices

An outfit called Qchex.com dramatically lowers the bar for entry. No longer is it necessary to have those few dollars for technology. It’s not even necessary to know the name of the account holder – only the account number and the routing code. Accounts can be opened by individuals, merchants who want to accept checks, and businesses and institutions who want to send checks to suppliers or receive payments from customers.

Unfortunately, it does not verify that the person issuing the check is the actual account holder.

Qchex would like you to register all your organization’s bank accounts with them – to prevent someone else from registering them under their own name. To me anyway, that just seems like positive reinforcement for bad behavior. Better to monitor the activity on your bank accounts daily as part of your cash-flow monitoring and control points.

Concluding Thoughts

Fraud is a serious problem for all organizations. Often, it indicates that internal controls were less than they should be. While Sarbanes-Oxley has made internal controls a key focal point, consideration of the losses that can accrue because of these frauds is a serious consideration. As the numbers from the ACFE demonstrate, successful frauds typically involve such serious amounts of money that the corporate world is well advised to take as many precautions as it can to prevent them.
Review Questions

1. According to the Association of Certified Fraud Examiners, which of the following is an effective way to prevent/detect fraud?
   A. Anonymous hotlines
   B. Insist employees take their vacation time
   C. Employ appropriate segregation of duties
   D. All of the above

2. Which of the following will not protect against check fraud?
   A. Using positive pay
   B. Closing inactive bank accounts
   C. Employing appropriate segregation of duties
   D. Using p-cards

3. Which of the following does not enable internal check fraud?
   A. Returning checks to requisitioners
   B. Rush checks
   C. Strong master vendor file practices
   D. Giving high level executives access to everything
Review Answers

1. A. Incorrect. While anonymous hotlines certainly help prevent or detect fraud, they are not the only item on this list that does so.
B. Incorrect. While insisting employees take their vacation time certainly helps prevent or detect fraud, it is not the only item on this list that does so.
C. Incorrect. While employing appropriate segregation of duties certainly helps prevent or detect fraud, it is not the only item on this list that does so.
D. Correct. All of the above are effective ways to prevent or detect fraud.

2. A. Incorrect. Use of positive pay is one of the best ways to guard against check fraud.
B. Incorrect. Closing inactive bank accounts helps protect against check fraud.
C. Incorrect. Employing appropriate segregation of duties is key to preventing check fraud committed by insiders.
D. Correct. Use of p-cards may reduce the number of checks written, but has no impact on check fraud.

3. A. Incorrect. Returning checks to requisitioners is a leading cause of internal check fraud. While most checks returned in this manner are not stolen, enough are to make it a poor practice.
B. Incorrect. As above, too many rush checks turn into fraudulent transactions. Hence, this is another reason organizations are advised to limit, if not eliminate, rush checks.
C. Correct. Good master vendor file practices make it a little more difficult for insiders to defraud their organizations.
D. Incorrect. Giving high level executives access to everything will make it easier for those few to commit check fraud.
Chapter 4
Internal Controls and Duplicate Payments

Learning Objectives

- Identify weak control practices that don’t curtail duplicate payments
- Show how poor controls make duplicate payments more likely to occur

Introduction

One of the unintended side effects of poor internal controls is the increased likelihood of duplicate payments. One of the dirty little secrets in the corporate world is that few duplicate payments are ever returned. That’s right; most vendors don’t return those payments. Initially they sit on the vendor’s books as open credits but eventually many open credits are used by vendors at the end of the quarter or fiscal year to clean up open outstanding disputed invoices, accrued late fees (which you vehemently refuse to pay) and unearned early payment discounts.

Practices put in place to prevent duplicate payments also tend to tighten controls. So, let’s take a look at some practices every organization should be using.


As the accounts payable world continues to evolve, some of the tactics used in the past to prevent duplicate and erroneous payments no longer work. Some of the old standbys no longer cut the mustard. It would be nice if this overpayment problem would go away; it’s been with us forever. Alas, that does not seem likely to happen. So, it is imperative that readers regularly review their procedures to make sure that they are not relying on practices that no longer prevent those nasty duplicates from occurring. What follows is a look at practices that no longer do the job as well as a list of those that do.
Chapter 4 – Internal Controls and Duplicate Payments

What Doesn’t Work

- Relying on the “our system will not accept duplicate invoice numbers” control. Even if your accounting system has this feature, virtually every processor knows that if they simply add a blank space, a period or a letter to the end of the invoice number, the “new” invoice will be accepted. Unfortunately, many routinely use this tactic to force invoices through.

- Never paying from copies or faxes. While this was a reasonable approach several years ago, advances in technology make it possible to produce numerous “original” invoices. What’s more, some suppliers are insisting on emailing or faxing invoices to save on postage. Upon reflection, receiving invoices electronically or by fax gets them into your process sooner. This makes the earning of early payment discounts a bit easier and avoids invoices lost in the mail – both internal and external.

- Relying on the memory of the processor. This is just as bad an idea today as it was years ago, yet many organizations still expect their processors to recognize duplicates. Let’s just say this about it: It doesn’t work.

What Does Work

- Require full backup for every single rush check.

- Go through the same rigorous three-way match, extinguishing the PO and receiver etc. when issuing a rush check as you would with an invoice processed for payment through normal channels.

- Eliminate all but the most essential rush checks. The number of rush checks issued each week should be in the single digits. If not, review your processes to determine the problem.

- Make sure POs are extinguished when payment is issued.

- Coordinate processes for payment made by checks, p-cards and ACH. Make sure the same rigorous procedures are used regardless of the payment mechanism.

- Have stringent coding standards for data in the master vendor file.
Chapter 4 – Internal Controls and Duplicate Payments

- Regularly deactivate inactive vendors in the master vendor file.

- Have a rigorous coding standard for invoice data entry that is constructed using the same approaches as your master vendor file coding standard.

- Make sure all your processors use the same coding standards and procedures and none develop their own workarounds.

**Concluding Thoughts**

Once you’ve done everything you can to eliminate duplicates, call in a contingency fee auditor to take a look at your books. Let them look for duplicates. If you are correct and you’ve done a good job, they’ll find very little and you’ll owe them even less. But, if a loophole has developed, they could find a significant amount of money that is rightfully yours. Yes, their fee could be higher than you’d like. But, at least you’ll recover a good portion of your money and you should be able to find the weak link in your processes that allowed the problem in the first place.

The auditors should give you a report detailing any weaknesses they find. You can use it to tighten your processes. It would be nice if vendors would return duplicate and erroneous payments but in reality that happens in only a small fraction of cases. That’s why savvy professionals watch their procedures like a hawk and crack down immediately when they identify a weak link.

**Best Practices to Avoid Duplicate Payments and Check Request Fraud**

Ahhh...check requests, those ubiquitous forms used to request payments for all sorts of things. Theoretically a solution (by making it easy to request a payment when an invoice is missing), in reality it can create numerous headaches for accounts payable, not to mention causing duplicate payments by the boatload. Here’s a look at some of the problems surrounding check requests and a few suggestions on avoiding them.

**Background**

Check requests are used in most organizations to request payment when an invoice is not available or was never provided. Ideally, there should be backup documentation augmenting the check request and providing details regarding the payment amount, the payee, and the reason for the payment. Since most payments made on check request forms will not go
through the rigorous three-way match in accounts payable, the documentation supporting the check request is of utmost importance.

The one exception to this is those organizations that require a check request for every single payment. This is not a best practice, although some organizations with unique industry or regulatory requirements might find it necessary to go this route.

**Where Check Requests Cause Problems**

Check request forms are often used to accommodate rush check requests. These are one-time payments made to vendors outside the normal invoice submission process. Typically this happens when a payment is late and the upset vendor threatens to put the organization on credit hold.

Whether the check request form is used for a rush check or simply because the invoice has been misplaced, if the proper documentation is not attached the chances for a duplicate payment skyrocket. Ideally the attached documentation should be the original invoice. Of course, if it were available, there might be no need for the check request form.

Without the invoice to perform the three-way match, the purchase order and receiver often remain open on the organization’s books. This can blossom into two types of problems. The most obvious is a duplicate payment made when the invoice finally shows up and is paid in accounts payable.

The less obvious issue is what happens to the open receivers and purchase orders when the financial statements are prepared. There is a chance that the states could view open receivers as unclaimed property.

The final problem relates to fraud. Alas, a great number of fraudulent payments, more than we’d like to think, are issued on check requests. How is this possible? The most obvious answer is a crooked employee fills out the check request form and either convinces an authorized signer to sign it or forges the signature himself.

The other way that fraud occurs with a check request form is in response to an irate vendor claiming non-payment. Some vendors have learned if they get on the phone and are generally abusive with the accounts payable staff threatening credit holds, they can sometimes get a harried controller to sign off on a check request form authorizing the payment. In one of the most egregious examples of this type of fraud a vendor pulled this screaming stunt every month for 18 months – getting double payment for each one. With murky documentation attached to each form, it was difficult to find the duplicates until the entire vendor file was pulled and reviewed.
Best Check Request Practices

There are a number of steps any organization can take to make the check request form work as it is intended without introducing the problems discussed above. Begin by requiring documentation for every check request form. If an invoice, or copy of an invoice, is not available, attach a copy of the contract, an e-mail detailing requirements, or whatever is available. Great care should be taken to avoid sending in the form without any supporting documents.

In the extreme cases where no documentation is available—and you know that will happen at some point—require an extra signature of a very high-level executive within the organization, perhaps the controller or the CFO. The person making the request should be ready with a really good explanation for why the check should be issued without documentation. Requests without documentation should be few and far between.

If there are outstanding POs and receivers related to these requests, that information should be included on the form so accounts payable can extinguish them when the payment is made.

If by some miracle, there is an invoice attached to the check request form, perform the normal three-way match extinguishing both the purchase order and the open receiver.

Reducing the Number of Check Request Forms

If you only have a few check request forms each month to process, there is, in all likelihood, little you can do to decrease the number of them. Like rush checks, a small number is an inevitable part of doing business.

If you get more than a few, for several months, track the requests keeping a log noting:

- The requestor;
- The payee;
- The date of the request; and
- The reason for the request.

When you have the data for a few months, take it out and analyze it. Are most of your requests coming from a few requestors? In that case you might want to have some discussions with those involved to determine where the problem lies.

But before you do that, take a look at the vendors receiving the payments. Are a suspiciously high number of these requests going to the same vendor? This could mean one of two things. The less sinister explanation is that there is a problem somewhere in the process that needs
to be fixed so the vendor can receive payment through the normal cycle. The more ominous reason is that there is an ongoing fraud.

If you suspect fraud, do not approach the individuals involved. Get all your facts lined up, ask your immediate supervisor to review them, and if you both agree something is fishy, get HR involved. They will know the correct way to approach this situation. Discretion is crucial in these cases for two reasons. First, you could be wrong and, second, if you are correct, you don’t want to tip your hand before the experts decide how to approach the matter.

Check request forms are a necessary evil in the accounts payable world. Work hard to implement best practices surrounding them and the troubles they cause will be held to a minimum.

**Five Scenarios that Cause Duplicate Pays and What You Can Do To Stop Them**

New improved payment processes can translate, unfortunately, into new ways to make duplicate payments. The same goes for some of the new wonderful ways to process invoices. This is not to say there is anything wrong with these new processes; quite the contrary. It simply means that the professionals who handle payments must be extra careful to ensure that when making payments, they take the time to ensure that the appropriate controls are put in place to guard against duplicate payments. New technologies sometimes mean new controls. In this section we’ll look at five scenarios that will open the door for duplicate payments if you are not careful.

**Background**

When the only way that bills got paid was to receive an invoice and issue a check, it was easier to control duplicate payments. Let me make it perfectly clear that I am not saying it was easy to prevent duplicates; that is never the case. But there were fewer issues to be concerned about. In this new payment world we find ourselves in, every payment professional needs to be concerned about:

- payments not being made twice using two different payment types
- other professionals outside accounts payable making payments but not necessarily using the same rigid standards used in accounts payable to ensure duplicate payments are not made
unscrupulous employees or vendors taking advantage of the increased “opportunities” to hide a duplicate payment and using them to enrich themselves at your organization’s expense.

**Scenario #1: Credit Card Payments and Invoices**

This issue has been with us for a few years and may be the hardest to fix. Certain vendors claim they cannot suppress the printing of invoices and continue to send invoices even though they were paid at the point of purchase with a credit card. Let’s assume this is true. If you suspect it is not, you should investigate whether your organization wants to continue doing business with the vendor. It is recommended that only one type of payment method be used with each vendor. While this works in theory, in practice it is not always possible.

Assuming it is not possible to limit payment methodology, there are two steps you can take to guard against paying these vendors twice. First, teach your processors to check invoices closely. Many of the vendors who cannot suppress the printing of the invoice will mark it with a note saying it was paid by credit card. True, many of these notes are in very small print so your processors will have to look closely to find the note.

If this is not sufficient, consider setting up a separate post office box for those vendors who you sometimes (or always) pay with credit cards. Invoices that arrive at this box can be checked against credit card statements to ensure payment is made only once.

**Scenario #2: Extinguishing POs and Receivers**

With the widespread introduction of ACH payments, responsibility for making payments is expanding outside accounts payable. That’s fine, if that works for the organization. However, and this is a big one, it is imperative that whoever makes the payment takes all the steps that might be taken by a professional in accounts payable. This means using the same rigid coding standards and extinguishing both the PO and the receiver.

We have heard numerous stories about these steps not being adhered to – simply because the professionals involved are not aware of them or do not realize their significance. If these items are left open and a second invoice shows up, the odds of it being paid a second time skyrocket. And there is a new issue looming.

Open receivers are the latest target of unclaimed property auditors. This has become a hot issue for some of the big warehouse stores. Some state auditors have taken the stance that open POs represent unclaimed property and the value of them should be remitted to the states. To call this ugly would be an understatement.
Scenario #3: Travel and Entertainment Reimbursement and Invoices

Occasionally an employee will pay for something with a personal credit card (or cash) and put in for compensation on his or her T&E expense reimbursement report. There is absolutely nothing wrong with this and in fact it is a recommended approach for small dollar items – another way to get those small dollar invoices out of the accounts payable department.

This assumes that the approach truly does get those small dollar invoices out of accounts payable. Occasionally, an employee has been known to put in for reimbursement on the expense report and submit an invoice for payment. Most of the time this is not an oversight on the part of the employee or the vendor, but fraud. It is very difficult to catch.

Any time this happens, the employee in question’s expense reports should be pulled for the last 18 months and reviewed to see if this was an honest mistake or is part of an ongoing fraud. It is possible that the vendor is the one pulling a fast one so be careful about pointing a finger – but investigate thoroughly.

Scenario #4: Check Request Forms and Invoices

Different organizations rely on check request forms to different levels. Some use them rarely and others rely on them quite frequently. The problem arises when the backup is scanty (or even nonexistent) and is for an invoice. If the invoice is not attached and/or if that information is not keyed into the system, a duplicate payment will invariably be made when that original invoice eventually finds its way into accounts payable – and you know it will.

In fact, research shows that rush checks (often issued with a check request form) are one of the leading causes of duplicate payments. We realize that check request forms and rush checks are here to stay. What we recommend is a stringent requirement for backup and that invoice information be keyed at the time the check is issued. Otherwise, prepare for an onslaught of duplicates.

Scenario #5: Printing Electronic Invoices

Are you part of the electronic revolution receiving invoices electronically? Do some of those invoices arrive as attachments to e-mail? If so, make sure your processors are not printing them before processing and then inadvertently processing the printed invoice as well as the electronic one.

If you have very rigid standards for entering invoice numbers and coding standards this should not cause you problems. But even the best
processors sometimes let one slip by. One manager we know took the print key off her processors’ computers to put an end to the printing of invoice information. She was concerned about the loss of productivity so the chance to reduce potential duplicates was just a side benefit.

**Closing Thoughts**

Clearly as the payment world evolves there will be loopholes that permit duplicate payments, if those using the new methodologies are not careful. By taking the time to set up the right controls and make sure that all affected parties adhere to the procedural instructions, you should be able to limit the problem.
Chapter 4 – Internal Controls and Duplicate Payments

**Review Questions**

1. Which of the following will protect your organization against duplicate payments?
   - A. Relying on your accounting system not to accept invoices with duplicate invoice numbers
   - B. Never paying from a copy
   - C. Stringent coding standards
   - D. Relying on the memory of the processor

2. Which of the following is a reason why invoices are sometimes paid twice?
   - A. Inadvertently paying with a credit card and then submitting the invoice for payment
   - B. Inadvertently putting in for reimbursement on an expense report and then submitting the invoice for payment
   - C. Double printing electronic invoices and processing both
   - D. All of the above
Review Answers

1. A. Incorrect. Relying on your accounting system not to accept invoices with duplicate invoice numbers never worked, despite the fact that it seems like a great idea. The reason is that too many processors simply add a space or a dot at the end of the invoice number to force the invoice through.
   B. Incorrect. Never paying from a copy no longer works because so many copies look like an original invoice.
   C. Correct. Insisting on stringent coding standards is probably the best defense any organization has against duplicate payments.
   D. Incorrect. Relying on the memory of the processor never worked as a way to prevent duplicate payments.

2. A. Incorrect. Inadvertently paying with a credit card and then submitting the invoice for payment is just one of many reasons why invoices are sometimes paid twice.
   B. Incorrect. Inadvertently putting in for reimbursement on an expense report and then submitting the invoice for payment is just one of many reasons why invoices are sometimes paid twice.
   C. Incorrect. Double printing electronic invoices and processing both is just one of many reasons why invoices are sometimes paid twice.
   D. Correct. All of the above are ways that invoices get paid more than once.
Chapter 5
Where Internal Controls Break Down

Learning Objectives

- Pinpoint places where internal controls most commonly break down in the accounts payable function
- Reveal reasons controls sometimes fail

The Internal Controls Breakdown: The Overlooked People Issues

Some of our internal control breakdowns occur in often-overlooked people issues. They are either tasks we forget to do or ones we dismiss as not being critical. Whether they occur through benign neglect or oversight, every organization needs to take steps to eliminate these potential control breakdowns. In this chapter we’ll take a look at common control failures related to segregation of duties, employee departures and expense reimbursements.

Segregation of Duties

One of the key tenets in a good internal controls program is the appropriate segregation of duties. When it comes to accounts payable, this ensures that no one individual handles or has access to more than one step in the procure-to-pay process. This makes it more difficult for fraud to slip through without some sort of collusion. Two of the most common times when appropriate segregation of duties are overlooked are 1) when an employee is promoted and 2) the exceptions. Let’s take a look to see what can go wrong in both these cases.

While we are strong advocates of promoting from within, we caution everyone that when it is done, care should be taken to ensure that the access the employee had in his or her old position is cut off. So, if you have someone who was processing invoices and promote them to handling the master vendor file, cut off their ability to process invoices right before you give them access to making changes to the master vendor file. This one little step is often forgotten in numerous organizations. And, this is not just a mistake made in accounts payable. Organizations make it across the board in all departments.
The second problem that occurs more frequently than we’d like to admit is when companies make one exception to the segregation of duties assignments. Usually they’ve done an exceptional job setting up their delegations for segregation of duties and then ruin it by making one big exception, usually for either the accounts payable manager or the controller. Unfortunately, this negates all their good work. They usually have a plausible excuse for this departure, but not a good enough one. At the end of the day, the need for appropriate segregation of duties trumps ease of operation and the like.

**Departing Employees**

Whether the company is dancing the proverbial jig or crying buckets over an employee who is leaving the company, the steps it should take with regard to internal controls are the same. These steps are rarely taken. When someone leaves an organization, you should:

1. Immediately cut off their system access.
2. Get all credit cards back. This includes T&E cards, fuel cards and any corporate procurement cards.
3. Notify the bank immediately and cancel all cards. Remember, just because the employee returned the credit cards, doesn’t mean the credit card numbers and expiration dates weren’t written down before the cards were turned in.
4. If the departing employee had any signing rights for checks or could approve or initiate wire or ACH transactions, immediately suspend those rights. Call the bank and follow up with a written notification.
5. If you enter your employees in the master vendor file for expense reimbursement purposes, don’t forget to deactivate them when they leave the company so they can’t slip through one last unauthorized expense report.

**Expense Reimbursements**

The IRS has strict requirements about what’s required as documentation of expenditures for accountable plans. So, when it comes to expense reimbursements, it’s not only a matter of internal controls, it’s also a matter of endangering the organization’s accountable plan status. And to be fair, this is also an issue of what the organization feels it should pay for and what the employee should pay for.
The first concern is that of who attended a business event. IRS requires the listing of every attendee at a business event. This information should include not only their name, but their title, name of their organization and business relationship with the organization. Your employees should include this on their expense reimbursement requests. Verifying this is difficult if not impossible, but you can get an idea of how many people attended – if you get the detailed meal receipt. That will show how many main courses were ordered. This is not a perfect control but probably the best you can do. We should also note that not every organization is willing to do this kind of verification although we are seeing a growing number request the detailed meal receipt.

The detailed meal receipt can also be used to verify that no employee has surreptitiously added a gift card when taking a guest out for a meal at the company’s expense. One would hope that if the organization required the detailed meal receipt, employees would be smart enough not to include a gift card for themselves.

The last overlooked expense reimbursement issue involves what was really ordered.

When an employee submits an expense report with only the total amount showing, there’s no way to tell what actually was ordered. Two anecdotal examples bring home this point. One involves an employee who frequently put in for business entertainment on a Friday night. When the detailed meal receipt for one particular Friday night was obtained it showed two adult meals and two kiddie meals. This makes one wonder who was actually at that dinner. The second involved what was supposed to be a job discussion. The detailed receipt showed a plate of wings and a dozen beers.

Do all employees play these games? We do not believe so; in fact, we think the number that does is a small minority. However, we have seen an increase in the number of companies requiring the detailed meal receipt and we can only think it is to address issues such as those discussed here. Please remember that just because you require all receipts or the detailed meal receipts doesn’t mean you have to check them all. The purpose of requiring the receipts is to serve as a deterrent to those employees thinking of ordering something they shouldn’t. Spot checking of receipts is typically sufficient.

Strong internal controls protect any organization. It is important to make sure yours cover the often overlooked people issues.
Internal Controls Breakdown: The Payment Process

Strong internal controls are the underpinning of a payment process that doesn’t leak profits and runs as efficiently as possible. They are a big component in any fraud prevention program and as an added bonus, go a long way in preventing duplicate payments. But occasionally, controls break down. This most typically happens when the process in question is something outside the norm. A company may have great controls for the bulk of its transactions but those one-offs and infrequent transactions can cause control problems if thought is not given to incorporating good processes for those rare occasions. When it comes to payments this can happen in three arenas; wire transfers, payments made outside accounts payable and recurring payments. Let’s take a look at each.

Wire Transfers

Traditionally, wire transfers were made when the payment amount was large and/or the payment was going across borders from one country to another. With the growing use of ACH some of the wire activity has migrated away to the ACH arena. Wire transfers are relatively expensive and result in next day availability of funds. They are made just as often outside of accounts payable as they are by individuals working in accounts payable.

The issue is complicated by the fact that often wire payments are made for no-purchase-order items. So, instructing organizations to use the proverbial three-way match and make sure POs and receivers are extinguished (one of the best ways to prevent duplicate payments of PO related invoices) is worthless. Since these payments are often for large dollar amounts, a duplicate payment is this arena can be costly indeed.

Very occasionally, a wire transfer will be made to cover a rush payment for an invoice that was not paid on time. When this is done, it is critical that the three-way match be completed and the purchase order and receiving document extinguished.

Here are a few controls you can add to your process to ensure wire transfers are paid only once:

1) Make sure there is adequate backup for each wire transfer, even though no three-way match is being completed. This way should someone suspect a duplicate, there will be sufficient information to make that determination.

2) If possible, limit the payment for particular vendors to one type (wire, ACH, check or p-card). If attempts are made to use another payment type, have the system alert the processor.
3) Periodically review the accounts of vendors typically paid by wire. This might include loan payments, interest payments, and leases.
4) Alert processors to vendors who are usually paid by wire so they can thoroughly research any invoice that comes in for payment using another payment vehicle.
5) Periodically run your list of wires against lists of other payments made looking for duplicates. Research any potential duplicates.

You should note that many duplicate payment auditors will automatically perform the last step as part of their recovery efforts.

**Payments Made Outside Accounts Payable**

While wires in many companies have always been made outside accounts payable, traditionally they were the only payments not made by the accounts payable staff. Since the items covered by wires were usually pretty easy to identify, the chances of a duplicate payment slipping through were not high, assuming the organization took a few basic steps to protect itself.

The advent of ACH is changing that situation. They are cheaper than both wire transfers and paper checks and appear to be the wave of the future for corporations making payments. Approximately 20% of all organizations have ACH payments initiated outside of accounts payable. Since the items being paid by ACH are the same as the items being paid by the accounts payable staff, problems can arise under a few circumstances. If the outside staff does not use the same strong rigid controls used by accounts payable, duplicate payments will arise. Specifically this means the staff outside accounts payable must:

1) use the same rigid coding standards used in accounts payable;
2) perform the three-way match; and
3) extinguish purchase orders and receivers once the payment has been made.

If they do not follow the same standards, and an invoice appears in accounts payable, it will be paid, for the staff will have no way of knowing it had already been addressed. Thus it is imperative that those organizations making payments outside accounts payable sufficiently train the staff making those payments so duplicates don’t slip through.
Recurring and Repetitive Payments

There are a whole variety of items that require the same payment to be made every month. This might include things like rent, equipment leases, loan payments etc. Depending on your industry, there might be other items as well. Rather than create a new voucher each month for the same exact payment, some organizations set these items up to be automatically paid on a recurring basis.

If care is not taken and an end date included in the arrangement, the organization could find itself paying for something it no longer was obliged to pay for. Hence it is critical that when recurring payments are set up, an end date be included rather than have them go on without a light at the end of the tunnel.

The second problem that can occur is when the item is paid off early. In the case of a loan this might be an early payment or a renegotiation to get a lower rate. In the case of a lease, occasionally the lessor will entice the lessee into a new lease for better/newer equipment or whatever. Both of these situations are fine as long as the initial payment is stopped when the new payment stream begins. More than occasionally this does not happen and the original payment continues as well as the new payment.

You can run into the same problem with repetitive payments for services, phones etc. If someone doesn’t stay on top of these accounts the organization can find itself paying for services never used. For example, if the phone company isn’t notified when a phone line is no longer needed, it will continue to bill for it. For most organizations this isn’t a problem as it uses all its phone lines. But those who have a significant downsizing initiative may find themselves paying for services not being used. The same can be said for subscriptions, online services, and specialized database access for employees who have left (voluntarily or not).

Strong internal controls protect any organization. It is important to make sure yours cover not only the functions used on a regular basis but also those only used occasionally.

Five Reasons Why Internal Controls Sometimes Fail and What You Can Do to Make Sure This Doesn’t Happen in Your AP Department

Strong internal controls are the first step towards safeguarding the organization’s assets. When it comes to accounts payable, these controls guard against duplicate payments, erroneous payments and fraudulent payments. More than occasionally controls fail, not because someone is deceitful but rather due to a lack of understanding of the principles or
how they should be implemented. Let’s take a look at five common reasons internal controls fail.

**Reason #1:** Lack of appropriate review. This happens frequently with approvers signing expense reimbursement reports. Unfortunately, it also sometimes happens with purchasers approving invoices for payment.

**Solution:** Make managers responsible for what they approve – really. A few organizations have gone so far as to make it a firing offense if a manager approves an obviously fraudulent expense reimbursement. Most are not willing to go that far. Some are making it a matter for consideration when calculating the annual salary increase.

**Reason #2:** Incomplete segregation of duties. When it comes to processing invoices for payment, it is critical that no one person can perform more than one leg of the operation. For example, someone shouldn’t have the ability to enter invoices and sign checks. Too often we see companies set up the segregation of duties correctly and then make one or two “exceptions,” usually for a trusted employee such as the controller or accounts payable manager. Smaller accounts payable departments are sometimes challenged when it comes to setting up processes so duties are appropriately segregated.

**Solution:** The first step is to realize that there can be no exceptions when it comes to separating duties. Remember, internal fraud is most likely to be committed by a long-term trusted employee. Regardless of the operational efficiencies that can be achieved by allowing these exceptions, the more important issue of fraud protection should override. So, allow no exceptions. Smaller organizations sometimes have to look outside accounts payable to help. Some common examples of segregating duties by taking advantage of help from other departments include putting the master vendor file elsewhere in accounting and having Treasury responsible for getting signatures put on checks (if they are not signed as part of the check printing cycle).

**Reason #3:** Incomplete knowledge regarding policies and procedures. Too often we don’t realize the knowledge we have regarding how the accounts payable department operates has been accumulated over a long period of time. When newcomers are hired, they are typically given a day or two of training before being hurled into the mix to sink or swim. Most do a fairly good job but occasionally do miss a fine point or a procedure that only comes up once in a blue moon.
**Solution:** Probably the best approach any organization can take when it comes to ensuring complete knowledge about policies and procedures is to have a detailed, up-to-date policy and procedures manual. Give this to every processor as a reference guide and they can check it when those odd transactions show up. Encourage even your seasoned staff to refer to the guide when they are not 100% certain how something should be handled. Refresher training is another step you can take to ensure you don’t run into this problem.

**Reason #4:** Sharing passwords. It is quite tempting when an employee is heading out for vacation to ask that employee to share his/her password with another employee who will take over the vacationing employee’s responsibility. Resist the temptation. This is a slippery slope and whether sharing a password for a vacation or on a regular basis, it is a bad idea. It completely obliterates the audit trail, making it impossible to tell who did what.

**Solution:** The answer is obvious. When someone needs to take over the responsibilities of another employee, set them up with their own password. When the vacation is over and if you don’t need/want that employee to have access, cancel the access. This may be an extra step but it protects your internal controls.

**Reason #5:** Overrides. Management overrides of transactions are an easy way to fix mistakes. Unfortunately, they are also an easy way for an unscrupulous employee to adjust the records to cover up a fraud.

**Solution:** If at all possible, do not use management overrides to fix a problem. Go through the more laborious route of doing the correct accounting to take care of the issue, even if it means owning up to some really stupid mistakes. If your organization does not want to go that route and insists on allowing overrides, then at a minimum have a form explaining the reason for the override and have it signed by at least one executive other than the person putting through the override. Internal controls are an important component of any organization’s fraud prevention program. They also go a long way toward helping ensure accurate records and financial statements. Don’t let the senseless issues discussed above get in the way of your controls. Implement the solutions suggested to strengthen your controls rather than weaken them.
Chapter 5 – Where Internal Controls Break Down

Review Questions

1. Which of the following will not help ensure a payment is only made once?
   A. Get adequate backup for all wire transfers
   B. Periodically run a list of wire transfers made and check them against payments made by check looking for duplicates
   C. If possible, limit the payment type for each vendor i.e. paying each only by credit card, wire, check or ACH
   D. Have all the wire transfers done in Treasury

2. Which of the following is not a reason internal controls sometimes fail?
   A. Incomplete segregation of duties
   B. Inadequate knowledge of procedures
   C. Sharing of passwords
   D. Use of p-cards
Review Answers

1. A. Incorrect. Getting adequate backup for all wire transfers is something that will definitely help limit the chances of a second payment.
   B. Incorrect. Periodically getting a list of wire transfers made and checking them against payments made by check looking for duplicates is an excellent way to identify potential duplicates.
   C. Incorrect. If possible, limiting the payment type for each vendor *i.e.* paying each only by credit card, wire, check or ACH will greatly reduce your chances of making a duplicate payment
   D. **Correct.** Having all the wire transfers done in Treasury will neither help nor hurt your chances of making a duplicate payment.

2. A. Incorrect. Incomplete segregation of duties is one reason internal controls fail. They make it easier for one person to get around the process.
   B. Incorrect. Inadequate knowledge of procedures is one way that controls fail, as those handling the transaction fail to take necessary precautions.
   C. Incorrect. Sharing of passwords is a complete negation of internal controls and elimination of a failsafe control.
   D. **Correct.** Use of p-cards will not impact internal controls if they are used correctly.
Chapter 6  
Purchase Orders and Their Role  
in Internal Controls

**Learning Objectives**

- Pinpoint places where purchase orders cause control problems
- Identify common purchase order problems and show how they can be fixed

**Introduction**

At the head of all accounts payable operations is the invoice processing function. In fact, given the diversity of the functions handled in accounts payable departments, some experts maintain that the only one constant across all thresholds is invoice processing responsibility.

Roughly speaking, invoices can be broken down into two categories:

1. Those requiring a purchase order; and  
2. Those without a purchase order

The purchase order is the first line of defense (as well as the first place where controls can start to go astray) in the invoice processing function.

**Purchase Orders**

As the title implies, purchase orders (PO) are forms, usually filled out in purchasing, that detail the parameters of a purchase transaction. They are usually sent to the supplier and in an ideal situation, a copy is also sent to accounts payable. In today’s electronic environment, these forms can be transmitted electronically and/or filed in an online database. In such cases accounts payable can and should have access.

As indicated above, the PO can either be the first line of defense or the first place where internal controls start to break down. Here are a few of the issues:
Chapter 6 – Purchase Orders and Their Role in Internal Controls

- How accurate is the information on the form?
- Is the form completely filled out?
- Are special deals documented on the PO?
- Is the PO filled out before the transaction is consummated or after the fact?
- When is the PO sent to accounts payable?

An invoice that is accurate, complete, and timely guards against an improper payment. An improper payment might be an incorrect amount or a payment to the wrong party or even worse a payment to a supplier who never delivered goods or services. Finally, there is the issue of payments for shoddy goods never ordered but delivered – a petty fraud that is ongoing (usually of copier toner, paper, or yellow pages ads).

The PO is one of the three key documents used to verify an invoice for payment. As those who work in accounts payable are well aware, the proverbial three-way match is used in most organizations. It matches the PO against the receiving documents and the invoice submitted for payment. When all three match, the invoice is processed and a payment scheduled. If there is no match, discrepancies must then be resolved.

**Purchase Order Problems**

Most PO problems signify a breakdown in internal controls. Accounts payable professionals who have problems getting some of these issues addressed can now use the threat of noncompliance with the Sarbanes-Oxley Act to harness management support for their initiatives. Specifically, and at a minimum, POs should:

- Be completely filled out (a big problem in some organizations)
- Be sent to accounts payable (or AP should have online access)
- Not be done after the fact

If the PO does not have all the information included it is difficult if not impossible to complete the three-way match. Companies that require this matching (and that is most of them) will sometimes end up without an invoice. When alerted to this fact, the purchasing professional will sometimes create one. This is really adding work, without adding value. However, it often is necessary within the confines of the operating policy of the organization – and is a complete breakdown in internal controls. It is also a prime example of how special terms can get lost – because they are never reported to accounts payable and the vendor, either intentionally or by mistake, has created the invoice using the standard terms rather than the special terms negotiated. Thus, the hard work the
purchasing professional put in getting the improved terms was for naught.

**Purchase Orders for Everything**

Some organizations require a PO for every payment that is made. Others require them for every material purchase made. This approach can be used to subtly pressure employees to use payment mechanisms (e.g., p-cards and reimbursements through T&E reports) that do not require a PO.

**Non Purchase Order Invoices**

Purchase orders are a great internal control. However, not every purchase lends itself to the purchase order methodology. When an invoice shows up that has no PO related to it, the internal controls are weakened. However, non-PO invoices are a fact of life for many organizations. Typically they are marked, “Okay to Pay,” and signed by an employee authorized to approve purchases. Sometimes these invoices are attached to a check request form and sometimes they are not.

As you can imagine, the controls on such purchases are weaker than the controls associated with a PO. Additional problems, especially with low-dollar non-PO invoices include:

- No real verification of the product received
- No verification of whether the produce was ordered, meets standards, and so forth
- No real verification as to whether this is a duplicate invoice
Chapter 6 – Purchase Orders and Their Role in Internal Controls

Review Questions

1. Which of the following will not cause purchase order problems?
   A. A purchase order for a special order without indicating the special terms
   B. A purchase order filled out after the fact
   C. A purchase order without all the details filled in
   D. A purchase order filled out ahead of time with all the details completed

2. Which of the following is a best practice with regards to purchase orders and accounts payable?
   A. Fill out the purchase order completely when it is first issued
   B. Purchase orders is sent to or shared with accounts payable
   C. Purchase orders are done when goods are ordered, not after the fact
   D. All of the above
Chapter 6 – Purchase Orders and Their Role in Internal Controls

Review Answers

1. A. Incorrect. A purchase order for a special order without indicating the special terms is almost a guarantee of trouble for the purchasing organization. The odds are high it won’t get the special terms promised.
   B. Incorrect. A purchase order filled out after the fact, by its very nature, is problematic.
   C. Incorrect. A purchase order without all the details filled in is one that creates problems for accounts payable in terms of additional work as well as increasing the possibility of errors.
   D. Correct. A purchase order filled out ahead of time with all the details completed is a best practice and one where problems will not be caused by the purchase order.

2. A. Incorrect. Filling out the purchase order completely when it is first issued is a best practice, but not the only one on this list.
   B. Incorrect. Sending or sharing a purchase order with accounts payable is a best practice, but not the only one on this list.
   C. Incorrect. Purchase orders completed when goods are ordered and not after the fact, is a best practice, but not the only one on this list.
   D. Correct. All of the above are best practices when handling purchase orders.
Learning Objectives

- Identify common invoice problems
- Demonstrate how best invoice control practices improve the processing function

Introduction

As the processing of invoices is the core function for accounts payable, it is time to turn our attention to that part of the process.

Dealing with Invoices without Invoice Numbers

Many non PO invoices, as well as some invoices associated with POs, have no invoice number. While to the uninitiated this may seem like a minor issue, it can create huge control issues. In fact, invoices without invoice numbers is one of the leading causes of duplicate payments. The reason for this is that in many organizations the controlling feature on determining if a payment has been made is the invoice number.

Without that feature, the controls go out the window – unless a strict numbering standard has been established to issue invoice numbers to these invoices. An even better approach is to require a purchase order number on all invoices. By returning invoices that are received without a purchase order number or name of a requisitioner with a polite letter explaining you need this information on all invoices in order to get them paid quickly, you will address this issue.

Documentation

An updated policy and procedures manual is critical for any accounts payable function that operates with an intent to have strong internal controls. Typically, these are held in each department. The PO issue straddles at least two department lines, which is one of the reasons why there is sometimes trouble.
Thus it is suggested that accounts payable and purchasing work together on the project of documenting PO requirements and the communication between the two departments over what’s on the PO and how that information is disseminated to accounts payable. What formerly may have been a territorial issue can no longer be that. Information must be shared and petty interdepartmental issues must be put aside. A comprehensive set of procedural instructions will go a long way in:

- Ensuring accurate information is shared on a timely basis
- Ensuring that only payments that are supposed to be made are made
- Ensuring that each department knows what they are required to do.

Oh, yes, and good documentation is a giant step in the right direction to ensuring everyone in your department handles the same tasks in the same manner – one of the principles of strong internal controls.

**Invoice Handling: Clear Instructions**

While the accounts payable department has a fairly good idea of who originates POs and who to contact to strengthen weak controls, the matter is much more difficult when it comes to invoices. For starters, virtually every invoice is initiated by a party outside the company’s direct control. While the accounts payable department can try to lay down rules for these parties, it has little control. However, it does have strong influence in that by providing clear and accurate instructions to vendors it can hasten payments to those who conform to its guidelines.

Thus, the first step to getting invoices sent in correctly is to provide vendors with clear instructions on where invoices should be sent. This is a bigger issue than it might appear at first glance. For starters, the company needs to have a policy regarding where invoices should be sent. This breaks down into two possibilities:

1. Directly to accounts payable
2. To the individual who authorized the purchase

These are virtually the only two choices and there appears to be no right way. Companies vary on what they require. Some want everything sent to accounts payable where it may be scanned before being sent out for approval. Others require that the invoice be sent to accounts payable only after it has been approved for payment. Which way is better? There
is no clear answer as both methodologies have problems associated with them.

However, even though most experts recommend that invoices be directed to someone’s attention, many come in addressed to no one and float through the company, eventually ending up in accounts payable. No wonder vendors don’t get paid on time! Even when the mailroom is told to forward anything that looks like an invoice to accounts payable, invoices float.

A decision regarding where invoices should be sent needs to be made within each company. Once that decision has been made this information needs to be communicated to all vendors. It should be included in the welcome package that is sent to new vendors. It can also be communicated through regular communication that purchasing has with suppliers. However, on the vendor’s side, this information needs to be transferred from the sales staff to the professionals responsible for billing. If there appears to be a breakdown in communication on this issue at the supplier (and some sales people have little interest in the billing side of things), accounts payable can take the lead and communicate this to the person responsible for billing.

There is also an issue when invoices arrive in accounts payable with no indication as to who ordered the items covered by the invoice. Some companies, usually the lead players in an industry, require that either the name of the person ordering the goods or the PO number be included on the invoice. Without these vital pieces of information, accounts payable may be clueless as to where to go to get the invoice approved for payment, a very necessary part of the payment process.

**Invoice Approval Process: Delegations**

Typically, in a well-run company, the Board of Directors delegates the authority for various functions through resolutions. This authority can then be sub-delegated. Thus, the Board might delegate purchasing authority at various dollar levels to several high level executives, typically by title (not name). These executives then sub-delegate to their appropriate staff.

All this information should be written down and updated whenever there is a change. This information should be given to the accounts payable department. It should also contain signature specimens similar to those obtained for signature cards for the banks. This is sensitive information and should be kept in a secure location, not lying around where anyone passing by might see it. Similarly, whenever the information is updated, old copies should be destroyed.
Chapter 7 – Invoice Processing: The Core of the Accounts Payable Function

It is important to remember that there is a difference between the person who submits something for payment and the person who approves that payment. The number of people who can submit for payment will be much higher than those who can approve. It is an internal control feature to have at least two sets of eyes view every purchase. No one should approve payments for items they have purchased.

Clearly, the number of people who can authorize a payment will be limited, even at large companies. This delegation is also limited by dollar levels. Thus, a $100 purchase may be approved by a supervisor, while a $100,000 purchase might require the authorization of a vice president.

**Getting the Approval**

If there is one area that causes accounts payable more headaches it is the invoice approval process. Some of the most egregious examples of how accounts payable and purchasing don’t get along revolve around the invoice approval process. Here’s how the scenario plays out when things are not going well. Accounts payable sends an invoice to purchasing for approval. The purchasing professional has many things to do and low on his list of priorities is checking that invoice and approving it for payment. Until it is approved and returned, accounts payable can’t do anything. So, it sits for weeks in purchasing getting buried deeper each day as more paper is dumped into the in-box.

Then the vendor calls looking for its payment. The purchasing guy, who wants to be the good guy and is unlikely to admit that he’s been sitting on the invoice, tells the vendor to call accounts payable, that he sent it back to them weeks ago. It’s a quick way to get rid of an angry vendor. He then quickly finds the invoice, signs off on it (without checking it!), puts it in an inter-office envelope marked accounts payable and forgets about the whole mess. Now, when the vendors call accounts payable, they are under the impression that their invoices have been there for weeks. So these conversations tend to be a tad on the touchy side.

In the ideal scenario, accounts payable sends the invoice to purchasing for approval (or does not receive it until it has been approved), purchasing approves it and returns it to accounts payable within 24 hours for processing for payment.

When an invoice is not paid by the end of the billing cycle (typically once a month), a follow up invoice is sent. While this may be marked COPY or DUPLICATE INVOICE, they are not always so marked. Many of these second invoices get paid, often before the original invoice winds its way back to accounts payable. And, what do you think happens when that original turns up in accounts payable, approved for payment? If you
Chapter 7 – Invoice Processing: The Core of the Accounts Payable Function

answered that it sometimes gets paid, you are correct. Getting that duplicate payment returned can be a tedious and expensive proposition.

Clearly, paying an invoice twice indicates a breakdown in internal controls. To address this issue, most companies run some sort of duplicate payment checking program to try and identify these payments before the money goes out the door. The programs have varying degrees of success, often depending on the level of controls in other parts of the accounts payable process.

The procedures for getting invoices approved, including the recommended timeframes for each step, should be documented as part of the policy and procedures manual. They should also be flowcharted as part of that exercise.

Electronic processes have addressed many of these problems. See the Electronic Invoicing section for a discussion on this issue.

The Three-Way Match

As mentioned above, the three-way match is a strong control feature used at most corporations. If the PO, receiving document and approved invoice match, the item is scheduled for payment. However, frequently the three do not match and then the fun begins. It is also where the best-intentioned internal controls can start to fall apart. Discrepancies can and should be investigated by the party in the best position to resolve them. That is rarely accounts payable, yet this is often where the responsibility for dispute resolution lies.

Strong dispute resolution mechanisms and policies should be developed. This can be helped along greatly if invoice automation is used. Some of the electronic invoicing modules currently on the market incorporate an online dispute resolution mechanism which is extremely helpful.

Discrepancies in the three-way match process can be tracked by vendor and approver to identify potential weak links in the PO and approval process. Once it becomes clear that there is an issue with a particular vendor or purchaser, steps can be taken to eliminate the root cause of the problem. Sometimes, all that is needed is a little education.

Handling Small-Dollar Invoices

Small dollar invoices are the bane of many accounts payable departments. They take a considerable amount of time and energy to process, taking precious time from larger transactions that deserve more scrutiny. Thus, many companies encourage the use of p-cards for small dollar
transactions. Others have developed mechanisms to review these invoices in a manner that utilizes fewer precious resources. One example is negative assurance. Approvers are notified of an invoice but not required to take any action unless they did not order the goods in question, hence the negative connotation in the nomenclature.

While these approaches are probably good from a workflow standpoint, they do open the door for potential small dollar fraud, if care is not taken. Thus, while it makes sense from an operational standpoint to implement these processes, extreme care needs to be taken to ensure that the appropriate controls are put in at the same time. Otherwise, the fraudsters will quickly home in on your weak links.
Review Questions

1. What is the best way to handle an invoice without an invoice number?
   A. Return the invoice to the vendor requesting an invoice number be included
   B. Create an invoice number for it yourself
   C. Have purchasing create an invoice number for it
   D. Use the date as the invoice number

2. Which of the following represents a situation where an invoice problem is created?
   A. Invoices are sent directly to accounts payable
   B. Invoices are addressed to no one
   C. Invoices include the purchase order number and/or the name of the requisitioner
   D. All of the above
Chapter 7 – Invoice Processing: The Core of the Accounts Payable Function

Review Answers

1. A. **Correct.** Returning the invoice to the vendor requesting an invoice number be included is the best way to avoid problems created by numberless invoices.
   
   B. Incorrect. Creating an invoice number yourself will not help if the vendor submits a second invoice. The likelihood is that a different invoice number will be created for the second invoice, creating all sorts of havoc when looking for duplicate items.
   
   C. Incorrect. Having Purchasing create an invoice number will not help if the vendor submits a second invoice. The likelihood is that a different invoice number will be created for the second invoice, creating all sorts of havoc when looking for duplicate items.
   
   D. Incorrect. Using the date as the invoice number will not help if the vendor submits a second invoice. The likelihood is that a different invoice number will be created for the second invoice, creating all sorts of havoc when looking for duplicate items.

2. A. Incorrect. Invoices sent directly to accounts payable is one way to guarantee that accounts payable receives invoices on a timely basis.
   
   B. **Correct.** Invoices addressed to no one are likely to float around the company, eventually coming to accounts payable. However, precious processing time will have been wasted and it can be difficult to get it paid on time. Also, a second invoice may have been submitted if it floated for too long.
   
   C. Incorrect. Invoices that include the purchase order number and/or the name of the requisitioner make it easier for accounts payable to get the correct approvals.
   
   D. Incorrect. All of the above is not the correct answer as only invoices addressed to no one will create problems. The other items are best practices.
Chapter 8  
Invoice Related Issues

Learning Objectives

- Recognize invoice automation control issues as they arise  
- Be aware of how control issues can fall apart in the accounts payable function in the month-end and year-end close

Introduction

The way invoices are handled in accounts payable has changed dramatically in the last five to ten years and continues to change as organizations in growing numbers look to automation to improve productivity. The key for these organizations is to make sure that the changes do not weaken controls. The good news is that often the new changes actually strengthen controls.

Contract Compliance

As companies everywhere look for ways to cut costs and improve efficiency, one area that continues to offer potential for some real bottom line enhancements is the area of contract compliance. This is especially true of organizations that have large complicated contracts involving many different items. The obvious example that springs to mind is a hospital that orders many different types of supplies and different drugs. The opportunities for volume discounts are numerous.

Often these contracts go on for pages and rarely are invoices checked against contracts to make sure that all the terms of the contract are taken advantage of. It will come as no surprise to most reading this to learn that the more complicated the contract, the less likely it is that a company will adhere to it even most of the time. In fact, there are organizations whose business offering is simply going through contracts and payments, finding discrepancies and then recovering those overpayments.

Again, the goal in this arena is to identify those potential overpayment situations before the funds are disbursed. A few companies have set up contract compliance groups, most often as part of purchasing, but occasionally under the accounts payable umbrella. This group is charged
with making sure that the invoices paid comply with the signed contract. On the face of it, this may seem like a fairly straightforward process. Going back to the hospital example, it is easy to see how prices, especially in heavily negotiated supplies, could be misquoted. Equally important are the terms and any potential penalties and, as mentioned elsewhere in this chapter, special deals that are arranged outside the master contract.

Contract compliance reviews go hand in hand with strong internal controls and good documentation. For most companies, this is a relatively untapped arena that offers one of the last few footholds for professionals to find cost savings for their firms. To be done correctly, this needs to be one or more individuals’ prime responsibility – not something to be handled off the side of their desks in the slow time (whenever that may be in accounts payable!).

**Master Vendor File**

The master vendor file is the repository of all significant information about the company’s suppliers. It is the reference point for accounts payable when it comes to paying invoices – and handled incorrectly it can (and does) lead to massive problems. Fraud and duplicate payments are just the tip of the iceberg. While a company may have been willing to live with those risks in the past, they risk getting a negative assessment in their Sarbanes-Oxley audit if they continue to employ the poor practices with regard to their master vendor files.

At a minimum, to have any chance of not being dinged when their master vendor file practices are reviewed, a company should:

- Limit access to the master vendor file
- Periodically disable inactive vendors in the file (but do not delete the entries as the payment history associated with that vendor needs to be retained)
- Establish a naming convention to be used when setting up vendors initially
- Require that certain information (like W-9s) be obtained before the vendor can be set up and/or paid
- Have a senior level review (yes, I know it is boring work) of all changes made to the file

The reason for the last requirement is that more than one thieving employee has been known to go into the master vendor file to change the mailing address to divert a legitimate payment from the vendor to an unintended party, usually themselves. Then, once the check has been
mailed, they go back into the file and change the address back to the correct mailing address. Without the review of the changes, the fraud could go on undetected for years, with different vendors being targeted each time.

**Electronic Invoicing**

Many of the problems facing the accounts payable function can be addressed through the use of electronic invoicing. For starters, the blame game that typically surrounds who got the invoice when, dissipates in the face of electronic workflow systems which not only leave an audit trail for everyone to see but also often include an automatic escalation to the approver’s boss should he or she be on vacation – or simply be neglectful of their responsibilities related to checking and approving invoices for payment.

Similarly, there can be no dispute over who received an invoice and the timing of that receipt. Likewise, the electronic feature lets accounts payable forward the invoice for approval without having to rely on the often dubious interoffice mail facilities. This also relieves them of the onerous task of making copies before the invoice is forwarded and then having to dig through that file to determine what’s been returned, where the invoice is in the approval chain, how long it’s been out there, what needs to be followed up on, and so on. All these tasks add no value and even worse, zap departmental productivity.

As you have probably figured out, the process described above does not demonstrate anything remotely resembling strong internal controls and worse, is an invitation to fraud and duplicate payments. The process is not conducive to timely reporting and getting the books closed at month end and the end of the fiscal year can be a real challenge as more accruals than should be necessary have to be prepared. The accountants reading this will point out that it is much better to record an invoice on the books than to try and accrue for it.

**Models**

Very roughly speaking, electronic invoicing models break down into three categories:

1. Simple e-mail
2. Third-party models
3. Proprietary models developed by a company for its own use
The e-mail models are generally quite simple. An invoice is created, perhaps in Word or Excel, and is attached to an e-mail and sent to the accounts payable department for processing. Sometimes these documents are converted to a pdf file before they are sent. While this greatly improves the timeliness of the process and improves the likelihood that early payment discounts can be legitimately taken, there are some flaws in the process – mainly from a control standpoint. Still there are some real benefits.

The third-party models incorporate a number of control features that may be missing in the home-grown e-mail approaches that many use. However, they can be (but are not necessarily) expensive, thus making it difficult for some managers to get the authorization to begin using them. And, depending on the features in the model and whether the process is actually outsourced, there can be SAS 70 concerns.

The proprietary models may be wonderful for the company that creates them, usually the purchaser, but are often a nightmare for the accounts payable departments that have to work with them. The reason for this is actually quite simple. When a company develops a model, often at considerable expense, it incorporates features that meet its own requirements. Often these are unique and might actually reflect the corporate culture.

And, you guessed it. It is unlikely that two companies developing two models separately will come up with the same approach. Even if they are similar, there will be variances. Now, think about this from a hypothetical accounts payable professional’s point of view. If 20 of the suppliers that the company buys from have developed their own electronic invoicing models, that’s 20 different systems the payables professional will have to learn.

Now, if you are thinking that no two invoices are the same and why should this create a problem, you need to know that many of the buyer centric models (this is described in the Electronic Invoicing Frameworks section) require that the customer go to their websites to “pick up” their invoices. Each will require a unique password and user ID, sometimes related to the customer number that the vendor has assigned to the purchaser. It can get onerous for the payables operation. If the supplier “delivers” the invoices to the payables in-box, some, but not all of the problems go away.

**Evaluation**

If it seems like we don’t think electronic invoicing is a good thing, we gave you the wrong impression. We think the advantages far outweigh
some of the smaller problems they may create. The huge advantage in the electronic invoicing world is the models that come with an online dispute resolution mechanism. This allows for discrepancies to be adjudicated in a timely manner and for payment to be made in an equitable time frame.

And, while I recognize that a small number of companies use disputes to “legitimatize” their poor payment practices, from a Sarbanes-Oxley and an internal controls standpoint, it is not a good practice. By leaving invoices unpaid for long periods of time the odds of fraud and duplicate payment increase. Additional accruals may need to be done which do not enhance the timely reporting and disclosure requirements.

---

**e-Mailed Invoices**

Not all invoices delivered electronically come through an electronic invoicing model. Just about every organization receives at least a few invoices via e-mail. Typically these are an attached pdf file of the invoice. Many third-party systems can take these pdfs and read them into their own process.

Most organizations not using a third party model still take invoices via e-mail. For them, there is a new control issue. Some vendors, in their zeal to make sure their invoices arrive, are both e-mailing (or faxing) their invoices, as well as mailing them through the postal service. Thus it is more imperative than ever that all organizations have good controls in place to identify those second invoices.

For without good controls, some of those second invoices will get paid. As discussed earlier, most vendors do not return duplicate payments unless prompted by a reminder either from the customer or its third party audit firm.

---

**The Month-End Close**

In the ideal environment, there would be no accruals done at the end of the month. Of course, in the real world that is unlikely to happen, no matter how good a company’s processes are.

The requirements for the issuance of financial statements are tight and cannot be met if individual reporting units, such as accounts payable, do not close their books on a timely basis.

In addition to the timeliness issue is the question of internal controls in the invoicing process. If the process of closing the books drags out, it can be a reflection of the adequacy of the internal controls – and not a positive one.
Chapter 8 – Invoice Related Issues

Year-End Close

Everything that applies to the month-end close is applicable to the year-end close in spades. Timely reporting and strong internal controls come into play. The year-end close may also have an ugly sub-certification requirement associated with it. Thus, it is important that the professional who signs that document ensure that not only is the work done, but the internal controls are adequate.

Recommended Invoice Processing Practices to Ensure Tight Controls

To ensure the fewest control issues in your invoice handling practices, use the following practices:

- Prenumber and account for all purchase orders
- Match invoices, receiving and purchase order information and follow up on missing or inconsistent information
- Record invoices accurately on a timely basis for all accepted purchases that have been authorized
- Restrict ability to modify data
- Reconcile vendor statements
- Implement standards to guard against inaccurate input of data
- Follow up on unmatched open purchase orders, receiving reports, and invoices and resolve missing, duplicate, or unmatched items, by individuals independent of purchasing and receiving functions
- Have a focus for action/control activities
- Uncover and take action quickly on invalid accounts payable fraudulently created for unauthorized or nonexistent purchase

Closing Thoughts

The invoice is where the payment process starts. It is therefore crucial that appropriate controls are incorporated at this stage. Otherwise, the door to fraud and duplicate payments is opened. Additionally, when thinking about segregation of duties as it relates to the payment process, it is imperative that the invoice handling phase be included in that equation. Otherwise, true segregation of duties may not be achieved.
Chapter 8 – Invoice Related Issues

Review Questions

1. Which of the following is not a master vendor file best practice that strengthens controls?
   A. Limiting access to the ability to add or change data in the vendor file
   B. Using a rigid naming convention
   C. Having a senior level review of all changes
   D. Keeping vendors active in the file forever

2. Which of the following could cause problems with invoices that are e-mailed to the company?
   A. The invoice is also sent through the postal mail
   B. The invoice is printed twice and processed both times
   C. Both of the above
   D. Neither of the above
Chapter 8 – Invoice Related Issues

**Review Answers**

1. A. Incorrect. Limiting access to the ability to add or change data in the vendor file is a great way to strengthen controls in the master vendor file.
   
   B. Incorrect. Using a rigid naming convention is one of the best strategies any organization can use to tighten internal controls.
   
   C. Incorrect. Although few senior level executives like to review all changes made to the master vendor file, it serves as a powerful deterrent and hence strengthens controls.
   
   D. **Correct.** Keeping vendors active in the file forever is a terrible practice and weakens controls.

2. A. Incorrect. Unfortunately, while e-mailed invoices are sometimes also sent through the postal mail and that does create problems in accounts payable, it is not the only problem on this list.
   
   B. Incorrect. While e-mailed invoices are sometimes printed twice and processed both times and that is a problem, it is not the only problem on this list.
   
   C. **Correct.** Both of the above issues will increase invoice problems.
   
   D. Incorrect. Neither of the above is incorrect because both of the issues mentioned in A and B above cause invoice processing problems.
Chapter 9
When Paying by Check: The Internal Control Migraine

Learning Objectives

- Implement the proper controls around the check production process
- Demonstrate why signature stamps represent a poor control and can cause your organization big problems

Introduction

When most people think about accounts payable, checks immediately come to mind. It is also the area in accounts payable that may be most vulnerable to weak controls. Much of this will depend upon the corporate culture of an organization. Depending on the size of the organization, segregation of duties can also be an issue when it comes to check-related activities. For example, did you know that the person who handles the bank account reconciliation function should not be involved in unclaimed property reporting?

If you are scratching your head over that one, the explanation is relatively straightforward. The person who reconciles the bank accounts could indicate on the bank reconciliation reports that an item had been escheated (turned over to the state). In reality he or she simply reissued the check to a friend or themselves. This example demonstrates just how easy it can be for a dishonest individual knowledgeable about a company’s inner workings.

Authorized Signers and Board Delegations

The authority to sign checks typically is set by the Board of Directors. This generally indicates who, by title, can sign and to what dollar limits. This authorization can typically be sub-delegated and in most cases the Board authorization will indicate whether the signer can delegate further.

The Board authorizations should also indicate whether one or two signatures are required on each check, at what levels a second signature is required, if a facsimile signature may be used, and so on.
Authorized Signers

In some companies, every executive over a certain level, say vice president, will be made an authorized signer on all bank accounts. This is viewed as a perk of the position, kind of an honorary thing. It is also a terrible practice from an internal control standpoint – although this is a battle that most accounts payable managers are loath to start.

To ensure accuracy, accounts payable should keep a list of authorized signers by bank account. This list is often the same one that lists all the company’s bank account numbers. Many times the signers are the same on all accounts so only one list is maintained. There are several control points that surround this issue. Before adding anyone to the list, some analysis should be given to the consideration of whether the organization gains anything by adding this individual. Will they really be available to sign in cases of emergency or is that just wishful thinking or an excuse to add an executive who thinks he or she should be on the list? Clearly this is an issue that the accounts payable manager needs to address gingerly.

Documentation: Check Signers and Accounts

First, the report with all the sensitive information should have a limited distribution. This is a need-to-know report not one that should be distributed to everyone who might have a passing interest in the data. Again, just because someone is a vice president does not mean that they need this information. If the individual is not going to be writing or signing checks, then they probably do not need to be on the distribution list for this report. While this may sound harsh, it is in the company’s best interest.

The list should be kept in a concealed location, not out on the desk of a clerk where anyone passing by can see it. And, in the evening it should not be left out on a desk, even in an office, where someone on the cleaning staff could see it.

As mentioned, the distribution of the report should be limited and whoever is responsible for generating it should keep a list of who received the report. It’s a good control point to mark the report with a statement asking that it not be copied. All the controls fly out the window if one of the recipients takes the report and makes copies for people specifically excluded from receiving the report. Don, the vice president in R&D, does not need to know that the controller is one of the backup signers.
Chapter 9—When Paying by Check: The Internal Control Migraine

Whenever a new report is generated, the old reports should be returned and destroyed. While you can ask the recipients to destroy their copies, a super careful manager would get the reports back and destroy them himself.

The list needs to be updated every time there is a change. And, those changes include when an employee who is an authorized signer leaves the firm. At that point, anyone with any responsibility for getting checks as well as the banks involved should be notified that the employee has left. This is an area that is often overlooked. This control is especially important if the employee in question was terminated or leaves disgruntled. Often notifying the bank and accounts payable is last on the list of things that anyone thinks about. It is crucial in those organizations that insist on putting every Tom, Dick, and Harry on the authorized signer list.

One last control point when it comes to check signers… If an employee who is also an authorized signer departs under unpleasant circumstances, the organization might want to consider closing all bank accounts on which that person was a signer. Yes, it's an expensive option but the losses that might occur with check fraud could far outweigh the cost, especially if blank laser stock is used. If the company is still using expensive preprinted check stock, this could be a costly and time-consuming solution.

Check Stock: Laser versus Preprinted

Handled incorrectly, an organization’s check stock can open the door to fraud. If the stock is managed in a prudent manner the risk is reduced. Readers are probably aware that even if they do everything correctly they still stand a good chance of being hit with fraudulent checks. The first matter to be decided is what kind of check stock should be used. This is probably the first control issue related to the check itself. In the business environment, paper checks come in two varieties: preprinted and laser stock.

Most everyone is familiar with preprinted checks. They come with the vital information already printed on them. They are also pre-numbered. Ideally they incorporate some security features to make fraud a little more difficult. They require a good deal of management because in the hands of the wrong individual they can be lethal. Corporations with numerous subsidiaries, each having their own bank account, can have a massive storage and control issue on their hands, if they use preprinted check stock. Still, many organizations, and virtually all individuals use preprinted check stock.
Laser checks, however, have none of the vital information pre-printed on them. Before printing, they are simply a piece of paper. While in theory, a company using a laser check-printing approach could use blank typing paper, this is not recommended and few, if any, do. Rather laser checks, although printed by a regular laser printer, are printed on special safety paper, which is often numbered. This numbering is not to be confused with the check number. Rather it is a control feature on the back of the item and is used by the organization in question to control its stock. Since the vital information is printed on the check at the time the check is printed, an organization with numerous entities does not need to purchase separate check stock for each one. Similarly, when an account is closed, there is no stock to be destroyed.

Let me make one thing clear. While there are many advantages from a business standpoint to laser checks, using pre-printed check stock does not mean an organization has poor internal controls and is therefore not in compliance with Sarbanes-Oxley. What it does mean however, is that organizations that use preprinted check stock will have to exercise a far higher number of internal controls in order to be in compliance with the Act.

**Security Features**

Controls on the check process start with the safety or security features built into the check itself. There are over 20 different security features that an organization can incorporate into its checks. It is not necessary to incorporate all of them to be considered to have decent internal controls in the check stock itself. It is generally considered a reasonable business practice to have at least three such features in your check stock. Less than that and your checks could be considered suspect if there was a check fraud.

Here’s one last note about security features. Sometimes, in an effort to cut costs, organizations will order their checks from an outfit that offers an inexpensive product. A check’s a check, goes the rationalization. While I don’t recommend spending any more than necessary, don’t cut your costs at the expense of security.

**Storage**

Do you keep the spare checkbooks for your organization’s bank accounts in your desk drawer or in an unlocked filing cabinet in the departmental work area? If you do, you have a bit of company, so don’t feel bad on that count. However, if your auditors uncover this during their audits,
they will ding you on the internal control issue. Now before you dismiss this issue as something that would not happen under your watch, think about the checkbook you use to reimburse petty cash and the one used to write quick checks to employees who are terminated. Where are they kept in your organization?

Check stock should be kept under lock and key with extremely limited access. This is another example of where all the executives in the department do not need a key to the check storage area. The more people who have access to the location, the less secure it actually is. Some organizations limit that access to two individuals. Those individuals should not leave the key to the storage area in their desks so “someone else can get in should they be absent.” This policy effectively undoes the internal control structure.

When it comes to segregation of duties, anyone who is a check signer should not also have access to the check storage area. In most organizations the responsibility for the check stock area lies with a middle manager.

**Check Signing Procedures**

If you take a look at the checks signed by most organizations, the first thing you will notice is they are not actually signed by hand, they are machine signed. This is often referred to as a facsimile signer. Typically, it is the signature of a senior executive who is one of the check signers. When signature cards are given to the bank, a signature card of the facsimile also needs to be provided.

As a control feature, many organizations require a second signature on all checks over a certain dollar limit. This limit varies widely from organization to organization. There is no right answer here. Whenever a check is given to an executive for signature, the backup for that item should accompany the check. Otherwise, frankly, it is a pointless exercise. Now this is not to say that all executives check that backup.

As many reading this are well aware, often the executive signs whatever is placed in front of him (or her). And this is not to say that accounts payable professionals don’t take advantage of this. If they have a rush check and they want a quick signature, they will look for the signer who signs first and asks questions later – if ever. While this is not great from a control standpoint, it is a fact of life.

Checks being passed around for hand signature should also be kept in a secure manner. It is not uncommon to see piles of checks waiting for signature lying on an executive’s desk or worse, out on the secretary’s
desk in an open area. This should be a control issue. It is also an opportunity for anyone walking by to filch a check.

Once the checks are signed they should be returned for processing immediately. Otherwise, another potential weak link has been introduced into the process. The point of enumerating what can go wrong is to give the professionals responsible for the process some ammunition to get the processes improved.

There are some segregation of duties issues associated with who can sign checks and who can do other tasks. So before adding someone to the approved check signer list, evaluate what that person’s other responsibilities are.

**Facsimile Signer: Rubber Stamps**

The first facsimile signer was probably the rubber stamp. Going back maybe 20 years it was an accepted practice to have a stamp made up with the authorized signer’s signature. As anyone who has ever used one of these knows, it was frequently given to the signer’s secretary who then signed away – even when the executive was out of the office and never saw the items in question. Today, not only is this not considered a good practice, it is among the very worst a company can employ.

Not only is an organization using one considered to be using inadequate controls, it will forfeit all its legal protections for check fraud. Companies using these stamps are considered negligent and therefore responsible for the entire loss, if check fraud occurs. So, if your organization is using them, make it your top priority to eliminate their use as quickly as possible.

**Other Facsimile Signers**

Typically, the facsimile signer is a plate that is put in either the computer that prints the checks or a separate facsimile signing machine. It contains the authorized signature and is used for signing checks. It is an authorized signer. Therefore, extreme care must be given to the storage and use of that plate. Placed in the wrong hands, it makes check fraud extremely easy.

The same care that is given to check stock should be given to the facsimile signer, sometimes referred to as a plate. And from a control and segregation standpoint, the signature plate should be kept separate from the check stock. In an ideal situation where the staff is large enough, different individuals should have responsibility for the check stock and the signature plate or machine.
Leaving the signature plate in the machine unattended can be a control issue. Leaving it in the machine (be it a printer or a check signing machine) all the time is an open invitation to fraud, if the machine is not in a secure location. Remember, any blank piece of paper can be used to generate a check.

**Rush Checks**

If asked what function they would most like to remove from their accounts payable department, over 80% of all accounts payable professionals would probably pick rush checks, sometimes referred to as ASAP or manual checks. These are checks issued outside the normal payment cycle. Typically they are drawn when the payee must be paid before the next check run. Reasonable excuses for these items include the sudden termination of an employee, expenses such as closings that cannot be forecast with any certainty, and checks to vendors when the original invoice was never received. It is the last item that causes all the headaches.

Regardless of the reason for the manual check, they cause a disruption in the workflow of the department and for that reason are costly. Because they are handled outside the check cycle, certain tasks must be performed twice to ensure that the company’s records are updated correctly. If positive pay is used (and as you will read shortly, it should be) the bank must be notified or the payee will not be able to cash the check. Rush checks are one of the leading causes for duplicate payments and fraud because of the breakdown in normal internal controls associated with the check production cycle.

As alluded to above, there are legitimate reasons for issuing an ASAP check. If the original invoice was not received and hence payment not made and the vendor is a key supplier threatening to put the organization on credit hold, a strong case can be made for issuing the check. This is especially true if not issuing it will result in a deficit of a key production ingredient that will bring a manufacturing facility to a halt. Unfortunately, at least for the accounts payable department, many times when the vendor is threatening credit hold, it is not really because the original invoice was never received. Rather it was received and disappeared into that black hole known as the approval process in purchasing. Of course, purchasing is telling the vendor that accounts payable is the abyss where its invoice was lost – but that is another story for another book.

The reality is that at many organizations rush checks are routinely issued to cover the hides of professionals who have fallen down on their jobs in a variety of other departments. And, often, management refuses to
back accounts payable’s requests to not issue rush checks. That is start-
ing to change in a number of organizations as these management teams
realize they could get dinged in their Sarbanes-Oxley audits if they rou-
tinely permit rush checks to be issued when purchasing neglects to re-
view invoices submitted for payment in a timely manner. If this has not
yet occurred to your management team, add this to your list of reasons
that rush checks should be limited. It really is an internal control point.

**Mailing Checks**

Not everyone realizes that how checks are handled after they are printed
and signed could be a control point. Leaving checks lying all day in the
mailroom is a really bad idea. Why? In many organizations a large num-
ber of individuals, including temps and employees from other compa-
ies, could pass through the facility. If an individual who has larceny in
his or heart happens through and sees a stack of envelopes clearly con-
taining checks waiting to be mailed, it will be a huge temptation. So, if
you must use the company mailroom facilities, do not deliver the checks
until right before the mail is taken to the post office.

Just because you are not taking the checks to the mailroom, does not
mean you have fulfilled your internal control issues. Don’t leave the
checks lying around the accounts payable department either.

Now if you think we are making too big an issue of this matter and
that your company’s checks are mailed in discrete envelopes, ask your-
self the following question. Does your firm mail checks either in window
envelopes or does it print and seal the check in an envelope in one pro-
cess? Either indicates that a check could be enclosed to someone looking
to steal checks.
Chapter 9– When Paying by Check: The Internal Control Migraine

**Review Questions**

1. Which of the following should be made an authorized signer on the organization’s checking accounts?
   A. Only vice presidents and above
   B. Only those who will sign checks
   C. Only the controller and CFO
   D. The president and CEO

2. Extra checkbooks with blank checks and preprinted check stock should be kept in which of the following locations?
   A. In a desk drawer
   B. In a locked secure location
   C. In a filing cabinet
   D. Any of the above

3. Which of the following describes the accepted view on use of a rubber stamp for signatures from a fraud prevention standpoint?
   A. The practice is acceptable
   B. The practice is acceptable but not desirable
   C. The practice is unacceptable
   D. The practice is preferable
Chapter 9– When Paying by Check: The Internal Control Migraine

Review Answers

1. A. Incorrect. If only vice presidents and above were given signing authorization, it would be difficult in many organizations to ever get checks signed. Rank within the organization should not be a consideration when deciding who should have authorization to sign checks.

   B. **Correct.** Only those who will sign checks is the right response for several reasons. The goal within any organization should be to have an adequate number of signers but no more than necessary. That is accomplished by providing authorization only to those who will sign on a regular basis and perhaps one or two backups for emergencies.

   C. Incorrect. If only the controller and CFO were given signing authorization, many organizations would grind to a standstill. Again, signing authorization should be given to those who need it, not granted based on title.

   D. Incorrect. The president and CEO have much more important responsibilities than that of signing checks.

2. A. Incorrect. Putting check stock of any sort in a desk drawer is an invitation to trouble. It is too easy for someone to see where the checks are being stored and remove them after hours. This is especially true if the desk in question is in a cubicle. Even in an office, a desk does not offer adequate protection.

   B. **Correct.** Check stock should be stored in a locked secure location so no one can get the checks unless they have the key. There should only be one or two keys to this location and they should NOT be kept in a desk drawer.

   C. Incorrect. The problems with keeping check stock in a filing cabinet are the same as those that occur when keeping check stock in a desk. It is too easy for someone to see where the checks are being stored and remove them after hours. This is especially true if the filing cabinet in question is in a cubicle.

   D. Incorrect. The only place check stock should be kept is a secure locked location, not a desk or filing cabinet.
3. A. Incorrect. The practice of using a rubber stamp for signing is not acceptable.
   B. Incorrect. The practice of using a rubber stamp for signing checks is neither acceptable nor desirable.
   C. Correct. The practice is unacceptable as it is too easy for crooks to replicate the stamp.
   D. Incorrect. The practice is not preferable; it is unacceptable from a fraud standpoint.
Chapter 10
Check Related Issues

Learning Objectives

- Identify poor controls related to check request forms
- Demonstrate why bank reconciliations have to be done on a very timely basis

Outsourcing Check Printing

As you can tell from what was written so far, for what at first glance appears to be a relatively simple process, check printing has numerous potential control issues and problems associate with it. And it definitely falls into the category of non-value added functions. Hence, some companies choose to outsource their check printing function – even if they outsource virtually nothing else.

Companies who employ this process for check printing go through their normal check production cycle for everything except they do not print checks. Instead they transmit their check issuance file to the outsourcer for printing. In most cases the outsourcer for this service is their bank. As long as the proper internal controls are associated with the process, the company is fine – and it avoids a slew of control issues.

If this approach is utilized, the organization needs to obtain a SAS 70 report from the check printer to cover its assessment of internal control responsibilities.

Check Request Forms

When a payment needs to be made and there is no invoice, companies typically use a form to initiate the payment. This is another area that tends to have some control issues and it can be the source of duplicate payments and fraud. While in an ideal world, there would be no need for check request forms, that is not the reality of the world in which we live.

Controls should be built around the check request form process to ensure that they are not inadvertently written for an item that will later be paid with a check. That’s another way that duplicate payments occur.
Chapter 10 – Check Related Issues

Check request forms are also a way that employee fraud is occasionally perpetrated. The very nature of the check request form makes it vulnerable to breakdowns in controls.

The backup requirements for check requests are often laxer than they should be. However that is starting to change, thanks to Sarbanes-Oxley. When Accounts Payable Now & Tomorrow polled a group of its readers, almost half indicated that they had strengthened their backup requirements for check requests because of the Act.

**Use of Positive Pay**

As those reading this are probably quite aware, check fraud in the United States is a huge problem. The very best protection against check fraud is a product called Positive Pay. With this product, at the time a company does a check run, it also produces a file containing the check numbers and dollar amounts for delivery to its bank. The bank then verifies each check presented for payment against this file. If it is not on the file, the check is not honored.

Some banks take the use of positive pay so seriously that they give their corporate clients a written offer. That letter asks them to use positive pay or sign that they have decided not to use it. By refusing the product, the company is giving up a lot of its protections against check fraud.

In response to crooks who understood how positive pay worked and adjusted their check frauds to get around it, some banks now offer what is known as payee name positive pay. In addition to the dollar amount and check number, the file contains the name of the payee. This is a much stronger control for those guarding against fraud.

**Timely Reconciliation of Bank Statements**

Before Sarbanes-Oxley, timely reconciliation of bank statements was required if a company wanted to have any chance of not being liable for fraud, should it occur. After the Act was enacted, that issue became clearer, although again timely reconciliation of bank statements is not spelled out in the Act. However, failure to do so will result in potential frauds going undetected, not being able to reverse unauthorized ACH (automated clearinghouse) debits and loss of check fraud protections.

Now many reading this may think that this is not a problem at their firms, that they have a group or person responsible for the reconciliations and they work pretty autonomously and rarely cause a fuss. Check and make sure they are no more than 30 days behind. If the backlog is any
greater, you have forfeited your protections and may get dinged on the Sarbanes-Oxley audit.

**Recurring Payments**

When you think of recurring payments, rent jumps to mind immediately. These are fixed payments made on a periodic basis, usually but not always, monthly. Loan payments and lease payments can fall under this umbrella, as well. Savvy professionals looking to streamline their payables operations often set these recurring payments up for automatic payment, either by having a check issued in the appropriate check production cycle or scheduling an ACH credit for the appropriate amount. Often these payments do not have a maturity date. Hence, in theory, they could go on forever.

And, the evergreen feature is where the first control issue arises. There can be issues even without an evergreen feature. In the case of a loan that is either paid in full or prepaid, or a lease that is terminated, the payments will continue unless the system is notified to stop. In the case of a loan or lease, the maturity is often programmed in. Thus, it is important to incorporate strong controls to ensure that payments stop when the lease or loan matures or is prepaid.

**Concluding Thoughts**

The payment cycle is fraught with “opportunities” for those with thieving hearts to exploit weaknesses in less than perfect systems. To limit the opportunities for fraud as well as to meet Sarbanes-Oxley requirements, internal controls need to be strong, duties need to be fully segregated, and care needs to be taken.
Chapter 10 – Check Related Issues

**Review Questions**

1. Which of the following will make it **less likely** that use of a check request will cause a duplicate payment or enable fraud?
   - A. Require the full legal name of the payee on the check request form
   - B. Require full back-up documentation for the check request form
   - C. Require the full mailing address on the check request form
   - D. All of the above

2. Which of the following is recommended, if your bank offers the product?
   - A. Payee name positive pay
   - B. Positive Pay
   - C. Neither of the above
   - D. Either of the above
Review Answers

1. A. Incorrect. Requiring the full legal name of the payee on the check request form is a good idea but will not fully protect against a duplicate payment. More information is needed for that.
   B. Correct. Requiring full back-up documentation for the check request form is the best way to ensure that all the information needed to avoid paying twice is available to the processor.
   C. Incorrect. Requiring the full mailing address on the check request form, like requiring the legal name, is a step in the right direction but will not provide enough information to identify potential duplicates.
   D. Incorrect. Only full back-up documentation will provide the best protection. The other items, while nice, don’t provide needed information to identify potential duplicates.

2. A. Correct. Payee name positive pay is the best protection against check fraud, if available.
   B. Incorrect. While straight positive pay is a good alternative if payee name positive pay is not available, payee name positive pay is the best bet.
   C. Incorrect. Positive pay and payee name positive pay are both recommended, with payee name positive pay being the preferred protection.
   D. Incorrect. Positive pay and payee name positive pay are both recommended, with payee name positive pay being the preferred protection.
Chapter 11
Corporate Procurement Cards

Learning Objectives

- Identify controls that should be incorporated into every corporate procurement program
- Reveal best fraud control strategies for your corporate procurement card program

Introduction

The corporate purchasing card is a means of streamlining the traditional purchase order and payment processes. Typically, it is used by organizations to pay for low-dollar purchases and is a way of getting all those small dollar invoices out of the accounts payable department. It is generally viewed as an attractive payment vehicle for organizations looking to lower transaction costs. These cards are also referred to as p-cards and corporate procurement cards. The IRS refers to them as payment cards.

Corporate purchasing cards, also referred to as procurement cards or corporate procurement cards or p-cards, are similar to charge cards and operate very much like the credit card you have in your wallet. They are given to those employees who regularly make purchases on behalf of your organization. They should not automatically be given to all employees over a certain level, only those whose jobs require that they regularly make purchases on behalf of the company.

How The P-Card Process Should Work

There’s no one set way that every best practice card program will operate. Corporate culture and unique organizational or industry requirements will impact the programs. However, some guidelines are appropriate. The National Association of Purchasing Card Professionals (NAPCP) recommends that:

- Plastic purchasing cards or non-plastic account numbers are issued to requisitioners.
Chapter 11 – Corporate Procurement Cards

- Each card/account is mapped to a general ledger (G/L) account. (In some cases G/L mapping can be done based on Merchant Category Codes or Point of Sale Information.)
- The requisitioner places orders with suppliers providing appropriate payment instructions.
- The supplier processes the order using their acquiring bank’s authorization process.
- Cardholders receive their purchasing card statements directly from the card issuer. The cardholder reviews and approves the statement. Cardholders do not submit a payment.
- A single electronic invoice is sent from the card issuer to the requisitioner’s organization on a monthly, weekly, or daily basis. The invoice is processed to create accounting entries and facilitate payment.

**Individual Limits**

One of the control features in the cards is the ability to set individual limits. Again, these should relate to job functionality and requirements, not title. Some of the ways companies control p-card usage while simultaneously encouraging employees to use it wherever possible are:

- Limit the dollar amount of each transaction. Some companies set this limit as low as $50 or $100 to start and then when they become more comfortable with the program or want to grow it, they increase the limits. There are those who have limits as high as $5,000 and a few have no limits.

- Limit the dollar amount that each employee can spend in a given month. A repair person might be limited to no more than $1,000 per month while the plant supervisor might have a limit that is ten times that amount. Limits can be initially set low and then raised as needed. Remember, this level is not related to an individual’s title.

- Use standard industrial code (SIC) blocks. For example, some companies block furriers and other luxury good stores. The problem with this issue is that sometimes companies are in more than one line of business, yet they are limited to one SIC code. There have been instances where employees have been blocked from making legitimate purchases. Only use these if you are concerned about inappropriate use.
• Insist that the manager review and sign off on all monthly statements. Remind managers that their signature makes them equally responsible for inappropriate charges.

Additionally, there should be a periodic review by someone independent of the cardholder.

**Fraud Prevention**

When p-cards first appeared on the scene there were some executives who refused to have the program in their shop because they were concerned that their employees would use the cards for personal purchases. Others didn’t go that far, but were extremely restrictive in who was given cards for basically the same reason. These fears were exaggerated. Yes, p-card fraud does occasionally occur, but then, so do other types of employee fraud.

Managers are urged to set up programs that have fraud protections built in. Some guidelines that will help include:

• Create a detailed cardholder agreement requiring the signature of the cardholder and the cardholder's supervisor. The agreement should contain a statement that the employee acknowledges the company’s right to fire him if he uses the card inappropriately. Although the primary responsibility for using the card appropriately lies with the cardholder, the supervisor has the ultimate accountability for how the card is used. Should someone flagrantly misuse the card, his employment should be terminated and this fact should be made public. Unfortunately, sometimes it is necessary to set an example to show that you are serious about enforcing the policy.

• Create a detailed policies and procedures manual and update it regularly to reflect the p-card program roles and responsibilities accurately. This document can be put online so everyone who may need to access it can do so. The manual will not only spell out everyone’s responsibilities, it will provide the framework for the entire administrative process, including internal controls and fraud prevention.

• Appoint a permanent administrator responsible for the p-card program. The administrator will ensure that all aspects of the card program are kept up to date and reflect the most current
technology and management controls available. This person will also be responsible for training and retraining cardholders and transaction reconcilers, as well as monitoring for incidences of possible unintentional personal use or obvious misuse.

- If possible, design the card so employees won’t accidentally mistake it for one of their own personal cards. If it looks like any other MasterCard, Visa or American Express it is an easy mistake to make. If your program is large enough, you may be able to get your logo put on the card. Recognize that honest mistakes do happen, but they occur very rarely.

- Establish reasonable card limits to reduce excessive or inappropriate use issues. Again, just because someone is a vice president, if their job does not require a $10,000 line don’t give it to them. There’s no sense tempting fate. While 99 times out of 100, there will be no problem, why open the door to temptation.

- Require training before issuing a p-card to a new cardholder, and require refresher training at least every two years for continuing cardholders. The training can be face-to-face or computer/Web-based. Some organizations insist that it be face-to-face for new cardholders, but that is not always logistically possible.

- Require original receipts for all purchases made on the p-card. Every receipt doesn’t have to be checked, but spot check and if you are at all suspicious, check all the receipts from the individual. Every photocopy increases the risk of fraud or abuse.

- Provide an anonymous hotline process to report suspected abuse. Every two years the Association of Certified Fraud Examiners (ACFE) produces a survey on Occupational Fraud entitled “Report to the Nation.” In the 2006 report, the top ways fraud was uncovered was by an anonymous tip 34.2% of the time and by accident 25.4% of the time. Can you really afford not to have a tip line? Make sure you publicize this fact through your training.

- Have meaningful and enforced policies governing consequences for misuse. As discussed earlier, if intentional fraud is uncovered, the employee should be terminated. If it is possible, legal action should be pursued. This may seem harsh but it is
important that your employees know there are consequences. The fraudster should be prosecuted, and the prosecution should be publicized. Not prosecuting and publicizing thefts only increases the chances that they will do it again.

- Establish a recurring audit process to evaluate compliance with program policies and requirements. Although routine monitoring is best handled by each operating unit's management, regular surprise audits of card usage will deter fraud significantly.

- Regularly review and update your policies and procedures as well as the limits on each card. This review does not necessarily mean that limits will be increased. If they are not being reached, they can and should be decreased.

- Don’t overlook the ability to seasonally increase limits if your business requires such action. The limits can be lowered once the high season has passed.

**Auditing the Program**

Many organizations are concerned about fraud. Others want to ensure that all purchases that should be put on the card are, because they want to receive as high a rebate as possible. This is not unusual and is becoming a larger issue. Thus many will want to set up an audit program to see if p-cards are being used as they should be and in all instances where they are supposed to be.

The information gathered in these audits can be used by the purchasing personnel to help them negotiate better pricing from preferred vendors if all the activity is aggregated to one or two suppliers for large purchases of certain products.

**End-User Training**

Without adequate training, even the most carefully planned p-card program will have a hard time succeeding. This is an area that is often overlooked. People think that p-cards are just like credit cards and that they know how to use them so why do they need special training. While they are correct in the similarities with p-cards, they are incorrect in the assertion that they do not need any training.
Without training, the cards will be used for items that they are not intended to be used for, reporting and monitoring of spending will be inaccurate and there will be clashes between the end users and the professionals responsible for monitoring the program.

The best training is onsite in-person instructions on how to use the cards and do the associated reporting. When the program is first rolled out, this is possible as there are usually a large number of employees who need to be trained. Unfortunately, onsite in-person training is often not possible for new hires or when employees are located in remote locations and there are only one or two in each branch using the card.

The next best training is given online, allowing each employee to take the training at his or her convenience. If possible, incorporate online testing to ensure that the employee has understood the material.

Some organizations go so far as to refuse to give a p-card to anyone who has not taken the training. As you might expect, you can anticipate some resistance, if not outright rebellion, to the last two recommendations.
Chapter 11 – Corporate Procurement Cards

Review Questions

1. Which of the following will not help prevent procurement card fraud?
   A. Getting a signed agreement from the cardholder indicating they can be fired for misuse of the card
   B. Requiring original receipts for all items/services purchased with the card
   C. Providing a detailed written policy to every cardholder
   D. Only giving cards to vice presidents

2. Which of the following should be used as a guideline when establishing limits for individual cardholders?
   A. The person’s title
   B. The length of service with the organization
   C. The business need the cardholder has for the card
   D. Everyone should have the same limit
Chapter 11 – Corporate Procurement Cards

Review Answers

1. A. Incorrect. Getting a signed agreement from the cardholder indicating they can be fired for misuse of the card definitely helps deter procurement card fraud.
   B. Incorrect. Requiring original receipts for all items/services purchased with the card helps deter fraud.
   C. Incorrect. Providing a detailed written policy to every cardholder is the first line of defense in any good fraud prevention program and will help prevent card fraud.
   D. Correct. Only giving cards to vice presidents does nothing to prevent fraud.

2. A. Incorrect. The person’s title has nothing to do with the cardholder’s need for a card and should not be considered when setting card limits.
   B. Incorrect. The length of service with the organization has little to do with the business need for a card and should not be a consideration when setting limits.
   C. Correct. The business need the cardholder has for the card is the primary determinant for setting the card limit.
   D. Incorrect. Everyone should *not* have the same limit; giving cards only to those who need them at the level they need is the best way to limit card fraud.
Chapter 12
Electronic Payment Alternatives

Learning Objectives

- Describe best control practices related to electronic payments
- Demonstrate why daily bank reconciliations are so important even if electronic payments are not being made

Introduction

Corporate America is finally starting to give up its paper-check security blanket. While wire transfers have long been used for high dollar payments, that mechanism is an expensive proposition. Financial Electronic Data Interchange (FEDI), once considered the reasonable alternative, has been adopted by only a handful of companies. If these were the only alternatives to the paper check, it is unlikely that we’d see the demise of even a small portion of the paper check market. But they are not the only alternatives.

There has been a seismic move in the corporate environs toward making payments via the Automated Clearinghouse (ACH), mostly through the use of ACH credits, and in limited instances through a debit vehicle referred to as an ACH debit. If you are planning on skipping the sections on ACH because your firm is not currently initiating payments through that mechanism, reconsider that idea. For starters there are types of ACH fraud that everyone, regardless of whether they actually use ACH, can be hit with. Then there is the issue that even companies who have no plans to use ACH suddenly find themselves making payments that way when large suppliers demand electronic payments.

Wire Transfers: Who's in Charge

Wire transfers may be a reasonable payment alternative when sending millions or even hundreds of thousands of dollars. The cost for a wire can be as high as $50, although typically it is somewhat lower. The first issue regarding wire transfers relates to where the responsibility for the function lies. This can be a serious consideration. In somewhere between 50 and 75% of all organizations the Treasury group does the wire transfers, while checks are issued in accounts payable.
In those numerous instances where wire transfers are handled by a different group than those who are responsible for checks, there needs to be coordination between the two groups. Why? This is because in more instances than anyone would like to admit in public, many invoices that are paid with a wire are then paid again with a check. One of the ways this happens is that when a payment is late, the vendor will insist on a wire transfer. Then, when the original invoice finally does show up, it gets paid. One way to avoid this is when the vendor screams for a wire transfer, try and convince them to take an ACH payment. This will keep the payment in accounts payable, keep the cost down and hopefully reduce the risk of a duplicate payment.

More to the point, to tighten controls consider moving the responsibility for wire transfers to accounts payable, where other payments are originated.

**Types**

Wire transfers can be broken into two broad groups. The first are those that are made on a recurring basis and the second are those one-time or irregularly made payments. This distinction is important when it comes to setting up wires online. It is also important when consideration is given to controls and fraud and duplicate payment prevention.

**Initiating a Wire Transfer**

Wire instructions can be sent to the bank online or by phone. Regardless of which initiation technique is used, the instructions need to be verified by a party other than the one that initiated the transaction. This is an important internal control point. It is especially important when it comes to preventing fraud. The list of people authorized to initiate wire transfers, as well as those authorized to approve the wires after they have been initiated should be limited to a small group of individuals. As with checks, this is not something that all executives should automatically have authority to do.

Now, when wires are done online, the process typically involves typing in the requisite information. Each approved person should have his or her own user ID and password. While it is not rocket scientist work, it is a task that involves some responsibility. Rarely is this task assigned to a clerical person – but that does not mean that in some organizations the clerical staff does not enter the data. Yes – that’s right; in some organizations the person who enters the data is not the one who is authorized to enter it.
Unfortunately, this can lead to fraud. Sharing passwords and user IDs is a really bad idea. Now, before you start to explain that the person in your organization, the person who’s been entering the wires even though not authorized is a long-term trusted employee, consider this. Most employee fraud is committed by long-term trusted employees.

**Fraud**
It is not uncommon for a company to receive a call asking for wire instructions by someone looking to pay the company. Most of the time these are legitimate requests. However, occasionally, they are not. Crooks have figured out that calling and asking for wire instructions claiming they are getting ready to pay a company is one of the easiest ways to get a company’s bank account number. And what are you going to do – not give someone the wire instructions???

Therefore, some companies use one account for wires and another for checks. If someone tries to write a check against the account it will bounce as the account cannot honor checks. This is not a Sarbanes-Oxley requirement but it is a good internal control point and could help you avoid getting dinged in the audit.

**Automated Clearinghouse (ACH)**
Americans’ love affair with the paper check is finally abating. This is one area where the United States lags the rest of the world. In fact, in many parts of the world checks are rarely written, with most payments being made electronically.

A reasonable number of organizations are making payments or are considering making payments in the near term using the ACH. The most common examples of ACH payments are direct deposit of payroll and of Social Security payments. These are what are referred to as ACH credits. If you allow your bank to automatically deduct your monthly mortgage payment from your bank account, you are using ACH debits.

This type of payment is infinitely more affordable than wire transfers. At approximately ten cents per item, ACH payments are even cheaper than paper checks. To be perfectly honest, ACH payments have fewer control problems associated with them. There is no concern about employees in the mailroom snatching the payments, payments don’t get lost in the mail, and so on.

**Authorization**
In order to pay vendors electronically, it is necessary to have them sign up. Care needs to be taken with the forms that vendors fill out with all
their secure information. It should not be kept where anyone can stumble across it. Treat it as though it were your own bank information.

Most companies, once they start making payments using the ACH, want to expand their programs. From a control standpoint it is important that all payment mechanisms (e.g., checks, wires, and ACH) are coordinated so that duplicate payments are not made and that weaknesses are not introduced into the processes that will allow fraud.

One of the good things about the ACH payment mechanism is that because it is relatively new in most organizations, the controls surrounding it are usually good. Typically, but not always, because there is generally some reluctance to start paying electronically, a company will have instituted decent internal controls around the process.

**Positive Pay**

Care needs to be taken when paying electronically. The reason for this is that positive pay does not work with ACH payments. While there is talk about developing a product, one is not currently available. Remember, ACH can work as either a credit or a debit. While ACH fraud is not nearly as prevalent as check fraud, it does exist and you need to protect against it. So, as a rule of thumb, unless you allow ACH debits, you can put an ACH block on your accounts.

There are other products available from banks to protect an organization against ACH fraud. Combined with strong internal controls they provide a framework for an integrated fraud-resistant payment process.

**Recurring Payments**

The ACH can be used automatically, as with checks, to make recurring payments (e.g., mortgage, rent, lease, loan payments, etc.) As with checks, it is a good control point to set these payments up with a maturity date so they do not go on after the maturity of the obligation. Additionally, it is a good idea to periodically review recurring payments to make sure that none should have been terminated. This might happen if a loan is prepaid or the interest rate renegotiated or if a property is sold, thus ending a mortgage obligation.

Some companies review their list of recurring payments each month before they are made to ensure that all the obligations are still outstanding.

**Daily Reconciliations**

It is a very good idea to reconcile bank accounts daily when it comes to ACH payments. This is for several reasons. Since positive pay doesn’t
work with ACH payments, the protection offered by that product is not available. Additionally, corporations have a very short timeframe to dispute incorrect or invalid items. Thus from an internal control standpoint – whether you use the ACH mechanism or not – frequent checking and verification are important.

For those organizations that have not put ACH blocks on their accounts, daily bank reconciliations are mandatory if they do not want to end up holding an empty bag. For they have only 24 hours to notify their bank of an unauthorized transaction. Waiting until the end of the month simply doesn’t work anymore.

**The ACH Control Best Practice Checklist**

**Best Practice #1:** Have detailed written procedures for your ACH program and include them in the accounts payable policy and procedures manual.

**Best Practice #2:** Make sure your ACH procedures mirror your check procedures.

**Best Practice #3:** Integrate strong internal controls throughout the process.

**Best Practice #4:** Check for duplicate payments made using other payment methodologies, i.e. paper check, T&E reimbursement and p-card. Ideally, each organization should be paid using one and only one payment mechanism.

**Best Practice #5:** Make sure receivers and POs are extinguished just as they would be if a paper check was the payment mechanism.

**Best Practice #6:** Put ACH blocks on all accounts where ACH activity will not be allowed. This is something every organization should do, regardless of its participation in the electronic payment arena.

**Best Practice #7:** Use ACH filters on those accounts where ACH debit activity will be allowed.

**Best Practice #8:** Have daily bank account reconciliations done on all accounts where ACH debits are permitted. Even better, reconcile all bank accounts on a daily basis.

**Best Practice #9:** Use a separate PC for all your online banking activities and do not use the computer for anything else.
Chapter 12 – Electronic Payment Alternatives

**Review Questions**

1. Which of the following is not a best practice with regards to ACH payments?
   A. Making sure ACH procedures mirror procedures for paying with a check
   B. Making sure purchase orders and receiving documents are extinguished when paying by ACH
   C. Making sure you perform a monthly bank reconciliation
   D. Using a separate computer for all online banking activity and nothing else

2. Why are daily bank account reconciliations recommended?
   A. They are required by most banks
   B. You only have 24 hours to notify the bank of an unauthorized ACH transaction to be guaranteed of the return of your money
   C. They are required by the Sarbanes-Oxley Act
   D. All of the above
Chapter 12 – Electronic Payment Alternatives

Review Answers

1. A. Incorrect. Making sure ACH procedures mirror procedures for paying with a check is a recommended best practice to ensure conformity in the payment process.
   B. Incorrect. Making sure purchase orders and receiving documents are extinguished when paying by ACH is a critical practice if you wish to avoid duplicate payments.
   C. Correct. Making sure you perform a monthly bank reconciliation will not protect you against ACH fraud. In order to be guaranteed the return of your money if an unauthorized transaction takes place, you must notify the bank within 24 hours. Hence, a monthly bank reconciliation won’t help.
   D. Incorrect. Using a separate computer for all online banking activity and nothing else is a new practice recommended first by the FBI and now by all fraud experts.

2. A. Incorrect. Virtually no banks have requirements when it comes to bank reconciliations.
   B. Correct. You only have 24 hours to notify the bank of an unauthorized ACH transaction to be guaranteed of the return of your money. This is why daily bank reconciliations are recommended.
   C. Incorrect. While daily bank reconciliations are a sign of strong internal controls, they are not explicitly mentioned in the Sarbanes-Oxley Act.
   D. Incorrect. Only the 24-hour requirement is currently a reason for daily bank reconciliations.
Chapter 13
The Policy and Procedures Manual:
Tying It All Together

Learning Objectives

- Show how a good policy and procedures manual can strengthen internal controls
- Demonstrate why updating the policy and procedures manual on a regular basis strengthens internal controls

Why a Policy and Procedures Manual Is Needed

Because many accounts payable departments have grown gradually or evolved as part of the accounting department, few have a written game plan. Instead, procedures are developed on an as-needed basis, in kind of a hodgepodge manner. Moreover, much of the knowledge about how things work and where information is located often resides with specific individuals. If those individuals get sick or accept another job, the company is left in the lurch.

Every accounts payable department should have a procedures manual, to serve not only as a guide in case of emergency, but also to provide managers with the necessary documentation to demonstrate to management the capabilities of the staff and the work they are handling. Without such a document, few understand the scope of information that is needed to run a successful department. This is especially important for those organizations subject to the strictures of the Sarbanes-Oxley Act.

The procedures manual can also be used to determine whether any processes can be eliminated. Needless to say, this document will not be the most interesting book ever written, but it is essential. As an added benefit, it will make the auditors happy. The manual should not only be prepared by those who are actually doing the day-to-day tasks, but it should also be updated regularly. Some choose to do this anytime a process is amended or added, whereas others do it annually. It is imperative that this be done. You’d be surprised to discover just how much processes change over the course of a year.

There is one other reason to have this manual and insist that everyone follow it. Left to their own devices, processors in accounts payable
Chapter 13 – The Policy and Procedures Manual: Tying It All Together

will gradually develop their own procedures. Without a careful and periodic review, each person will end up handling transactions differently. There is a word for this, and it is chaos. If one processor has an idea for an improved way of doing a particular task, the suggestion should be raised with the manager. If it is determined that the suggestion is superior to the methodology in use, everyone should change how they handle that particular task, and the policy and procedures manual should be updated to reflect this change.

Now, if this seems to be a cumbersome and costly task, think again. Thanks to the Internet, many companies now post their manuals on their corporate intranet site. This makes it available to anyone who may need to check it. It also makes updating a snap, and there are no costly printing charges each time the manual is updated. Finally, putting all the latest changes on the intranet removes that old chestnut of an excuse: “nobody told me.” E-mail alerts can be sent to everyone who is affected each time the policy is updated.

If your accounts payable department does not have a policy and procedures manual, the staff should bite the bullet and prepare one. If topics are divided among the staff and each one writes a chapter or two, the work will not seem overly burdensome. If you need some samples, do a search on the Internet.

You’ll come up with numerous samples that you can modify to fit your own procedures. One word of caution regarding those Internet policies, however: Most are written by universities. If you are in a manufacturing environment, you may have to add several sections. Still, having something to start with is a big help.

Finally, once the manual is completed, especially if it includes your T&E procedures, all affected parties should be notified that they will be expected to conform to the policies. Expect a certain amount of complaining. To make sure the policy is enforced, the first notice to the staff should come from a high-level executive (e.g., the controller or the CFO). Some companies put a short note from this executive on the front page of the policy so everyone understands that they will be expected to adhere to it. This is especially important when it comes to issues like T&E, rush checks, and not returning checks to requisitioners.

**The Policy and Procedures Manual from a Control Standpoint**

Like the semiannual visit to the dentist, most professionals know they should have a policy and procedures manual, but only a small percentage actually do. Even in those organizations that finally do get one put to-
Chapter 13 – The Policy and Procedures Manual: Tying It All Together
gether, it is rarely updated. While Sarbanes-Oxley doesn’t actually mandate a policy and procedures manual for accounts payable, it’s hard to visualize many situations where one would be considered in compliance without one.

If you’ve flowcharted your processes, a good portion of the work producing the manual has been completed. The task at hand is converting that diagram into words, keeping it updated, and making sure it reflects what actually goes on in the department.

What sometimes happens, with both the manual and the flowchart, is that over time, processes drift from the documented policy to something else. Unfortunately, that something else often introduces weaknesses and control points into the process. Sometimes, in an effort to speed up the work, steps are omitted from the process or the segregation of duties requirements are voided.

The policy and procedures manual should be shared with all affected parties. This means that, for example, purchasing should have input into and be given the final version of all sections that affect it. It is meaningless to write a policy that will require a three-day turnaround time of invoices if interoffice mail is used and it is slow. Similarly, if the purchasing manager is required to approve all invoices and he travels extensively, a lengthy approval time will be required unless electronic mechanisms are used or the board authorization for spending approvals can be further delegated.

Many organizations now post their accounts payable policy and procedures manual on their company intranet sites. This makes the information available to anyone who needs it, makes updating it relatively easy, and keeps it on the forefront of everyone’s mind. It also makes it easy to refer people with questions to the manual rather than have accounts payable answer every question. From a control standpoint, this is recommended.

It forces everyone to use the same source document for procedures rather than relying on one individual’s memory, which may or may not be accurate. Readers should be aware that having a policy and procedures manual can come back to haunt them if the staff does not adhere to it. By posting it on the intranet, or making it readily available using some other mechanism, the department is announcing its requirements. It makes it relatively easy to uncover situations where the policy is not adhered to by the accounts payable staff.
The Policy and Procedures Manual: An Ongoing Project

Very little in life remains static, and accounts payable is no exception. Even if you think you have policies and procedures exactly the way you like them, circumstances outside the control of the department may force a change. A move to a new accounting system, starting to use electronic payment alternatives, a demand by a key supplier, a physical move by a group within the organization, a new CFO, or any one of a thousand other things can cause the department to need to implement changes.

The very best manuals are updated every time a change to the procedures is made. This is one of the benefits of posting the manual online instead of printing hard copies. Of course this is probably not realistic in most organizations. At least once a year the manual should be reviewed and updated. This is also a good time to ensure that the procedures detailed in the manual are actually being followed in the department. You will be surprised to find how often they are not.

Including a Flowchart Is Not a Bad Idea

Most experts recommend that the department’s operations be flowcharted as part of the Sarbanes-Oxley compliance process. This is a good idea even without the Act. It forces the discipline of reviewing the ongoing process and documenting it. This flowchart should not be completed in a vacuum. It needs to accurately represent the work flow of the department, not what the manager or executives would like the work flow to look like.

It should be completed with input from the individuals who do the work. When it is completed, someone should verify that what’s in the chart is how the work is actually done. This is a great opportunity for the manager who believes some of the group’s processes are more cumbersome than they need to be. Once the chart is completed, it should be reviewed for two reasons:

1. To ensure that the appropriate controls are in place
2. To determine whether there are any processes on the chart that are unnecessary

This last analysis is the key to getting rid of non-value-added steps. There is a good reason for eliminating these extraneous steps. They can actually weaken controls. Here’s an example: In some organizations all hand-signed checks must be reviewed by an assistant treasurer before they are mailed. At the company in question, the checks often sit on this
individual’s desk for two or three days before he or she releases them. While ostensibly this is a review process, the real reason for the review is that this is how the assistant treasurer monitors what other departments are spending — something that is none of his professional business.

If the appropriate up-front controls are in place, this review adds nothing but time and additional risk (someone could take the checks from his frequently unoccupied office) to the process. By including this step in the process, it highlights the inefficiency. To further highlight the process, include estimated timeframes with each step. This will become useful in those situations where management is demanding (often rightly so) that the procure-to-pay cycle be accelerated. Simply take out the flowchart, with the timeframes noted, and ask where time should be cut from the process.

One of the biggest bottlenecks in many organizations is the invoice-approval process. It is not unusual to see two-thirds or more of the cycle time being allotted to getting the invoice approved. This is especially true if electronic invoicing, imaging, and workflow are not being used. The flowchart will highlight these inefficiencies. Accounts payable professionals can use this chart to back their recommendations for imaging, workflow, and/or electronic invoicing.
Chapter 13 – The Policy and Procedures Manual: Tying It All Together

Review Questions

1. The accounts payable policy and procedures manual should be updated how frequently?
   A. Annually
   B. Bi-annually
   C. Any time there is a change; if no changes, then annually
   D. Never – practices should be set in stone not changed

2. Who should have input into the accounts payable policy and procedures manual?
   A. Only accounts payable
   B. Anyone included in the accounts payable process
   C. Only management
   D. Everyone
Review Answers

1. A. Incorrect. Annually is only partially correct. If you wait and put in all changes at one time, the manual will be incorrect for a portion of time and not useful as a guide or reference manual.
   B. Incorrect. If you wait and put in all changes at one time, the manual will be incorrect for a portion of time and not useful as a guide or reference manual.
   C. Correct. Any time there is a change; if no changes, then annually is the best way to go. Any time a change is made to policy or procedure, the manual should be updated if it is to serve as an accurate reference guide and teaching manual.
   D. Incorrect. Best practices should continually change to reflect changes in the business community. They should never be set in stone and remain unchanged.

2. A. Incorrect. If only accounts payable has input, the manual will not accurately reflect what related parties (like purchasing) are doing and how that affects the accounts payable process.
   B. Correct. By including anyone touched by the accounts payable process, you ensure not only an accurate manual but one that serves everyone in the organization who might be affected by the accounts payable function.
   C. Incorrect. In most organizations, management does not have input into the day-to-day accounts payable process. They simply set policy and leave the running of the department to the managers. Hence, they would not be in a good position to dictate how the entire manual should be written.
   D. Incorrect. Letting everyone in the company have input into the accounts payable manual would be a recipe for disaster. What’s more, unaffected parties would have no interest and no basis for offering opinions.
Glossary

A
ACFE – Association of Certified Fraud Examiners

ACH – Automated Clearing House.

ACH credit – An electronic payment initiated by the payor.

ACH debit – An electronic payment initiated by the payee.

B
B-Notice – An annual IRS notification to payers, that IRS Forms 1099 have been filed with either missing or incorrect name/TIN combinations.

D
Duplicate Payment – The unintentional second payment of an invoice. One type of erroneous payment and unfortunately, rarely returned by the vendor unless the customer or its audit firm discover the overpayment.

E
e-Invoice – An electronic invoice either provided through an automated approach or as a simple attachment to an e-mail. Some do not consider files attached to e-mail as true electronic invoices.

F
Form 1099 – The Form 1099 is used to report different types of taxable income; the most common for the accounts payable groups being Form 1099MISC. This is used to report income paid to independent contractors.

I
Glossary

**Internal Controls** – The group of policies and procedures implemented within the organization to prevent intentional or unintentional misuse of funds for unauthorized purposes.

**M**

MCC – Merchant Category Code.

**N**


NAPCP – National Association of Purchasing Card Professionals.

**P**

P-card – Sometimes referred to as corporate procurement card or purchasing card.

Packing slip – Sometimes referred to as receiving documents, delineate exactly what was delivered in a particular shipment. Used in the three-way match.

PO – Purchase Order.

**R**

Receiving documents – See packing slip.

**S**

S-Ox – Sarbanes Oxley Act.

Segregation of Duties – With regards to accounts payable, it is the division of work so that one person does not perform more than one leg of the procure-to-pay function. It is one of the foundation principles of strong internal controls.
Glossary

T
Three-way Match – Comparison of invoice with purchase order and receiving documents before payment is made. If there is a discrepancy, some investigation is required to eliminate the discrepancy before payment is made.

T&E – Travel and Entertainment.

U
UCC – Uniform Commercial Code.

W
W-9 – Its full name is Request for Taxpayer Identification Number and Certification and it is provided to customers who need to verify certain tax reporting information.
Index

A
Access, restricting, 8
Accountable plans, 43
Accounts payable fraud, 1
ACFE, 17, 19, 28, 92, 111
ACH, 9, 10, 12, 32, 37, 43, 45, 46, 85, 86, 97-101, 111
ACH best practices, 101
ASAP checks, 26
Association of Certified Fraud Examiners (ACFE), 17
Audit trail, 4
Authorized signers, 27, 73, 74

B
Background checks, 1
Backup documentation, 33
Bank statement reconciliation, 73, 85
Billing schemes, 18
B-Notices, 2

C
Cash larceny, 17
Check fraud, 2, 4, 5, 25-27, 75, 76, 78, 85, 100
Check request best practices, 35
Check requests, 33, 34, 36, 85
Check requests, reducing, 35
Check signing procedures, 77
Check stock, 77
Check tampering, 18
Checks and balances, 14
Checks, storage of, 76
Coding standards, 12, 27, 32, 33, 37, 38, 46
Collusion, 8, 13, 19, 22, 42
Contract compliance, 65

D
Demand draft fraud, 27
Departing employees, 43
Dispute resolution mechanisms, 61
Documentation, 57
Duplicate payments, 2, 3, 5, 12, 26, 31, 33, 36, 38, 39, 45, 46, 47, 57, 66, 67, 69, 70, 79, 84, 100, 101
Duplicate payments, causes of, 36
Duplicate payments, prevention of, 31

E
Electronic invoices, 38
Electronic invoicing, 61- 69, 108
Electronic payments, 12, 25, 97
E-mail models, 68
E-mailed invoices, 69
Employee theft, 20
Erroneous payments, 47
Exceptions, 12, 13, 42, 48
Expense reimbursement schemes, 18
Expense reimbursements, 43
Extinguish purchase orders, 46

F
Facsimile signer, 1, 77, 78
Favorites, playing, 12, 13
Financial Electronic Data Interchange (FEDI), 97
Flowchart, 107
Form 1099 errors, 24
Fraud, 1, 2, 8, 13, 14, 17-27, 34, 36, 38, 42, 45, 48, 49, 53, 62, 67, 69, 70, 75, 79, 84-93, 97-100
check, 25
demand draft, 27
internal check, 25
practices that enable, 25
small dollar invoices, 23
suspicion of, 22
vendor, 23
Fraud deterrence, 21
Fraud, who commits, 19
Fraudulent disbursements, 17, 18
Fraudulent invoices, 23
Fraudulent payments, 47

G
G/L mapping, 90
## Index

### H
- Hiring, 1
- Hotline, anonymous, 19, 92

### I
- Inactive bank accounts, 25
- Internal check fraud, 25
- Internal control breakdowns, 42
- Internal controls, 4, 8, 11, 12, 14, 17-20, 23, 28, 31, 42-49, 52-54, 57, 58, 61, 66, 67, 69, 70, 76, 79, 84, 86, 91, 100, 101, 104, 112
- Invoice approval process, 60
- Invoice handling, 58
- Invoices, inappropriately addressed, 12
- Invoices, without invoice numbers, 57

### J
- Job rotation, 21

### L
- Laser checks, 76

### M
- Mailing checks, 80
- Manual check, 26, 79
- Master vendor file, 4, 5, 10, 11, 12, 14, 23, 27, 32, 33, 42, 43, 48, 66
- Monitoring reports, 4
- Month-end close, 69

### N
- National Association of Purchasing Card Professionals (NAPCP), 89
- Negative assurance, 62
- Non purchase order invoices, 54

### O
- Onsite conferences, 5
- Other departments, cooperation from, 11, 12, 48, 79, 108
- Overrides, 49

### P
- Paper checks, 12, 46, 75, 99
- Paper trail, 4
- Passwords, sharing, 49
- Payee name positive pay, 85
- Payments made outside accounts payable, 46
- Payroll schemes, 18
- P-card limits, 90
- P-cards, 12, 19, 32, 54, 61, 89, 91, 93
- Petty cash box, 3, 22
- Policies and procedures, 48
- Policy and procedures manual, 49, 57, 61, 101, 104, 105, 106
- Positive pay, 3, 25, 79, 85, 100
- Preprinted checks, 75
- Procure-to-pay cycle, 8, 9, 21, 42, 108, 112
- Promoting from within, 42
- Proprietary models, 67
- Purchase orders (POs), 10, 24, 32, 37, 45, 52, 53, 54, 57, 58, 59, 61, 112
- Purchasing cards, 89, 90, 112

### Q
- Qchex.com, 28

### R
- Receivers, 34, 35, 37, 45, 46, 101
- Recurring payments, 47, 86, 100
- Register disbursement schemes, 18
- Repetitive payments, 47
- Review, lack of appropriate, 48
- Rubber stamp, 78
- Rush checks, 3, 13, 26, 32, 35, 38, 79, 80, 105

### S
- SAS 70, 68, 84
- Security features, 75, 76
- Segregation of duties, 1, 8, 11, 14, 19, 20, 21, 26, 27, 42, 43, 48, 70, 73, 77, 78, 106
- potential conflicts, 9
Index

Sharing passwords, 49, 99
SIC code limitations, 19
Signature plate, 78, 79
Skimming, 17
Small dollar invoices, 61
Special deals, 53
Special requests, 13
Sub-certification, 70
Surprise audits, 22

T
T&E expense reimbursement report, 38
Third-party models, 67
Three-way match, 23, 32, 34, 35, 45, 46, 53, 61, 112
Tips, 19
Training, 5, 93

U
Unpaid invoices, 69

V
Vacation, employee, 19
Vacations, mandatory, 21
Vendor fraud, 23
Vendors, new, 23

W
W-9, 3, 23, 24, 113
Weak controls, 58
Wire transfers, 45, 46, 97-99

Y
Year-end close, 70