Wiley
BEST PRACTICES

ACCOUNTING CONTROL Best Practices

SECOND EDITION

Steven M. Bragg

Accounting Control Best Practices

Second Edition

Steven M. Bragg

WILEY

John Wiley & Sons, Inc.

To my parents, who exercised just enough control over me as a child to mitigate the risk of such dreadful occurrences as poor grades, car accidents, and entering politics

This book is printed on acid-free paper. ♾

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

Published simultaneously in Canada.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services, or technical support, please contact our Customer Care Department within the United States at 800-762-2974, outside the United States at 317-572-3993 or fax 317-572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

For more information about Wiley products, visit our Web site at http://www.wiley.com.

Library of Congress Cataloging in Publication Data

ISBN–978-0-470-40542-0

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

Contents

Preface v

About the Author vii

Chapter 1 Introduction 1

Chapter 2 Controls for Accounts Payable Best Practices 9

Chapter 3 Controls for Order Entry, Credit, and Shipment Best Practices 59

Chapter 4 Controls for Inventory Management Best Practices 91

Chapter 5 Controls for Billing Best Practices 143

Chapter 6 Controls for Collections 161

Chapter 7 Controls for Cash-Handling Best Practices 169

Chapter 8 Controls for Payroll Best Practices 209

Chapter 9 Controls for Fixed Assets Best Practices 245

Chapter 10 Controls for Budgeting 265

Chapter 11 Controls for Financial Reporting 275

Index 289

Preface

This book addresses one of the primary concerns in accounting today—how to develop a comprehensive system of accounting and operational controls. This concern has been exacerbated by the provisions of the Sarbanes-Oxley Act, which requires public companies to report an assessment of their internal control structures, and which has led to comprehensive control examinations by all types of companies.

This second edition of *Accounting Controls Best Practices* describes a complete set of controls for a paper-based accounting process as well as for a computerized system, and then describes controls for more advanced best practices that are layered onto the basic computerized system. The second edition includes new chapters describing control systems for budgeting, collections, and financial reporting. By reviewing the nearly 500 controls for the various systems presented here, the accountant or systems analyst can devise a set of controls that is precisely tailored to the needs of his or her system.

Accounting Controls Best Practices encompasses all of the major accounting and operational processes, including the following:

Billing
Budgeting
Cash receipts
Collections
Credit management
Evaluated receipts
Financial reporting
Fixed assets transactions
Inventory transactions and valuation
Investments
Just-in-time manufacturing
Manufacturing resources planning
Order entry
Payroll
Perpetual inventory record keeping
Petty cash
Procurement cards
Purchasing
Shipping

In addition, each chapter includes control flowcharts for all major processes. Further, to ensure that only enough controls are applied to not excessively reduce process efficiency, they are divided into primary and ancillary controls. This in-depth treatment makes *Accounting Control Best Practices* the guidebook needed to ensure that a company has constructed a durable and efficient set of controls.

This book is intended to be a reference handbook for accountants and systems analysts who design, monitor, and revise accounting systems, as well as for the internal and external auditors who review those systems for control weaknesses. It is also useful for accounting managers who must be aware of the control issues associated with any best practices they wish to install in their accounting systems.

STEVEN M. BRAGG
Centennial, Colorado
November 2008

About the Author

Steven Bragg, CPA, CMA, CIA, CPIM, has been the chief financial officer or controller of four companies, as well as a consulting manager at Ernst & Young and auditor at Deloitte & Touche. He received a master's degree in finance from Bentley College, an MBA from Babson College, and a bachelor's degree in economics from the University of Maine. He has been the two-time president of the Colorado Mountain Club, is an avid alpine skier and mountain biker, and is a certified master diver. Mr. Bragg resides in Centennial, Colorado, with his wife and two daughters. He has published the following books through John Wiley & Sons:

Accounting and Finance for Your Small Business
Accounting Best Practices
Accounting Reference Desktop
Billing and Collections Best Practices
Business Ratios and Formulas
Controller's Guide to Costing
Controller's Guide to Planning and Controlling Operations
Controller's Guide: Roles and Responsibilities for the New Controller
Controllership
Cost Accounting
Design and Maintenance of Accounting Manuals
Essentials of Payroll
Fast Close
Financial Analysis
GAAP Guide
GAAP Implementation Guide
Inventory Accounting
Inventory Best Practices
Just-in-Time Accounting
Managing Explosive Corporate Growth

Outsourcing
Payroll Accounting
Payroll Best Practices
Sales and Operations for Your Small Business
The Controller's Function
The New CFO Financial Leadership Manual
The Ultimate Accountants' Reference
Throughput Accounting

Also:

Advanced Accounting Systems (Institute of Internal Auditors)
Run the Rockies (CMC Press)

Subscribe to Steve's accounting best practices podcast at www.accountingtools.com.

Chapter 1

Introduction

Introduction

This book contains hundreds of very specific controls over the basic processes of a business—order entry, shipping, billing, purchasing, and the like. These controls are presented in layers, beginning with those needed for a very basic paper-based system and progressing through computerized systems and the use of selected best practice enhancements to the computerized systems. Thus, users can find within these pages a variety of control systems for different levels of system complexity. As a supplement to the many controls detailed in later chapters, this chapter contains additional comments about the overall system of controls, high-risk areas, the segregation of duties, implied controls, the impact of the Sarbanes-Oxley Act, and the occasional need to deinstall controls.

1–1 Control Point

This book is entirely about the control point, which is an activity within a business process that will prevent or detect a process breakdown. For example, the requirement to have a supervisor sign checks is a control point; the key element in this control point is not the actual signing of the check, but rather the assumption that the manager will not sign the check without first reviewing the attached payment documentation to ensure that the payment is necessary. However, this control point is necessary only in a relatively disorganized purchasing environment where many people can authorize purchases. If a company were to impose a rigid requirement that all acquisitions must involve an authorizing purchase order, there is no longer a need for a control point represented by the check signer, since the purchasing department has taken over this role. Thus, control points can be activated or discarded, depending on the structure of the underlying process.

A control point itself can break down through inattention, lack of formal training or procedures, or intentionally, through fraud. To mitigate these issues, some processes involving especially high levels of asset loss are more likely to require two controls to attain a single control objective, thereby reducing the risk that the control objective will not be attained. However, double controls are not recommended in most situations, especially if the controls are not automated, since they can increase the cost and duration of the processes they are designed to safeguard.

The controls outlined in the chapters that follow are broken into two types: primary controls that usually are highlighted on a control flowchart and ancillary controls that can be added to the primary controls to provide an additional layer of security. For example, detective controls designed to find errors after they have occurred are rarely designated as primary controls (which are intended to prevent control breaches from initially occurring) and instead are to be found in the list of ancillary controls. Primary controls are more likely to be an authorization, whereby a supervisor reviews a key aspect of a transaction before it is completed, or corrective, so that an error is spotted at or close to its source and fixed immediately.

Besides the detective controls already noted, verification controls usually can be considered supplemental. For example, an inventory audit or review of a petty cash box is a verification control, but because it is not conducted as an integral part of a process flow, it is considered supplemental to the primary set of controls. For the same reason, a passive control, such as installing a surveillance camera near a cash register, is considered a supplemental control.

There are many supplemental controls to choose from. However, just having a large selection of supplemental controls does not mean that they must all be used. Quite the contrary. Most controls add to a company's costs and clutter the work required of employees, so it is best to first determine exactly what risks must be addressed and what controls are required to do so, and to avoid using all other controls to the greatest extent possible.

To some degree, the use of ancillary controls is driven by a company's control environment, which includes these elements:

- *The enforcement of ethical standards.* A company that promulgates a written ethical standard, informs employees about it regularly, and enforces its parameters has established an excellent mind-set throughout the organization that a certain ethical standard is expected. This standard should be supported by the board of directors, while the board's audit committee should be active in investigating ethical (as well as control) breaches.

- *The operating style of management.* If the management team sets unrealistic goals for bonus payments or tells employees to meet stretch targets by whatever means possible, then it is creating an environment in which employees are indirectly encouraged to breach the control system. Alternatively, a focus on long-term results and reasonable short-term objectives tends to enforce compliance with the existing control system. Further, the establishment of free lines of communication between management and staff, so that control problems can be quickly and easily communicated throughout the corporate hierarchy, is an essential element of management's operating style.
- *Structure of the organization.* If a company is highly decentralized, with minimal overview of operations by the corporate staff, then controls will likely be enforced locally with minimal rigor. Conversely, a strong interest in control compliance by corporate management, with attendant auditing reviews, will assist in achieving a strong controls environment.
- *Assignment of control responsibility.* Controls will be followed with considerably greater enthusiasm when local managers are assigned direct responsibility for their consistent application. Without local assignment of control responsibility, controls tend to be looked on as hindrances to the efficient completion of processes and so are circumvented where possible.
- *Experience and expertise of employees.* If employees have a fundamental understanding of company systems, which comes from a combination of experience and intensive training by the company, then they will understand why controls are used, as well as the ramifications of their absence. Conversely, the lack of experience or training tends to result in the lapsing of controls.

Thus, the presence of a strong control environment is directly related to a reduced need for ancillary control points.

1–2 High-Risk Areas

All areas of a company contain some control weaknesses, but some harbor key risk areas, especially the diversion of company assets or misrepresentation of financial results. Of primary concern are those areas where these two issues coincide. The paragraphs that follow note how this book's controls can mitigate these risks, but also point out areas in which problems will still exist.

A major risk area is revenue recognition, for there are a variety of ways to manipulate it to accelerate revenues improperly, thereby reporting excessively profitable financial results. The bulk of the revenue recognition controls described in this book address the mechanics of ensuring that suppliers receive an accurate invoice in a timely manner—which unfortunately addresses only part of the revenue recognition control problem. Management still may have the capability to adjust revenue with a few well-placed journal entries or by altering the timing of transactions.

Another area of significant risk is the capitalization of assets. Chapter 8 addresses the basic controls needed to properly record expenditures large enough to exceed the corporate capitalization limit. However, once again (as has been proved at WorldCom), expenses can be capitalized on a massive scale by management, completely avoiding the intentions of the existing capitalization control system.

Yet another high-risk area is the valuation of reserves, such as for bad debts, warranty claims, or product returns. Anyone responsible for these valuations can easily adjust them (within limits) to arrive at enhanced financial results. Since reserve valuations fall entirely outside of any normal process flow, they can be more easily abused.

Several other high-risk areas are also unrelated to basic process flows—the valuation of acquired assets, related-party transactions, contingent liabilities, and special-purpose entities. Thus, even with in-depth and comprehensive controls over such key processes as purchasing, billings, and cash receipts, significant areas that can be circumvented easily—usually by management—still lie outside the traditional control systems.

Consequently, this book provides only part of the controls solution: It shows how to control both basic business processes and best practice improvements to those processes, but it does not provide a control system for management. That level of control requires a different set of approaches, such as tight board oversight of operations, an active and well-funded internal audit team that reports directly to the board of directors, good recruitment procedures, clear lines of authority, constant attention to ethics training throughout the organization, a fraud hotline, and the imposition of a corporate code of ethics. Unfortunately, these approaches are much fuzzier than the precise control points laid out in this book, which still leaves room for control breaches by management. In short, all manner of controls over management can be attempted, but there will always be a higher risk of control breaches by them.

Segregation of Duties

One of the fundamental concepts of control systems is that the level of control increases when duties are segregated among employees—and the more employees, the better. By segregating duties, one person typically is responsible for handling an asset (i.e., cash), while another records the transaction and a third approves the transaction, with no one being responsible for more than one of the handling, recording, or authorization tasks. If a process flows through multiple departments, the use of duty segregation can lead to the involvement of a dozen or more people in the process.

The advantage of using segregation of duties is that a massive level of collusion would be required to commit fraud. A typical case of fraud involving collusion results in a loss averaging six times the amount lost when a single person is involved, so there is certainly a valid point behind the use of duty segregation. However, it is also an extremely expensive proposition, for the involvement of many people in a process results in lengthy wait and queue times that yield a highly inefficient operation.

Due to the exceptional cost of duty segregation, it is increasingly common to find corporate risk managers evaluating the cost and benefit of such systems and sometimes deciding against an excessive level of segregation. The deciding factor is typically the size of the potential loss; for example, the handling of corporate securities will always call for the use of a considerable degree of duty segregation, while petty cash management will not.

Implied Controls

This book contains few references to automated data entry accuracy checks, since it is assumed that they are already present. Such controls include these validations:

- *Completeness*. A transaction is not considered complete until a specific set of required fields are completed. For example, the entry of a supplier invoice requires a supplier invoice number, invoice date, and dollar amount, and the computer system should not record an entry unless all of these fields have been completed.

- *Duplication.* The computer warns of the existence of a duplicate record already containing the same information. For example, the computer should reject a supplier invoice number that has already been entered.
- *Limit.* A transaction is flagged for supervisory review or rejected outright by the computer if a numerical value is too high. An example is a payroll application where the entry of an hourly wage rate is rejected if it is higher than a predetermined amount or lower than the minimum wage.
- *Table lookups.* The computer employs table lookups to determine the validity of entered data. For example, an entered part number will be compared to the item master file and rejected if the part number does not exist.

These automated controls are extremely useful for enhancing the completeness and accuracy of entered information.

Impact of the Sarbanes-Oxley Act on Controls

The Sarbanes-Oxley Act (Sarbanes) requires that an internal control report be included in a public company's annual report that contains an assessment of the effectiveness of the company's internal control structure and procedures for financial reporting. To determine if the control system meets this requirement, it is useful to complete these five steps:

1. Determine which accounts feed into the financial statements and which disclosures are key to the overall accuracy of the statements.
2. Document the process flows that materially impact the accounts and disclosures identified in the first step.
3. Identify the key risk elements in each if the highlighted process flows.
4. Document the effectiveness of existing preventive and detective controls in mitigating the identified risks.
5. Identify the need for alternative controls to mitigate the key risk elements down to targeted levels, and implement those changes.

Since this book is a broad-based source of control concepts, it is useful for completing steps 4 and 5 of the Sarbanes review process just noted. Within these pages, readers can locate controls for many key risk elements identified during their process reviews. To accomplish step 5 in the review process, it may be useful to audit a process once the controls described in this book have been installed, in order to identify any residual risk and then to adjust the control points to achieve the targeted risk level.

Deinstalling Controls

Though this book is concerned entirely with the selection and installation of controls to a process, a further consideration is when to deinstall a control. By its nature, a control usually involves non–value-added work, which either directly or indirectly increases company expenses. Therefore, you should conduct a periodic review of the existing control structure to determine which controls are no longer needed. A good time for this is just prior to the annual audit, when the external auditors likely will want to see some documentation of the company's system of controls. Another trigger for a controls review is whenever a process flow is altered, perhaps due to the installation of a new best practice. Whatever the reason for the review, all controls should be formally documented, thereby making subsequent reviews substantially easier.

Summary

The increased emphasis on controls that is mandated by the Sarbanes-Oxley Act makes it necessary to determine carefully what risks must be guarded against throughout a company's systems and to construct a set of controls to mitigate those risks. However, a company should not be ruled by a vast array of multilayered controls, unless it wants to see its operating efficiencies vanish. A better approach is to review the need for controls continually, both on regularly scheduled dates and as new best practices are installed, to ensure that only the correct controls are used in precisely measured amounts. This book is designed for such an approach, since it describes different sets of controls, depending on what best practices are being used. The reader can then assemble and disassemble controls as needed to match the specific systems in use.

An important concept to remember when reading this book is that even the most intricate, interlocking set of controls will not ensure the complete elimination of risk from a process. On the contrary, it creates only a reasonable expectation of that achievement. The reasons that risk cannot be completely eliminated are a combination of unforeseen circumstances for which controls were not installed, the occasional breakdown of the control system, and the presence of collusion, which effectively undermines many controls.

A final thought: It is possible to continue past the scope of this book and experiment with new types of controls, which can become best practices in their own right. This endeavor is particularly useful if controls can be created that require no capital or labor cost, and that do not interfere with the natural flow of a process.

Chapter 2

Controls for Accounts Payable Best Practices

Overview

This chapter covers three general sets of controls. First, it addresses the system of controls needed for an entirely paper-based accounts payable system, with descriptions for a supporting set of controls. Second, it reveals the controls needed for a basic, computerized accounts payable system, such as is installed in most companies today. Finally, it shows how to modify the controls for a computerized system in order to incorporate a number of payables best practices, including evaluated receipts, procurement cards, the replacement of checks with electronic payments, and more. Each set of controls includes a flowchart, showing necessary control points, as well as an itemization of supplemental control points.

2–1 Basic Accounts Payable Controls

Though it may seem unlikely that some companies still use entirely paper-based systems to conduct their accounts payable processes, this is still the case for some smaller businesses. The flowchart in Exhibit 2.1 shows the basic process flow for these organizations, with the minimum set of controls needed to ensure that it operates properly. The small black diamonds on the flowchart indicate the location of key control points in the process, with descriptions next to the diamonds.

The controls noted in the flowchart are described at greater length next, in sequence from the top of the flowchart to the bottom.

- *Manually review for duplicate invoices.* A noncomputerized accounting system has no way to automatically verify a supplier's invoice number

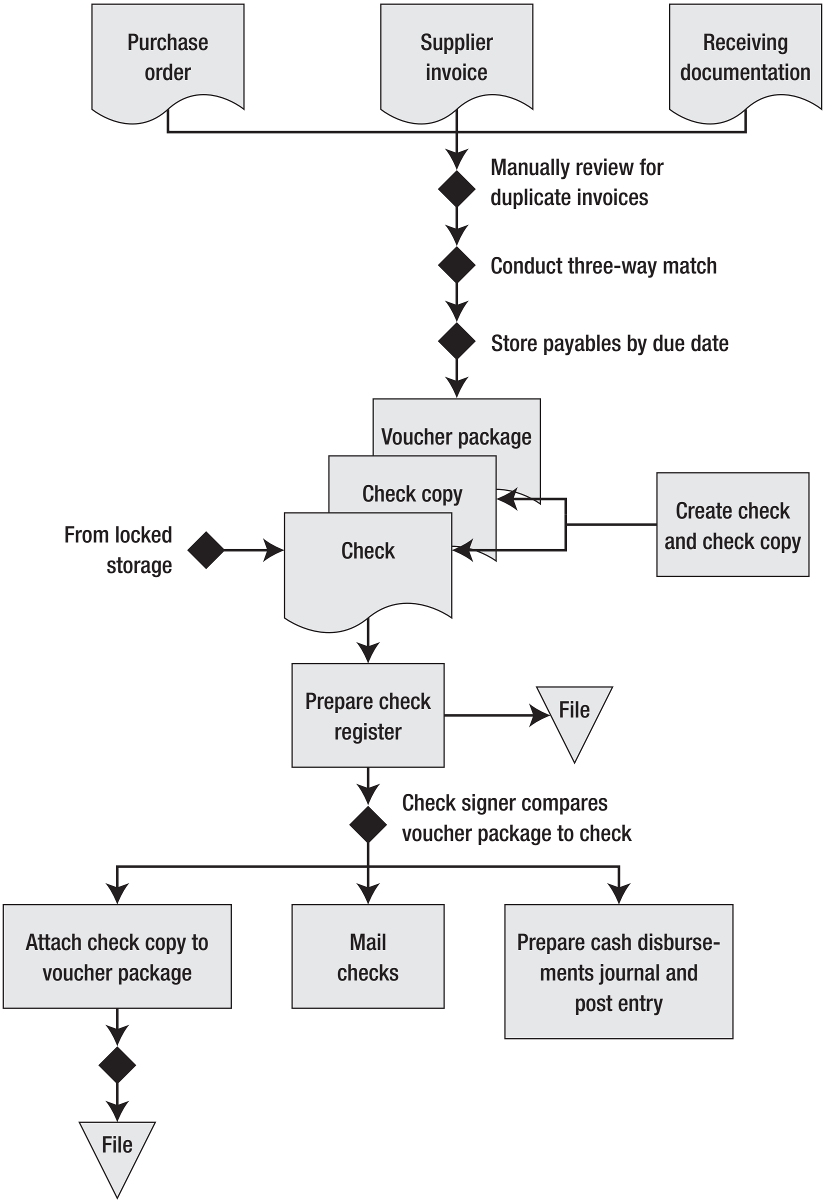
Purchase order
Supplier invoice
Receiving documentation
Manually review for duplicate invoices
Conduct three-way match
Store payables by due date
Voucher package
Check copy
Check
From locked storage
Create check and check copy
Prepare check register
File
Check signer compares voucher package to check
Attach check copy to voucher package
Mail checks
Prepare cash disbursements journal and post entry
File

Exhibit 2.1 System of Controls for Paper-Based Accounts Payable

against the invoice number of invoices previously paid. Consequently, the payables staff must compare each newly received supplier invoice against invoices in two files: both those in the unpaid invoices file and those in the paid invoices file.

- *Conduct three-way match.* The payables staff must compare the pricing and quantities listed on the supplier invoice to the quantities actually received, as per receiving documents, and the price originally agreed to, as noted in the company's purchase order.
- *Store payables by due date.* The company must pay its bills on time, which calls for proper filing of unpaid supplier invoices by payment due date. Otherwise, suppliers can give the company a lower credit score or charge late fees. This control assumes that unpaid invoices will be stored based on the dates when the company can take early-payment discounts.
- *Check stock from locked cabinet.* Unused check stock should always be kept in a locked storage cabinet. In addition, the range of check numbers used should be stored in a separate location and cross-checked against the check numbers on the stored checks, to verify that no checks have been removed from the locked location.
- *Check signer compares voucher package to check.* The check signer must compare the backup information attached to each check to the check itself, verifying the payee name, amount to be paid, and the due date. This review is intended to spot unauthorized purchases, payments to the wrong parties, or payments being made either too early or too late. This is a major control point for companies not using purchase orders, since the check signer represents the only supervisory-level review of purchases.
- *Perforate voucher package.* The voucher package can be reused as the basis for an additional payment unless the package is perforated with the word "Paid" or some other word that clearly indicates the status of the voucher package.

Though the preceding controls are the basic ones needed for a paper-only accounts payable system, the next controls can also be used to bolster the level of control over the process.

- *Prenumber receiving reports.* A key part of the three-way matching process is to ensure that the items being paid for have actually been received, and in the correct quantities. It is easier to ensure that all receiving reports are being transferred to the accounts payable department by prenumbering the receiving reports and tracking down any reports whose numbers are missing.

- *Lock up blank receiving reports.* If three-way matching is used, then the receiving report is considered evidence that the quantity of an item contracted for has arrived at a company location. If someone were to steal a blank receiving report, he or she could take the goods and still submit a completed receiving report, resulting in undetected theft. Consequently, it may be useful to lock up unused receiving reports.
- *Prenumber purchase orders.* The purchase order is a key part of many accounts payable systems, since it provides the central authorization to pay. Consequently, if the purchasing system is paper-based, it makes sense to keep track of the stock of purchase orders by prenumbering them.
- *Lock up blank purchase orders.* The purchase order represents a company's official authorization to acquire goods and services. If someone could obtain blank purchase orders and fraudulently affix a company officer's signature to it, that person could obligate the company to a variety of purchases with relative impunity. Consequently, in cases where purchase orders are printed in advance, they should be stored in a locked cabinet.
- *Maintain a register of unapproved supplier invoices.* If a company issues new supplier invoices to those empowered to authorize the invoices, then there is a significant chance that some invoices will be lost outside of the accounting department and will not be paid. To avoid this, update a register of unapproved supplier invoices on a daily basis, adding invoices to the register as they are sent out for approval and crossing them off the list upon their return. Any items remaining on the list after a predetermined time limit must be located.
- *Conduct a daily review of unmatched documents.* The three-way matching process rarely results in a perfect match of all three documents (purchase order, receiving report, and supplier invoice), so these documents tend to pile up in a pending file. To keep the associated supplier payments from extending past early-payment discount dates or from incurring late-payment penalties, there should be a daily review of the

pending file as well as ongoing, active measures taken to locate missing documents.

- *Reconcile supplier credit memos to shipping documentation.* If a company negotiates the return of goods to a supplier, then it should deduct the amount of this return from any obligation owed to the supplier. To do so, it should maintain a register of returned goods and match it against supplier credits. If no credits arrive, then use the register to continually remind suppliers to issue credit memos.
- *Only fund the checking account sufficiently to match outstanding checks.* If someone were to fraudulently issue a check or modify an existing check, a company could lose a large part of the funds in its bank account. To avoid this, only transfer into the checking account an amount sufficient to cover the total amount of all checks already issued.
- *Destroy or perforate and lock up cancelled checks.* Once a check is created, even if it is cancelled on the in-house accounting records, there is still a chance that someone can steal and cash it. To avoid this problem, either perforate it with the word "cancelled" and store it in a locked cabinet or shred it with a cross-cut shredder.
- *Add security features to check stock.* A wide array of security features are available for check stock, such as watermarks and "Void" pantographs, that make it exceedingly difficult for a forger to alter a check. Since the cost of these features is low, it makes sense to add as many security features as possible.
- *Verify that all check stock ordered has been received.* It is possible for both inside and outside parties to intercept an incoming delivery of check stock and to remove some checks for later, fraudulent use. To detect such activity, always compare the number of checks ordered to the number that has arrived. Also, verify that the first check number in the new delivery is in direct numerical sequence from the last check number in the last delivery. In addition, flip through the check stock delivery to see if any check numbers are missing. Further, if the check stock is of the continuous feed variety, see if there are any breaks in the delivered set, indicating that some checks were removed.
- *Limit the number of check signers.* If there are many check signers, it is possible that unsigned checks will be routed to the person least likely

to conduct a thorough review of the accompanying voucher package, thereby rendering this control point invalid. Consequently, it is best to have only two check signers—one designated as the primary signer to whom all checks are routed and a backup who is used only when the primary check signer is not available for a lengthy period of time.

- *Restrict check signer access to accounting records, cash receipts, and bank reconciliations.* The check signer is intended to be a reviewer of a nearly complete disbursement transaction, which requires independence from all the payables activities leading up to the check signing for which this person is responsible. Consequently, the check signer should not have access to cash receipts, should not perform bank reconciliations, and should not have access to any accounting records. It is best if the check signer is not even a member of the accounting department and is not associated with it in any way.
- *Never sign blank checks.* Though an obvious control, this should be set up as a standard corporate policy, and reiterated with all check signers.
- *Separate disbursement and bank account reconciliation duties.* If a person involved in the disbursement process were to have responsibility for bank reconciliations, that person could improperly issue checks and then hide the returned checks. Consequently, always separate the disbursement function from the reconciliation function.

2–2 Controls for a Computerized Accounts Payable Environment

The accounts payable process flow most familiar to readers is the one shown in Exhibit 2.2. This process flow takes advantage of the basic features of a computerized accounting system, including the minimum set of controls needed to ensure that it operates properly. The small black diamonds on the flowchart indicate the location of key control points in the process, with descriptions next to the diamonds.

The process flow in Exhibit 2.2 includes many steps already seen in the paper-based payables process flow. By consolidating some accounting information into a central accounting database, the accounting staff now has access to more online information for the three-way matching task, but most computer-enabled users still conduct a manual matching, rather than attempting to automate the process. There is also no need to review the system

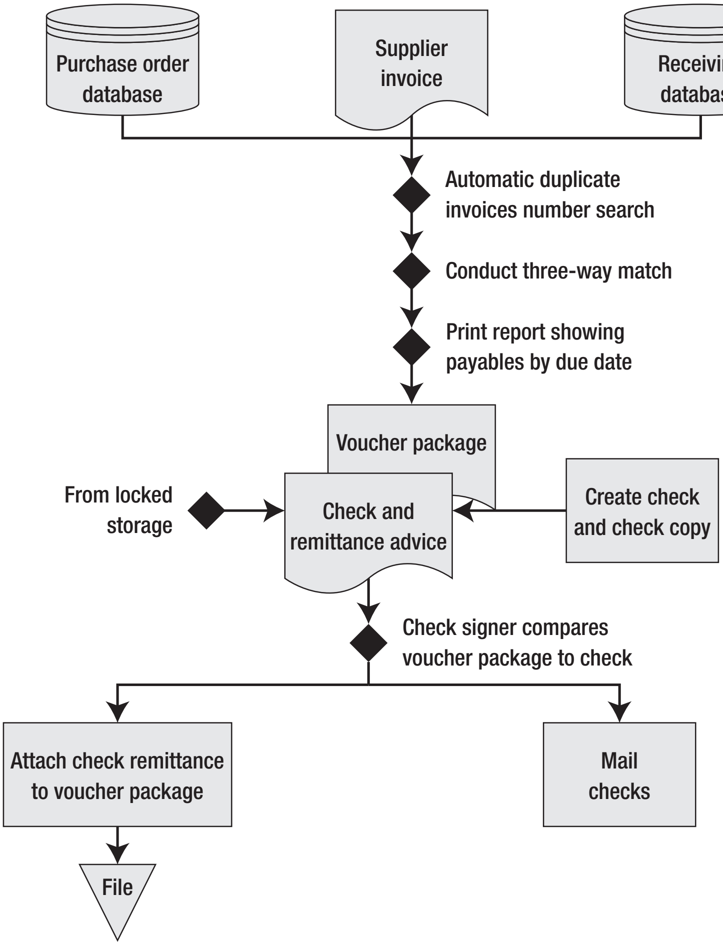
Purchase order database
Supplier invoice
Receiving database
Automatic duplicate invoices number search
Conduct three-way match
Print report showing payables by due date
Voucher package
From locked storage
Check and remittance advice
Create check and check copy
Check signer compares voucher package to check
Attach check remittance to voucher package
Mail checks
File

Exhibit 2.2 System of Controls for Computerized Accounts Payable

for duplicate supplier invoices manually, since this can be done by the accounting database. Further, the system will inform users when payables are due for payment, so no manual tracking of due dates is necessary. In addition, since checks are usually printed on a laser printer, there is only a single page printed, one portion of which is used as the in-house check copy. Thus, a separate page is no longer used as the check copy. Finally, there is no need to construct or print a check register or cash disbursements journal, since these documents are created automatically by the accounting software. Thus, computerization of the accounts payable process results in a number of efficiencies, though the overall process bears numerous similarities to the original paper-based system.

The controls noted in the flowchart are described in the bullet points that follow, in sequence from the top of the flowchart to the bottom.

- *Automatic duplicate invoices number search.* The accounting software automatically checks to see if a supplier's invoice number has already been entered and warns the user if this is the case, thereby avoiding the need for manual investigation of potentially duplicate invoices.
- *Conduct three-way match.* The payables staff must compare the pricing and quantities listed on the supplier invoice to the quantities actually received, as per receiving documents, and the price originally agreed to, as noted in the company's purchase order.
- *Print report showing payables by due date.* Since the computer system stores the invoice date and number of days allowed until payment, it can report to the user the exact date on which payment must be made for each invoice, thereby eliminating the need to manually monitor this information.
- *Check stock from locked storage.* Unused check stock should always be kept in a locked storage cabinet. In addition, the range of check numbers used should be stored in a separate location, and cross-checked against the check numbers on the stored checks, to verify that no checks have been removed from the locked location.
- *Check signer compares voucher package to check.* The check signer must compare the backup information attached to each check to the check itself, verifying the payee name, amount to be paid, and the due date. This review is intended to spot unauthorized purchases, payments to the wrong parties, or payments being made either too early or too late. This is a major control point for companies not using purchase orders, since the check signer represents the only supervisory-level review of purchases.

Perforating the voucher package after a check has been signed was one of the controls needed in a manual system, since it is an effective way to keep the same backup materials from being used a second time to authorize an additional payment. Though this control can still be used in a computerized system, there is less need for it, since the software automatically warns users of the presence of duplicate invoice numbers.

The preceding list of controls constitutes the basic controls needed for a computerized accounts payable system, but the controls that follow can also be used to bolster the level of control over the process.

- *Restrict access to the vendor master file.* For a variety of reasons that are enumerated in the next bullet points, it is unwise to allow unrestricted access to the vendor master file. Instead, use password access to restrict access to the smallest possible number of people, and only to those people who have no other responsibilities within the accounts payable and bank reconciliation areas.
- *Separate the supplier record creation and payment approval functions.* A strong risk of fraud arises when the same person can create a supplier record in the vendor master file and approve payments to the same suppliers, since this person is capable of creating a fake supplier and approving payments to it. Instead, split these two responsibilities among different employees.
- *Use a standard naming convention to create supplier names in the vendor master record.* Having multiple supplier records for the same supplier presents a problem when attempting to locate duplicate supplier invoices, since the same invoice may have been charged multiple times to different supplier records. One of the best ways to address this problem is to adopt a standard naming convention for all new supplier names, so that it will be readily apparent if a supplier name already exists. For example, the file name might be the first seven letters of the supplier name, followed by a sequential number. Under this sample convention, the file name for Smith Brothers would be recorded as SMITHBR001.
- *Review daily changes to the vendor master file.* An employee with access to the vendor master file could alter a supplier's remit-to address, process checks having a revised address that routes the checks to him or her, and then alter the vendor master record again, back to the supplier's remit-to address. If this person can also intercept the cashed check copy when it is returned by the bank, there is essentially no way to detect this type of fraud. The solution is to run a report listing all changes to the

vendor master record, which includes the name of the person making changes. A second control that provides evidence of this type of fraud is to only use a bank that creates an electronic image of all checks processed, so there is no way for an employee to eliminate all traces of this type of crime.

- *Require independent review of additions to vendor master file.* To reduce the risk of having an employee create a shell company to which payments are made by the company, have a person not associated with the payables process review all additions to the vendor master file and confirm that they are acceptable prior to any payments being made. Under this approach, only collusion that involves the reviewer will result in shell company fraud.
- *Purge the vendor master file.* The vendor master file within the accounting software can become clogged with multiple versions of the same supplier information, if not regularly reviewed and cleaned up. Having multiple supplier records presents a problem when attempting to locate duplicate supplier invoices, since the same invoice may have been charged multiple times to different supplier records. The solution is to conduct a regularly scheduled review and purge of the vendor master file.
- *Run a credit report on every new supplier added to the vendor master file.* A clear sign of fraud is when a shell company is set up specifically to receive fraudulent payments from someone within the accounts payable department. By running a credit report on every new supplier, it is possible to see how long a supplier has been in business and investigate further as necessary.
- *Run a report listing identical remit-to addresses for multiple suppliers.* Sometimes even the best manual review of the vendor master file will not detect all instances of duplicate records, because the variety of names used for a single supplier may be widely separated within the vendor master file. A good way to spot this problem is to sort the vendor master file by remit-to address, which tends to cluster multiple instances of the same supplier close together in the report.
- *Match supplier addresses to employee addresses.* Employees can create shell companies and fraudulently have checks sent to themselves. To detect this issue, create a computer report that matches supplier addresses in the vendor master file to employee addresses in the

employee master file (assuming that the payroll function has also been computerized).

- *Reconcile supplier statements to payment detail.* When a supplier's monthly statement reveals that some payments are overdue, this can be evidence of a diverted payment by an employee. Consequently, the timely comparison of any supplier statements containing overdue payment notices to the vendor ledger in the computer system can be a good way to detect fraud. This control is also possible for a paper-based payables system, but requires considerably more review time, since payment records must be manually assembled for comparison purposes.
- *Access the vendor history file when paying from a copy.* There is a greatly increased chance of duplicate payment when paying from a document copy, since the original document may already have been processed for payment. To mitigate this risk, always review the vendor history file to see if the same invoice number or an identical dollar amount has already been paid. An additional control is to require more approval signatures whenever a document copy is used.
- *Match quantities ordered to MRP requirements.* When the purchasing department orders more materials than are required by the material requirements planning (MRP) system, this may represent fraud by the purchasing staff, which may be diverting the excess materials for their own uses. Using the computer to match quantities ordered to actual requirements needed will spot this problem.
- *Match purchase order records to actual quantities received.* If a company has a policy of paying the full amount of the purchase order if the delivered quantity is within a small percentage of the ordered amount, a canny supplier can continually short-ship deliveries by a small amount and never be caught. To detect this problem, run a computer report comparing the purchased amount to the delivered amount to see if there are any suppliers who have an ongoing pattern of delivering less than the ordered quantity.
- *Track changes in customer complaints related to suppliers.* A supplier can improve its profits by selling low-quality goods to the company. Though this problem is difficult to detect, an indication is a sudden increase in customer complaints related to the materials provided by the supplier. Running a summary-level report itemizing customer complaints by supplier or type of complaint can spot this problem.

- *Track short-term price changes by suppliers.* There is a possibility that suppliers will offer a kickback to a person in the purchasing department in exchange for allowing price increases by the supplier. To detect at least the possibility of this type of fraud, run a report listing short-term price changes by suppliers. By screening the report to show only significant price increases, the probability of the report showing evidence of fraud will increase. However, if a canny supplier increases prices only by a small amount, such a report will still not detect the problem, unless the filter is set to report on price changes of any size.
- *Audit acquisitions made within authorized purchase levels.* Employees sometimes attempt to circumvent maximum purchase authorization levels by having suppliers split invoices into multiple smaller-dollar invoices. To detect this control circumvention, have the internal auditors run a report listing multiple small payments to suppliers within a short time period, and see if these payments are related to a single acquisition.
- *Investigate payments made for which there are no purchase orders.* If the purchase order is the primary control over the payables process, then it is critical to ensure that all payments made (above a minimum-dollar threshold) are supported by an authorizing purchase order. To locate control failures in this area, run a report comparing the payables file to the purchase order file, and list all payments for which there is no authorizing purchase order record.
- *Use varying font sizes for each character in a check payment.* Using a computer to print checks has the advantage of allowing for a wide array of printing techniques that makes it more difficult for someone to alter a printed check. One approach is to have the computer use a different font size and type for each character of the written payment amount listed on the face of a check. This type of printing is extremely difficult to modify.
- *Restrict access to check-signing equipment.* If a company uses any form of computerized check-printing equipment, it may be necessary to lock down all access to it. This can include any printers in which check stock is maintained, signature plates, and signature stamps.
- *Require a manual signature on checks exceeding a predetermined amount.* This control is useful when signature plates are used for smaller check amounts. When signature plates are used, there is no longer a final review of payments before they are mailed. Therefore, requiring a