K2's Small Business Internal Controls, Security, And Fraud Protection

Continuing Professional Education Series



K2 Enterprises www.k2e.com

K2E Canada Inc. www.k2e.ca

Copyright © 2026, by K2 Enterprises and K2E Canada Inc.

All rights reserved. No part of this publication may be reproduced or transmitted in any form without the express written consent of:

K2 Enterprises
1905 W. Thomas St., Suite D #363
Hammond, LA 70401-2901
985.542.9390

K2E Canada Inc.
174 Brewer Court
Burlington, Ontario, L7L4G4
905-746-1581

You may email requests to reproduce or transmit to info@k2e.com or caroline@k2e.ca. You may also obtain additional information on the web at www.k2e.com or www.k2e.ca.

The use of trade names and trademarks in these materials does not convey endorsement of these vendors or products. All trade names and trademarks used in these materials are the property of their respective owners. Any abbreviations used herein are solely for the reader's convenience and do not constitute any intent to compromise trademarks.

The statements in these materials about specific companies or specific hardware and software products should in no way be misconstrued as statements of fact but rather are opinions of the authors and K2 Enterprises and K2 Canada Inc. We take great care in providing views that we think will be useful in helping our participants make informed decisions. K2 Enterprises and K2 Canada Inc. reserve the right to independently evaluate companies' merits and the hardware and software products referenced in our seminars and conference presentations.

K2 Enterprises and K2 Canada Inc. make no representations or warranty regarding the contents of these materials and disclaim any implied warranties of merchantability or fitness for any particular purpose. The contents of these materials are subject to change without notice.

CONTRIBUTORS: The shareholders, associates, and staff of K2 Enterprises and K2 Canada Inc. contributed to producing these materials.

Table of Contents

Introduction V
Three Rules of this Seminar V
Course Development V
About K2 Enterprises V
Our Mission Statement VI
Our Instructional Team VI
The K2 Seminar Curriculum VI
On-Site Training VIII
Web-Based Training IX
K2 Internet Sites IX
Chapter 1 – Internal Control Fundamentals 1
Learning Objectives 1
Definitions and Concepts 1
Internal Control and the Five Components of Internal Control 1
Impact on Small Businesses 3
Implementing and Maintaining Internal Control in Small Businesses 5
Types of Internal Control Activities 10
Preventive Controls 10
Detective Controls 11
Deterrent Controls 11
Compensating Controls 11
Administrative and Accounting Controls 12
Administrative Controls 12
Accounting Controls 13
Alternative Controls 14
Detective and Deterrent Nature of Alternative Controls 15
Effective Small Business Alternative Control Procedures 16
Evaluating Alternative Controls 16
Chapter 2 – Fraud Today 19
Learning Objectives 19

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

The Current State of Affairs 19
Fraud in the United States 19
Fraud On An International Level 20
Summary of Fraud Studies 21
The Role of Accountants and Auditors 34
Chapter 3 – General Controls And Security Measures 39
Learning Objectives 39
Facilities Controls 40
Limiting Physical Access to Facilities and Assets 40
Physically Securing Company Information Systems 41
Firewalls 42
Network Firewalls 43
Personal Firewalls 43
Malware Protection 44
Data Protection and Recovery 44
Backup Protection 45
RAID 47
Business Continuity 48
Operating System and Application Updates 48
Chapter 4 – Key Information Security Controls And Authentication Methods 49
Learning Objectives 49
Authentication Overview 49
User IDs and Passwords 50
User IDs 50
Passwords 50
Why Use Strong Passwords? 51
Characteristics of Weak Passwords 52
Password Management Software 54
Multi-Factor Authentication 54
Cryptography Basics for Accountants 55
Encryption 56
AES Encryption 57
Overview of Email Security Issues 57

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Understanding the Issues 57
Solutions to Email Security Issues 59
Secure Alternatives to Email 60
Cloud-based Portals 60
End-User Controlled Repositories 61
Hard Disk Encryption 62
Overview of Hard Disk Encryption 62
Document Level Security 63
Securing Microsoft Office Documents 63
Chapter 5 – Desktop Tools For Preventing And Detecting Fraud 67
Learning Objectives 67
ODBC Queries 67
Sample ODBC Query with Excel and QuickBooks 68
Using Access as an Audit Tool 71
Using Access to Detect Duplicate Transactions 71
Using Access to Store Data Queried by Excel 75
Using Excel as a Fraud Detection Tool 75
Benford's Law 77
First Digit Probabilities 77
Second Digit Probabilities 78
First Two-Digit Probabilities 79
Utilizing Benford's Law 79
Applying Benford's Law in Excel 81
First Digit Test in Excel 81
Second Digit Test in Excel 84
First Two-Digit Test in Excel 86
Limitations of Using Benford's Law 88
Chapter 6 – Accounting Software Controls 89
Learning Objectives 89
Controls and Tools Available in Accounting/Business Management Products 89
General Controls in Accounting Software 90
Controlling Authorization with User IDs and Passwords 91
Accounting Controls Overview 95

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Prerecorded Data Input 95
Revenue and Cash Controls 96
Controlling Access to Credit Memos 97
Preventing Unauthorized Sales Discounts 98
Approval of Customer Credit Limits 99
Revenue Control Procedure Checklist 100
Purchasing Payable and Payroll Controls 102
Application Control Procedures for Purchasing/Payables 102
Preventing and Detecting Duplicated Transactions 105
Using Reports for Controlling Payables 107
Control Procedures for Payroll 108
Using Reports, Dashboards, and Alerts to Ensure Timely Processing and Notifications ... 109
Purchasing, Payables, and Payroll Control Procedure Checklist 110
Inventory, Production, and Fixed Asset Control Procedures 113
Application Control Procedures for Inventory, Production, and Fixed Assets 114
Using Automatic Reorder Functions to Optimize Stocking Levels 114
Conducting Physical Inventory Counts 116
Reports as Inventory Controls 116
Inventory, Production, and Fixed Asset Control Procedure Checklist 118
Controls for Cash 119
Appendix A – Segregation Of Duties 121

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Introduction

Three Rules of this Seminar

1. **There Are No Dumb Questions.** Please ask questions if you need further explanation. We welcome your questions and will do our best to provide accurate and meaningful answers.

2. **Obtain the Information for Which You Came.** If you have a specific interest in a topic, please let us know. If your topic is not part of the course materials, we will do our best to accommodate your request. Your instructor is anxious to meet your needs.

3. **Share and Share-Alike.** Your instructor is here to share relevant information about the course. We hope that you will be willing to do the same. If you have helpful tips or experiences, please share them with the other participants and us.

Course Development

The shareholders, associates, and staff of K2 Enterprises and K2E Canada Inc. developed this course and the related course materials. We aim to deliver high-quality educational practices that help you use and understand the tools and concepts discussed in this session more effectively.

We designed our course presentation style for busy professionals. Through numerous short case studies and feature reviews, we deliver concise, easy-to-understand, easy-to-absorb information.

To maximize your time and the value of attending this course, we have carefully filtered out trivial and obscure features. Our goal is not to cover every keystroke and menu option, but to provide a fast-paced course that focuses on state-of-the-art information technology and how it can benefit you and your staff.

About K2 Enterprises

For over three decades, our team members have delivered more than 45,000 technology-focused seminars, webinars, and conferences worldwide. To stay on top of technology, our team members read numerous technology trade magazines, attend conferences, and speak with technology companies each year to stay current with the latest information for our courses. Also, we experience everything we teach and recommend to our audiences. Because our shareholders and associates are based in different states and provinces, using technology efficiently and appropriately is essential to our business's success and survival.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Our Mission Statement

K2 aims to develop and deliver the highest-quality technology seminars and conferences for business professionals. We work cooperatively with professional organizations such as state CPA societies, associations of Chartered Professional Accountants, and technology vendors. We make every effort to maintain high integrity, family values, and friendship among all involved.

Our Instructional Team

For a complete listing of instructors and bios, please visit:

K2 Enterprises

Instructors - K2 Enterprises

K2E Canada Inc.

Instructors - K2E Canada Inc

The K2 Seminar Curriculum

Full-day Seminars

- K2's Advanced Excel
- K2's Business Intelligence, Featuring Microsoft's Power BI Tools
- K2's Case Studies In Fraud And Technology Controls
- K2's Excel Best Practices
- K2's Excel Essentials For Staff Accountants
- K2's Excel PivotTables For Accountants
- K2's Excel Tips, Tricks, And Techniques For Accountants
- K2's Next Generation Excel Reporting
- K2's QuickBooks For Accountants
- K2's Small Business Internal Controls, Security, And Fraud Prevention And Detection
- K2's Technology For CPAs – Don't Get Left Behind

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Half-day Seminars

- K2's Artificial Intelligence For Accounting And Financial Professionals
- K2's Best Word, Outlook, And PowerPoint Features
- K2's Better Productivity Through Artificial Intelligence and Automation Tools
- K2's Case Studies In Fraud And Technology Controls
- K2's Data Analytics For Accountants And Auditors
- K2's Ethics And Technology
- K2's Excel Charting And Visualizations
- K2's Implementing Internal Controls In QuickBooks Online Environments
- K2's Improving Productivity With Microsoft 365Cloud Applications And Services
- K2's Mastering Advanced Excel Functions
- K2's Microsoft Teams
- K2's Securing Your Data: Practical Tools For Protecting Information
- K2's Technology Update
- K2's Top PDF Features You Should Know

Besides the seminars listed above, K2 also produces numerous one and two-day technology conferences annually. You can find a complete listing of our course offerings, including dates, locations, and course descriptions, on our website at:

K2 Enterprises
Technology Conference - K2 Enterprises



K2E Canada Inc.
Technology Conference - K2E Canada Inc.



Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

On-Site Training

Working cooperatively with state CPA organizations and associations of Chartered Professional Accountants, we are pleased to offer all our seminars and conference sessions as on-site training opportunities. On-site training provides companies of all sizes with numerous advantages, including the following.

- ***Customization***. K2 can customize the content of all on-site training events to meet your organization's specific needs. For example, we can combine selected parts of existing courses into a focused learning experience to meet your team's needs. Likewise, we can develop custom content from the ground up and deliver it to your team members, ensuring we meet your training objectives.

- ***Cost savings***. For organizations of all sizes, on-site training can provide significant cost savings compared to public training venues. In addition to potentially reduced registration fees, these cost savings materialize in the form of reduced travel costs and reducing the amount of time team members spend away from the office.

- ***Convenience***. Because you select your on-site training event's date, time, and location, on-site training is more convenient for you and your team than traditional training options. Many organizations schedule on-site training with staff meetings, retreats, and customer/client events to leverage the value of all participants' time.

Customization, ***cost savings***, and ***convenience*** are the three C's of "training to go." For more information on how you and your organization can experience these benefits or schedule an on-site training event, please visit:

K2 Enterprises
On-site Training - K2 Enterprises

caroline@k2e.com

K2E Canada Inc.
Seminars - K2E Canada Inc

caroline@k2e.ca

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Web-Based Training

K2 offers web-based CPE and CPD to accounting and business professionals throughout the United States and Canada. K2's award-winning instructors deliver two-, four-, and eight-hour webinars on numerous technology-focused topics.

Additionally, K2 provides on-demand training. On-demand courses offer you the advantage of receiving top-quality training at a time and location that fits your busy schedule. You can start a class today and complete it in the future. For more information, please visit:

For more information on either platform, please visit:

K2 Enterprises
Webinars - K2 Enterprises

K2E Canada Inc.
Webinars - K2E Canada Inc

K2 Internet Sites

K2 maintains multiple websites containing information and links relevant to CPAs and other business professionals as a service to the profession. Further, the content of these sites can enrich your experience during and after our seminars. In addition, our pages contain links to some of the top accounting and content management software solutions and even to a few sites that are just fun places to visit. If you have any comments or questions regarding our web pages, please email *webmaster@k2e.com*.

K2 has two primary websites. You can view information regarding CPE and CPD opportunities, access a library of technology tips and articles, and link to K2-related websites.

www.k2e.com

www.k2e.ca

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

www.cpafirmtech.com

CPA Firm Technology contains technology-related information explicitly targeted at public accounting firms. We include product reviews, hardware and operating system discussions, affinity programs for CPA firms, and Cloud computing resources.



www.accountingsoftwareworld.com

Accounting Software World provides information related to accounting and financial management solutions. Here, you can find software and service reviews, product comparisons, white papers, and other material of interest to those seeking information about accounting software and service solutions.



www.totallypaperless.com

For information about document management and paperless processes, please visit **Totally Paperless**. In addition, you will find reviews on hardware and software used by all types of businesses in document imaging and management processes.



Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Internal Control Fundamentals

Chapter 1

For many small business owners and managers, internal controls are simply those policies and procedures enacted to prevent theft and fraud. While safeguarding assets is one desirable outcome of an effective internal control structure, it is certainly not the only reason a business – regardless of size – should design, implement, and monitor a system of internal controls.

Learning Objectives

Upon completing this chapter, you should be able to:

- Define what internal controls are and why they are beneficial;
- List and describe the five interrelated components of internal control;
- Identify the necessary steps to implement a system of internal control policies; and
- List and describe the four types of internal control activities.

Definitions and Concepts

Internal Control and the Five Components of Internal Control

Most generally accepted descriptions of internal controls reflect that safeguarding assets is but one objective of an effective internal control structure.

For example, consider the definition of internal controls outlined in the AICPA's **AU-C 315**.

> ***A process effected by those charged with governance, management, and other personnel that is designed to provide reasonable assurance about the achievement of the entity's objectives with regard to the reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations. Internal control over safeguarding of assets against unauthorized acquisition, use, or disposition may include controls relating to financial reporting and operations objectives.***

AU-C 315's predecessor – **SAS 78** – defined the following five interrelated components of internal control.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

1. The control environment sets an organization's tone, influencing its people's control consciousness. In addition, it is the foundation for all other components of internal control, providing discipline and structure.

2. Risk assessment involves the entity identifying and analyzing relevant risks to achieve its objectives, forming a basis for managing risks.

3. Control activities are those policies and procedures that help team members execute management's directives.

4. Information and communication are the identification, capture, and exchange of information in a form and time frame that enable people to carry out their responsibilities.

5. Monitoring is a process that assesses the quality of internal control performance over time.

Figure 1 represents these five components graphically**.**



Figure 1 - Five Interrelated Components of Internal Control Framework

This definition of internal control, adopted by the American Institute of Certified Public Accountants (AICPA) in December 1995 and revised with the recent clarification project, is consistent with the Treadway Commission's Committee of Sponsoring Organizations (COSO) report published in 1992. Key concepts emphasized by COSO include the four listed below.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

1. Internal control is a process. It is a *means* to an end; it is not an end.

2. People affect internal control. It is not merely policy manuals and forms; it is people at every level of an organization.

3. Internal control provides only reasonable assurance, not absolute assurance, to an entity's management and board.

4. Internal control helps the organization achieve objectives in one or more separate but overlapping categories.

Impact on Small Businesses

How does this definition of internal control, including the five components of internal control and the four COSO concepts outlined above, impact small businesses? First, it means that appropriate internal control does more than protect against theft and fraud. Well-designed and implemented internal control helps small business owners meet objectives established for the organization, including those not accounting-oriented. For example, perhaps the owner set a goal for the entity to increase revenue by 15% for the upcoming year. Management should implement appropriate internal control measures to meet that objective.

Second, the presence of the five interrelated components of internal control indicates that the effectiveness of internal control over a particular transaction is not determined solely by completing a given control procedure or activity. Instead, all five internal control components' cumulative effect on that transaction determines internal control effectiveness. To illustrate, assume that a small business owner has established an operational objective that indicates all payroll tax returns are to be filed on time, thereby eliminating costly penalties and interest. Suppose the monitoring component of internal control is not present or does not function correctly. In that case, the business owner cannot know whether the company has met the objective, regardless of how well the other four components may function.

Much professional debate lately has centered on the fifth interrelated component of the internal control framework – monitoring. In response to Sarbanes-Oxley legislation, many companies – including smaller businesses – have struggled with implementing the monitoring element of the framework on a cost-effective basis. As specified by COSO:

> *Monitoring ensures that internal control continues to operate effectively. This process involves assessment by appropriate personnel of the design and operation of controls on a suitably timely basis and the taking of necessary actions. It applies to all activities within an organization and sometimes to outside contractors as well…. Monitoring the effectiveness of already designed and implemented internal controls is an integral part of the IC Framework. A properly designed and structured internal control process should provide feedback through monitoring as to whether the control system is operating effectively to achieve the organization's control objectives.*

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Third, because internal control is a process, it must evolve within an organization to match organizational changes and external influences. These changes include staffing, technology, and moving into different geographic or product markets. Failing to modify the control structure to reflect the current operating environment will almost certainly lead to ineffective internal control.

Fourth, internal control's foundation is people. Recognizing that honest mistakes in judgment will occur, managers should anticipate them. Because of this human element, the quality of a small business' staff will directly impact the effectiveness of the entity's internal controls. Consequently, small business management teams should make all efforts necessary to attract and retain the best people possible for positions in the company.

Fifth, internal control provides *reasonable assurance* – not *absolute – that an entity achieves its* objectives. As stated in SAS 78:

> *The likelihood of achievement is affected by limitations inherent to internal control. These include the realities that human judgment in decision making can be faulty and that breakdown in internal control can occur because of such human failures as a simple error or mistake. Additionally, controls can be circumvented by the collusion of two or more people or management override of internal control.*

Also affecting the degree of assurance offered by internal control is the inherent cost versus benefit consideration relevant to all risks and proposed controls. Specifically, the cost of any internal control procedure should never exceed the expected benefit. Control procedures should reduce risk to a prudent and acceptable level. Because of this cost-benefit relationship, a small business may accept a relatively high level of risk for a specific transaction or process and, in doing so, not incorporate control measures to mitigate the risk, thereby allowing the risk to manifest. This situation most often arises when management misjudges the level of risk or calculates the control measures' cost inaccurately. Internal controls should be proactive, add value, and adequately address exposure to achieve a balance between cost and risk. Failing to do so will result in excessive controls or excessive risks.

Figure 2 demonstrates the concept of balancing controls and risks. Recognizing that there are costs associated with controls, just as there are costs associated with risks, professionals should seek to find the point that *minimizes overall costs*.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

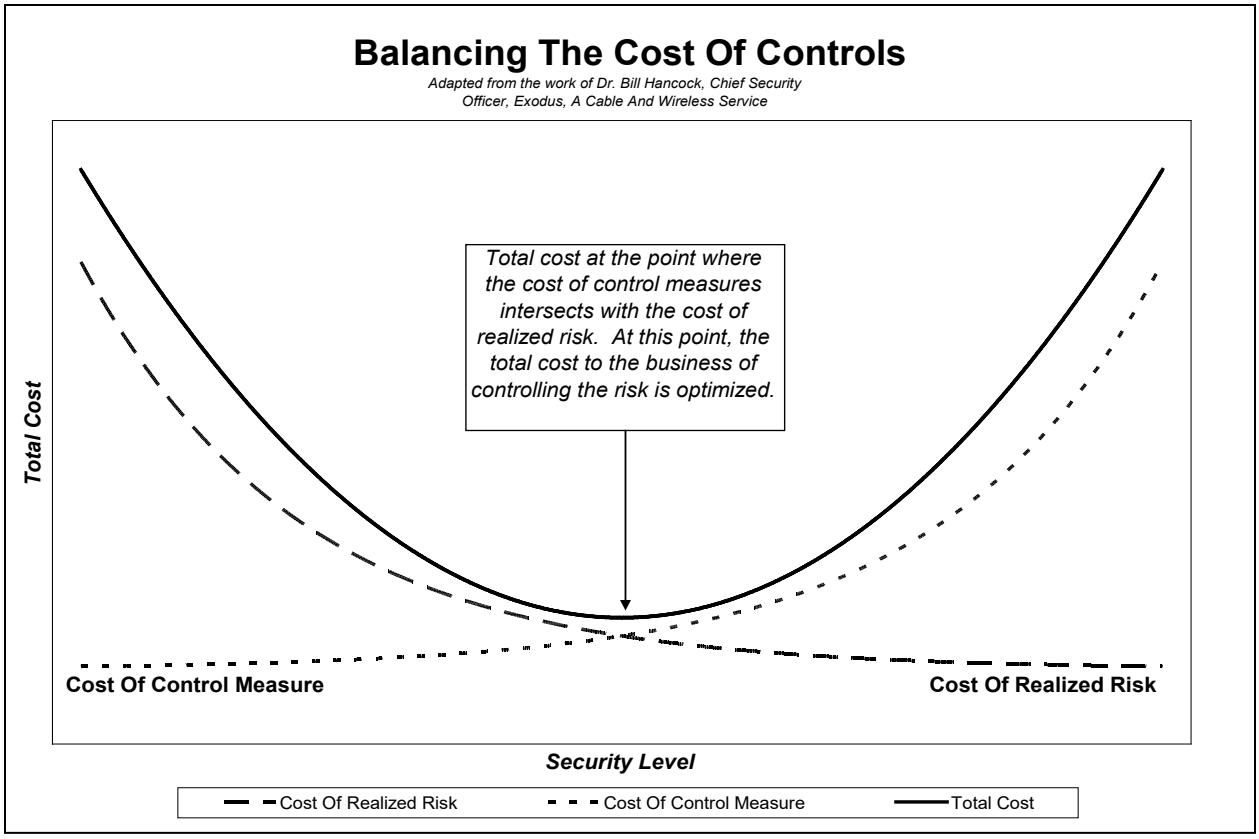


Figure 2 - Balancing the Cost of Controls

Finally, and perhaps most importantly, internal controls help business owners and managers achieve defined objectives. It is fair to assume that many owners and managers have not clearly defined what they are trying to achieve or control in small businesses. Time pressures often force small business owners and managers into "putting out the hottest fire," leaving little time for planning. In the absence of clearly defined entity objectives, the effectiveness of internal control will be substantially limited. Accordingly, identifying those objectives that warrant investing a company's resources is a prerequisite for effective internal control. After defining and documenting these objectives, we develop appropriate internal controls to mitigate the risks of not meeting the goals.

Implementing and Maintaining Internal Control in Small Businesses

As shown in **Figure 3**, there are four distinct phases associated with the process of implementing and maintaining an adequate internal control structure in a small business:

1. Defining specific organizational objectives;
2. Assessing the risk to the organization of not meeting the defined goals;
3. Responding, as appropriate, to the estimated threats; and
4. Monitoring to ensure the satisfaction of objectives over time.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

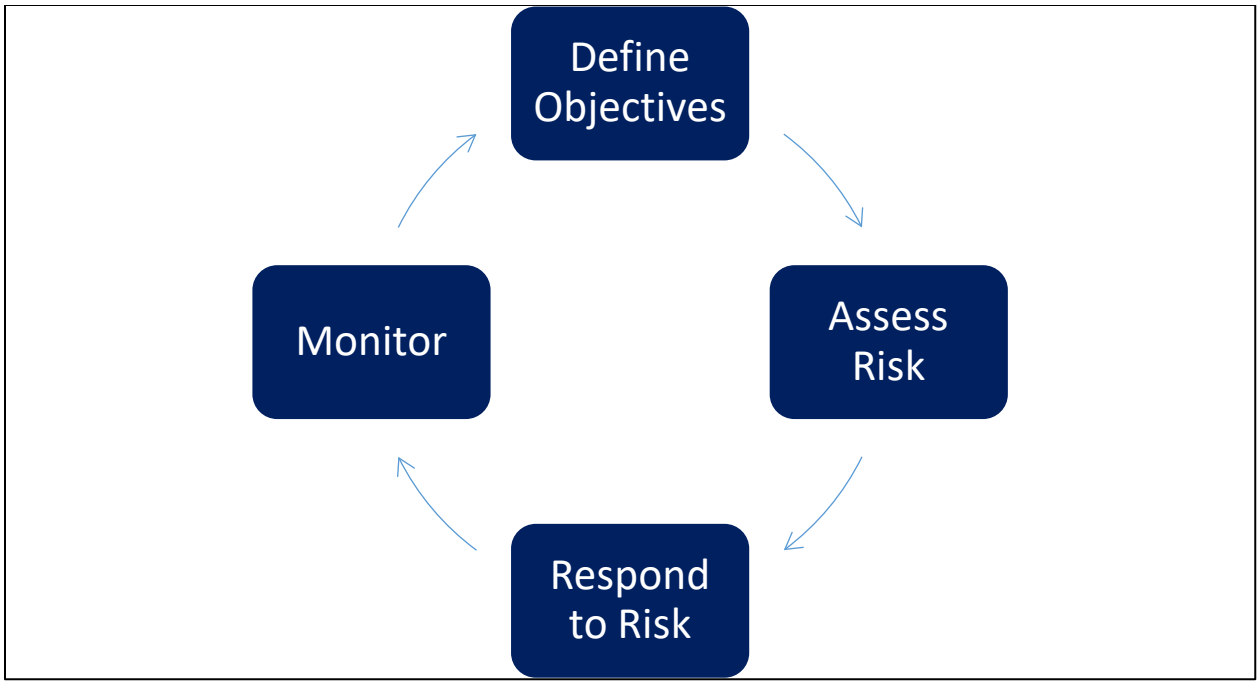


Figure 3 - Four-step Process to Implement and Maintain Internal Controls

Defining Organizational Objectives

As established in AU-C 315 and SAS 78, internal control's central theme is satisfying organizational objectives. Therefore, setting objectives for the organization is a prerequisite to developing control procedures.

An entity's mission statement, business plans, strategic plans, and operational plans establish its' organizational objectives at the highest level. Down the line, departmental objectives should support the company's mission statement and strategic plan. We can classify these goals and objectives into the following three categories.

1. ***Operations objectives***. These objectives pertain to achieving the department's primary mission(s) and the effectiveness and efficiency of its operations, including performance standards and safeguarding of assets.

2. ***Financial reporting objectives***. These objectives include preparing reliable financial reports and preventing misleading or fraudulent financial statements.

3. ***Compliance objectives***. These objectives pertain to adhering to applicable laws and regulations.

Assessing Risks

We can view risk as the likelihood of an event or action adversely impacting the organization. Therefore, for the small business to achieve the established objectives, internal controls must

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

mitigate risk to a prudently acceptable level. Of course, this does not mean we will *eliminate* risk with internal control, for implementing a foolproof internal control system would consume all the entity's resources. Accordingly, the small business owner must accept some risk level with each transaction made by the business. Therefore, the key to success lies in identifying those risks that pose the greatest threats to the company and allocating scarce resources to minimize these risks to an acceptable level.

Internal controls exist to help business owners and managers cope with risk. Responses to risks reduce risk – not eliminate it, in most cases – to an acceptable level. Business owners receive reasonable assurance regarding achieving objectives by performing this function, as outlined in AU-C 315 and SAS 78.

A risk assessment identifies, analyzes, and quantifies the risks associated with achieving operational, financial reporting, and compliance objectives. Fundamentally, risk assessment involves two questions.

1. What could go wrong?

2. What would be the consequences if the items identified in the first question did go wrong?

What Could Go Wrong?

We should ask critical questions to determine the riskiest areas for each established objective. These questions include those listed below.

- How could this process fail?
- What must go right for us to succeed?
- Where are we vulnerable?
- What assets do we need to protect?
- Do we have liquid assets or assets with alternative uses?
- How could someone steal in this process?
- How could someone disrupt this process?
- How do we know if we are achieving our objectives?
- On what information do we rely most?
- To what do we commit the most resources?
- How do we bill and collect revenue?
- What decisions require the most judgment?
- What activities are the most complex?
- What activities are regulated?
- What is our greatest legal exposure?

By asking these questions relative to each objective established by the business, it is possible to identify the risks associated with each objective. Note that the risk identified for each objective may include both internal and external threats.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Transaction types often resulting in higher levels of perceived risk include the following.

- Petty Cash
- Off-site Inventory & Equipment
- Assets with Alternative Uses
- Software Licenses
- Cash Receipts
- Computer Hardware
- Payments to Consultants
- Vendor Rebates & Credits
- Travel Expenses
- Payroll
- Drop-ship Purchases

What Would Be the Consequences?

After identifying the risks, it is necessary to quantify them. To do so, consider the following two factors:

1. Likelihood and
2. Impact.

Likelihood is the probability that an adverse event will occur. It is based on assessing threats (both internal and external) and vulnerabilities (internal).

Impact is the cumulative effect of adverse consequences resulting from threats and vulnerabilities. Whenever possible, express in monetary terms.

The following equation can then define and quantify the risk to the small business.

Risk = Impact x Likelihood

For instance, suppose a manager considers the risk of entering the incorrect due date on accounts payable invoices when inputting the invoices into the accounting software. Observations indicate that this error occurs in 4% of the cases and that the average annual volume is 15,000 invoices. Further, the average dollar loss to the company because of these errors is $2.00 per error. Therefore, in this example, we can compute the annual risk as $1,200: ***Risk = $2.00 x (15,000 x 4%).***

If this risk is unacceptably high, management will implement appropriate internal control responses to reduce the error rate. On the other hand, if the business owner(s) and key managers felt this risk was acceptable, management would likely take no action.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Contrast the above example to the risk of not making backups of critical data on the company's server. The impact of a single failure here may cost the company $200,000, for instance, and the likelihood of needing the backup at some point may be as high as 50%. In this case, the quantified risk is $100,000, an amount that is likely to prompt management to implement internal control procedures over data backups.

Responding to Risks

Once risks have been identified and quantified, the small business owner(s) and managers may choose three action courses.

1. ***Accept the risk as is***. The business owner(s) or managers may accept the risk. This action is the likely – and correct – course of action when the quantified amount of the risk is relatively small. Investing scarce resources is generally not warranted in these cases.

2. ***Attempt to prevent or mitigate the risk***. When the risk is unacceptably high, the business owner(s) or managers should choose to reduce or eliminate the risk by implementing specific control procedures, as long as the controls' cost does not exceed the risk.

3. ***Transfer the risk***. Transferring the risk to a third party may be wise in some cases. Common examples include outsourcing payroll, bank "lockbox" services, and bonding employees who handle cash. This action effectively transfers the risk to a third party.

A holistic approach to the business is essential when determining the appropriate response to risk. In other words, while one segment of the company may carry a high perceived level of risk, there could be compensating controls elsewhere in the organization that effectively reduce the risk. Accordingly, before implementing additional control procedures, it is critical to ensure that the risk is significant and not controlled elsewhere.

Monitoring

Monitoring is the last phase of a small business's internal control system. Monitoring can occur in many ways. For example, business owners and senior managers reviewing key reports and investigating discrepancies are examples of monitoring. Reconciling accounts could be another example of monitoring; likewise, periodic counts of inventory and fixed asset verifications are also a type of monitoring.

Due to their fluid nature, monitoring the internal control structure's ongoing effectiveness is particularly important to small businesses. Because of the lack of corporate overhead and bureaucracy, small companies can make decisions and move much more quickly than their larger counterparts. Thus, change is a constant in a small business; customers, vendors, employees, and information systems continually change. As a result, there is no assurance that risks remain reduced to a prudently acceptable level without adequate monitoring.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Types of Internal Control Activities

SAS 78 defined control activities ***as those policies and procedures that help ensure management directives are carried out***. Examples of common control activities found in many small businesses include:

- Requiring dual signatures on checks;
- Matching purchase orders, receiving reports, and accounts payable bills; and
- Requiring management approval of increases in customers' credit limits.

Four types of control activities fall under the umbrella of accounting controls.

1. Preventive controls.
2. Detective controls.
3. Deterrent controls.
4. Compensating controls.

The following sections discuss each of these.

Preventive Controls

Preventive control activities are those activities that should help to ensure that an entity achieves its control objectives. Managers in small businesses should implement preventive controls to avoid processing invalid transactions and preclude asset misappropriation.

By their nature, preventive controls often require significant amounts of manual effort and intervention. Therefore, they are frequently the costliest form of control to implement. Accordingly, they are typically reserved for situations in which the level of risk is deemed high. Examples of preventive controls include those listed below.

- Dual signatures on checks to prevent unauthorized disbursements, including possible theft
- User IDs and passwords over computer systems to prevent unauthorized access to applications and data
- Physical security over valuable inventory to prevent theft

Control measures that focus on approval, authorization, verification, data security, and segregation of duties are examples of preventive control activities.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Detective Controls

Detective control activities identify instances where undesirable actions have occurred. They provide evidence that an unwanted or adverse event has happened but do nothing to prevent the unwanted action.

Listed below are typical examples of detective controls.

- Reconciliations of accounts to identify errors or irregularities in account balances
- Reporting actual versus budget variances to reveal, after-the-fact, potential overspending
- Exception reports indicating attempts to gain unauthorized access to computing resources to expose, after-the-fact, unsuccessful attempts by users to gain access to applications or data

Moreover, detective controls generally involve reconciliations, performance reviews, and comparing recorded amounts to assets' existence.

In the discussion on preventive controls, a statement was made that preventive controls tend to be relatively expensive. Clarifying the cost of detective control measures is necessary because some professionals contend that detective controls are very costly. Often, detective control measures are relatively inexpensive to implement; however, ***failing to act on situations exposed by the detective control measures can be expensive***. For instance, suppose an actual versus budget variance report detected early in the year that actual spending was running far ahead of budgeted expenditures. Further, suppose that management chose not to act on that information. In that case, no one should be surprised at the year's end when net income falls short of expectations.

Deterrent Controls

Deterrent controls discourage individuals from intentionally violating company policies or procedures. These usually take the form of constraints that make it difficult or undesirable to perform unauthorized activities or threats of consequences that influence a potential violator not to act.

Examples of deterrent controls include the following.

- Effective internal policies and procedures relating to potentially risky areas.
- Warning messages displayed by software applications advising of potentially hazardous actions.
- Admonishing and disciplining employees for improper behavior.

Compensating Controls

As discussed elsewhere in this manual, businesses of all sizes – and small businesses in particular – often have one or more areas of weak internal control. For instance, preventive internal control

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

procedures are frequently inadequate in a small business where the owner is actively engaged in revenue production. This weakness occurs because the business owner is preoccupied with other functions and lacks time to execute preventive control measures. In such cases, compensating controls can be developed to mitigate the risks associated with certain transactions.

Common examples of compensating controls follow.

- Exception reports indicating expenditures over a certain level, customers over credit limits, customers with balances more than ten days past due
- Preauthorized and negotiated pricing for items purchased from vendors
- Reports indicating new customers or vendors added to the accounting system

In each of the examples provided, the control measure functions similarly to a detective control; though subtle, the primary difference is that the ***compensating effort counteracts known internal control weaknesses*** while the detective control complements other control measures.

One effective form of compensating control is owner-manager controls, also known as alternative controls. Owner-manager controls are those procedures assigned to and executed by an owner or senior manager to overcome weaknesses elsewhere in the control structure.

?	Reflecting on the mix of internal control activities in your organization or that of a client, what relative percentage would you assign to each of the following four internal control activities? • Preventive controls? • Detective controls? • Deterrent controls? • Compensating controls? Given your responses, what actions might be appropriate to improve the internal control structure in that organization?

Administrative and Accounting Controls

Two broad classifications of internal controls exist – administrative controls and accounting controls. In a well-designed system of internal controls, these two types of controls complement each other.

Administrative Controls

Administrative controls govern operations and transactions up to authorization and promote operational efficiency and adherence to company policies. Examples of administrative controls

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

include establishing written codes of conduct for employees, developing personnel recruiting and hiring policies, and documenting an entity's organizational structure.

Control Environment of Small Businesses

Many small businesses fail to address the issue of administrative controls adequately. For instance, job descriptions, employee handbooks, and other policies and procedures are often not documented. This lack of documentation is a significant weakness when addressing an entity's internal control procedures because failing to maintain strong administrative controls weakens the control environment.

Regarding the control environment of small businesses, several common issues often give rise to internal control deficiencies.

- Management's Philosophy and Operating Style
- The Entity's Organizational Structure
- Methods of Assigning Authority and Responsibility
- Management's Control Methods for Reviewing Performance
- Personnel Policies and Practices

Generally, organizations that foster an effective control environment increase internal control effectiveness.

Accounting Controls

Accounting controls ensure the safeguarding of assets and the reliability of financial records. Accounting controls directly affect the transactions recorded in the accounting system. It is important to note that the term "accounting system" refers to the process whereby an entity records, processes, and reports transactions throughout this course***.*** Therefore, the term accounting system does not necessarily imply using a computerized accounting application in this context. Many small businesses utilize an accounting system consisting of manual and automated procedures. However, the accounting system remains a system of only manual processes for a modest number of small businesses.

We can subdivide accounting controls into two subcategories: *general controls* and *application controls*. ***General controls apply to many, if not all, parts of the accounting system***. Backups, facilities security, and computer access controls are all examples of general controls. ***Application controls relate to a specific module of the accounting system***. For example, when entering accounts payable invoices into an accounting software application, having that application execute an edit on the invoice number field to ensure that the invoice is not already in the system represents an application control.

Because so many small businesses utilize off-the-shelf accounting software in their accounting system, specific examples of application controls associated with some of the more popular accounting software applications are provided later in this course.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

The Relationship between Administrative and Accounting Controls

When evaluating or designing internal controls for small businesses, accounting and finance professionals should recognize that an effective internal control structure combines administrative and accounting controls to achieve organizational objectives. Stated differently, administrative and accounting controls are complementary – each strengthens the other. In many cases, though, the administrative controls in a small business will be relatively weak. A robust set of accounting controls often overcomes this weakness. However, though the accounting controls may be both adequate and effective, it could be possible that the administrative controls are so weak that the entire internal control structure is inadequate and ineffective. Therefore, exercise appropriate caution when relying only on accounting controls.

To illustrate this relationship, suppose a company had implemented thorough accounting controls over the purchasing process:

- Prices were negotiated and contracted at the beginning of the year;
- Purchase orders are utilized and accounted for;
- Receiving reports were completed upon each receipt of a shipment, etc.

Yet, suppose the administrative controls leading to authorizing a purchase were inadequate. In that case, the company could stock sub-optimal inventory levels despite strong accounting controls. In this example, the administrative controls should address such items as who is authorized to issue purchase orders and the desired minimum and maximum inventory levels. By combining effective accounting *and* administrative controls, the company is more likely to achieve its objective of maintaining and optimizing its investment in inventory. **Figure 4** presents a flowchart model of administrative and accounting controls.

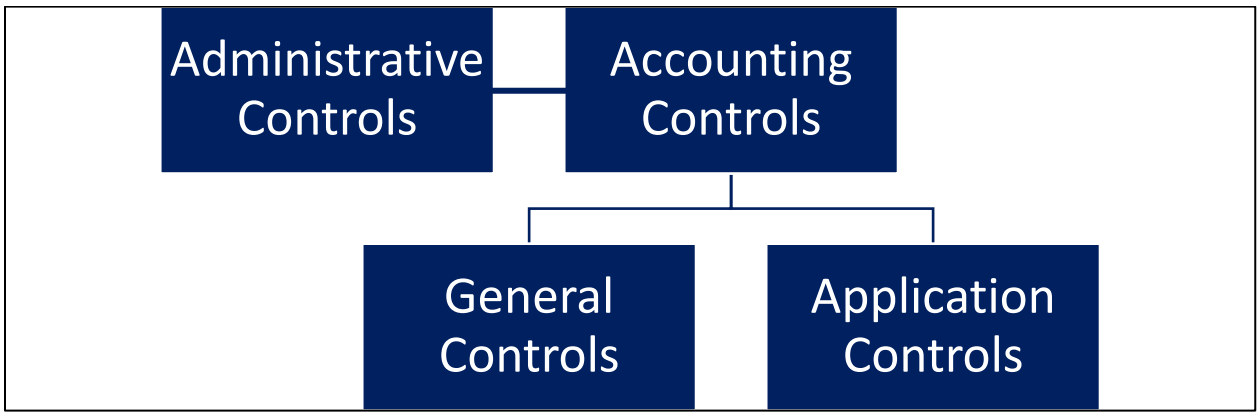


Figure 4 - The Relationship between Administrative and Accounting Controls

Alternative Controls

Business owners and senior managers perform ***owner-manager controls*** to enhance an entity's internal control's overall effectiveness. In addition, businesses frequently implement these

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

controls to compensate for weaknesses in other areas. Alternative controls are particularly important in small companies where proper segregation of duties is absent. Should segregation of duties not exist in areas of the business or transactions, it may be possible for the owner or a key manager to execute specific measures to compensate for the lack of segregation of duties. Using alternative controls in this fashion elevates the business's overall internal control structure.

Some common examples of alternative controls used in small businesses today are listed below.

- An owner's or senior manager's signature is required on all checks.
- An owner or senior manager is personally involved with preparing payroll checks.
- An owner or senior manager performs the delivery of paychecks.
- Mail is received and opened by an owner or senior manager.
- An owner or senior manager supervises physical counts of vulnerable inventory items.
- Critical accounting estimates, such as depreciation, percentage of completion on construction contracts, and bad debt allowances, are personally approved by an owner or senior manager.

When designing and implementing alternative controls, one critical consideration is the time required of an owner or senior manager to perform these functions. In many small businesses, owners and senior managers are generally heavily involved in generating revenue, producing products, or delivering services. Consequently, any time spent on alternative control measures will take away from time available for other responsibilities. Therefore, the owner or senior manager must perceive that they are engaged in controlling the business's high-risk areas. In other words, owners or senior managers should not perform menial tasks involving areas with minimal risk; they must use their time wisely.

Detective and Deterrent Nature of Alternative Controls

Many effective alternative control procedures will be more of a detective and a deterrent than a preventive nature. Particularly when owners and senior managers are preoccupied with other tasks, it will be challenging to implement preventive alternative control procedures. Preventive controls are generally the most expensive; reserve them for the operation's riskiest areas.

The widespread use of small business accounting software facilitates implementing detective and deterrent alternative controls through two different means. First, in many cases, we can control the authorization of transactions to some degree by the application software. For instance, a Sage 50 Quantum software feature can automatically generate purchase orders based on pre-established reorder points. However, assuming access to the reorder points remains restricted, it may not be necessary for owners or senior managers to approve every purchase order. Instead, managers effectively established each purchase's authorization upon entering the reorder points for individual items. Therefore, having an owner or senior manager sign off on purchase orders based on pre-established reorder points approved previously by an owner or senior manager is a potentially unnecessary control procedure and a wasteful allocation of scarce resources. On

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

the contrary, if justified by risk, more effective internal control over purchasing might include one or more of the following alternative control procedures.

- Ensuring that an owner or senior manager reviews an exception report of purchase orders exceeding a predetermined amount.
- Owners or senior managers review and approve exception reports of purchase orders issued to vendors not listed as the primary or default vendor for the items ordered.
- Create an exception report of items ordered and received where the invoice amount differed from the amount on the purchase order and have the report reviewed by an owner or senior manager.

In each of these examples, exception reports identify potentially questionable transactions. However, the transactions have already been entered and executed in these examples. Therefore, the control procedure is either detective or deterrent instead of preventive. An important consideration is this – because the transactions identified on the exception reports are, by definition, questionable, so investigate each one thoroughly. Failing to do so could lead to potentially disastrous consequences.

Effective Small Business Alternative Control Procedures

Several critical alternative control procedures are available in small business accounting software applications. When a control weakness exists, owners and managers should consider utilizing these software-driven tools. Some of the most common features include the following.

- Audit Trail Reports
- Exception Reports
- Database Queries
- Digital Dashboards
- Actual vs. Budget Reports

Evaluating Alternative Controls

Alternative controls can effectively strengthen a small business's internal control, mainly when properly segregating duties is not possible or practical. First, however, consider several key questions when designing and implementing alternative control procedures, including the following.

- Does the individual(s) charged with the tasks understand and appreciate their responsibility for managing risks relative to the company's success?
- Does the individual(s) executing the procedures have the skills, training, and resources to complete the tasks without exception?

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

- Does the individual(s) charged with the tasks have the integrity and objectivity to protect the owner(s) interests?
- Does the individual(s) charged with the tasks have the specific authority to act on information obtained while executing this/these assignment(s)?
- Who, if anyone, will perform these tasks when the individual(s) with primary responsibility is/are away from the office for an extended period?

Further, in cases where the small business is struggling, professionals must understand that an owner or senior manager may be motivated to circumvent internal control related to financial reporting. When this occurs, the intent is often to generate fraudulent financial statements. This risk increases when there is a threat of imminent bankruptcy or foreclosure. It also could materialize when owners guarantee significant debts. For such reasons, alternative control measures do not cure all ills. Instead, consider them another component of effective internal control for small businesses.

?	Could you remedy specific internal control deficiencies in an organization by implementing alternative controls? If so, what alternative controls would be appropriate to improve the internal control structure in that organization?

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Fraud Today

Chapter 2

Fraud is alive and well! From large, multinational companies to small, family-held businesses, fraud plagues organizations worldwide, costing billions annually. This chapter examines the breadth and depth of fraud to illustrate the need for more efficient and practical techniques to prevent and detect the schemes that drain profits and productivity from the economy.

Learning Objectives

Upon completing this chapter, you should be able to:

- List the significant occupational schemes fraud activities and their related costs;
- Identify the general characteristics of those who commit fraud;
- Differentiate between asset misappropriation, corruption, and financial statement frauds and identify the risk factors contributing to each; and
- Identify the roles of accountants and auditors in efforts to deter fraud.

The Current State of Affairs

Fraud in the United States

Fraud continues to plague businesses at epidemic levels, and virtually every study on the subject supports this statement. For example, dating back to 2013, consider KPMG's comments in the *Integrity Survey*.

> *The prevalence of misconduct that could cause "a significant loss of public trust if discovered" increased. Of the employees surveyed in 2013, 56 percent characterized the misconduct they had observed as serious and possibly resulting in a significant loss of public trust, as compared to 46 percent in 2009 and 50 percent in 2005.*[1]

[1] "Integrity Survey 2013," KPMG Forensics, https://www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Documents/Integrity-Survey-2013-O-201307.pdf

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Perhaps it is not surprising then to find that ***73% of the respondents to this survey reported that they had observed misconduct in their organizations within the prior twelve months***.

Likewise, consider the following quote from the same study published by KPMG Forensics.

> *One of the most commonly-cited drivers of misconduct continues to be attributed to pressure to do "whatever it takes" to meet business goals. Other commonly-cited causes included not taking the organization's code of conduct seriously, having in place systems that rewarded results over means, and the fear of job loss if targets are not met.*

The KPMG study results are consistent with other studies and surveys on the matter. Perhaps the leading organization in the battle against fraud is the Association of Certified Fraud Examiners (ACFE). The ACFE conducts a semi-annual survey on occupational fraud's pervasiveness in the United States, Canada, and other countries worldwide. The ACFE published these studies in 1996, 2002, 2004, 2006, 2008, 2010, 2012, 2014, 2016, 2018, 2020, 2022, and 2024. Key findings of the most recent survey are listed below.

- The median estimate of Certified Fraud Examiners is that occupational fraud consumes 5% of all business revenues.
- Annual occupational fraud losses approximate $4.7 trillion worldwide.
- The average loss per case is $1,783,000, and the median loss caused by a single case of occupational fraud in the United States and Canada is $120,000 (USD).

Based on these numbers, there can be little doubt that fraud is alive and well today.

Fraud On An International Level

Interestingly, this problem seems to transcend borders and is not limited to the United States. For example, in a PricewaterhouseCoopers study of fraud on an international level, 45% of the respondents reported that they had suffered a fraud loss within the past two years; the average amount of the loss exceeded US$1.7 million.[2] Likewise, a KPMG study of fraud in Australia and New Zealand indicated that 47% of respondents had experienced fraud within the past year, with an average loss of US$714,000.[3]

---

[2] "Global Economic Crime Survey 2005," PricewaterhouseCoopers, http://www.pwcglobal.com/gx/eng/cfr/gecs/PwC_2005_global_crimesurvey.pdf

[3] "Forensic Fraud Survey 2006," KPMG Forensic, http://www.kpmg.com.au

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Summary of Fraud Studies

We have summarized data from the following publications to help you better understand the nature and pervasiveness of fraud. With this understanding, you can implement solutions to prevent and detect fraud.

1. *Occupational Fraud 2024: A Report to the Nations* published by the Association of Certified Fraud Examiners and
2. *Global Economic Crime Survey* published by PwC Global.[4]

Effective anti-fraud measures, including technological tools, can be implemented only with a complete understanding of the fraud environment.

Who is Committing Fraud?

It would be misleading to imply that only one group or class of employees commit fraud. According to the PwC report, 36% of responding organizations had experienced at least one economic crime; at this frequency of occurrence, it is clear that employees commit fraud throughout all levels of organizations. The ACFE report indicates that managerial and executive employees commit over half of all frauds (60%). Further, when an owner/executive or manager commits fraud, the loss is significantly higher than in those cases where a rank-and-file employee commits the act, as shown in **Figure 5**.

[4] "Global Economic Crime Survey 2016," PwC Global, http://www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey.html

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

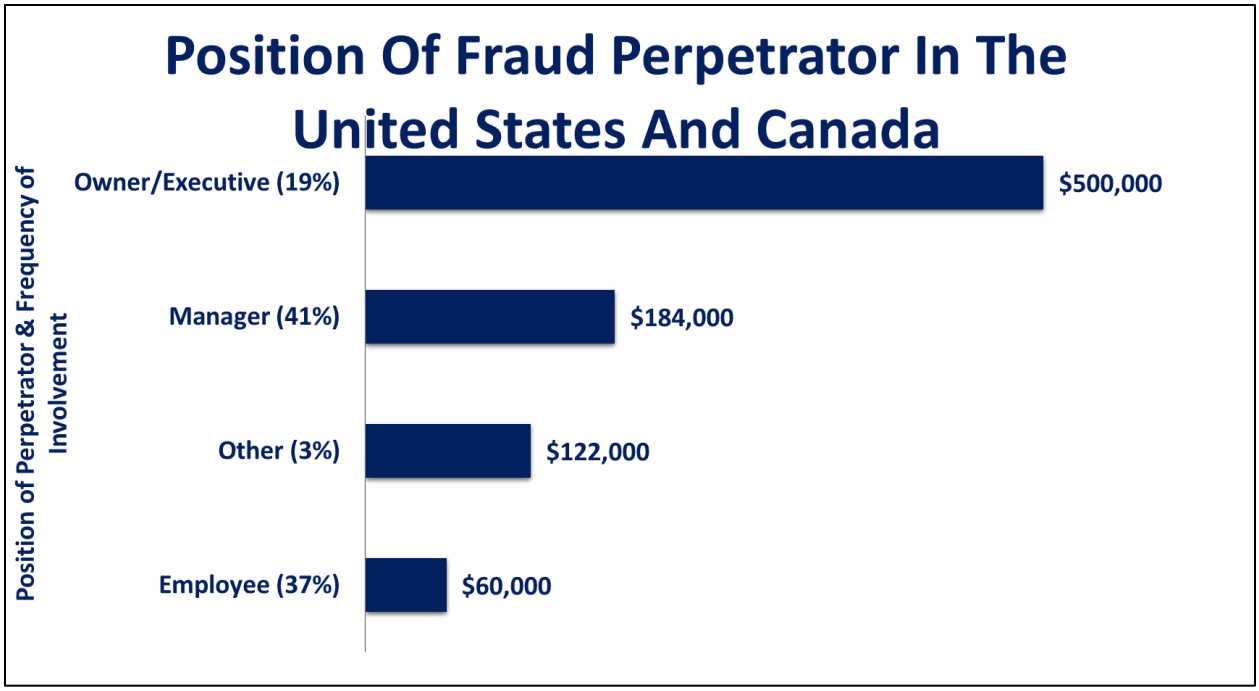


Figure 5 - Position of Perpetrator Chart

There is a correlation between an employee's tenure and the amount of fraud loss. As shown in **Figure 6**, according to the ACFE report, employees with a longer tenure at an organization commit more expensive frauds than team members with a shorter tenure. This condition is probably attributable to most organizations' higher trust in longer-tenured employees. It also reflects that, in many cases, senior managers and employees with higher earnings have longer than those with fewer responsibilities and smaller incomes.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

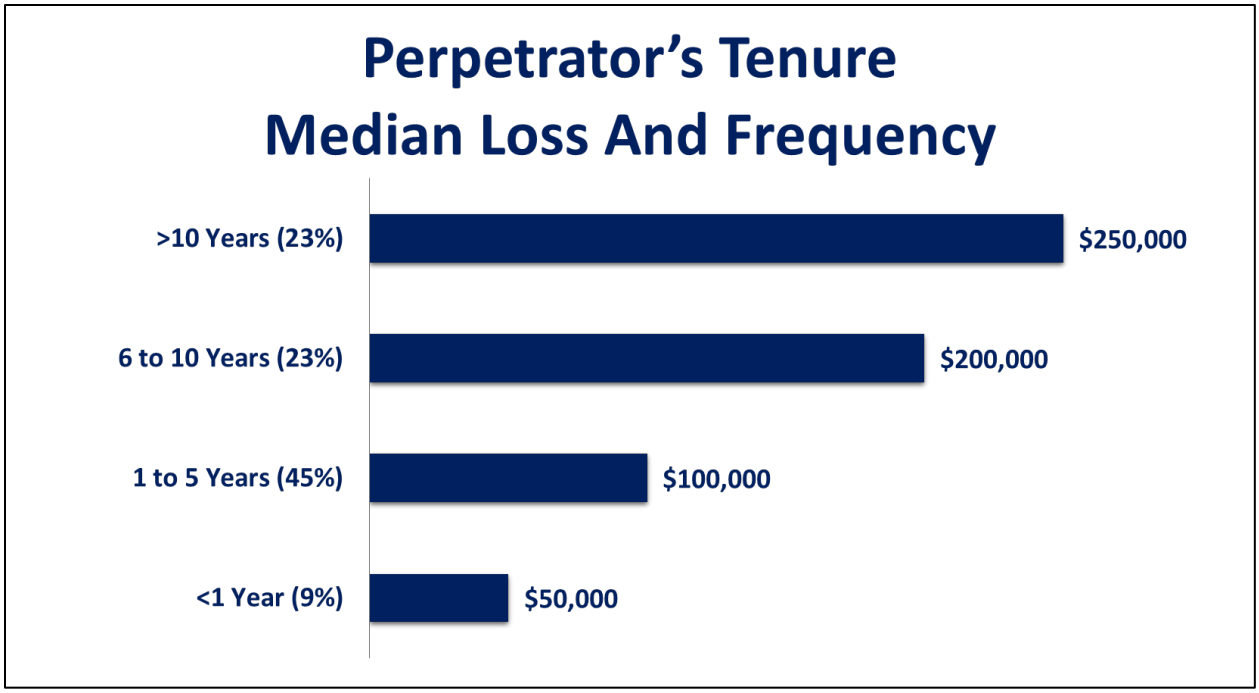


Figure 6 - Perpetrators' Tenure Compared to Median Loss

An interesting statistic associated with perpetrators' positions is that frauds committed by higher-level perpetrators take, on average, longer to detect than frauds committed by lower-level perpetrators, as confirmed in **Figure 7**.

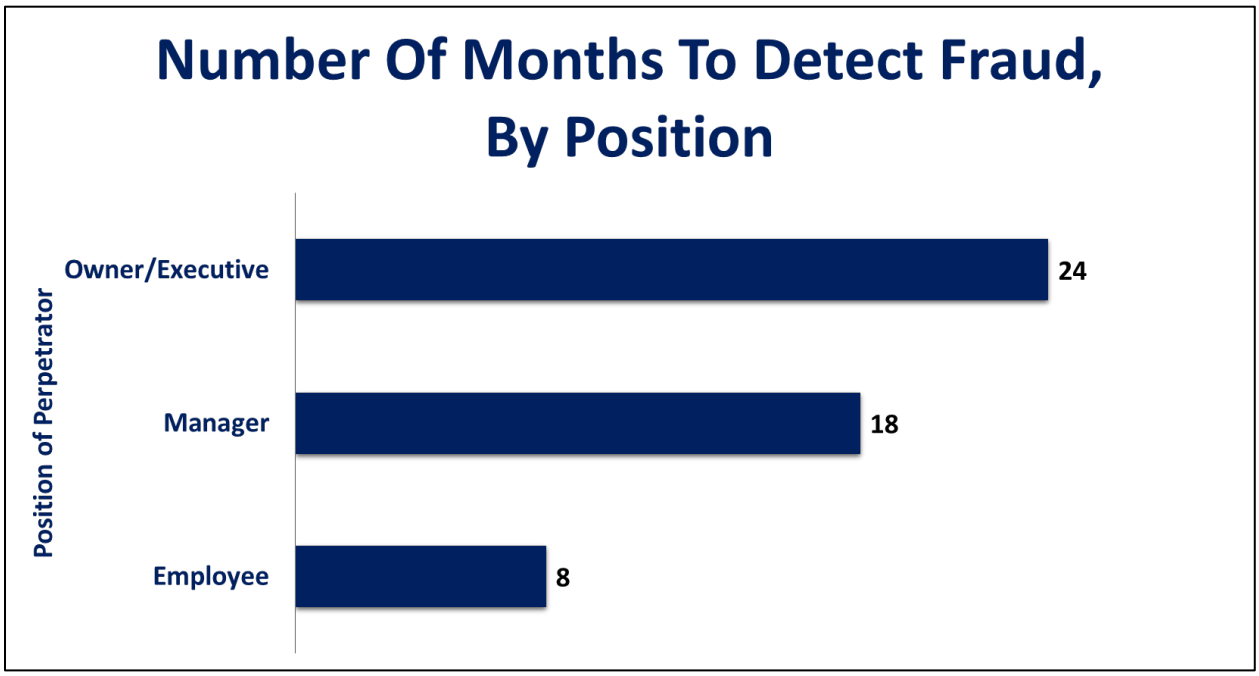


Figure 7 - Months to Detect Fraud by Position of Perpetrator

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

The ACFE reports also indicate that just one employee does not always commit fraud. More specifically, as shown in **Figure 8**, collusion among two or more persons is involved in over half of all scams.

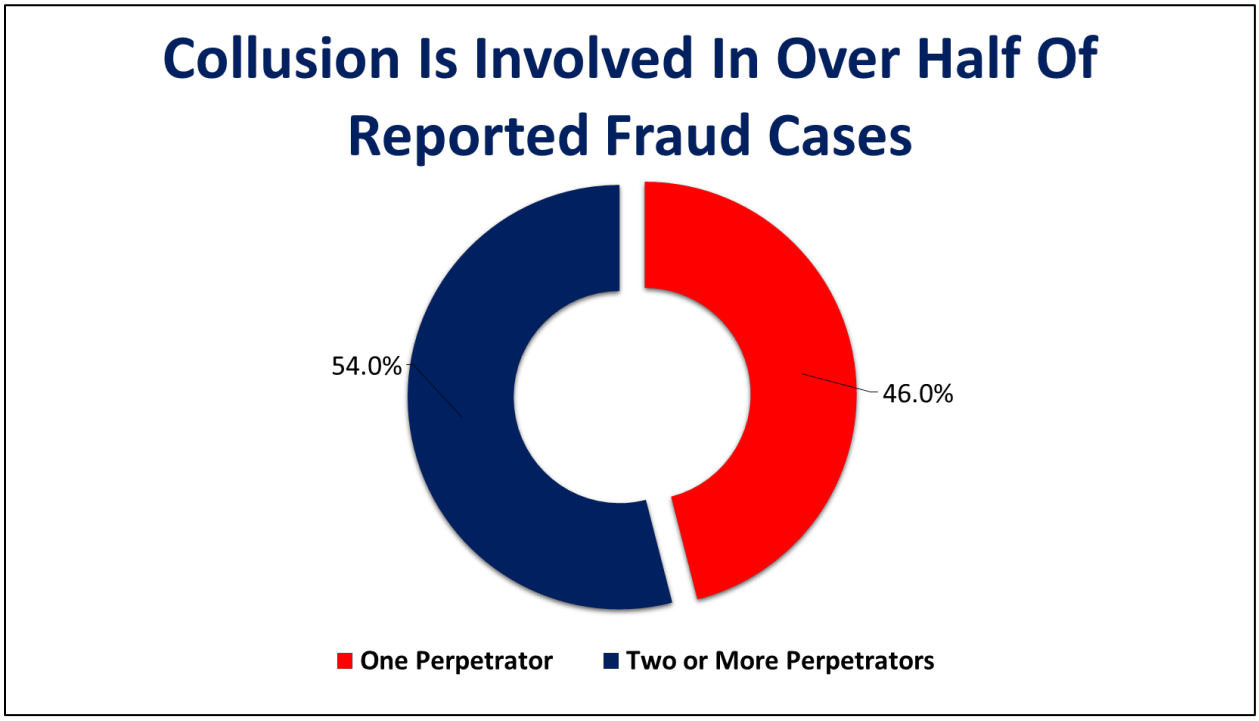


Figure 8 - Number of Perpetrators Chart

As shown in **Figure 9**, the median loss is significantly higher when collusion exists.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

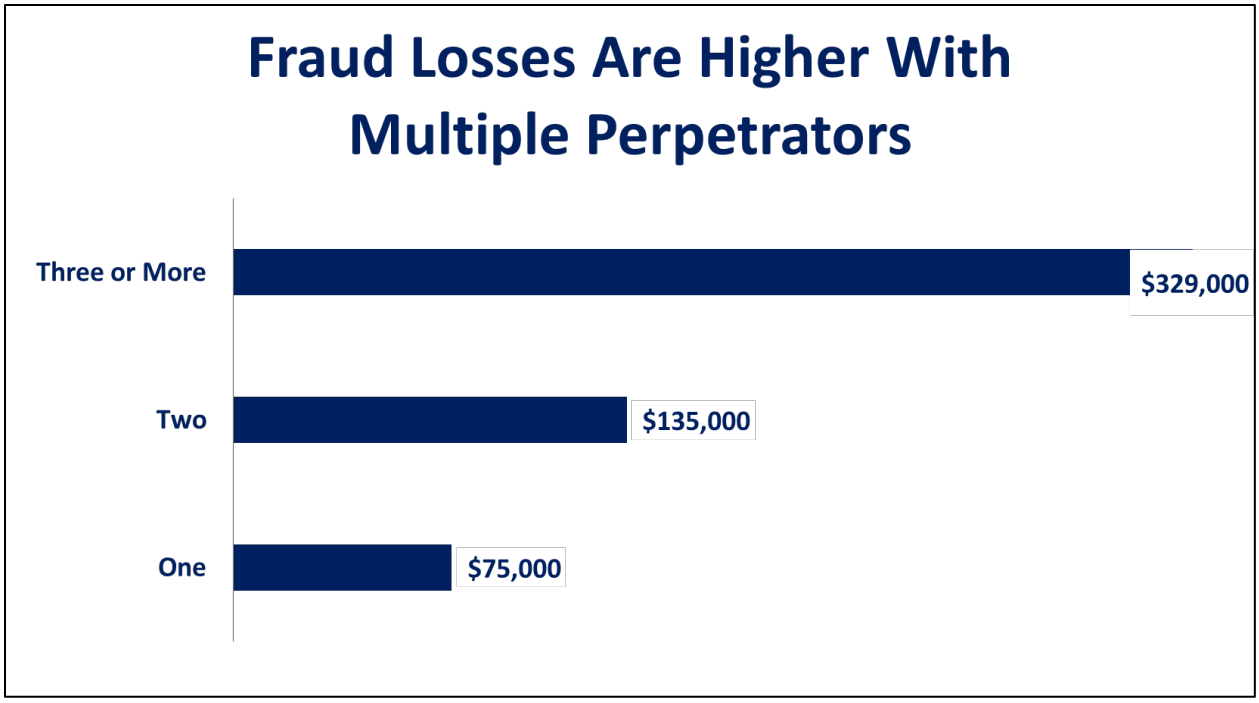


Figure 9 - Fraud Losses by Number of Perpetrators

One common question involves the history of those charged with committing occupational fraud. As shown in **Figure 10**, 87% of the perpetrators identified in the ACFE report had no prior fraud charges or convictions.

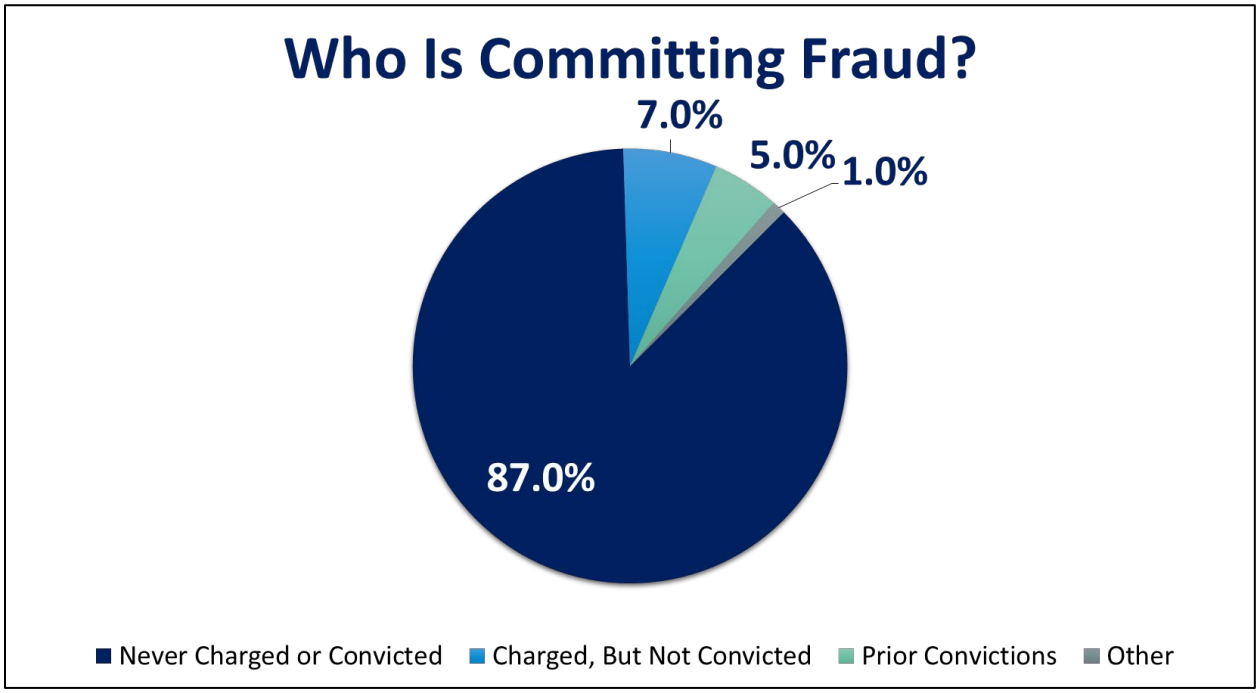


Figure 10 - Perpetrators' Prior Criminal History Chart

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

?	With the benefit of hindsight applied to an instance of occupational fraud with which you are familiar, what could have or should have been some of the early warning signs that the person(s) committing the fraud was facing financial difficulty?

What Types of Frauds Are Being Committed?

The ACFE defines occupational fraud as:

> *The use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets.*

These frauds have four common characteristics.

1. The activities are clandestine. When committing occupational fraud, the perpetrators make attempts to conceal their actions. These attempts might involve altering or destroying documents, failing to record transactions, or deleting information from computer systems.
2. The activities violate the perpetrator's fiduciary responsibilities and positions of trust within the employing organization. Employers entrust all team members with some level of fiduciary responsibility. When committing fraud against an employer, an employee breaches that trust. As demonstrated in the previous section, employees in whom employers place large amounts of trust are in positions to commit frauds of greater magnitudes.
3. The activities are committed for personal enrichment, either directly or indirectly. For example, criminals do not commit fraud as a hobby. Instead, there is some financial gain to derive from the activity. This gain can accrue directly to the perpetrator or benefit a third party of the perpetrator's choosing – for example, a family member.
4. The activities exact a cost on the employing organization. Because frauds enrich their perpetrators, the employing organization has an offsetting loss. The scam might result in the direct loss of assets, or it might result in less apparent losses, such as reputation damage and loss of investor confidence.

There are three types of occupational fraud: misappropriation of assets, corruption, and financial statement fraud. As shown in **Figure 11**, asset misappropriation is the leading source of fraud, according to the ACFE, though financial statement fraud is the costliest.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

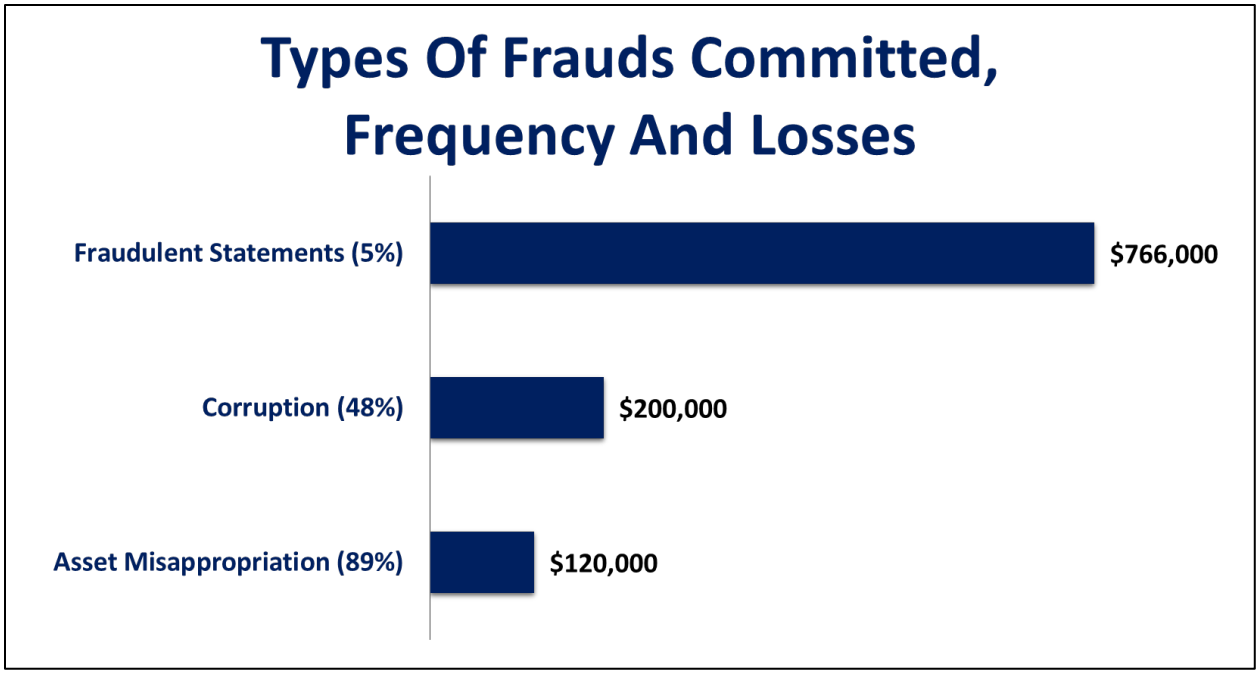


Figure 11 - Relative Frequency of Fraud and Associated Loss *(Percentages do not total to 100% because some fraud instances involve more than one fraudulent activity.)*

In an asset misappropriation scheme, cash is the asset most often stolen, according to the ACFE. **Figure 12** details asset misappropriations, including the three cash misappropriation schemes. These three types of cash fraud schemes are:

1. Those involving cash receipts (skimming and cash larceny);
2. Those involving cash disbursements (billing, check tampering, expense reimbursement, payroll, and register disbursements); and
3. Those involving cash on hand.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

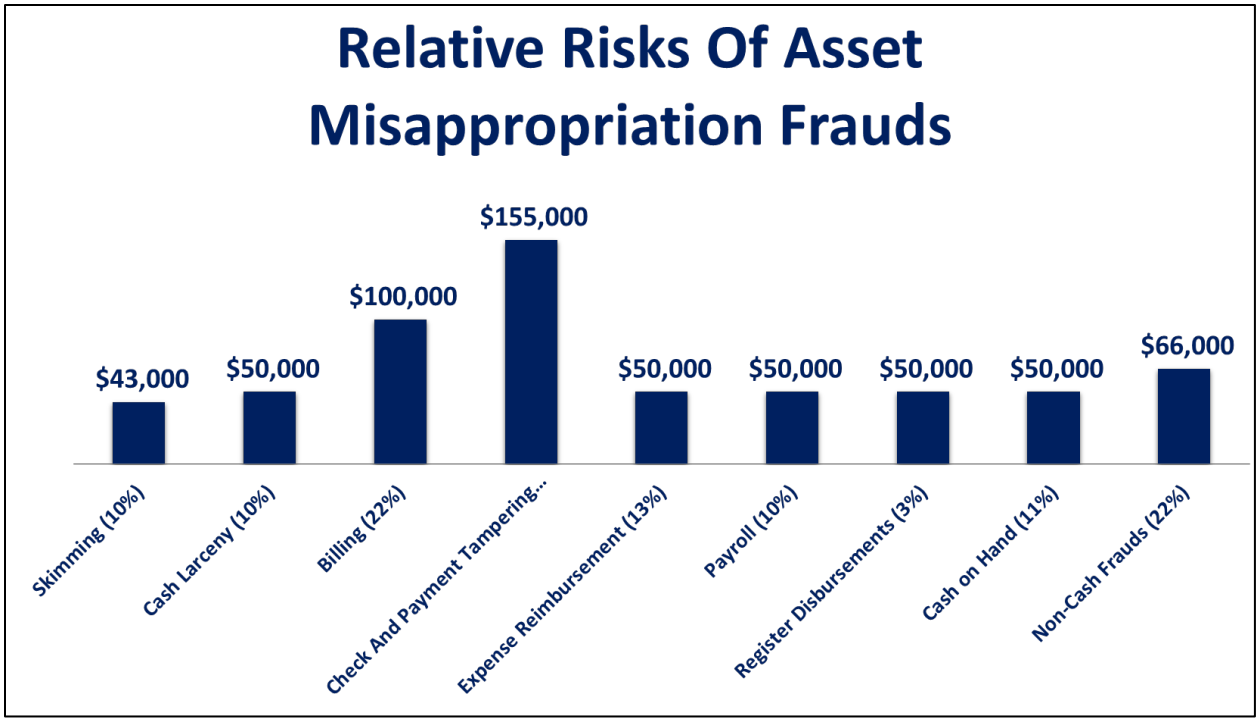


Figure 12 - Breakdown of Asset Misappropriations *(Percentages do not necessarily total 100% because some frauds include more than one fraudulent activity.)*

How Much is Fraud Costing?

As stated earlier, occupational fraud is estimated to cost organizations 5% of their annual revenues; in the United States, this extrapolates into over $1 trillion yearly or over $8,200 per full-time employee. According to the ACFE, public and private companies realized median fraud losses of $150,000 per incident. Further, national governmental organizations reported estimated median losses of $210,000, while nonprofit organizations reported median losses of $76,000.

In addition to the variation in fraud losses based on the type of organization involved, fraud losses also vary based on the victim's industry, as indicated in **Table 1.**

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Industry	Median Loss
Mining	$550,000
Wholesale Trade	$361,000
Manufacturing	$267,000
Construction	$250,000
Real Estate	$200,000
Government & Public Administration	$200,000
Insurance	$190,000
Services (Other)	$170,000
Information	$166,000
Agriculture, Forestry, Fishing, & Hunting	$165,000
Energy	$152,000
Technology	$145,000
Transportation & Warehousing	$121,000
Banking/Financial Services	$120,000
Utilities	$100,000
Service - Professional	$100,000
Health Care	$100,000
Food Service and Hospitality	$100,000
Religious, Charitable, or Social Services	$85,000
Education	$50,000
Retail	$48,000
Arts, Entertainment, & Recreation	$44,000

Table 1 - Median Fraud Losses by Industry

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

By size of the organization, **Figure 13** depicts the frequency and the median loss of frauds.

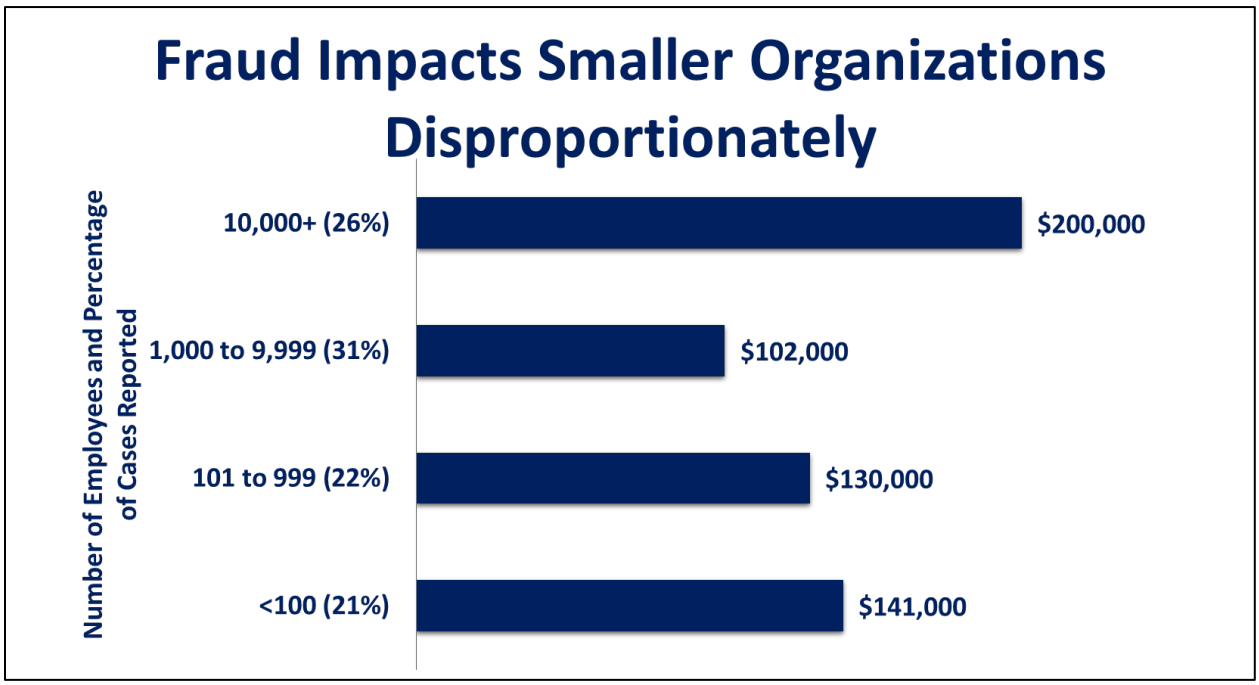


Figure 13 - Losses by Number of Employees Chart

Fraud Schemes in Small Businesses

Given the disproportionate impact of fraud on small businesses (those with fewer than 100 employees), it is helpful to understand the types of fraud committed most frequently in these organizations. For example, small businesses are not as often victims of corruption fraud as larger organizations (44% of cases in small companies versus 52% in larger organizations). However, small businesses are susceptible to many other fraud schemes at a greater rate than their larger counterparts, as shown in **Figure 14**. This chart should be instructive for owners and managers working in small businesses and trusted advisors providing services to small companies when allocating anti-fraud resources.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.



Figure 14 - Fraud Scheme by Size of Victim

What Are the Internal Control Weaknesses That Contribute to Occupational Fraud?

How can large and small organizations continue to experience such sizeable occupational fraud losses? One of the key reasons is the internal control structures – or lack thereof! – in many organizations. **Figure 15** illustrates that the lack of internal controls, override of existing internal controls, and lack of management review are primarily responsible for many occupational frauds.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

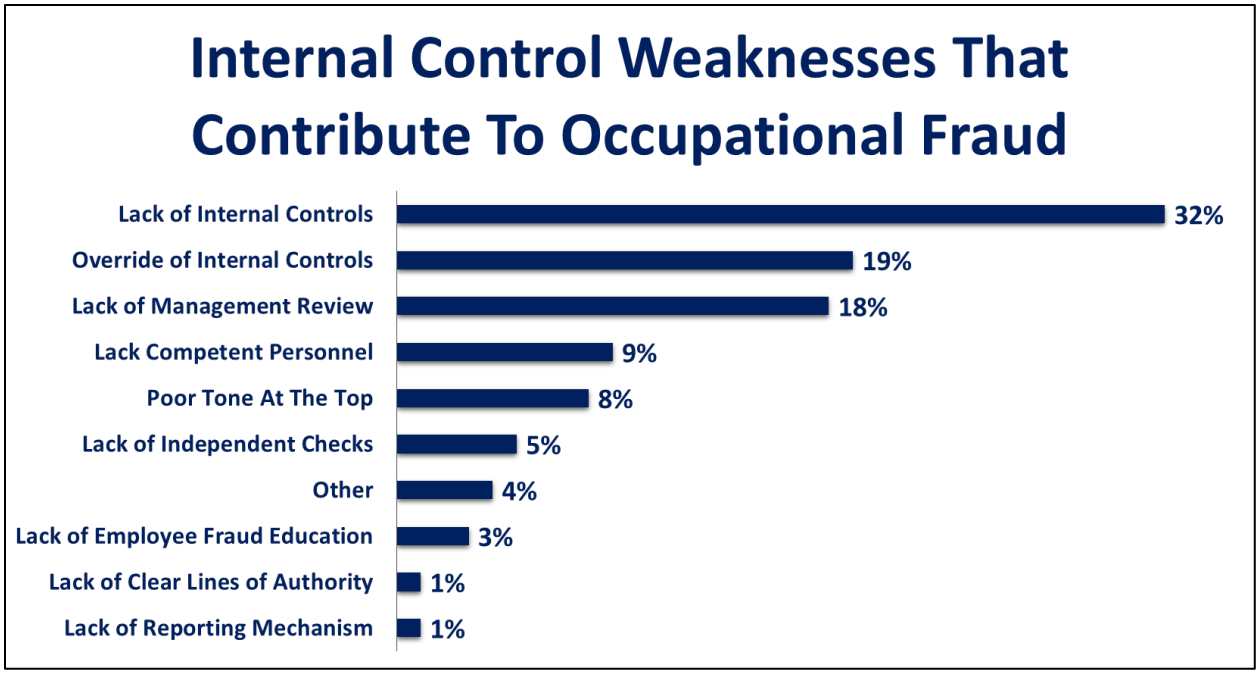


Figure 15 – Internal Control Weaknesses That Contribute to Occupational Fraud

How Is Fraud Being Detected?

Many accountants and auditors instinctively assume that internal controls are the leading fraud detection source when considering fraud detection. In fact, according to the ACFE report, tips were the number one source of fraud detection. This fact is significant from a stand-alone perspective. However, when you view it in light of the Sarbanes-Oxley requirement that mandates audit committees establish a means of "anonymous submission by employees of the issuer of concerns regarding questionable accounting or auditing matters," it takes on even greater significance.

Figure 16 presents a summarization of how frauds are initially detected. Interestingly, accidental detection is more likely than detection through more established measures, such as account reconciliations, document examinations, and external audits.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

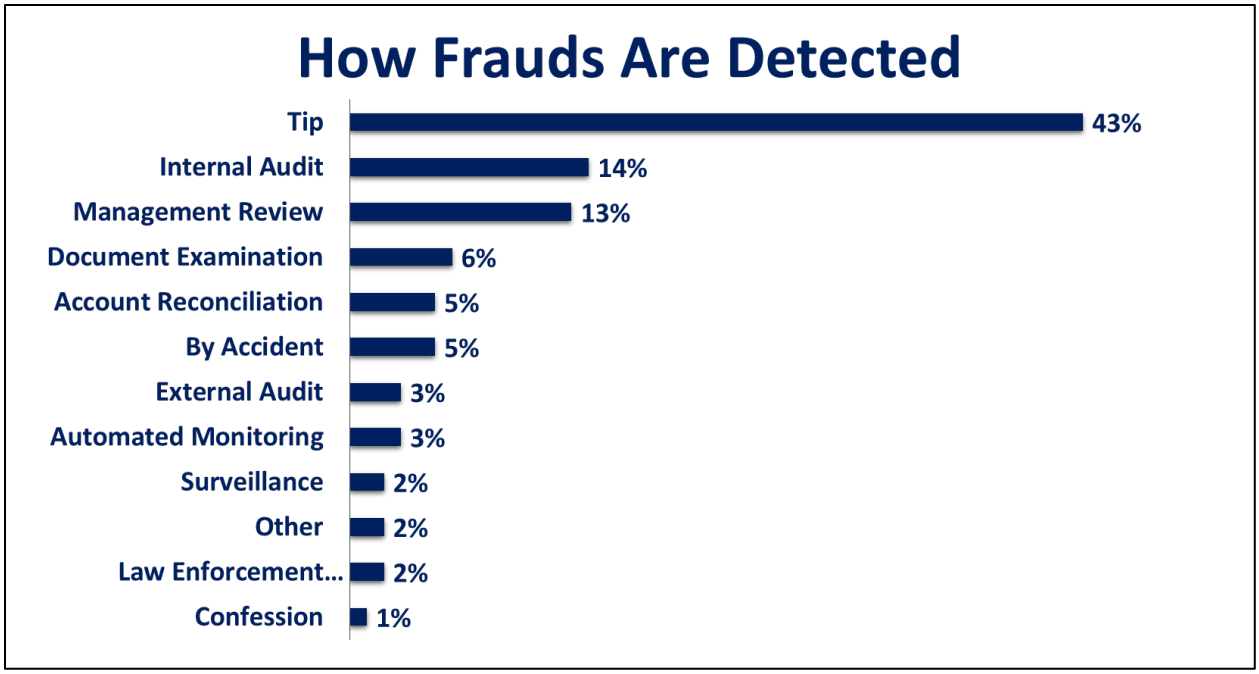


Figure 16 - How Frauds Are Detected Chart *(Percentages may not total 100% due to rounding.)*



Figure 17 – Sources of Tips for Occupational Fraud
(Percentages may not total 100% due to rounding.)

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

?	Given the fraud statistics outlined in this section, where do you see vulnerabilities in your organization or a client's? What internal control activities could you implement to reduce the organization's exposure to theft and fraud?

The Role of Accountants and Auditors

Occupational and organizational fraud is an international economic epidemic, the effects of which are surfacing and being understood and quantified. So, how did the situation get this dire?

First, it is necessary to understand that fraud is not new. Recent headlines involving fraud might cause one to assume that fraud is a relatively new phenomenon. However, accounting literature is replete with sordid stories of fraud and deception, including the rash of frauds at Enron, Tyco, WorldCom, Parmalat, and other publicly traded companies. Certainly, one of the more notable is the scheme masterminded by F. Donald Coster at McKesson & Robbins.

By orchestrating bogus purchase orders and shipping documents and transferring cash among numerous accounts, Coster was able to cause McKesson's inventories and accounts receivable, as of December 31, 1937, to be overstated by 20%. The scheme unraveled in 1938, and Coster committed suicide before prosecution.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

As a result of the fraud at McKesson, the *Journal of Accountancy* opined that

> *Like a torrent of cold water the wave of publicity raised by the…case has shocked the accountancy profession into breathlessness. Accustomed to relative obscurity in the public prints, accountants have been startled to find their procedures, their principles, and their professional standards the subject of sensational and generally unsympathetic headlines.*[5]

"Where were the auditors?" one might ask in the McKesson case; this is often the refrain heard after any fraud scheme becomes public. Perhaps closer scrutiny by the auditors would have revealed that F. Donald Coster was an assumed name for Philip Musica, who had been convicted of fraud twice by the time he turned thirty. Further, diligent analysis of the fictitious purchase orders and shipping documents and inspection of payments made to W.W. Smith & Co. (a fictional sales agency established by Musica and three brothers) would have perhaps detected the fraud at a much earlier stage. These types of steps – while in hindsight easy to see – were not performed by McKesson's auditors. The auditing standards of the day did not even require them. As a result of the McKesson case, the American Institute of Accountants, later to become the American Institute of Certified Public Accountants, issued Statements on Auditing Procedures Number 1, entitled *Extensions of Auditing Procedure*. As a result of this standard, observing inventory and confirming accounts receivable became standard audit procedures. Also, accountants and auditors began to assume responsibility for detecting fraud.

Second, we must equip accountants and auditors with more than professional standards and concepts to prevent and detect fraud. Accountants and auditors now assume the responsibility for preventing and detecting fraud, recovering lost profits, and restoring the public's faith and confidence in the financial reporting system. Yet, reliance on professional standards and concepts alone is almost certainly a recipe for further loss.

From the perspective of preventing fraud, one of the fundamental concepts universally espoused as a tool is segregating duties properly. This lone action is the foundation upon which most companies construct their internal control structures. However, what about the instances where proper segregation of duties does not or cannot exist? For example, proper segregation of duties in many small businesses is virtually impossible due to the organization's size. At a minimum, proper segregation of duties requires at least three *qualified* and *competent* people to be involved with each transaction. Planners must split these team members' functions between *authorization*, *recordkeeping*, and *custody of the assets*. Managers in small businesses may find it impossible to involve three or more people, as described here, to segregate duties properly. In these cases, managers and owners often assume additional responsibilities to compensate for the lack of adequate segregation of duties. However, as shown earlier, managers and owners

[5] Journal of Accountancy, February 1939.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

combine to commit over half of all the reported frauds. Further, the frauds they commit are the most costly.

It was not until the adoption of SAS 16 in 1976 that auditors were required to consider fraud as part of the audit process. In the ensuing decades, SAS 16 gave way to other pronouncements. Each of these subsequent pronouncements placed increasing responsibilities on auditors for detecting fraud. Moreover, each of these standards has provided guidelines on how auditors should approach detecting fraud. Yet, despite more robust audit standards, fraud continues to occur at alarmingly high levels, and – perhaps most disturbing – statistics indicate one has a better chance of detecting fraud through a tip or by accident than by internal or external audit. As far back as 1996, the ACFE noted that the "*expansion of computers in organizations likely will increase losses due to occupational fraud and abuse. The use of computers in business has drastically changed the speed with which financial transactions can be accomplished…Many experts see increasing reliance on computers as a likely cause of additional offenses*." Clearly, both internal and external auditors need better auditing tools to prevent and detect fraud.

Third, managers must accept that fraud prevention is one of their primary duties. Without strong anti-fraud leadership at the organization's top, team members may slip into complacency and allow fraud to eat away at the organization. While many studies have confirmed that fraud is less likely in companies where senior managers have implemented strong anti-fraud measures, some management teams are reluctant to accept responsibility for fraud prevention and detection. The landscape changed in 2002 with the passage of Sarbanes-Oxley legislation. Though some hold that Sarbanes-Oxley was an overreaction in certain areas, there can be no doubt that the bill captured senior managers' attention in large and small organizations. As indicated below in **Figure 18**, a KPMG survey revealed that 74% of the respondents implemented anti-fraud programs because of Sarbanes-Oxley.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

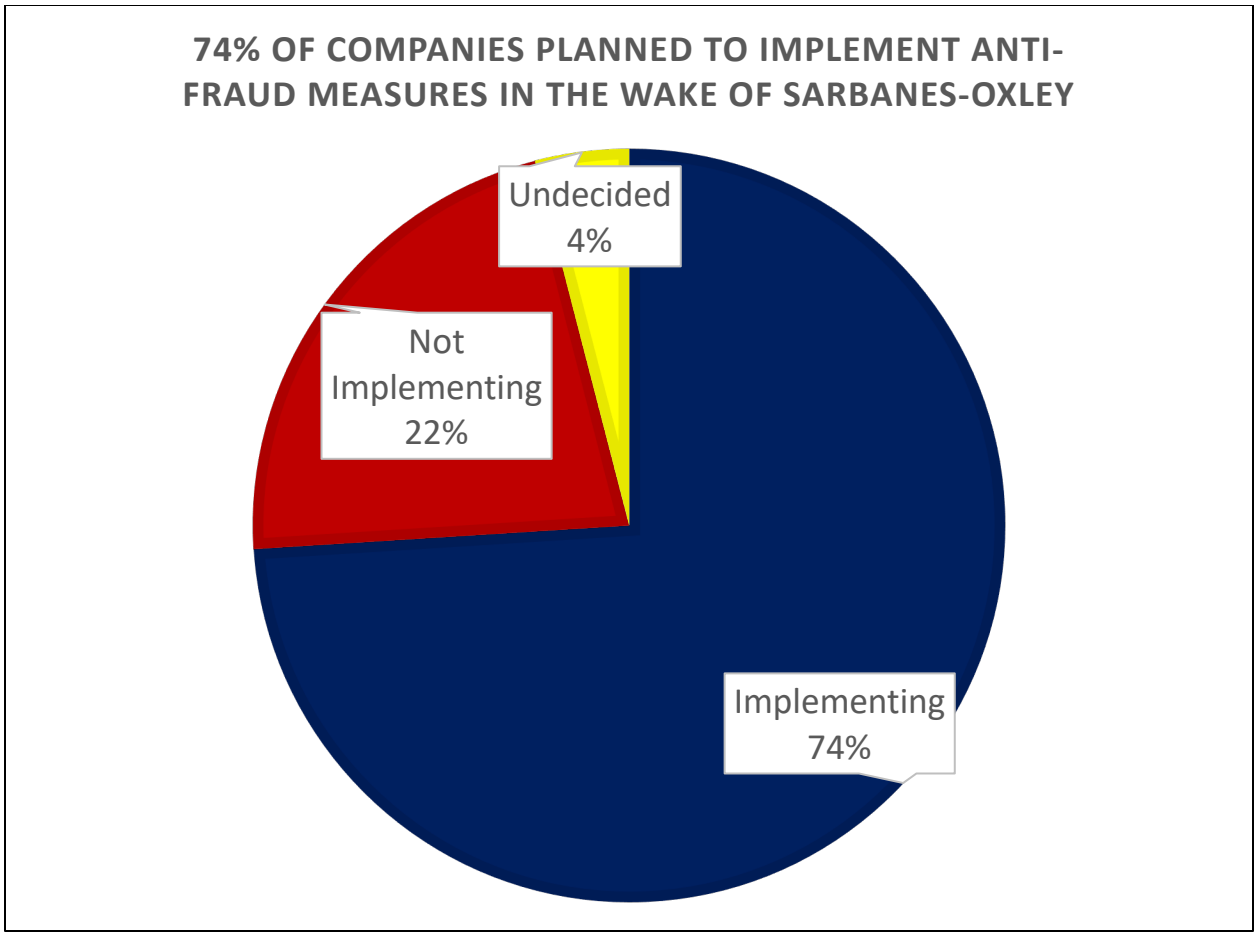


Figure 18 – Planned Anti-Fraud Actions in the Wake of Sarbanes-Oxley

Finally, individuals must be held responsible for their actions. ***Individuals*** – not companies and not auditing firms - decide to commit fraud. Therefore, ***individuals*** must be held accountable for their actions. Increasingly, companies prosecute those who commit fraud, sometimes under an intense public spotlight. Rational individuals who know they will be caught and prosecuted for fraudulent actions will likely think twice before acting.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

General Controls And Security Measures

Chapter 3

Protecting The Accounting System With General Controls

Implementing and monitoring appropriate application controls represents a significant step in developing and maintaining an effective internal control system in a small business. However, it is only part of a complete solution. In addition to appropriate *application controls*, adequate general controls must be developed and maintained. Such controls will help to ensure authorization, data maintenance, and security. General controls offer a "first line of defense" against unauthorized transactions, changes to master file data, and disclosure of sensitive business information. Without these controls, the risk to the accounting system and its data remains unacceptably high. Moreover, without adequate general controls, there can be no assurance that application controls work consistently and as intended.

Learning Objectives

Upon completing this chapter, you should be able to:

- Define the term "general controls" and list examples of general controls;
- Identify why facilities controls are necessary and provide examples of facilities controls;
- Identify why antivirus and antimalware measures are necessary components of general controls supporting information technology; and
- List the roles of data backup, recovery, and business continuity measures as components of general controls.

In the few instances where a small business's accounting system is maintained strictly through manual procedures, the general controls relevant to protecting the accounting system will center on physical security and facility controls. However, most small businesses use computer systems with manual processes to initiate transactions and store and manage accounting data in today's business environment. Therefore, physical security and facility controls will be applicable in these cases, and various controls over the computer system will also be appropriate. *Importantly, because computer systems are configured differently based on multiple circumstances, professionals should check with their local network administrators or information technology consultants before implementing any computer controls discussed in this text.*

Are general controls necessary in a small business environment? Consider the results of the "2010/2011 Computer Security Institute (CSI) Computer Crime and Security Survey."

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

- 41% of respondents experienced a security incident in the previous year.
- Of the approximately half of respondents who experienced at least one security incident last year, 45.6% reported they'd been the subject of at least one targeted attack.
- 44% of the respondents employed fewer than 500 people, indicating the impact of technology on small businesses.
- 59% of the losses were attributable to insiders.
- 67% of the respondents cited malware propagated by an Internet connection as a significant point of attack.

For those accounting and financial professionals attempting to convince small business owners and senior managers of the need for effective general controls over the accounting system, the statistics in the CSI report cited provide a chilling perspective on just how vital these control measures are. Failing to design, implement, and monitor adequate general controls presents an intolerable risk scenario for most small businesses. Yet, striking an appropriate balance between costs and controls is necessary.

Facilities Controls

One of the most fundamental aspects of general internal controls is providing adequate physical security over company facilities and assets. These *facilities controls* cover limiting physical access to company facilities and assets and physically securing company information systems.

Limiting Physical Access to Facilities and Assets

Implementing effective facility control procedures begins with limiting physical access to facilities. Small businesses should restrict access to company offices, warehouses, and other facilities to only those with a legitimate need to be there. One way of accomplishing this is by issuing keys to facilities solely to those with a demonstrated need. However, it is imperative to maintain a record of these keys and recover them as team members leave the company or as their needs for access change. Over time, keys may become unaccounted for, and, in these cases, when justified based on risk, management may decide to change locks and reissue keys. Because of this logistical issue, many small businesses are moving toward electronic access systems such as keypads and card scanners to physical facilities. There are two primary advantages to using these types of systems.

1. ***Ease of administration***. These systems allow quick and easy changes to employees' authorization levels.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

2. ***Production of access logs***. These systems generally provide a printed record – on demand – of employee entry and exit times, allowing managers to determine which employees were on-site and at what times.

Again, proper segregation of duties is not practical or possible for many small businesses. For example, while, in theory, it is good practice to restrict the access of the accounting clerk responsible for maintaining inventory records to the inventory storage facilities, this is not always feasible. In such cases, viewing or printing logs of this person's access to the warehouse becomes an essential general control procedure.

Other physical controls to consider based on the assessed risk in the business are as follows:

- Storing transaction records such as invoices, purchase orders, and canceled checks in locked file cabinets
- Utilizing off-site, fire-protected storage facilities for crucial business documents
- Maintaining unused forms such as checks, invoices, and purchase orders in locked cabinets

Additionally, depending on the small business's nature and assessed risk level, there could be a need for more extensive physical controls. Examples include:

- Video surveillance,
- Floor-to-ceiling walls, and
- On-site security guards.

Physically Securing Company Information Systems

Just as limiting access to company facilities is essential, using physical controls to secure company information systems is equally important. While logical controls such as user IDs and passwords are critical in the overall security scheme, this section focuses only on implementing physical controls. A discussion of logical controls occurs later in this chapter.

First, locate computer servers, routers, and other sensitive equipment in a restricted-access area. Of course, only those employees with a demonstrated need should have access to this area. Without this type of security measure, removing hardware or making unauthorized changes to the system becomes possible.

Second, you should consider physical security measures such as antitheft cables to prevent thefts of desktop and laptop computers. Some might ask, "Is this level of security necessary in small businesses?" Consider the following statistics.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

- **34% of respondents reported laptop theft.** *CSI, The 15th Annual Computer Crime and Security Survey, 2010/2011*

- **According to the University of Pittsburgh, companies recover less than 2% of lost or stolen laptops.**

Obviously, loss and theft of computer equipment remain significant business risks. Yet, you can manage this risk using inexpensive antitheft devices.

Third, companies should assign all computing assets to individuals and periodically inventory them to ensure they are still in team members' possession. As previously indicated, computer equipment is particularly susceptible to theft, and computer equipment theft can be quite costly. Accordingly, it is appropriate to designate a custodian for each computer asset. Further, a periodic physical inspection and count of these assets should occur, and discrepancies should be investigated and resolved.

Fourth, upon determining that a computing asset has become obsolete, delete all sensitive data from that asset before disposing of it. Many computer users unknowingly risk compromising sensitive corporate data when disposing of computers, tablets, and other devices. Examples include customer lists, supplier information, price lists, chemical formulas, account numbers, and passwords. Some users will "delete" this information from their hard drives before disposing of the asset; however, it is quite possible (and relatively easy) to recover "deleted" files from a hard drive. Accordingly, managers should take additional measures to ensure that sensitive company information is not exposed. If it is appropriate to erase all data on the hard drive, it should be sufficient to reformat it in Windows. On the other hand, if a user only wants to ensure that outside parties cannot recover "deleted" files, running the Windows defragmentation utility after deleting the files is usually adequate. Alternatively, many third-party products are available from vendors such as Symantec, SysWipe, and Paragon.

Combining sufficient facilities controls with physical controls over computing assets can mitigate the risk of compromising hard assets or company information at relatively little cost to the business.

Firewalls

A firewall helps to prevent unauthorized access to or from a private network. Firewalls can exist as either hardware or software or as a combination of hardware and software. Most commonly, firewalls prevent unauthorized Internet users from accessing private networks connected to the Internet. Firewalls are one of the front lines of defense in minimizing the threat of an external attack on a small business network.

Importantly, firewalls provide a means of enforcing access control and acceptable-use policies. Businesses of all sizes should develop these policies to document what type of uses of company-owned computing assets are appropriate. For instance, most would argue that using company-owned assets or services to access websites promoting pornography, gambling, or illegal

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

activities is unacceptable and diminishes the internal control environment. To that end, you can configure to restrict access to sites that do not meet acceptable-use criteria.

Generally, it is wise to use a network firewall with a personal firewall for each computer to achieve maximum protection from firewalls.

Network Firewalls

A network firewall resides physically between the Internet and end-users, allowing only authorized traffic to flow. Network firewalls are often hardware devices and are increasingly combined with routers and antivirus mechanisms to form a single device.

Administrators must configure network firewalls to support and address management's desired security policies. For example, if leadership aims to restrict access to FTP services, block port 21 at the network firewall. Doing so prevents any FTP traffic, assuming the administrator has not forwarded the FTP traffic to another port.

Another beneficial aspect of network firewalls is using them to accumulate and report on network traffic. For example, it is a common practice to generate reports showing which users or departments consume the most bandwidth, the most commonly visited websites, and the nature of outside attacks on the firewall. By utilizing these reports, management can identify nonproductive and noncompliant behavior and take steps to address these issues.

Personal Firewalls

In addition to a network firewall, it is also wise to implement a personal firewall on each workstation. Some might argue that implementing a personal firewall is redundant and that the network firewall alone is sufficient protection. Indeed, a personal firewall is likely to add little protection against threats originating outside the LAN. However, as discussed previously, a network firewall does not protect against inside attacks. Recall that disgruntled team members cause a large percentage of attacks. These attacks often occur while the business employs the individual and uses a computer connected to the LAN. Therefore, to ensure protection against internal threats, it is necessary to utilize personal firewalls on each workstation. In addition, personal firewalls offer additional benefits, including those listed below.

- Protection against Trojan horses, viruses, and other forms of malware
- Script filtering
- Pop-up ad filtering
- Control of cookies

A personal firewall is part of business-oriented versions of the Windows operating system and is available for use at no additional charge. Microsoft enables this firewall by default, and only a user with administrative rights on the computer can turn it off.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

You can enhance internal control significantly by implementing effective firewall security measures. These measures include installing and maintaining network and personal firewalls, whether hardware-based or software-based. Proper deployment of firewall security will minimize the threat of attacks from both external and internal sources. Further, firewalls can assist in enforcing company-specified policies regarding using computing assets and services. Finally, management reports from a network firewall provide management with information necessary to manage company bandwidth more effectively and efficiently.

Malware Protection

Perhaps the most well-known and well-publicized threat to computer systems is contracting a virus or other forms of *malware*. Once infected with a virus, worm, Trojan horse, ransomware, or other malicious software, the impact on a single computer can range from annoying to devastating. Further, suppose the infected computer connects to the company's network. In that case, the infection can replicate across the network, perhaps causing the entire system's catastrophic failure.

Despite the alarming statistics on malware infections, many small businesses remain virtually unprotected against viruses and other forms of malware. Protecting individual computers, servers, and networks from malware can be relatively inexpensive and straightforward, like most other topics in this chapter. Small businesses can significantly reduce the risk of infection and enhance internal data maintenance and security controls by implementing the following procedures.

- Install antimalware software on all workstations and servers.
- Ensure that virus signatures update contemporaneously.
- Configure the antivirus software to perform a full system scan on at least a daily basis.
- Set **Macro Security** settings to "High" inside Microsoft Office products.
- Scan all email attachments using anti-malware software before opening.
- Do not open email attachments from unknown senders.
- Refrain from using web-based email.
- Ensure that team members apply application and operating system updates on schedule.
- Educate team members about threats and how to prevent attacks.

With a relatively small investment of time and money, it is comparatively easy to implement adequate internal control procedures to minimize the risk associated with computer viruses, ransomware, and other malware.

Data Protection and Recovery

One key element of general control is data redundancy and backup protection. Computers and peripherals – including data storage devices such as hard disks – will ultimately fail. New devices often replace older ones before malfunctioning, avoiding possible harmful results. However, in other cases, device failures can occur suddenly and without warning, causing the business to

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

suffer potentially ruinous consequences. One National Archives and Records Administration study reported that only 43% of companies suffering from a disaster recover sufficiently to resume business. Further, 93% of companies that lost their data center for ten days or more declared bankruptcy within one year. You can mitigate the risks associated with data loss by implementing appropriate internal controls that ensure data redundancy and backup protection.

Backup Protection

It is well-known that many small businesses do not back up data consistently or with concern for retrieval. As a result, when it is necessary to recover data because of hard disk failure, virus infection, fire or water damage, or natural disaster, the small business is often unable to retrieve the data necessary to continue operations without interruption. Therefore, small businesses must implement an effective backup policy to ensure crucial data's continued availability and reliability. This policy should address the following issues.

- **Identification of the data to be stored** - A key point here is not to exclude workstations – many users store critical data on local hard drives. For example, team members often save Outlook data files and spreadsheets on local hard disks rather than servers. To prevent disruption, ensure that this data is identified for backup as specified by the backup policy.

- **Frequency and type of backups** - Many small businesses create a differential backup daily, backing up only those data files that have changed since the last differential backup. Additionally, they make a full backup weekly, backing up all data previously discussed.

- **Storage media** - The backup policy should indicate what storage media to use. Some companies back up data to external disk drives. Other companies may use DVDs. And others may back up to Internet-based facilities. Depending on network configuration, it is possible to back-up data over a VPN to an off-site storage device. An essential factor to consider when selecting the storage media is that the backup media's storage capacity and relative speed should complement the amount of data involved.

- **Off-site storage of backups** - One of the critical failures experienced by many small businesses is not storing completed backups off-site. Store backup media off-site to facilitate data recovery if a disaster strikes. This need sometimes translates into a key employee keeping the media in their home. In other cases, this might mean storing the media in a safety deposit box or vault at a bank. In all circumstances, maintain a recent full backup in an off-site storage facility so that data recovery is possible if a disaster strikes.

- **Using backup logs** – Maintain backup records to verify that team members faithfully execute all backup procedures. These logs should indicate the date, media, method, person responsible, and success or failure of each backup. Management should carefully

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

review these logs to ensure backups execute even when the person overseeing the process is absent.

- **Testing backups** - Like computers and hard disks, backup media will fail over time. Therefore, it is critical to the backup strategy's overall success to test the backup media periodically to ensure that team members can restore data from the backup if a catastrophic event occurs.

Online Backups

One significant trend in backups is that of online backups via the Internet. With almost all small businesses having access to high-speed Internet connections, many small companies outsource their backup function now. You can accomplish this by contacting a vendor providing these services and contracting for a certain amount of disk storage space on that vendor's network. Then, schedule backups to transfer the data identified by the company to the vendor's storage device periodically. The primary advantages of utilizing this type of service are listed below.

- **Automation** - Because the backups run via software instruction, clerical personnel do not need to remember to change tapes or execute backup jobs.

- **Off-site storage** - The data is securely transmitted over the Internet to an off-site storage facility, ensuring availability in a disaster.

- **Scalability** - As business needs evolve, you can modify the subscription service to increase or decrease the amount of off-site storage space.

- **Web-based architecture** - The services offered by many vendors are built on web-based architecture, allowing you to recover data from any computer with an Internet connection and a web browser.

- **Cost savings** - A typical solution costs less than $100 monthly for a small business with five workstations.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Some of the more well-known vendors of online backup services for small businesses are listed below.

- Abacus – www.abacus.com
- Barracuda – www.barracuda.com
- Carbonite – www.carbonite.com
- iDrive Business – www.idrive.com
- MozyPro – www.mozypro.com

RAID

Redundant Array of Independent Disks (RAID) is a technique that maximizes data availability, given the potential for hard disk failure. When properly implemented, RAID employs two or more hard disks in tandem to optimize fault tolerance and performance. Although it is possible to implement RAID at the workstation level, RAID is generally implemented only on servers.

Several RAID configurations are available; among the more common are the following.

- **Level 0**: This provides data striping (spreading each file's blocks across multiple disks) but no redundancy. This technique improves performance but does not deliver fault tolerance.

- **Level 1**: This provides disk mirroring, where data is written to two disks simultaneously.

- **Level 3**: This is the same as Level 0, but it also reserves one dedicated disk for error correction data. It provides good performance and some level of fault tolerance.

- **Level 5**: This provides data striping at the byte level. It also includes stripe error correction information. This method results in excellent performance and good fault tolerance.

It is important to note that certain events – such as a lightning strike, flood, or fire – could affect all hard disks in a given RAID configuration; therefore, do not view RAID as a substitute for an effective backup policy. Instead, use RAID in concert with the backup policy to minimize the risks associated with data loss.

?	List four general controls you have in place over your desktop or laptop computer. 1. 2. 3. 4.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Business Continuity

Business continuity planning is simply preparing to recover from an event – great or small – that affects the organization's ability to continue operating. Events range from large-scale natural disasters like hurricanes and floods to business-specific issues like computer failures. Yet, no matter the event's nature, such catastrophes can keep an unprepared business from continuing as a going concern. Therefore, a contingency plan for business continuity is crucial.

Businesses today are driven by transactions and data-intensive procedures. Many organizations, such as those providing health care services, cannot tolerate extended downtime or significant loss of access to data. These businesses must develop an appropriate disaster recovery plan focusing on the critical steps necessary for business continuity. Some of these include the following.

- Determining what types of disasters can occur
- Identifying data to save
- Securing a backup utility (on-site or cloud-based)
- Obtaining suitable replacement hardware for recovered data
- Locating an appropriate brick-and-mortar replacement site
- Monitoring and testing the operation of the business continuity plan
- Making adjustments to accommodate changes in the way the business operates

Operating System and Application Updates

Although operating systems and applications have improved remarkably in terms of stability and performance, there are still numerous "bugs" in virtually all software code. Some of these are relatively benign; some can cause significant problems. Because Microsoft's Windows platform and Office applications dominate the business technology landscape, they are often the targets of those seeking to exploit bugs and security flaws in the software code. As researchers detect vulnerabilities in Windows, Office, and other applications, software publishers release patches and updates to address these issues. Therefore, administrators or end-users must download and install these updates to minimize the risks associated with weaknesses in the code. Fortunately, most tools and applications offer settings that enable automatic updates as new code is released. This approach is likely the best way to ensure that operating system and application updates are applied contemporaneously from a practical perspective.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Key Information Security Controls And Authentication Methods

Chapter 4

A wide array of technology-based security controls exists. Many new and improved tools are available today, and more are in development. However, for many businesses – large and small – some of the more basic "tried and true" methods for safeguarding information are today's primary information security and authentication controls. For example, the primary means to keep sensitive data safe from unauthorized access is to authenticate the user attempting to view the content. This chapter discusses authentication in detail, including tools such as multi-factor authentication, digital signatures, security tokens, and biometric devices.

Learning Objectives

Upon completing this chapter, you should be able to:

- Identify the importance of user IDs and passwords as they relate to authentication measures;
- Classify internal control issues related to email and describe options for securing sensitive content in email messages;
- List and describe two options for improving document-level security;
- Define the concept of cryptography, how it relates to internal control, and how to use it to improve internal control; and
- Define authentication and list three methods, in addition to passwords, for implementing authentication controls in an organization.

Authentication Overview

Controlling who has access to information involves *authentication*. Today, the standard authenticating approach uses a user ID and a password. Unfortunately, there are serious risks associated with using only this method.

The problem is not the technology; instead, it is the users. Randomly created, fifteen-character passwords are typically considered "unbreakable." Unfortunately, however, the quality of this authentication procedure is often seriously diminished because people are involved. Unfortunately, team members frequently compromise security by writing down, simplifying, or redundantly using passwords.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Because of this, businesses should examine alternative solutions to use in conjunction with user IDs and passwords or alternatives to user IDs and passwords. The solutions selected will depend on the level of risk an organization is willing to accept and its ability to commit resources to this issue. Fortunately, many cost-effective and fundamentally sound authentication solutions are available today, and most are easy to implement.

User IDs and Passwords

User IDs and passwords are the first lines of defense – and sometimes the only line of defense – for user access control. Effective user IDs and passwords prevent unauthorized access to the computer information systems of small businesses. This session's fundamental guidelines are appropriate for organizations where computers operate in virtually all environments.

User IDs

User IDs, or user names, serve as the identification component of the authentication process, allowing the system and its administrators to know who is connecting to information. In addition, creating separate user IDs for each user makes it possible to develop specific user profiles, allowing some users to have different rights and privileges than others. For example, some users possess “administrator” rights, which will enable them to change settings on the computer. Examples of such changes include:

- Adding, changing, or deleting other users;
- Installing new hardware and software; and
- Accessing data files on that device and peripherals connected to that device.

Other users might have “limited” rights, restricting their actions while working with the device. The process of creating user IDs varies depending on the operating system, administrator preferences, and the technology environment (network, stand-alone, and active directory, for example).

Passwords

In addition to managing user IDs, utilizing solid passwords is essential to internal control over data and maximizing information security. Unfortunately, many small businesses fail to recognize and stress the importance of passwords. Consequently, password construction is often weak, making the password more susceptible to hackers. Additionally, passwords in many organizations are shared among users and are rarely changed. These shortcomings place systems and data at considerable risk.

The following list provides a set of general guidelines regarding passwords.

- Establish a corporate policy regarding passwords. An example of such a policy is available from the Security Policy Project at www.sans.org.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

- Passwords should be a minimum of fifteen characters in length. At least two of the characters should be alpha characters, at least two should be numeric, and at least one should be a special character, such as a punctuation mark.

- Require passwords for all users and all applications.

- Passwords should not be a word found in a dictionary.

- Passwords should not be a pet's name, a birthday, or any other object that someone could easily guess.

- Never share passwords. If a password is shared or potentially compromised, it should be changed immediately.

Establishing and enforcing effective passwords over system and application access significantly strengthens internal controls. In addition, strong authentication controls reduce the probability that an unauthorized individual might access sensitive data.

Why Use Strong Passwords?

The following information is essential for businesses and individuals seeking to limit sensitive information access.

- Most experts consider the current standard encryption methods (128 AES and 256 AES) unbreakable with today's technology.

- Weak passwords and weak password management techniques serve as an entry point for those seeking rights to secure information.

- To compromise a document secured with a password, a hacker must defeat the password or decode the document's encryption.

Based on these considerations, using strong passwords is essential when authenticating access to sensitive information. For example, passwords granting access to bank accounts, corporate networks, and email should follow previously discussed guidelines; unfortunately, evidence indicates that many people do not follow these guidelines.

To illustrate, The Gartner Group reported improper access to online banking accounts, and the losses amounted to $2.4 billion in just 12 months. Gartner estimates indicate that 1.98 million adults suffered losses. Malicious programs that collect passwords and other confidential data accounted for most of the problem. (*Source: Microsoft Security Guide for Small Business*)

The security features built into the applications used in an organization are another factor in deciding password strength. For example, Microsoft's ubiquitous Excel application is subject to *brute-force attacks*. Because the software allows users to enter one password after another

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

without ever locking, password-cracking software can attempt to open a workbook using millions of passwords. Consider the information pictured in **Table 2**. Some password-cracking software can try 15 million passwords per second when accessing Excel and other non-locking software applications. Of course, sensitive data stored in documents opened with non-locking applications need appropriate access controls, including "long and strong" passwords.

length: 4, complexity: a-z	==> less than 1 second
length: 4, complexity: a-z, A-Z, 0-9 + symbols	==> 4.8 seconds
length: 5, complexity: a-z, A-Z	==> 25 seconds
length: 6, complexity: a-z, A-Z, 0-9	==> 1 hour
length: 6, complexity: a-z, A-Z, 0-9 + symbols	==> 11 hours
length: 7, complexity: a-z, A-Z, 0-9 + symbols	==> 6 weeks
length: 8, complexity: a-z, A-Z, 0-9	==> 5 months
length: 8, complexity: a-z, A-Z, 0-9 + symbols	==> 10 years
length: 9, complexity: a-z, A-Z, 0-9 + symbols	==> 1,000 years
length: 10, complexity: a-z, A-Z, 0-9	==> 1,700 years
length: 10, complexity: a-z, A-Z, 0-9 + symbols	==> **91,800 years**

Table 2 - Time Needed to Crack Password (Using 15 Million Passwords per Second)

Applications not subject to brute force attacks may not need quite as strong a password. For example, some secure flash drives self-destruct if you incorrectly type the password ten times consecutively. This feature makes executing a brute-force attack on the device virtually impossible.

Characteristics of Weak Passwords

Any exceptions aside, organizations' primary risk when individuals use only username/password authentication is that passwords are frequently not appropriately managed. Following is a list of some of the more common mistakes.

- Using weak passwords.
- Sharing passwords with others.
- Writing down passwords.
- Using the same passwords for multiple logins that need high security.
- Using the same passwords repeatedly.
- Becoming victims of keystroke logging malware.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

- Leaving systems on, open, and logged in when leaving a workspace.

- Allowing others use the device while the previous user remains logged in.

- Voluntarily providing a password to someone using social engineering to acquire the password.

What, then, is needed for a secure password? As mentioned, one outstanding resource is the **SANS Institute** (www.sans.org). SANS is a trusted information security training, certification, and research source. It is a worldwide association of over 150,000 information security professionals. One of the services provided is a library of policies and procedures that includes recommendations on dealing effectively with security issues. The following guidelines are from the SANS Password Security Policy.

Password Policy Guidelines

Strong passwords have the following characteristics.

- They contain upper and lower case characters (e.g., a-z, A-Z).

- They have digits and punctuation characters as well as letters (e.g., 0-9 or !@#$%^&*()_+|~-=\`{}[]:";'<>?,./).

- They are at least fifteen alphanumeric characters long and are a passphrase (Ohmy1stubbedmyt0e).

- They are not words in any language, slang, dialect, or jargon.

- They do not use personal information like family members' names.

- Team members should never write passwords or store them in their web browsers. Instead, it would help if you use passwords you can remember easily. One way to do this is to create a password based on a song title, affirmation, or other term known to you. For example, the phrase might be "This May Be One Way to Remember," and the password could be "TmB1w2R!" or "Tmb1W>r~" or some variation.

Flawed, weak passwords have the following characteristics.

- The password contains fewer than fifteen characters.

- The password is a word in a dictionary (English or foreign).

- The password is a common usage word such as:
    - Names of family, pets, friends, coworkers, or fantasy characters;

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

- Computer terms, names, commands, sites, companies, hardware, or software;
- The words "<Company Name>," "sanjose," "sanfran," or any similar derivation;
- Birthdays and other personal information such as addresses and phone numbers;
- Word or number patterns like “aaabbb,” “qwerty,” “zyxwvuts,” or “123321”;
- Any of the above spelled backwards; or
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

Password Management Software

It is simple: individuals not using password management software probably do not use strong, secure passwords. However, products such as **LastPass**, **Password Depot**, **Dashlanee**, and **RoboForm** all facilitate using long, complex passwords without remembering or writing them down. To take advantage of these tools, you only need to recall the password that gives you access to the password manager tool.[6]

Another step that you can take to strengthen password management is to incorporate biometric devices such as fingerprint readers. With these devices in place, you need not remember anything other than which fingerprint you used to authenticate yourself to the software.

?	Have you considered implementing password management software to assist with authentication controls? If not, are your passwords as “long-and-strong” as they need to be to provide adequate control over unauthorized access to your computers, tablets, and smartphones?

Multi-Factor Authentication

User IDs and passwords are the first steps toward effectively securing the information system and data. Businesses of all sizes should enable multi-factor authentication (MFA) for maximum security effectiveness. MFA involves logging in to a device, an application, or a website using at least two of the following three criteria.

1. Something the user knows, such as a user ID and password,
2. Something the user has in their physical possession, such as a smartphone and
3. Something the user “is,” such as a fingerprint.

Consider the following example. Pat uses MFA to access the company’s online bank account. In addition to her user ID and password, Pat has an authentication app loaded onto their smartphone. Upon visiting the bank’s website, Pat enters the username and password. Then, the

[6] You can learn more about password management tools and read reviews of many of the leading solutions in this market by visiting https://www.pcmag.com/picks/the-best-password-managers.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

site sends a six-digit code back to the authentication app on Pat's smartphone. Finally, Pat inputs the six-digit code into the bank's website to complete authenticating to the site and logging in.

Pat's use of MFA reduces risk to the organization because a hacker trying to access the company's bank account would need to know Pat's user ID and password, but the hacker would also need to have Pat's smartphone in their possession. Without the smartphone, the hacker would not receive the six-digit code; therefore, the hacker could not authenticate it to the website. You can substantially reduce the risk of unauthorized access by requiring multiple factors to log in. Notice the emphasis on the word "reduce" in the previous sentence. MFA does not ***eliminate*** risk; it is doubtful that any security technique truly "eliminates" risk. Instead, MFA reduces risk because, in Pat's case, it is highly improbable that a hacker would know Pat's user ID and password and have Pat's smartphone in their possession to receive the six-digit code from the bank.

Biometric Authentication

Biometric authentication refers to using a person's physical characteristics to authenticate them for access to a resource. The elements commonly used include a fingerprint, retinal pattern, palm prints, signature or voice recognition, and even DNA sequences. Because these characteristics are unique and do not change much over time, they offer strong proof of identity. However, some of these approaches are more expensive to acquire and maintain. Therefore, they are often used to control sensitive or classified information access.

Although biometric authentication may appear bulletproof, it has a potentially weak underbelly. It is vital to secure the comparison data because it is easier to attack the stored comparison statistics or images than to copy the unique physical characteristics. This data will be the focus of attacks on many of these systems. Therefore, biometric authentication is sometimes a part of MFA authentication.

One relatively common form of implementing biometric authentication is fingerprint readers. Users place a finger on a small fingerprint-reading device to authenticate to a server using a fingerprint reader. This device measures various characteristics of the user's fingerprint patterns and typically transmits these measurements to a server. The server compares the reader's measurements against that individual's registered set of measurements. The server authenticates the user only if the two fingerprints correspond closely.

Cryptography Basics for Accountants

Cryptography is the science of keeping confidential information confidential. According to Wikipedia, cryptography is "…the practice and study of hiding information." Cryptography is considered a branch of mathematics and computer science. Further, it incorporates information theory, computer security, and engineering. Moreover, cryptography is native to many products and services we utilize regularly. Some of these include ATM cards, computer passwords, and electronic commerce.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Encryption

For most business professionals, cryptography refers almost exclusively to encryption. Encryption converts ordinary information (plaintext) into unintelligible gibberish (i.e., ciphertext). Decryption is the reverse, moving from unintelligible ciphertext to plaintext. A cipher is a pair of algorithms that encrypts and decrypts data. To illustrate, **Figure 19** illustrates the encryption and decryption flow. The detailed operation is controlled both by the algorithm and, in each instance, by a key. The key is a secret parameter (ideally known only to the communicants) for a specific message exchange context. Keys are essential because ciphers without variable keys are trivially breakable and useless for most purposes.

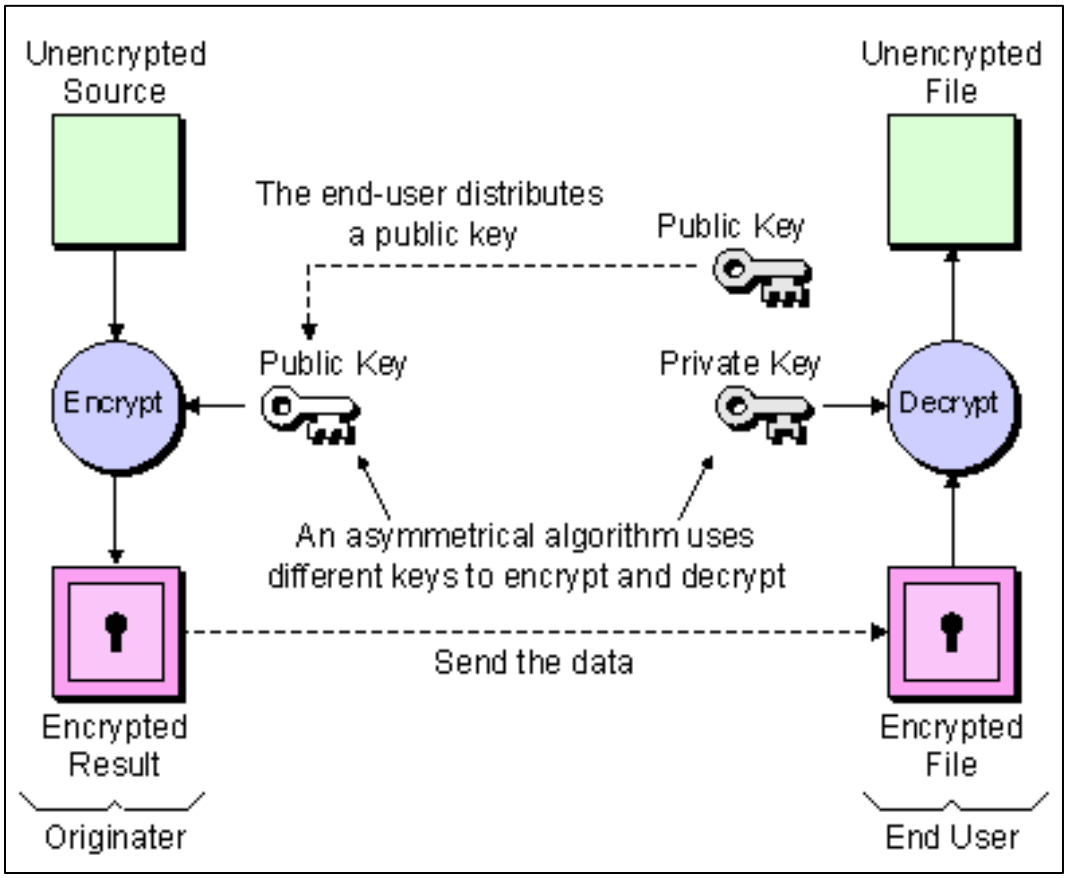


Figure 19 - Encryption Flow Chart

The state of encryption is such that breaking strong encryption is virtually impossible. Of course, not all encryption is strong, but the encryption we rely on daily for business transactions is. For example, web browsers routinely use 128-bit SSL (Secure Socket Layer) encryption for financial transactions. According to one estimate based on a French researcher breaking 40-bit SSL encryption, it would take "…significantly longer than the universe's age to crack a 128-bit key." SSL certificates with a 256-bit key are available.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

AES Encryption

The Advanced Encryption Standard (AES) is a block cipher adopted as an encryption standard by the U.S. government. It has been analyzed extensively and is now a worldwide standard. The predecessor of AES is the Data Encryption Standard (DES). AES was announced by the National Institute of Standards and Technology (NIST) on November 26, 2001, after a five-year standardization process. Researchers and scientists presented and evaluated fifteen competing designs during those five years before selecting AES as the most suitable. It became effective as a standard on May 26, 2002. Today, AES remains one of the most popular algorithms used in symmetric key cryptography. It is available by choice in many encryption packages. Importantly, AES marks the public's first access to a cipher approved by the NSA for top-secret information.

Overview of Email Security Issues

Email is the most widely used technology tool for business today. Of course, not everyone works in Excel, and many do not use word processing applications. However, almost all business professionals have an email account and use email heavily, routinely sending and receiving countless messages daily.

Hackers wishing to have the most significant effect often focus on high-volume applications. Accordingly, email is an area where many security risks exist, and countless attacks occur. Furthermore, email has become a pervasive and necessary part of working, and an extended email outage or disruption poses a serious business risk.

In a perfect world, everyone would have a personal digital ID (discussed later in the chapter), and all email communications would be secure and only readable by the intended recipient. Unfortunately, few professionals use personal digital IDs, and many organizations do not employ safe alternatives for communicating sensitive data.

Understanding the Issues

Most small business users (and many in larger organizations) have sent and received sensitive information via unsecured emails for many years. Unless you encrypt your outbound messages, email transmits as clear text over the Internet. Quite literally, countless hackers have the opportunity to use packet sniffing software to view the contents of your email messages if you have not encrypted them. Likewise, if you are the recipient of a message and the sender did not encrypt it, countless individuals can intercept the contents of that message before it reaches you. The following extraction from an article at http://luxsci.com/extranet/articles/email-security.html summarizes confidentiality threats for unencrypted email.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Security Threats to Your Email Communications

Eavesdropping

The Internet is a big place with many people on it. It is very easy for someone with access to computers or networks through which your information is traveling to capture this information and read it. Like someone in the next room listening in on your phone conversation, people using computers "nearby" the path your email takes through the Internet can potentially read and save your messages!

Identity Theft

If someone can obtain the username and password that you use to access your email servers, she can read your email and send false email messages as if they are you. These credentials can often be obtained by eavesdropping on SMTP, POP, IMAP, or WebMail connections, by reading email messages in which you include this information, or through other means.

Invasion of Privacy

If you are very concerned about your privacy, then you will be concerned about the possibility of "unprotected backups," discussed below. You may also be concerned about your SMTP email recipients being able to tell what IP address your computer has! This information may be used to tell in what city you are located or even, in some cases, to find out what your address is! This is not an issue with WebMail, POP, or IMAP, but it is an issue when sending email, securely or insecurely, from any email client over SMTP.

Message Modification

Anyone who has system administrator permission on any SMTP Servers that your message visits can read your message and delete or change it before it continues to its destination. Your recipient has no way to tell if someone has tampered with the message. Further, the recipient would not even know if someone deleted the message.

False Messages

It is easy to construct messages that appear to be from someone other than from who they actually are. Many viruses use this facility to propagate themselves. Generally, there is no way to ensure that a message's apparent sender actually sent the message.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Unprotected Backups

> *Because messages are stored in plain text on all SMTP Servers, any backups of these servers' disks may also contain plain text copies of your messages. Since backups can be kept for years and can be read by anyone with access to them, your messages could still be laying around in insecure places even after you think that all copies have been "deleted."*

Repudiation

> *Because individuals can forge email messages, there is no way for you to prove that someone sent you a particular message. This means that even if someone did send you a message, he can successfully deny it. This has implications concerning using email for contracts, business communications, and electronic commerce.*

Solutions to Email Security Issues

One of the least painful and most straightforward email security solutions for organizations is an email provider that encrypts messages between the sender and the email provider's server. If your email provider supplies this capability, your communications with others in the organization will be secure. Unfortunately, this feature does little to secure email that goes to people outside the organization who are not using the same email provider. **Figure 20** provides a conceptual representation of sending an encrypted email message.

Example of Unencrypted Outbound Email Message		**How that Same Message Might Appear after Encrypting It**
Hi John, and I hope you're having a good day. The bank account number you need is 087634562846, and the routing number is 984345467. If you need additional info, just let me know. Thanks.		Df98dfsakdfsal240030340430340f< dldfklg9<+&#sdjfkjsgdfkfghsdgfsdff jgnfl93?{}@jg@&mgfafofofdgofdgo 943mnm"+~!fgakfga@*fjksdfgjgdfs 0n575?,mfdjhdfsj][+asksakas357lkds 696mbnsdfosdf34354jfuydspire{fkfk

Figure 20 – Conceptual Representation of Sending an Encrypted Email Message

Another solution is to use Asymmetric Key Encryption. In layperson terminology, this technique involves getting a pair of "keys" that your email client uses to encrypt and unencrypt email. This technology is inexpensive and easy to use. However, a significant drawback is that individuals can only send encrypted emails to others with keys (i.e., digital signatures). In addition, communicating encryption keys can be cumbersome and, for some, challenging to understand. Accordingly, while technically sound, this encryption form remains relatively scarce.

A third solution is to send confidential information as an attachment in an encrypted document. Many professionals currently use this practice because securing the content is straightforward

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

and understandable. To encrypt a file – such as a PDF document or an Excel workbook – team members need only to add a password to the file, and the source application applies encryption. Users then attach the encrypted document to an outbound email message and send it to the intended recipient(s). Of course, the sender must also communicate the password to the recipient(s) so they can open the attachment. For obvious reasons, never include the password in the body of the email message. It is important to note that you should always use a strong password to encrypt the attachment.

Data Loss Prevention Tools

A discussion of email security is incomplete without mentioning the potential role of Data Loss Prevention (DLP) tools in enforcing compliance with established security standards. Among other actions, DLP tools can scan outbound email messages to determine if they contain sensitive data – such as Social Security numbers, bank account numbers, and credit card numbers – and block these messages from being sent. DLP tools look for patterns in the body of an outbound email message and any ***unencrypted*** attachments. If the scan identifies data that matches a design associated with sensitive information, the DLP tool follows a prescribed rule for handling the message, including blocking the outbound message altogether. If the message contains an ***encrypted*** attachment, the DLP tool cannot examine the attachment's contents for sensitive data because of the encryption. Many popular email services offer DLP capabilities, including Microsoft 365/Office 365 and Google's G Suite.

Secure Alternatives to Email

Due to ease of use or improved security, some products designed to communicate electronic content serve as viable and even preferred alternatives to email. Two of these – cloud-based portals and user-controlled document repositories – are popular now and gain popularity daily. Let us look at cloud-based portals to illustrate how they can securely transmit information, bypassing email.

Cloud-based Portals

A cloud-based portal contains information that the portal's users believe will be needed by the targeted user group. For example, some portals distribute information to others – such as sales materials to prospective customers – while others are secure websites that require authentication to access confidential information. As mentioned above, anecdotal evidence suggests that many business professionals email sensitive documents such as tax returns and payroll reports, potentially resulting in an accidental breach of confidential information. Portals provide a more secure way to perform these tasks.

ShareFile

ShareFile (www.sharefile.com) is an excellent example of a cloud portal. It allows subscribers to post and share content easily with others, both inside and outside the organization. In addition, ShareFile has branding capabilities. Businesses can apply logos, color schemes, and other

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

formatting elements to make the leased space look and feel similar to the organization's primary website. Pricing varies depending on space requirements and the number of users who have posting access.

Like many similar services, ShareFile offers numerous subscription options tailored to meet business users' needs in various industries, including professional services firms such as accounting practices, law firms, and consulting organizations. Pricing starts at $50 monthly for the Standard plan and ranges to $122 monthly for the Premium plan. All subscriptions offer unlimited data storage, custom branding, two-factor authentication, and access from mobile devices. In addition, other offerings allow you to tailor a plan to meet your needs. **Figure 21** provides an example of the ShareFile user interface.

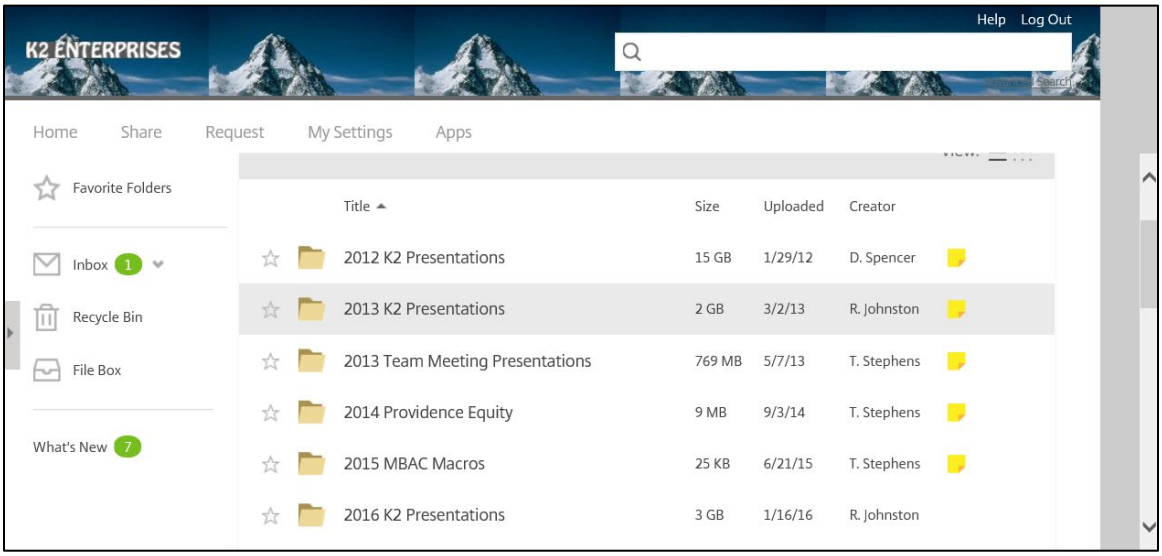


Figure 21 - ShareFile Hosted Portal Site

End-User Controlled Repositories

Conceptually, a user-controlled repository is very similar to a cloud-based portal. It provides a cloud-based tool to facilitate authorized users uploading and retrieving documents. The primary difference between these options is that organizations create, manage, and maintain user-controlled repositories.

An example of a user-controlled repository is Microsoft's **Teams** offering. With Teams, an organization can establish a cloud-based portal and designate which team members can access specific folders. Further, administrators can make selected folders in Teams accessible by users outside the organization, such as clients, customers, and vendors. One potential advantage to using this platform is cost – Microsoft includes Teams in most business-oriented Microsoft 365/Office 365 subscriptions, so the organization incurs no incremental expenses for using this platform. **Figure 22** illustrates the Teams user interface.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

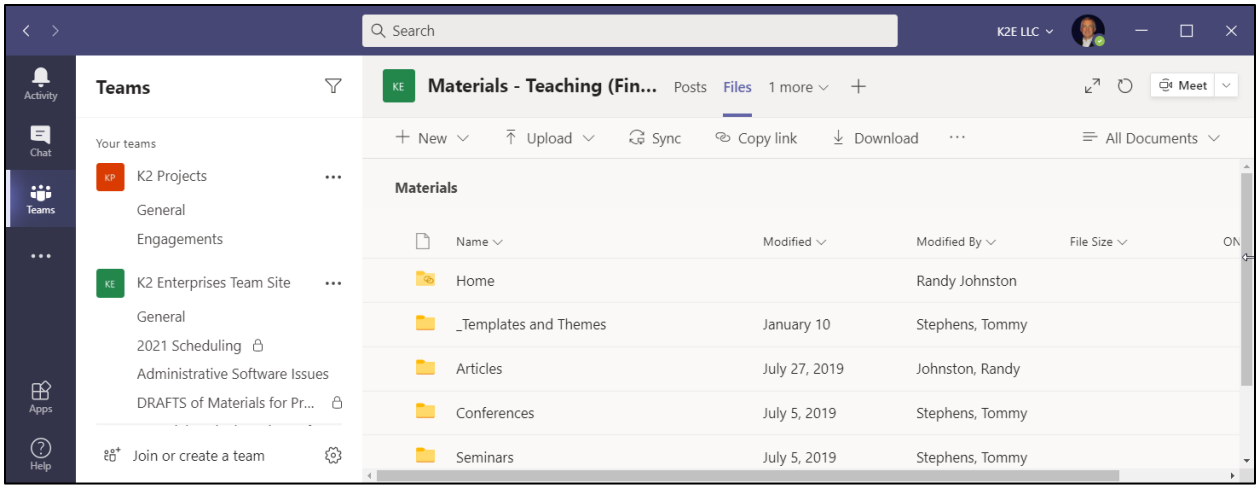


Figure 22 – Example of the Teams User Interface

Hard Disk Encryption

Now that we have discussed encryption and understand what it accomplishes, our next step is identifying what data you can encrypt within a business organization. The primary storage medium for data, whether sensitive or not, are hard disks installed on servers, desktops, and laptop computers. So, let us look more closely at hard disk encryption to secure electronic content.

Overview of Hard Disk Encryption

All business professionals should strongly consider hard disk encryption, often called whole disk encryption. Hard disk encryption is available for almost all operating systems, including Windows, MacOS, and Linux. To help protect against potential data breaches, businesses of all sizes have turned to hard disk encryption. Some possible solutions to encrypt and protect your data include those listed below. For the sake of brevity, we will focus only on Bitlocker.

- BitLocker
- PGP Desktop Professional
- Beachhead Solutions
- McAfee Endpoint Encryption

BitLocker

BitLocker is a feature in the business-oriented versions of Microsoft's Windows operating system. BitLocker is a tool worthy of consideration for business professionals who need whole disk encryption. It works seamlessly with the operating system and has built-in support for a TPM chip. The technology is reliable, third-party software manufacturers have adjusted their software to work with BitLocker, and it is easy for non-technical employees. Bitlocker also offers key recovery capabilities and works with Active Directory.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

- Benefits
    - Verification of boot-up integrity
    - 128- or 256-bit AES sector-level encryption
    - Transparent to the user
    - TPM chip integration (optional)
    - Emergency recovery options (including AD backup)
- Requirements
    - Windows 10/8/7/Vista (business-oriented editions only)
    - Windows Server 2008 (or later)

BitLocker is a reliable product that works as advertised. The product has been used widely for several years and generally receives good reviews.

Document Level Security

There are several ways to secure documents individually. In the following paragraphs, we explore how to use tools built into many popular business applications to encrypt sensitive data.

Securing Microsoft Office Documents

Many document creation applications have built-in security features. For example, Microsoft Word, Adobe Acrobat Pro, and Microsoft Excel can encrypt the documents you create and manage using these applications. Beginning with Office 2007, Microsoft enhanced security relative to previous versions. The default level of protection invoked when you add a password is much stronger than in earlier versions of these products. Specifically, recent versions of Office provide 128-bit AES encryption as their default.

Those who need a higher security level by default can use Group Policy or a registry modification to change the default encryption level to 256-bit AES encryption. **Figure 23, Figure 24,** and **Figure 25** illustrate how to encrypt documents in Microsoft Office applications, folders in the Windows operating system, and PDF files.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

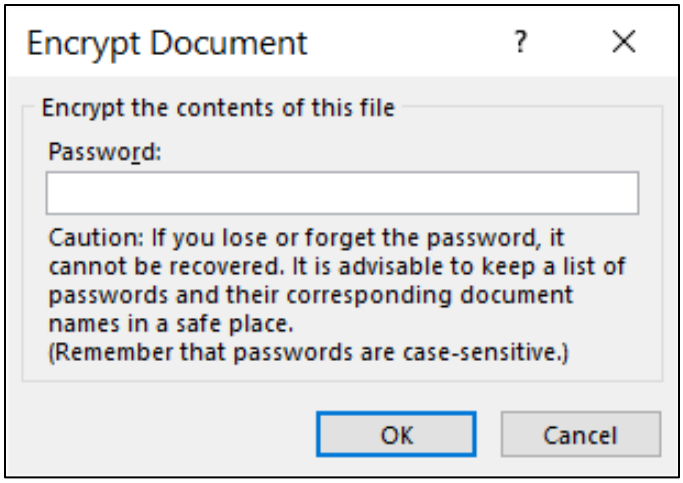


Figure 23 - Adding a Password to Encrypt a Microsoft Office Document

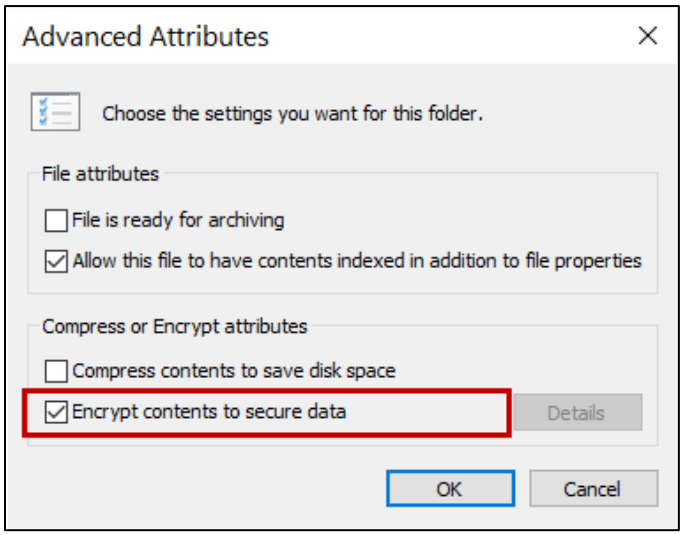


Figure 24 - Using the Windows EFS to Encrypt a Document

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

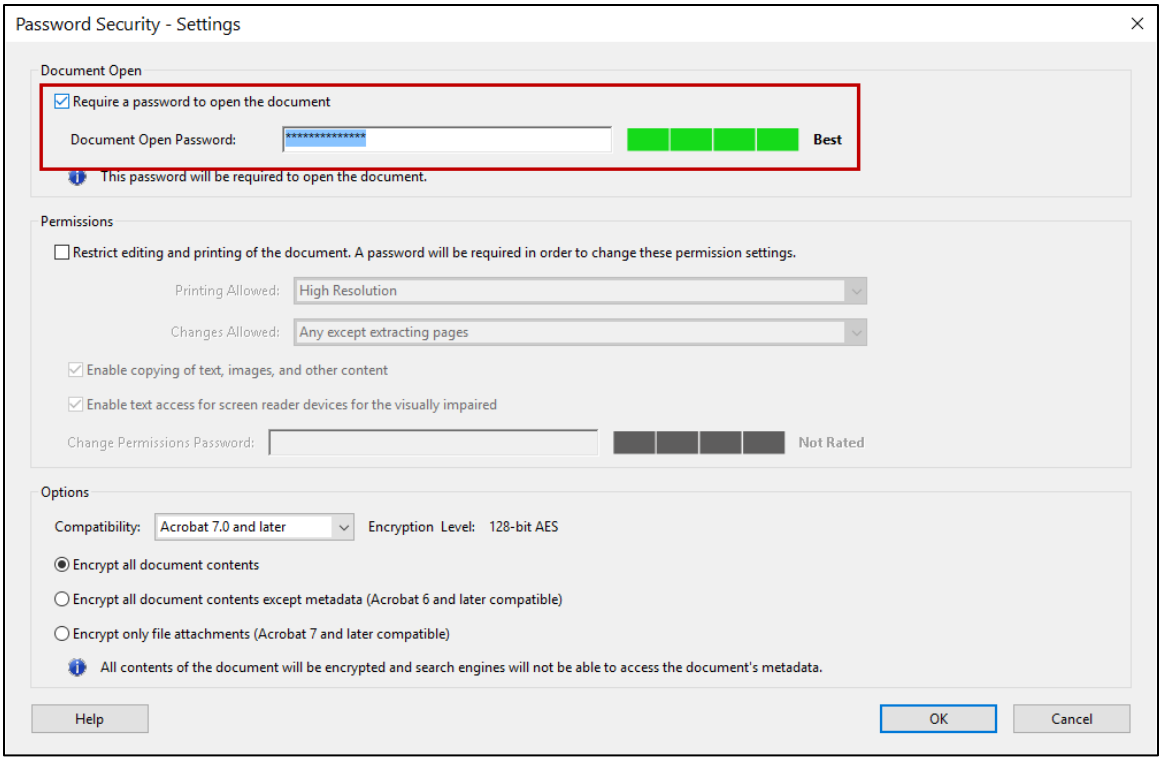


Figure 25 - Using Adobe Acrobat to Secure PDF Files

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Desktop Tools For Preventing And Detecting Fraud

Chapter 5

Every business professional can access some of the most robust fraud prevention and detection technology tools. Tools and applications such as Windows, Excel, and Access contain numerous features to prevent and detect fraud. We will discuss and demonstrate many of these features in this chapter.

Learning Objectives

Upon completing this chapter, you should be able to:

- Define ODBC queries and identify how they can assist in detecting fraud;
- Identify opportunities to use Microsoft Office Access and Excel as auditing and fraud detection tools; and
- List opportunities to use Benford's Law as a fraud detection tool.

ODBC Queries

Open Database Connectivity (**ODBC**) is a specification allowing users to share information in a database across multiple, diverse applications. For users taking advantage of ODBC, the benefits include the following:

- Allowing Windows applications to access various data sources through a single method, regardless of file formats;
- Overcoming the problem of different databases having different means of providing access to the information contained in them; and
- Simplifying access requirements so users no longer need advanced database management skills to access data.

Examples of applications compliant with ODBC include Microsoft SQL Server, Microsoft Access, Microsoft Excel, Borland Delphi, Crystal Reports, and Visual Basic. For instance, because Excel complies with the standard, an Excel user could link data from a Microsoft SQL Server database to create custom reports or queries for audit or fraud detection purposes.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

ODBC is an enabling technology that facilitates data extraction and analysis, report writing, and data exchange between applications. To some extent, many tools and technologies discussed elsewhere in this session depend on ODBC compliance. For example, **Figure 26** illustrates using ODBC to link data from a SQL Server database into Excel.

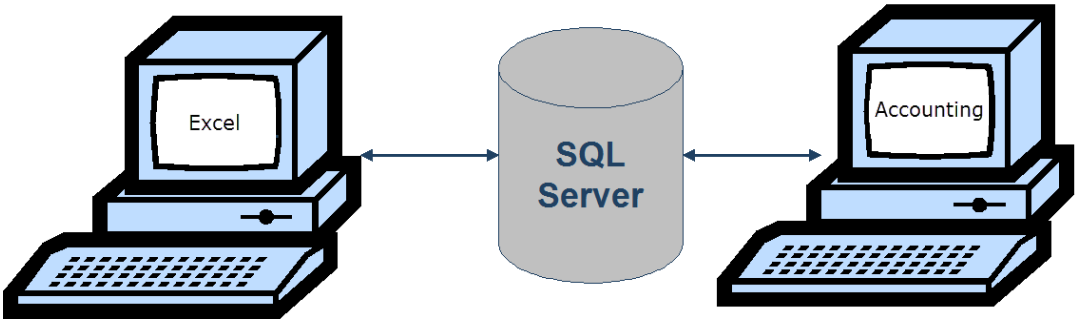


Figure 26 - Example of Sharing Data via ODBC

Sample ODBC Query with Excel and QuickBooks

As discussed above, ODBC is an excellent technology that allows users to access data easily through desktop applications. In the following example, we use Excel to analyze data queried via ODBC from QuickBooks.

To establish the query, in Excel, select **Get Data** from the **Data** tab of the Ribbon. Then, choose **From Other Sources**, **From ODBC** to open the **From ODBC** window shown in **Figure 27**. Next, select your desired data source and click **OK** as shown to begin linking the desired data into Excel.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

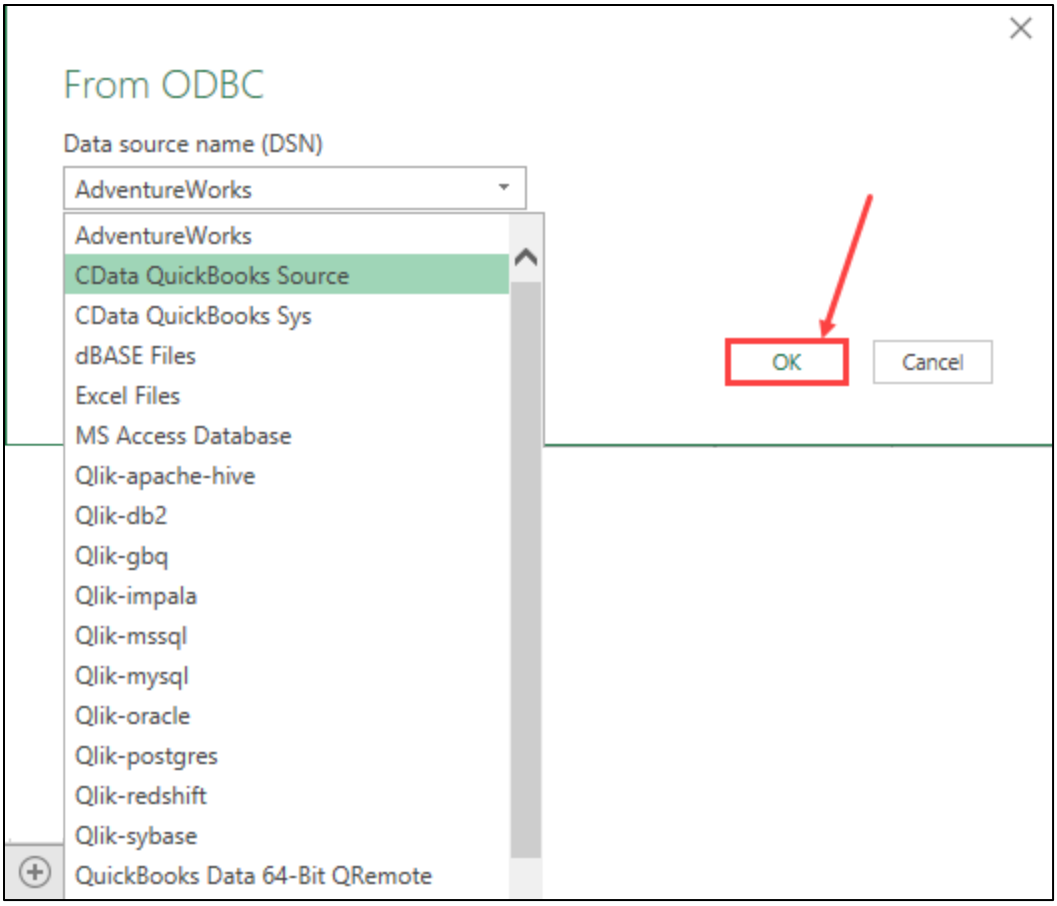


Figure 27 - Selecting QuickBooks as the Data Source

Next, select the appropriate table or tables that contain the data to analyze. In the example presented in **Figure 28**, the auditor chose the **Bill Expense Items** table. Click **Next**.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

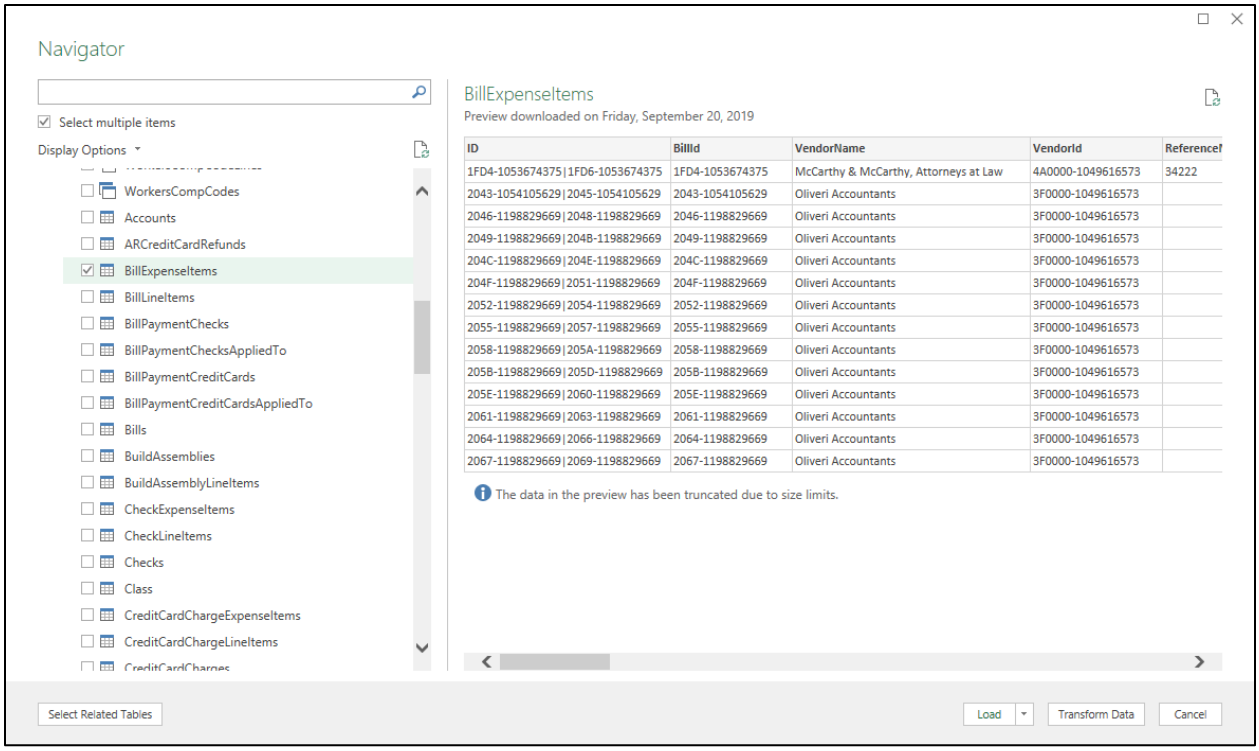
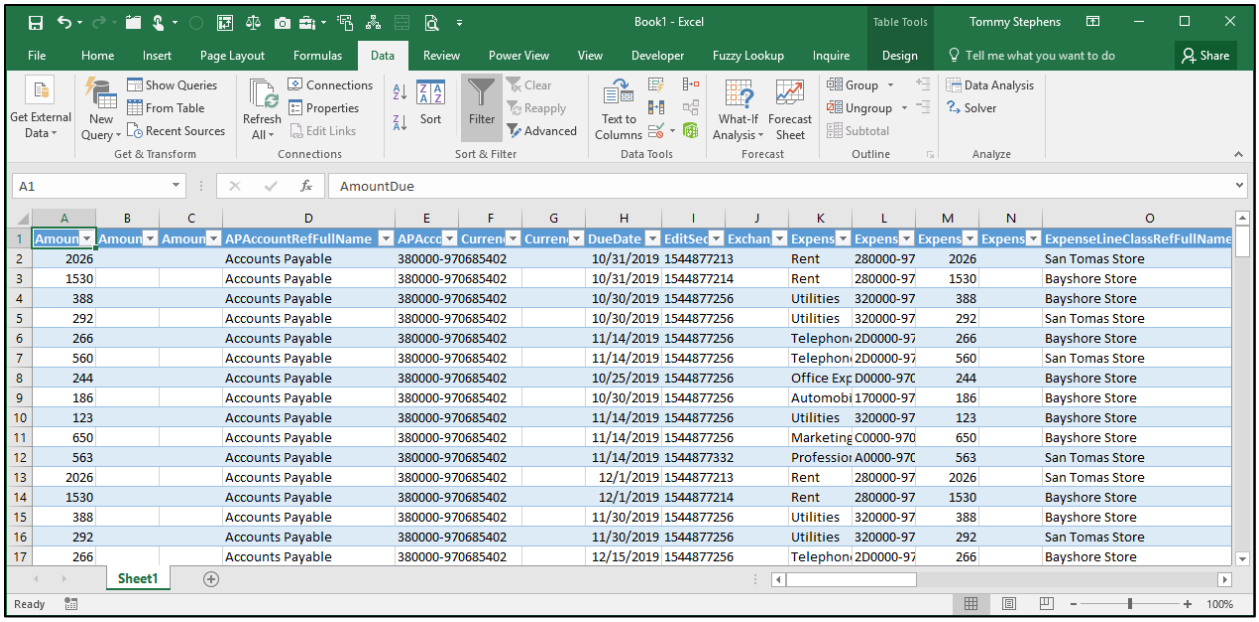


Figure 28 - Selecting Bill Expense Items Table

When querying the data, you can instruct Power Query to perform transformations on your data, such as sorting and filtering it before completing the query and returning its results to Excel. Click the **Transform Data** button near the window's lower right corner, pictured in **Figure 28,** to initiate these transformations. Alternatively, you can click the **Load** button to link the data to Excel.

Figure 29 shows a sample of how the extracted data would appear in Excel. Note that once you create the query, you can save it as is, edit and save it, or delete it. Also, note that you can modify a query's properties to include a timed data update. In effect, ODBC queries allow for the analysis of 100% of data with minimal effort. Importantly, now that you have linked the data into Excel, you can create your fraud detection tests and run them against the linked data on demand.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	Amoun	Amoun	Amoun	APAccountRefFullName	APAcco	Curren	Curren	DueDate	EditSeq	Exchan	Expens	Expens	Expens	Expens	ExpenseLineClassRefFullName
2	2026			Accounts Payable	380000-970685402			10/31/2019	1544877213		Rent	280000-97	2026		San Tomas Store
3	1530			Accounts Payable	380000-970685402			10/31/2019	1544877214		Rent	280000-97	1530		Bayshore Store
4	388			Accounts Payable	380000-970685402			10/30/2019	1544877256		Utilities	320000-97	388		Bayshore Store
5	292			Accounts Payable	380000-970685402			10/30/2019	1544877256		Utilities	320000-97	292		San Tomas Store
6	266			Accounts Payable	380000-970685402			11/14/2019	1544877256		Telephon	2D0000-97	266		Bayshore Store
7	560			Accounts Payable	380000-970685402			11/14/2019	1544877256		Telephon	2D0000-97	560		San Tomas Store
8	244			Accounts Payable	380000-970685402			10/25/2019	1544877256		Office Exp	D0000-97(	244		Bayshore Store
9	186			Accounts Payable	380000-970685402			10/30/2019	1544877256		Automobi	170000-97	186		Bayshore Store
10	123			Accounts Payable	380000-970685402			11/14/2019	1544877256		Utilities	320000-97	123		Bayshore Store
11	650			Accounts Payable	380000-970685402			11/14/2019	1544877256		Marketing	C0000-970	650		Bayshore Store
12	563			Accounts Payable	380000-970685402			11/14/2019	1544877332		Professior	A0000-97(	563		San Tomas Store
13	2026			Accounts Payable	380000-970685402			12/1/2019	1544877213		Rent	280000-97	2026		San Tomas Store
14	1530			Accounts Payable	380000-970685402			12/1/2019	1544877214		Rent	280000-97	1530		Bayshore Store
15	388			Accounts Payable	380000-970685402			11/30/2019	1544877256		Utilities	320000-97	388		Bayshore Store
16	292			Accounts Payable	380000-970685402			11/30/2019	1544877256		Utilities	320000-97	292		San Tomas Store
17	266			Accounts Payable	380000-970685402			12/15/2019	1544877256		Telephon	2D0000-97	266		Bayshore Store

Figure 29 - Extracted Purchase Order Data from the ODBC Query

Using Access as an Audit Tool

Like its Microsoft Office Excel counterpart, Access can be a valuable audit tool for analyzing data and detecting fraud. Accordingly, using Access qualifies as a detective and a deterrent internal control measure.

Auditors and fraud examiners can perform virtually all the previously described Excel auditing techniques in Access. In addition, because auditors and fraud examiners are generally more familiar with Excel, they will most likely continue using it for these functions. Therefore, we will not repeat those steps in this section. Instead, we will examine using Access for two specific purposes in auditing and fraud detection environments: 1) using Access to detect duplicate transactions and 2) using Access to store data queried by Excel.

Using Access to Detect Duplicate Transactions

Access contains a predefined query that identifies duplicate information in a field. This feature can help identify potential duplicate transactions, such as duplicate payments of the same invoice – an issue that could be important in a fraud detection environment.

To begin working with this feature, select **Find Duplicates Query Wizard** and click **OK**, as shown in **Figure 30**.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

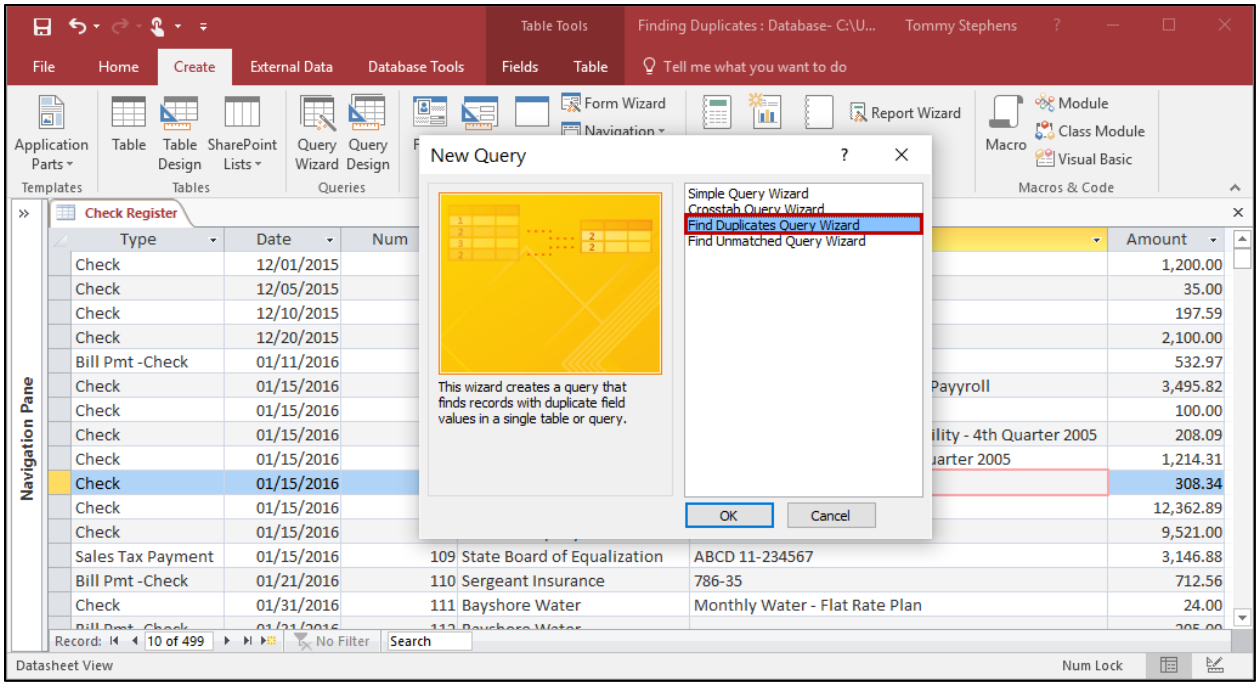


Figure 30 - Selecting Find Duplicates Query Wizard

Next, select the source of the data to query. The source can be from a table, a query, or a combination of the two. **Figure 31** demonstrates this process.

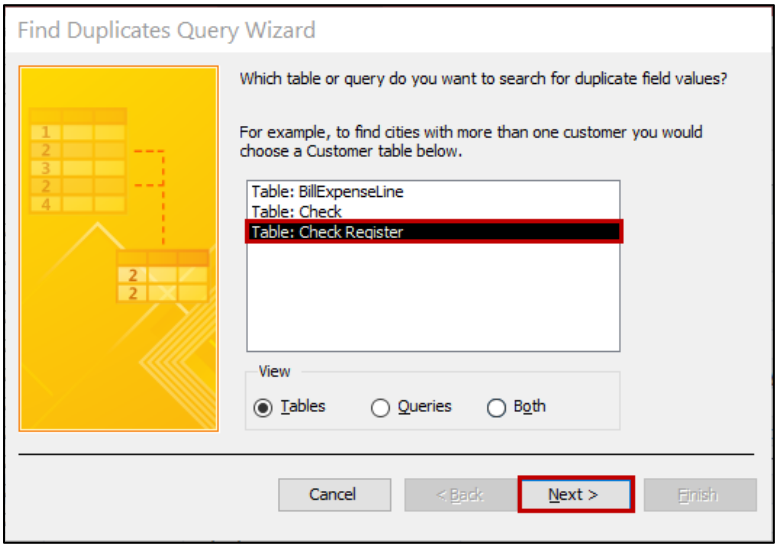


Figure 31 - Selecting Source of Data for Find Duplicate Query

Once you determine the data source(s), select the field(s) containing possible duplicate values. **Figure 32** demonstrates this process.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

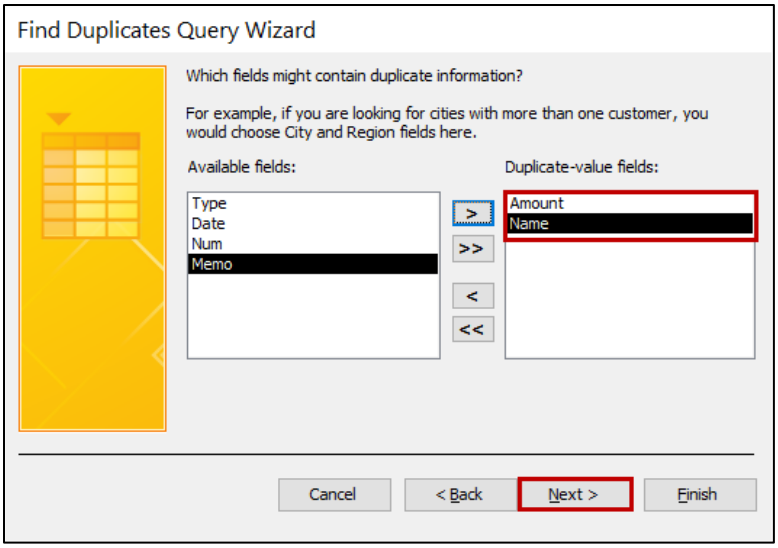


Figure 32 - Selecting Data Fields on Which to Search for Duplicate Values

After selecting the data source(s) and field(s), choose any additional fields for display when running the query, as shown in **Figure 33**. Note that any fields selected at this point are for display purposes only; Access does not search them for possible duplicate values or entries.

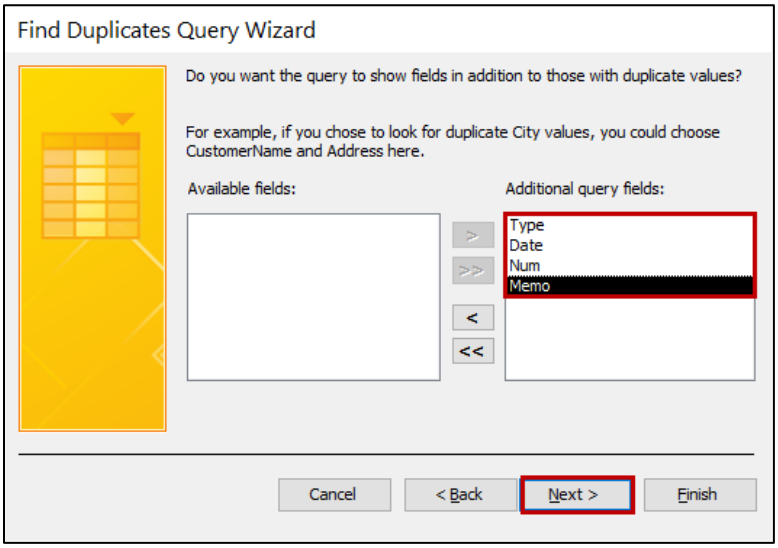


Figure 33 - Selecting Additional Fields to Display in Find Duplicates Query

Finally, name the query for future recall and click **Finish** to view the results, as shown in **Figure 34**.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

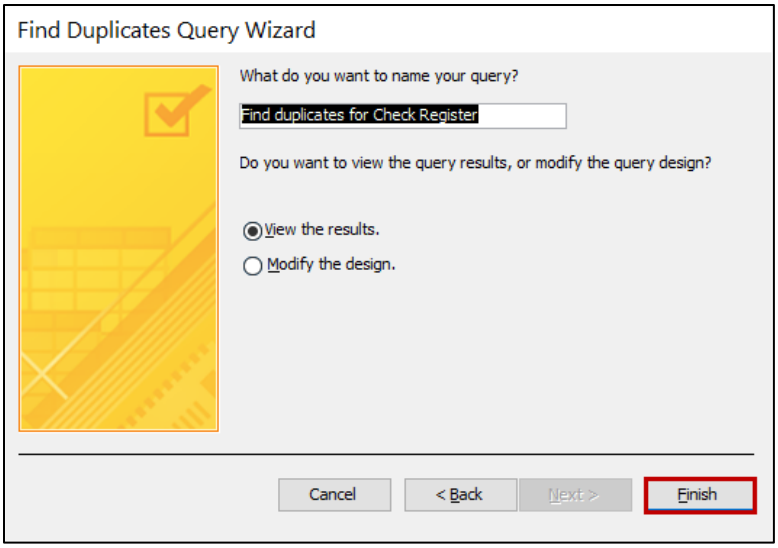


Figure 34 - Naming and Running the Find Duplicates Query

Figure 35 presents a sample of the results generated by the query. The query identified 233 possible duplicate payments in the sample data set used. The auditor or fraud investigator must research each item to determine if duplicates exist. Factors to consider when investigating the results of the query might include:

- The absence/presence of a purchase order,
- The relative proximity of the dates of the possible duplicate payments, and
- The amount of the potential duplicated payment.

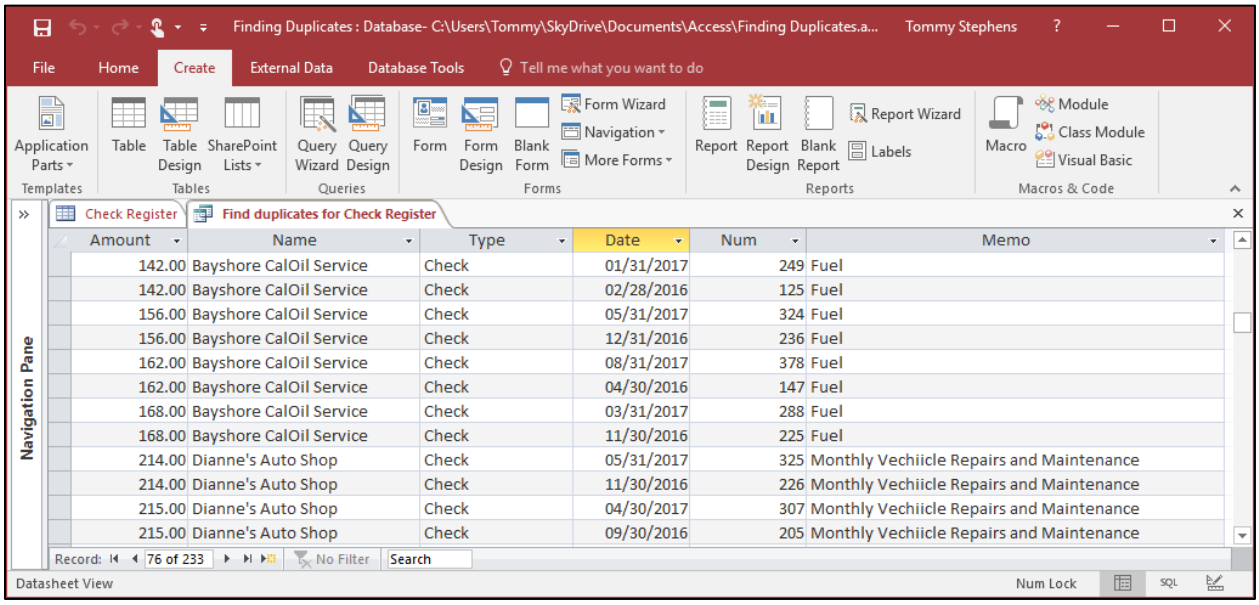


Figure 35 - Results of Find Duplicate Query

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

With Access, you can create powerful queries to search databases for other potentially fraudulent conditions. For instance, auditors and fraud examiners could use Access to generate routines searching for situations where vendor addresses include post office boxes, employee and vendor addresses are identical, and data are missing from a table[7].

Using Access to Store Data Queried by Excel

One issue that often faces those seeking to perform fraud tests in Excel is the sheer volume of transactions to examine. Excel 2007 greatly expanded the number of records that Excel can store to 1,048,576. Still, some users' computers may not have sufficient memory to process such a large quantity of data in Excel efficiently. Consequently, large volumes of data can restrict Excel's usefulness.

On the other hand, Access is a relational database management system (RDBMS) capable of processing a much greater volume of records than Excel. Therefore, Access is often the preferred application for storing large volumes of transactions to be tested. Fortunately, for those desiring to perform audit procedures or fraud detection tests in Excel, it is possible to query Access data into Excel.

Using Excel as a Fraud Detection Tool

Accounting and finance professionals probably use Excel more than any other application except Outlook. Currently, many use Excel when conducting an audit or fraud examination; however, few use Excel to get the job done more effectively. For instance, many auditors currently utilize Excel to assist with some or all the following functions.

- Amortization schedules
- Trial balances
- Journal entries
- Financial statements
- Supporting schedules
- Working papers

---

[7] An excellent example of using Access to search for billing scheme fraud was presented in an article entitled "Detecting Occupational Fraud: Billing Schemes" and published in the April 2005 issue of *The CPA Journal*. This article, written by Mark W. Lehman and Marcia L. Weidenmier, can be found online at http://archives.cpajournal.com/2005/405/essentials/p58.htm.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Notably, most of Excel's current uses in auditing environments relate to documentation; rarely is Excel used as a tool for conducting audits or fraud examinations.

Excel's existing functionality makes it attractive as an auditing and fraud detection tool. For instance, Excel can be used effectively in auditing and fraud examination processes to assist with various tests and procedures. Included are those listed below.

- Horizontal and vertical analysis
- Ratios
- Trend analysis
- Statistical measures and summarizations
- Stratifications
- Regression analysis

Further, Excel's ability to link to an ODBC-compliant database allows quick and easy data extraction, in many cases permitting the examiner to analyze 100% of the data instead of a sample. Moreover, using PivotTables in Excel can be an essential asset at the examiner's disposal when analyzing data and generating reports.

Excel has limitations in its ability to serve as an auditing and fraud examination tool. First, and as previously mentioned, there is a limitation on the number of records in a worksheet. With current versions of Excel, worksheet capacities are 1,048,576 rows and 16,384 columns. However, workbook size limits may still create issues for those analyzing vast data sets.

A second limitation is that Excel does not automatically document or log auditor activities in the worksheet, perhaps making references and working paper documentation less efficient than necessary. However, Excel's **Track Changes** feature can partially overcome this limitation.

Third, because users can change data easily in Excel, examiners can unwittingly change source data and impact Excel-based test results. You can partially overcome this limitation by using Excel's worksheet and workbook protection features to reduce the likelihood of accidentally changing data or formulas.

Excel remains an excellent resource for many auditors to increase audit efficiency and effectiveness and prevent and deter fraud despite the abovementioned limitations. However, in those cases where the drawbacks pose insurmountable obstacles to using Excel, Access and audit-specific software represent potentially attractive alternatives.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Benford's Law

In 1881, Astronomer Simon Newcomb noticed that his logarithm books' pages that contained smaller numbers were much more worn than those that started with larger numbers. Newcomb postulated that the reason for this was that numbers beginning with smaller digits – such as "1" and "2" – occurred more frequently than numbers beginning with higher digits – such as "8" and "9." Therefore, he and others using the logarithm books would have used more pages with numbers beginning with smaller digits than those starting with larger digits. Newcomb published his findings in *The American Journal of Mathematics* in 1881. Subsequently, in 1938, Frank Benford made essentially the same observation and came to the same conclusions as Newcomb while working as a physicist for GE Research Laboratories. Benford then tested and validated his theory – known as **Benford's Law** despite Newcomb's work a half-century earlier – against twenty different data lists with over 20,000 observations.

Benford's Law is a powerful tool for detecting fraud because it allows examiners to test data against recognized norms. In doing so, you can identify and investigate significant deviations from these expected values to determine if there is evidence of fraud. Benford's Law is beneficial for identifying bogus transactions and spotting transactions manipulated to avoid authorization and approval.

First Digit Probabilities

The following formula serves as the foundation for Benford's Law.

$$P\{d\} = \frac{\ln\left[1 + \frac{1}{d}\right]}{\ln(10)}$$

Based on this formula, one can project that the first digits' probability distribution would approximate the following for a given population of numbers.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

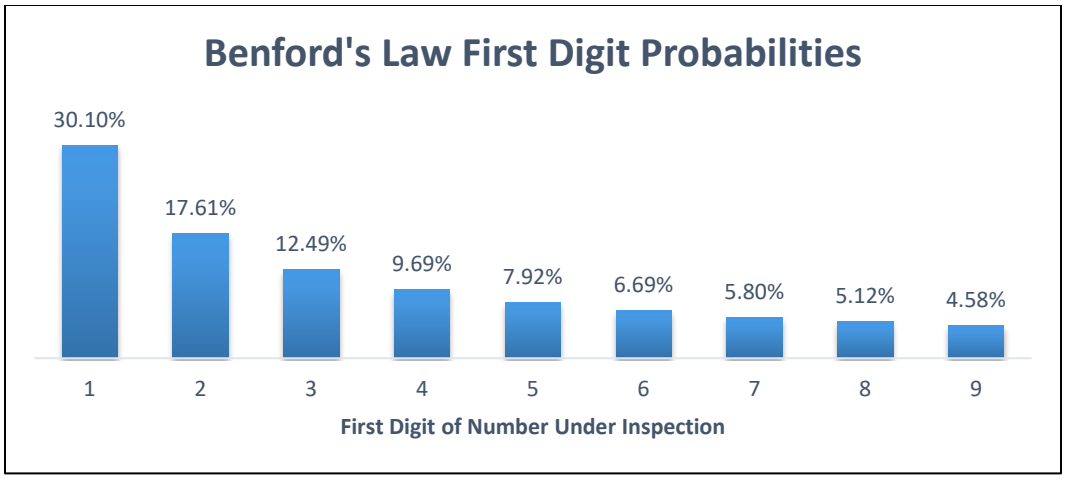


Figure 36 - Benford's Law: First Digit Probabilities

As shown in **Figure 36**, numbers that begin with "1" occur approximately seven times more frequently than numbers that start with 9. Understanding this pattern, suppose an auditor discovered that the digit "9" began, for example, 35% of the values in a population of transactions. Knowing that Benford's Law predicts that the number should be approximately 4.6%, the auditor should likely perform some testing to identify the cause of such a significant deviation. Perhaps the numbers are legitimate, and no errors or irregularities exist. On the other hand, maybe someone recorded fraudulent transactions – bogus accounts payable invoices, for instance. We cannot use Benford's Law to conclude that there is a problem; instead, it only helps to identify more work is necessary.

Second Digit Probabilities

Just as Benford's Law can predict first-digit probabilities, it predicts second-digit probabilities, too. **Figure 38** displays the second-digit probabilities predicted by Benford's Law without becoming bogged down in formulae.

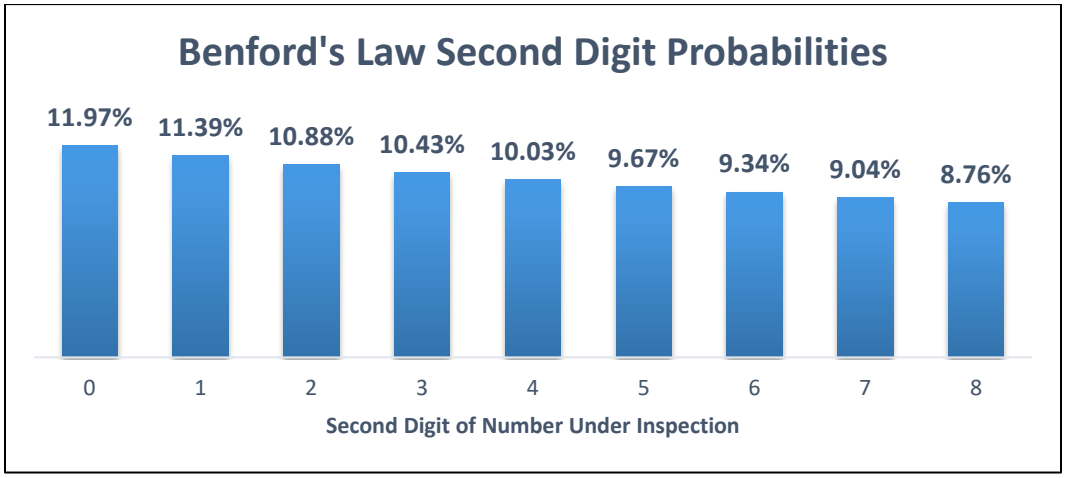


Figure 37 - Benford's Law: Second Digit Probabilities

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

While the variation in the percentages associated with second-digit probabilities is not as significant as with first-digit probabilities, there remains a distinct pattern of lower digits occurring more frequently than higher ones. You can use this pattern in the same fashion as the pattern for first-digit probabilities shown in Figure 36 to identify potentially fraudulent or erroneous transactions.

First Two-Digit Probabilities

By combining probabilities for the first and second digits, you can construct a set of probabilities for the first two digits of a number. **Figure 38** displays these probabilities.

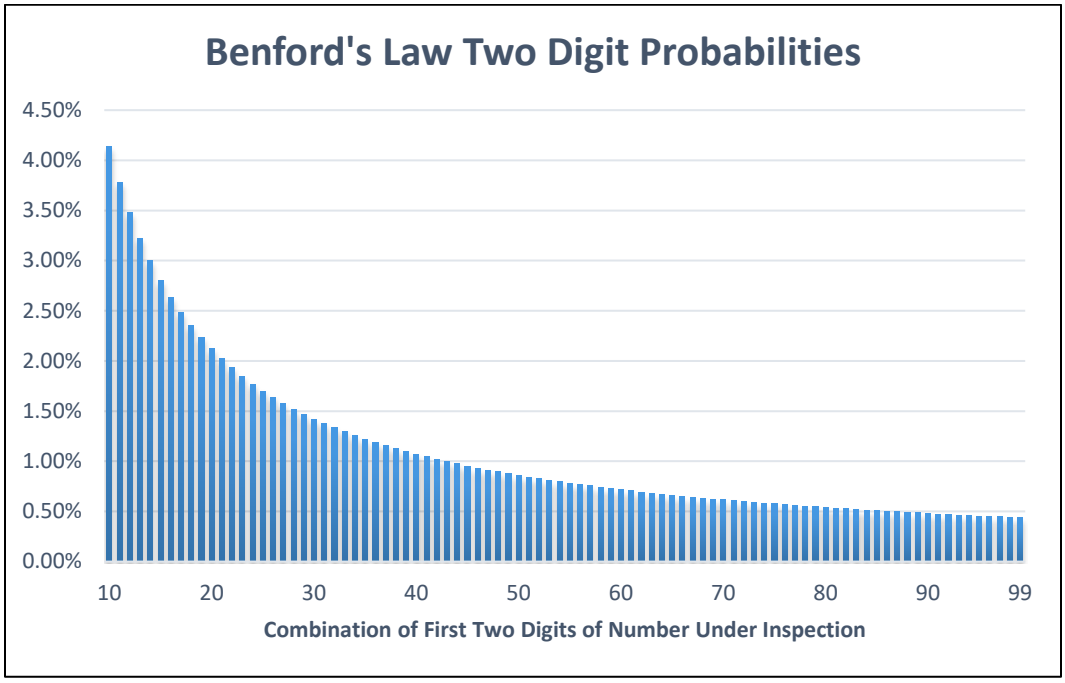


Figure 38 - Benford's Law: First Two Digits Test

Using this information, an auditor can see that numbers – invoice amounts, for example – beginning with "10" and "11" should occur much more frequently in a sample or a population than numbers starting with "98" or "99."

Utilizing Benford's Law

Benford's Law provides accountants and auditors with a potent tool for helping to detect fraud. To see how this tool can help a fraud detection scenario, consider the case of *The State of Arizona vs. Wayne James Nelson*. As reported by Mark Nigrini in the May 1999 issue of the *Journal of Accountancy*, Nelson, a manager in the Arizona State Treasurer's office, was found guilty in 1993 of defrauding the state of approximately $2 million by issuing bogus checks to fictitious vendors. Nelson, of course, diverted the checks to his personal accounts.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

As shown in **Table 3**, the amounts of the checks Nelson caused to be issued did not fit the expected distribution, as set forth by Benford's Law. Of the twenty-three disbursements issued, only one began with the digit "1;" likewise, only one check led with the digit "2." According to Benford's Law, 30.10% of the payments (approximately seven) should have led with "1." Also, Benford's Law indicates that 17.61% of the checks (about four) should have started with "2."

Check Date	Amount
October 9, 1992	$1,927.48
October 9, 1992	27,902.31
October 14, 1992	86,241.90
October 14, 1992	72,117.46
October 14, 1992	81,321.75
October 14, 1992	97,473.96
October 19, 1992	93,249.11
October 19, 1992	89,658.17
October 19, 1992	87,776.89
October 19, 1992	92,106.83
October 19, 1992	79,949.16
October 19, 1992	87,602.93
October 19, 1992	96,879.27
October 19, 1992	91,806.47
October 19, 1992	84,991.67
October 19, 1992	90,831.83
October 19, 1992	93,766.67
October 19, 1992	88,338.72
October 19, 1992	94,639.49
October 19, 1992	83,709.28
October 19, 1992	96,412.21
October 19, 1992	88,432.86
October 19, 1992	71,552.16
Total	**$1,878,688.58**

Table 3 - Fraudulent Checks in the Case of the State of Arizona vs. Wayne James Nelson

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

The fact that 21 of the 23 checks began with the digits “7,” “8,” or “9” does not comport with the probabilities predicted by Benford’s Law. According to Benford’s Law, only approximately four checks should have led with these digits.

Benford’s Law provides an excellent means of highlighting transactions that do not fit expected norms. This tool is valuable to accountants and auditors who are suspicious of bogus or illegal transactions. However, be aware that if the perpetrators are aware of Benford’s Law, then it is likely that they will cause the fraudulent transactions to fit the expected distributions defined by Benford’s Law.

Applying Benford’s Law in Excel

First Digit Test in Excel

With smaller data sets like the one presented in Table 3, applying Benford’s Law requires only a quick visual observation and inspection of the data. However, when applying Benford’s Law to hundreds or thousands of transactions, a more efficient analysis is necessary, and Excel offers such a means. Using familiar Excel commands such as **LEFT** and **COUNTIFS**, you can construct a Benford’s Law test in Excel for any single-digit or multiple-digit probabilities.

In the example below, an Excel worksheet contains data for credit memos issued by a company. An auditor concerned about fictitious credit memos wants to run the first digit Benford’s Law test on the population. The credit memo data appears in **Figure 39**.

	A	B
1	Check Number	Invoice Amount
2	1001	41.90
3	1002	5,060.28
4	1003	986.87
2188	3188	99.90
2189	3189	31.00
2190	3190	53.90
2191	3191	91.70
2192	3192	959.70
2193	3193	23.80

Figure 39 - Worksheet Containing Credit Memo Data to Analyze with Benford’s Law

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

The first step in creating a first-digit Benford's Law test is extracting the first digit from the *Invoice Amount* field. You can accomplish this by creating the following formula in cell C2 and copying the formula down through the data set.

=LEFT(B2,1)

As entered, the formula instructs Excel to extract the first character of the entry in cell B2. Upon entering and copying the formula, the worksheet resembles that shown in **Figure 40**.

	A	B	C
1	Check Number	Invoice Amount	First Digit
2	1001	41.90	4
3	1002	5,060.28	5
4	1003	986.87	9
2188	3188	99.90	9
2189	3189	31.00	3
2190	3190	53.90	5
2191	3191	91.70	9
2192	3192	959.70	9
2193	3193	23.80	2

Raw I ...

Figure 40 - Credit Memo Worksheet with First Digit Extracted

As Benford's Law defines, it is necessary to count each digit's number of occurrences in column B and compare that to expected norms. Next, add a second worksheet to the workbook, similar to that pictured in **Figure 41**.

	A	B	C	D	E	F
1	Digit	Count	Expected Proportion	Actual Proportion		
2	1		30.10%			
3	2		17.61%			
4	3		12.49%			
5	4		9.69%			
6	5		7.92%			
7	6		6.69%			
8	7		5.80%			
9	8		5.12%			
10	9		4.58%			
11	Total		100.00%			

Raw Data | First Digit Test | S ...

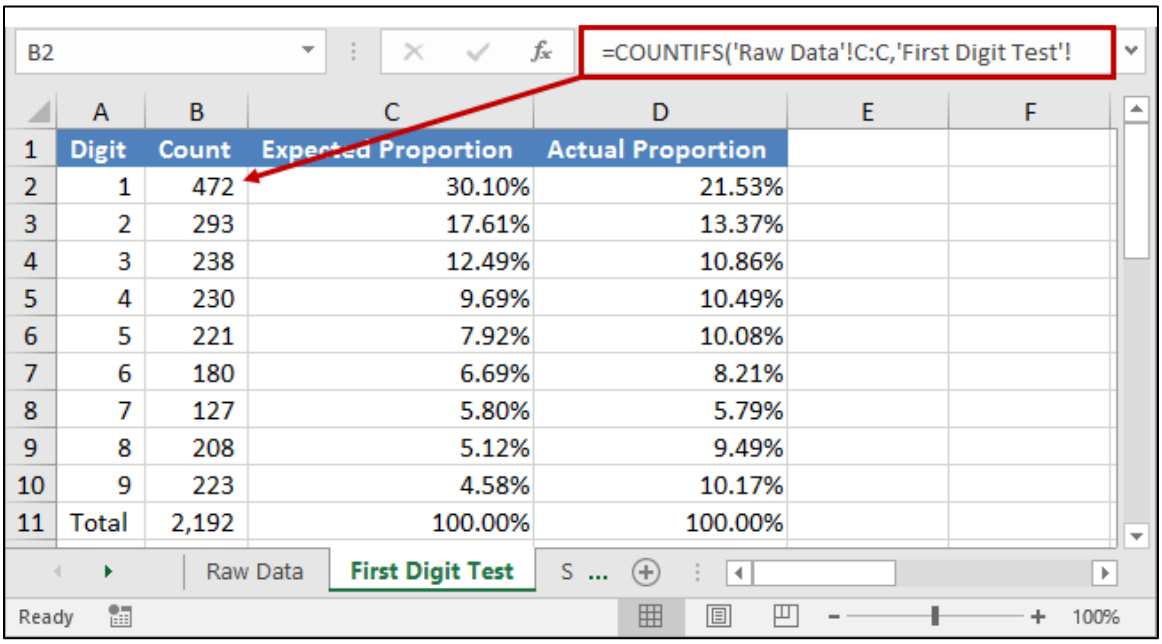
Figure 41 - Data Analysis Worksheet Benford's Law Test

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

In cell B2 of the First Digit Test worksheet shown in **Figure 42**, enter the following formula to count the number of instances of each digit in the Raw Data worksheet.

=COUNTIFS('Raw Data'!C:C,'First Digit Test'!A2)

Using Excel's **COUNTIFS** function, the worksheet counts and summarizes all occurrences of the digit in cell A2 of the First Digit Test worksheet found in column C of the Raw Data worksheet. Copy this formula down through cell B11 of the First Digit Test worksheet. Adding **SUM** formulas to cells B11, C11, and D11 and percentage calculations to column D transforms the First Digit Test worksheet to that shown in **Figure 42.**



	A	B	C	D	E	F
1	Digit	Count	Expected Proportion	Actual Proportion		
2	1	472	30.10%	21.53%		
3	2	293	17.61%	13.37%		
4	3	238	12.49%	10.86%		
5	4	230	9.69%	10.49%		
6	5	221	7.92%	10.08%		
7	6	180	6.69%	8.21%		
8	7	127	5.80%	5.79%		
9	8	208	5.12%	9.49%		
10	9	223	4.58%	10.17%		
11	Total	2,192	100.00%	100.00%		

Figure 42 - Data Analysis Worksheet with First Digits Counted

In the first-digit Benford's Law example presented above, far too many transactions appear to begin with the digits "8" and "9." Additionally, there seem to be too few transactions starting with "1" and 2." This anomaly appears in the graph below in **Figure 43**, comparing expected to actual percentages derived from the first-digit Benford's Law test. Whether or not these findings represent errors or fraud is not determined solely by applying Benford's Law; however, Benford's Law helps identify those areas where additional testing and evaluation are required.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

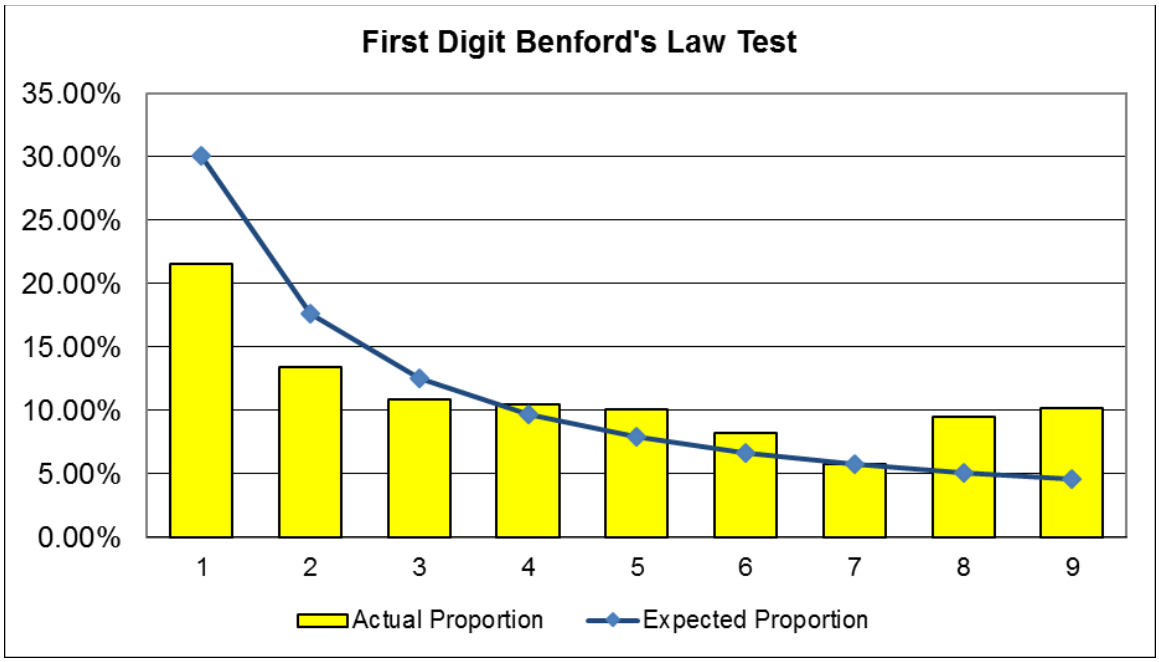


Figure 43 - Expected Versus Actual Percentages Graph

Second Digit Test in Excel

In addition to creating a first-digit Benford's Law test in Excel, you can make a second-digit test relatively easily. The steps to create a second-digit test closely resemble those used in the first-digit test; however, we will use Excel's **MID** function instead of the LEFT function to identify the second digits.

As shown in **Figure 44**, you can use the following formula to identify the second digit in the *Invoice Amount* column.

=MID(B2,2,1)

This formula instructs Excel to return the contents of cell B2, beginning with the second character and continuing for one space. Excel ignores the dollar sign applied to data in column B because that is a format only.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

	A	B	D
1	Check Number	Invoice Amount	Second Digit
2	1001	41.90	1
3	1002	5,060.28	0
4	1003	986.87	8
2188	3188	99.90	9
2189	3189	31.00	1
2190	3190	53.90	3
2191	3191	91.70	1
2192	3192	959.70	5
2193	3193	23.80	3

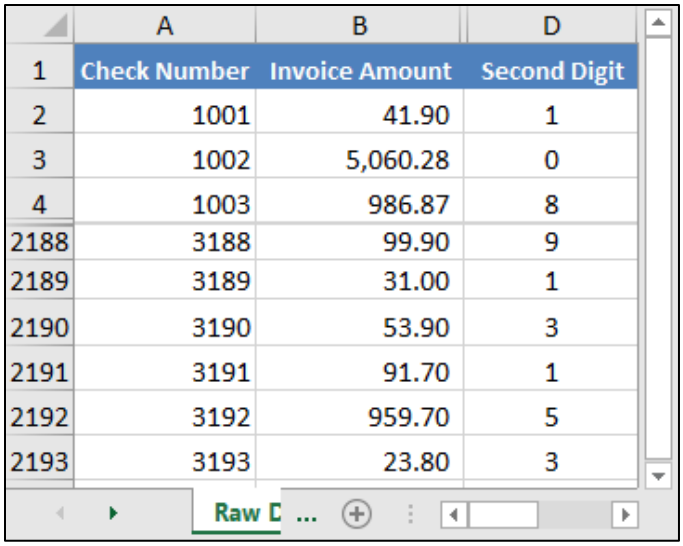


Figure 44 - Identifying the Second Digit in Excel Using the MID Function

Copying the formula through the data set generates a listing of all the second digits. These can be summarized and analyzed using the same approach for conducting a first-digit test. One notable exception when applying a second-digit test is considering "0" because it is a valid second digit. Conversely, you can ignore "0" when performing a first-digit test because it is an invalid first digit.

	A	B	C	D
1	Digit	Count	Expected Proportion	Actual Proportion
2	0	220	11.97%	10.04%
3	1	157	11.39%	7.16%
4	2	213	10.88%	9.72%
5	3	281	10.43%	12.82%
6	4	201	10.03%	9.17%
7	5	225	9.67%	10.26%
8	6	231	9.34%	10.54%
9	7	201	9.04%	9.17%
10	8	237	8.76%	10.81%
11	9	226	8.50%	10.31%
12	Total	2,192	100.00%	100.00%

Figure 45 - Analyzed Data in a Second Digit Benford's Law Test

Finally, when viewed graphically (see **Figure 46**), the second digit of Benford's test shows relatively significant deviations from expected norms with the digits 0, 1, 2, 3, 8, and 9. Again, this does not necessarily indicate erroneous or fraudulent transactions. Instead, it reveals that additional audit work may be necessary.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

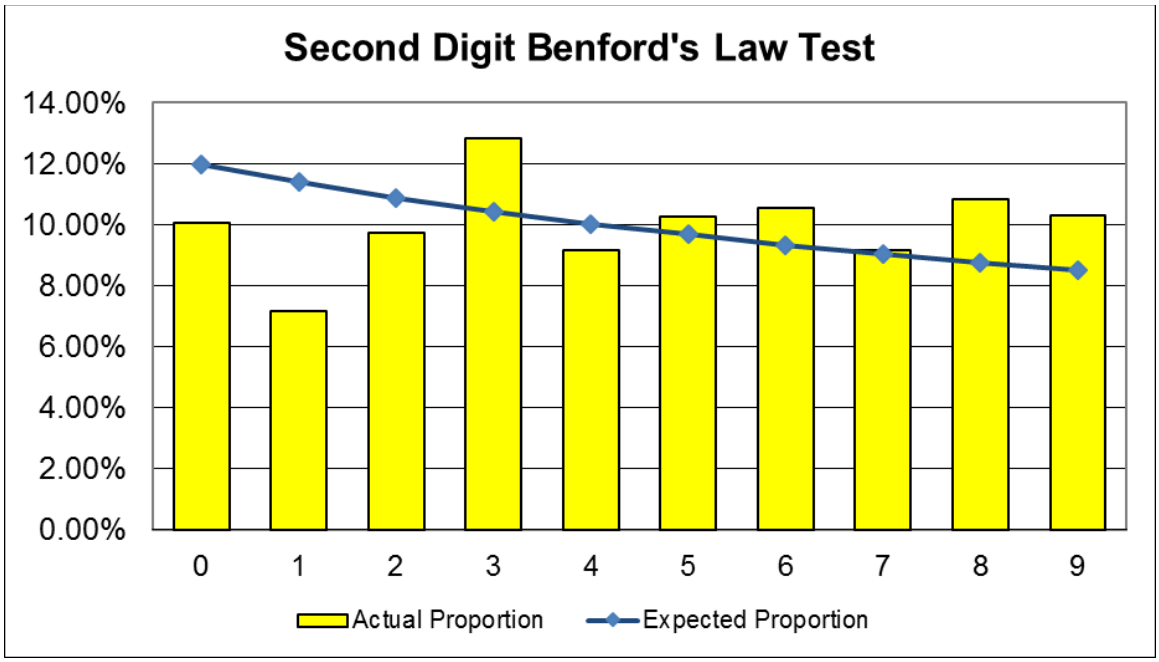


Figure 46 - Expected Versus Actual Percentages

First Two-Digit Test in Excel

Just as you can use Excel for a single-digit test – either first or second, as shown previously – you can also test the conformity of the first two digits to Benford's Law. The procedure will be like that of the first-digit test. However, we will modify the formula containing the LEFT function slightly. Specifically, changing the LEFT formula to resemble that shown below will cause it to return the first two characters of the cell instead of just the first character.

=LEFT(B2,2)

Once we identify the two left characters of the cells under consideration, as shown in **Figure 47**, we can analyze the data to determine its conformity with the results predicted by Benford's Law.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

	A	B	E
1	Check Number	Invoice Amount	First Two Digits
2	1001	41.90	41
3	1002	5,060.28	50
4	1003	986.87	98
2188	3188	99.90	99
2189	3189	31.00	31
2190	3190	53.90	53
2191	3191	91.70	91
2192	3192	959.70	95
2193	3193	23.80	23

Figure 47 - Identifying Characters for First Two-Digit Benford's Law Test

Using the same analysis techniques employed with the first and second-digit tests, you can easily create a chart to provide a pictorial representation of the data values that do not fit the expected distribution of numbers according to Benford's Law. **Figure 48** provides an example of such a chart.

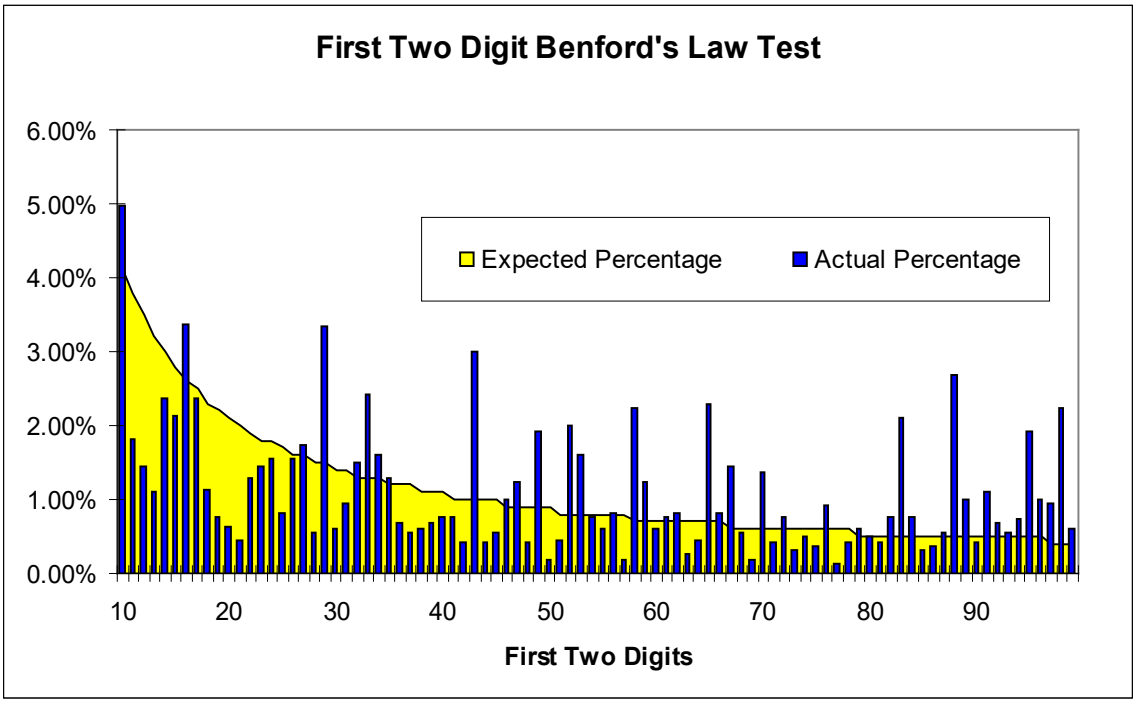


Figure 48 - Results of First Two Digits Benford's Law Test

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Limitations of Using Benford's Law

Though Benford's Law provides accountants and auditors with a robust fraud detection tool, its use certainly has distinct and significant limitations. Failing to understand these limitations could result in excessive examinations of data and incorrect conclusions based on data observations.

First, large data sets are more likely to fit Benford's Law than smaller ones. As with virtually all mathematical models, large data sets are more reliable. When applying Benford's Law, small sample sizes or populations may not contain enough observations to produce reliable test results.

Second, any data set based on assigned numbers may not follow Benford's Law. A good example would be Social Security Numbers issued based on a prescribed order and methodology. Likewise, checking account numbers will usually not adhere to Benford's Law. Banks typically bias the numbers based on whether the account is for an individual or business and the state where the customer opened the account.

Third, any set of numbers where the population has defined minimum values, maximum values, or both will likely not conform to Benford's Law. For instance, an analysis of hourly wage rates may be biased away from Benford's Law due to minimum wage requirements or union-negotiated rates. Likewise, annual contributions to Individual Retirement Accounts or 401(k) plans may not conform due to the defined maximum values that team members can contribute.

Most data populations that introduce bias or skew will likely not follow Benford's Law. Therefore, from a fraud detection standpoint, you must take great care to understand all the tested data's relevant characteristics. For instance, many companies round selling prices so that the cents section is always "95" or "99." Failing to understand this characteristic when applying a Benford's Law test to the population of selling prices might cause an examiner to reach incorrect conclusions on the validity of sales prices.

?	Given what you have learned about Benford's Law, is this a tool you should consider implementing in your organization or using on behalf of a client? Further, should you immediately conclude that fraud has occurred if you implement Benford's Law and receive results that a particular data set does not align with Benford's probability distributions?

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Accounting Software Controls

Chapter 6

Large and small businesses utilize accounting applications to aid their accounting function. Inexpensive offerings such as QuickBooks and Sage 50 serve the entry-level and small business markets. Mid-size organizations use applications with a more robust feature set, such as those provided by Open Systems, Microsoft, and Sage. Finally, larger businesses tend to use ERP tools provided by companies such as Oracle and SAP. Even though the price point and feature sets range widely from one product to another, most available solutions offer built-in internal control options to secure the information and ensure that the accounting procedures follow management's intentions. This chapter examines the general and application controls typically found in accounting solutions used by small businesses.

Learning Objectives

Upon completing this chapter, you should be able to:

- Identify accounting/business management software general controls and list examples of general controls commonly found in commercial accounting applications;
- Define application accounting controls and list examples available in many commercial accounting software applications; and
- List examples of application controls in each of the following three areas:
    - Revenue and cash;
    - Purchasing, payables, and payroll; and
    - Inventory, production, and fixed assets.

Controls and Tools Available in Accounting/Business Management Products

Accounting application developers determined long ago that, while the primary goal is to record accounting information correctly, a significant secondary objective is controlling accounting access to accounting data. Because of this, most accounting applications provide appropriate internal control options incorporated into the software. These options usually address the need for general and accounting controls. Let us continue in this chapter by looking at these controls more closely.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

General Controls in Accounting Software

Recalling Chapter Three, companies use general controls to secure data, establish access rights, and direct the overall operation of, in this case, the accounting software. Some of the most notable general controls include limited access to data based on username and password, limited access to software functionality based on username and password, automatic backup of data upon exit from the application (shown in **Figure 49**), and built-in global audit trails for after-the-fact review of application activity.

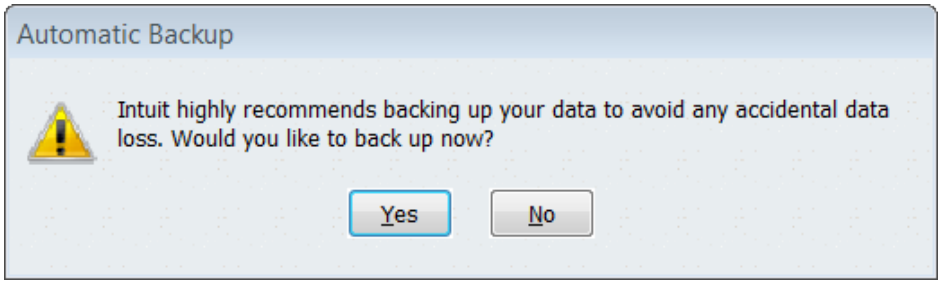


Figure 49 - Automatic Backup Prompt Found in QuickBooks

Other helpful general controls are also available, enhancing the usability and functionality of the software. For example, a large and growing number of products allow for document-specific printer setup. This feature enables users to generate a check from one printer and an invoice from another. We show an example of this in **Figure 50**. This procedure saves time and reduces the risk of printing on the wrong form or paper type. Another general control found in almost all products – and is often taken for granted – is date-range validation. For example, if a user requires a report for the first quarter of a calendar year but inadvertently enters the date range as "03/31/XX to 01/01/XX," the software stops the process and asks the user to correct her entry.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

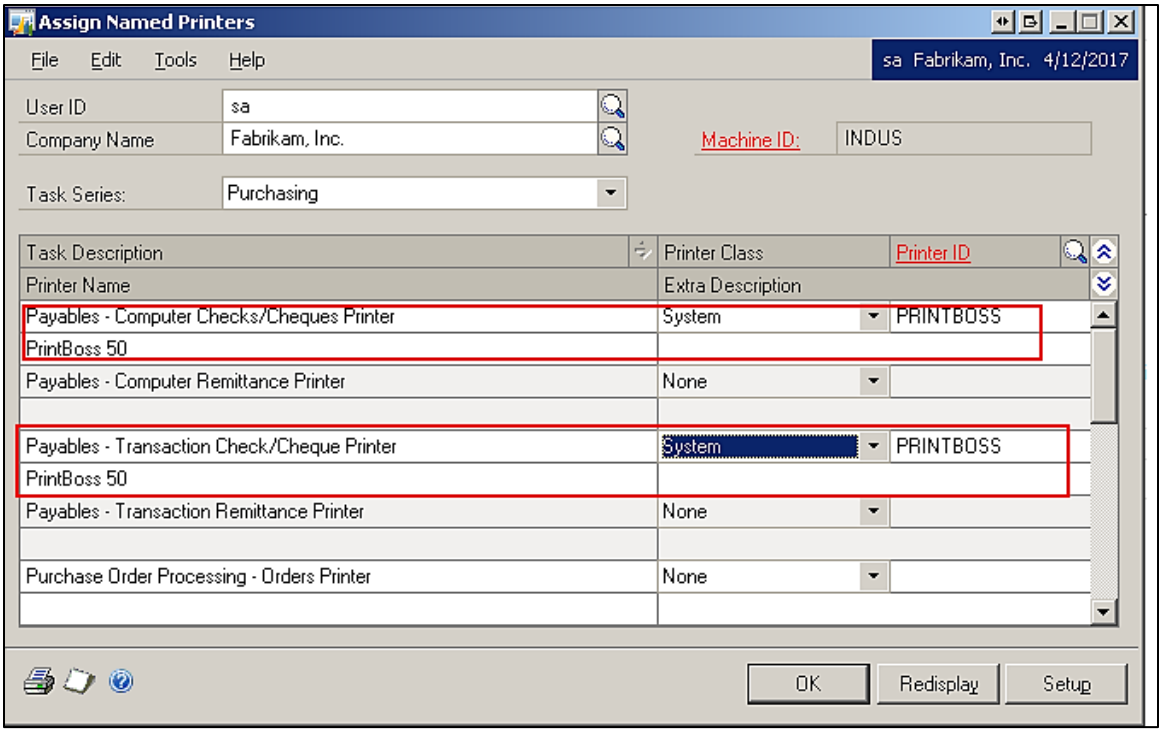


Figure 50 - Named Printers Setup Screen in Dynamics GP

Because of the large number of general controls found across the entire accounting/business management software market, it may behoove class participants to review the documentation for the product used at their organization to see if any unimplemented general controls are available.

Controlling Authorization with User IDs and Passwords

Assigning and using unique user IDs and passwords is one of the most fundamental internal control procedures in all organizations. Businesses should employ this activity at both the workstation and application levels. Unfortunately, many small businesses ignore this most basic internal control procedure.

You should assign user IDs and passwords so employees can access only those areas they need to perform their job responsibilities. All other areas within the application should be off-limits and restricted by the user ID's privileges. Further, it is critical to maintain and preserve the integrity of user IDs and passwords. Of course, change passwords immediately if there is a breach or suspicion of one. Additionally, verify the integrity of all rights assigned to each user. **Figure 51** displays the process of setting up user rights in QuickBooks.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.



Figure 51 - Establishing Users in QuickBooks

You should assign a separate user ID and password to each user. Further, you should ensure that the rights afforded to each user align with that user's job responsibilities. QuickBooks users must pay particular attention to the choices "Full Access" and "Selective Access" and the different levels of "Selective Access." You can enhance authorization control by restricting a user's privileges within the application.

User IDs and passwords in Sage 50 Quantum use "role-based security." You assign each user to a predefined role in this environment, as shown in **Figure 52**. **Figure 53** and **Figure 54** illustrate the role-assignment windows in Sage 100 and Microsoft Dynamics GP, respectively.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

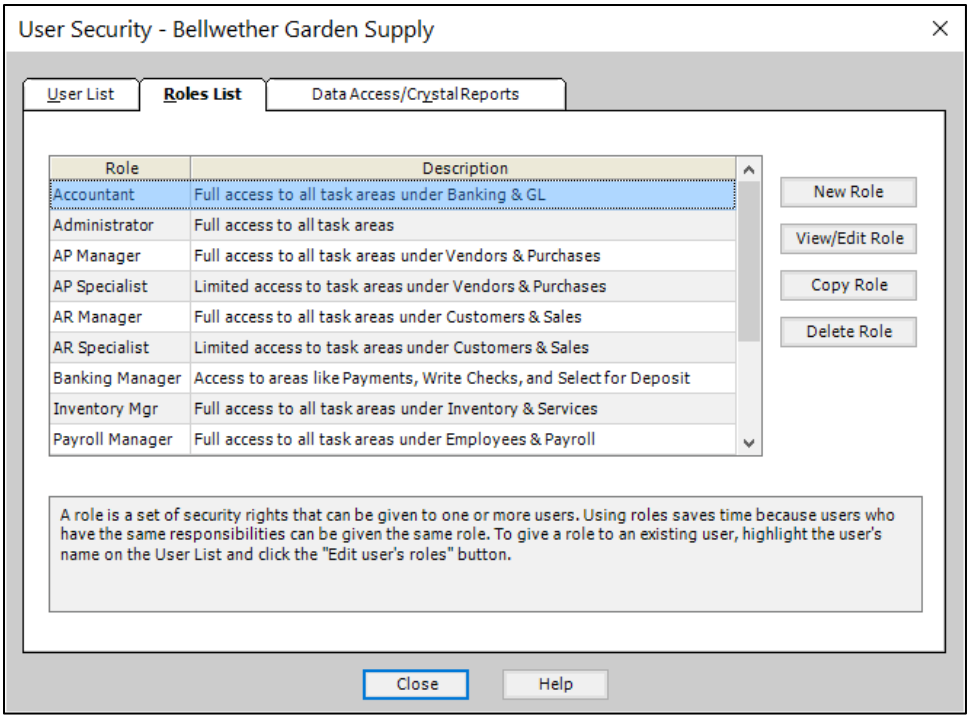


Figure 52 - Establishing User Roles in Microsoft Sage 50 Quantum

Other applications using a role-based security model include Sage 100, Microsoft Dynamics GP, and QuickBooks Enterprise Solutions. Role-based security models allow administrators to assign rights and privileges to roles and, in turn, associate roles with individual users or groups of users. This method of managing user rights works particularly well in organizations where multiple users require the same rights. For instance, when assigning rights and privileges to a group of accounts payable clerks, an administrator could create an “accounts payable clerk” role and confer that role to each user. Later, if the clerks' rights and privileges require modification, the administrator only needs to modify the role. Upon doing so, all the changes propagate to individual users. Of course, proper management and maintenance of the roles are essential for an effective control procedure.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

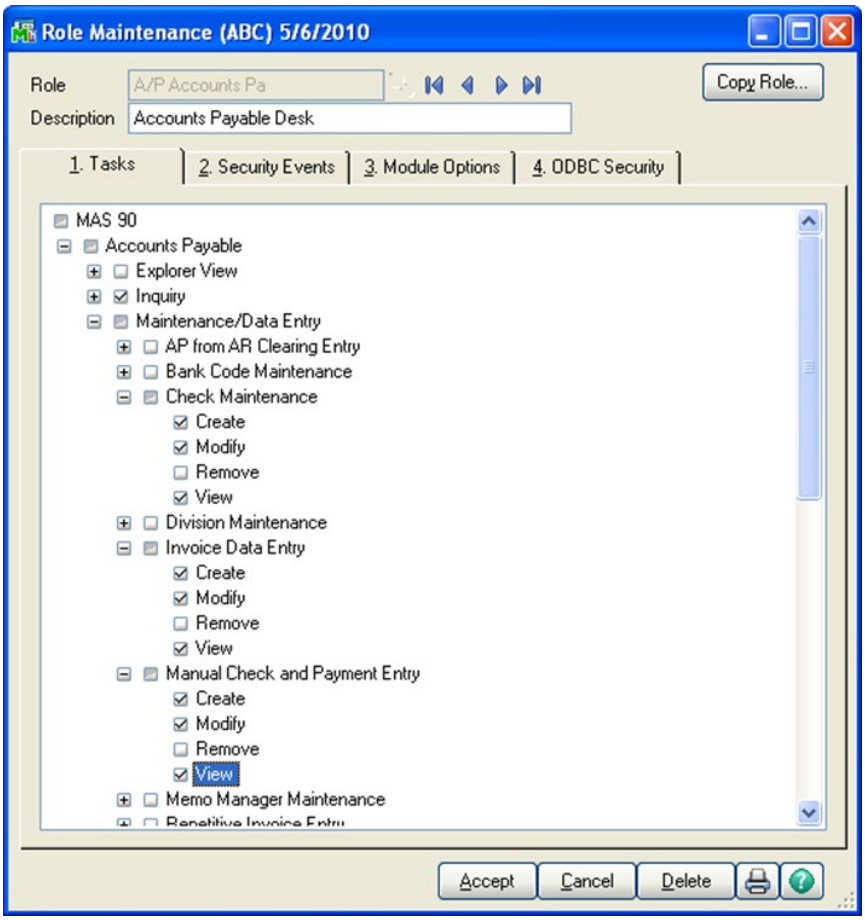


Figure 53 – Role-based Security in Sage 100

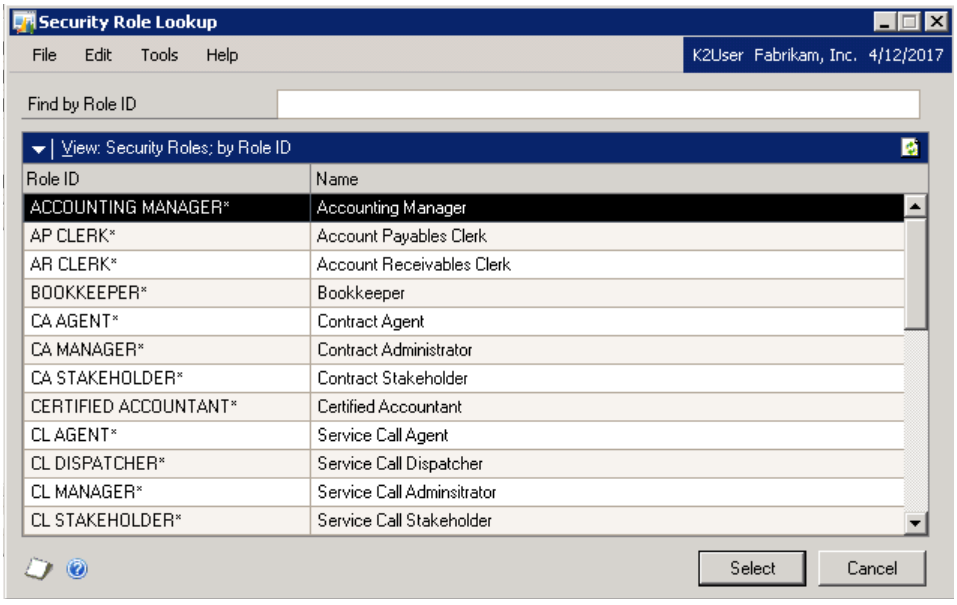


Figure 54 - Managing Roles in Microsoft Dynamics GP

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

?	When thinking about your accounting software or that used by one of your clients, what primary authentication controls are available in the application? Has each of those authentication controls been enabled? Are they used routinely, or does each user log in with the same credentials?

Accounting Controls Overview

Organizations use accounting controls to govern the operation of accounting procedures. These include using authorization limits, prerecorded information, sequential document numbering, and automated workflow functionality. Let us consider the example of a three-part purchasing procedure. Many businesses require a purchase order, proof of receipt, and an invoice from a vendor before issuing payment for goods purchased. In this scenario, the company might use authorization limits to control the value of goods a team member can buy. Further, pre-numbered purchase orders and workflow tools could help direct the purchase request to a staff member with the authority to approve the purchase. All these tools are accounting controls designed to streamline and secure the application. We show the purchase order transaction screen in **Figure 55.**

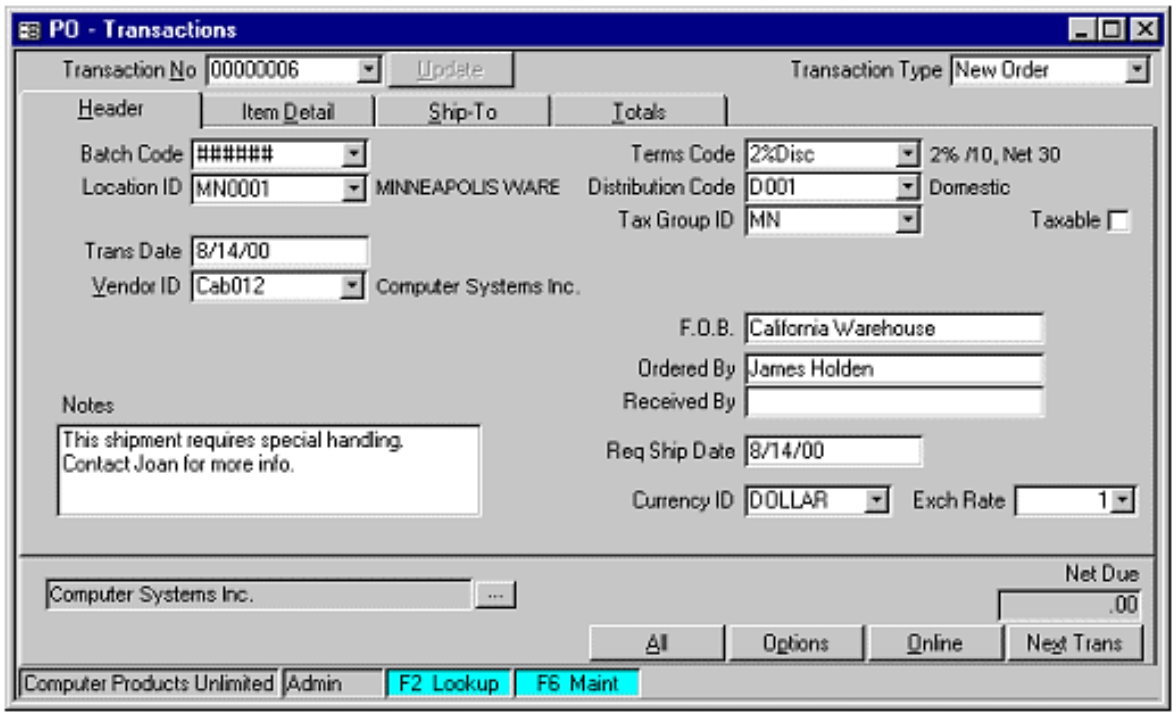


Figure 55 - OSAS Traverse Purchase Order Transaction Screen

Prerecorded Data Input

Using prerecorded data can be an effective control to help achieve proper authorization of a transaction. For example, to ensure that items' selling prices follow management's general and

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

specific authorization, pre-established prices and price levels can be maintained, allowing authorized team members to designate per item and customer pricing.

Figure 56 illustrates the use of price levels in QuickBooks. In the example provided, every customer classified as "Retail" receives the prices indicated in the "Custom Price" column. Prerecorded data – such as price lists – helps ensure selling prices are authorized.

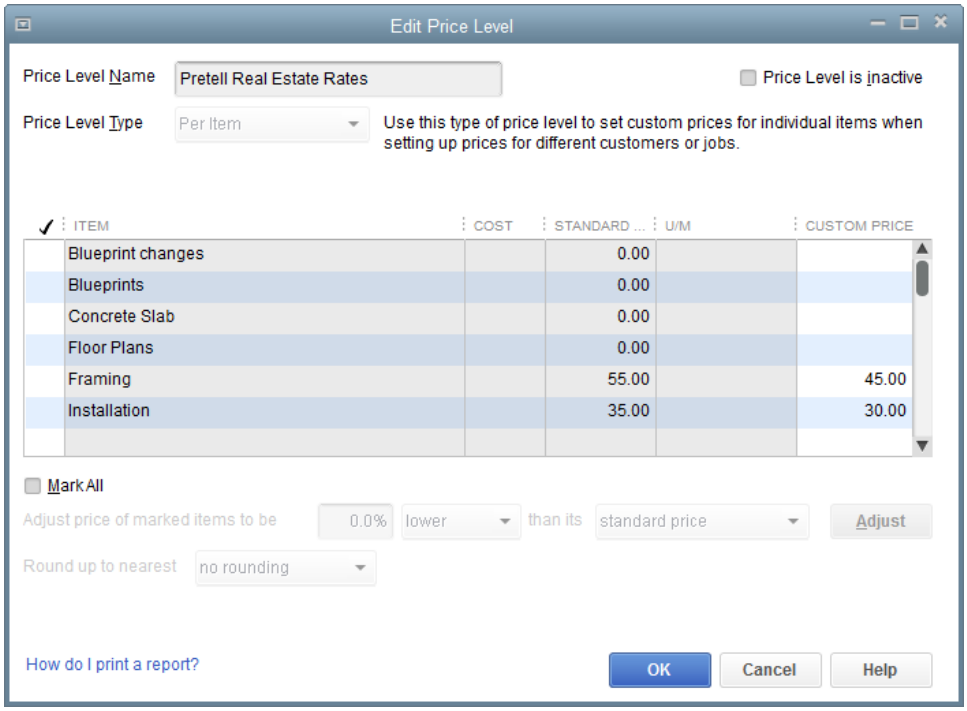


Figure 56 - Establishing Price Levels in QuickBooks

Revenue and Cash Controls

Protecting the revenue stream and the resulting cash flows into the business is a significant concern for many small business owners. And rightfully so. The business's survival is jeopardized if the revenue stream and resulting cash inflows are compromised or disrupted.

To the extent that the management team assesses the risks associated with revenue and cash as significant, and if management cannot otherwise mitigate these risks through outsourcing, they must develop appropriate internal control procedures, considering cost versus benefit. Of course, when designing, implementing, and evaluating the control procedures relevant to the revenue cycle, it is necessary to understand the flow of transactions and personnel's responsibilities within the accounting function as these responsibilities relate to the revenue cycle.

Revenue-related transactions should carry management's general and specific authorization. Off-the-shelf accounting applications often utilize the following procedures to assist with approval controls.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

- User IDs and passwords restricting access to the applications and data
- Prerecorded data input for fields such as credit limits, prices, and terms
- Utilizing workflow tools

Users can also generate exception reports indicating which transactions are subject to particular approval procedures. These types of reports represent an example of potential detective control procedures.

Controlling Access to Credit Memos

One of the areas of most significant concern to small business owners and managers is employees stealing cash receipts in the revenue cycle. Of course, the lack of proper segregation of duties is often the control failure contributing to this crime. In addition, guilty employees frequently attempt to cover their tracks by writing off the stolen balance by issuing a credit memo. Therefore, controlling which employees can access the credit memo function in the accounting software application is critical.

As shown in **Figure 57**, Sage 50, for instance, allows users to control access to the credit memo function through the assignment of user rights and privileges. In the following example, Jane Doe can access most other sales functions but cannot perform credit card functions and only view credit memos.

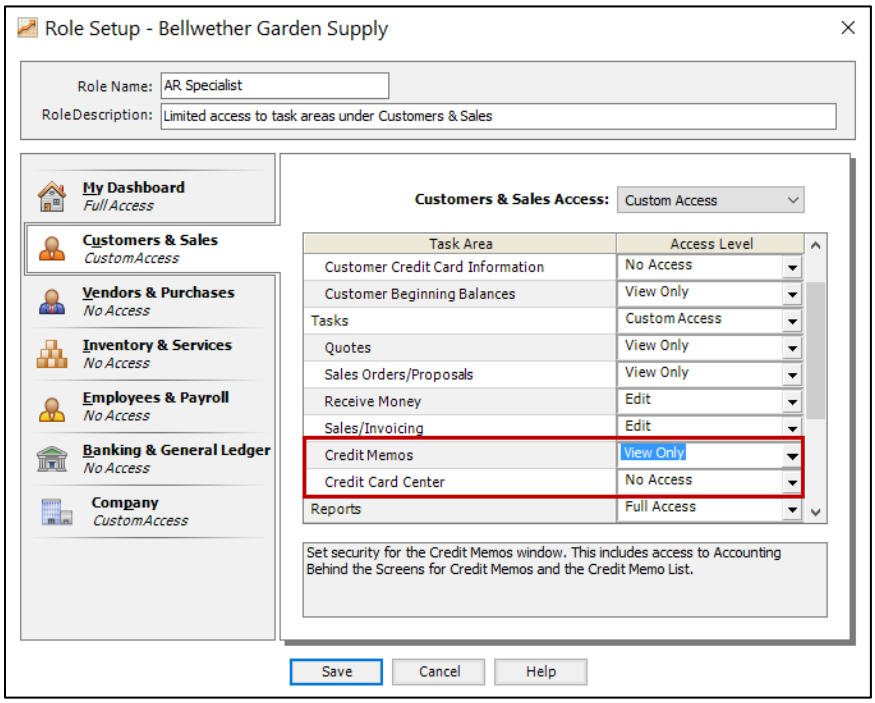


Figure 57 - Controlling User Access in Sage 50

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Preventing Unauthorized Sales Discounts

Another concern for small business owners is employees granting unauthorized discounts to customers during the sales cycle. In addition to a detective control such as reviewing reports to ascertain if unauthorized discounts exist, a preventive control of requiring a password to override selling prices is available in some accounting applications. To illustrate, as shown in **Figure 58**, Microsoft Dynamics GP allows administrators to establish password-based controls over price overrides when creating customer invoices.

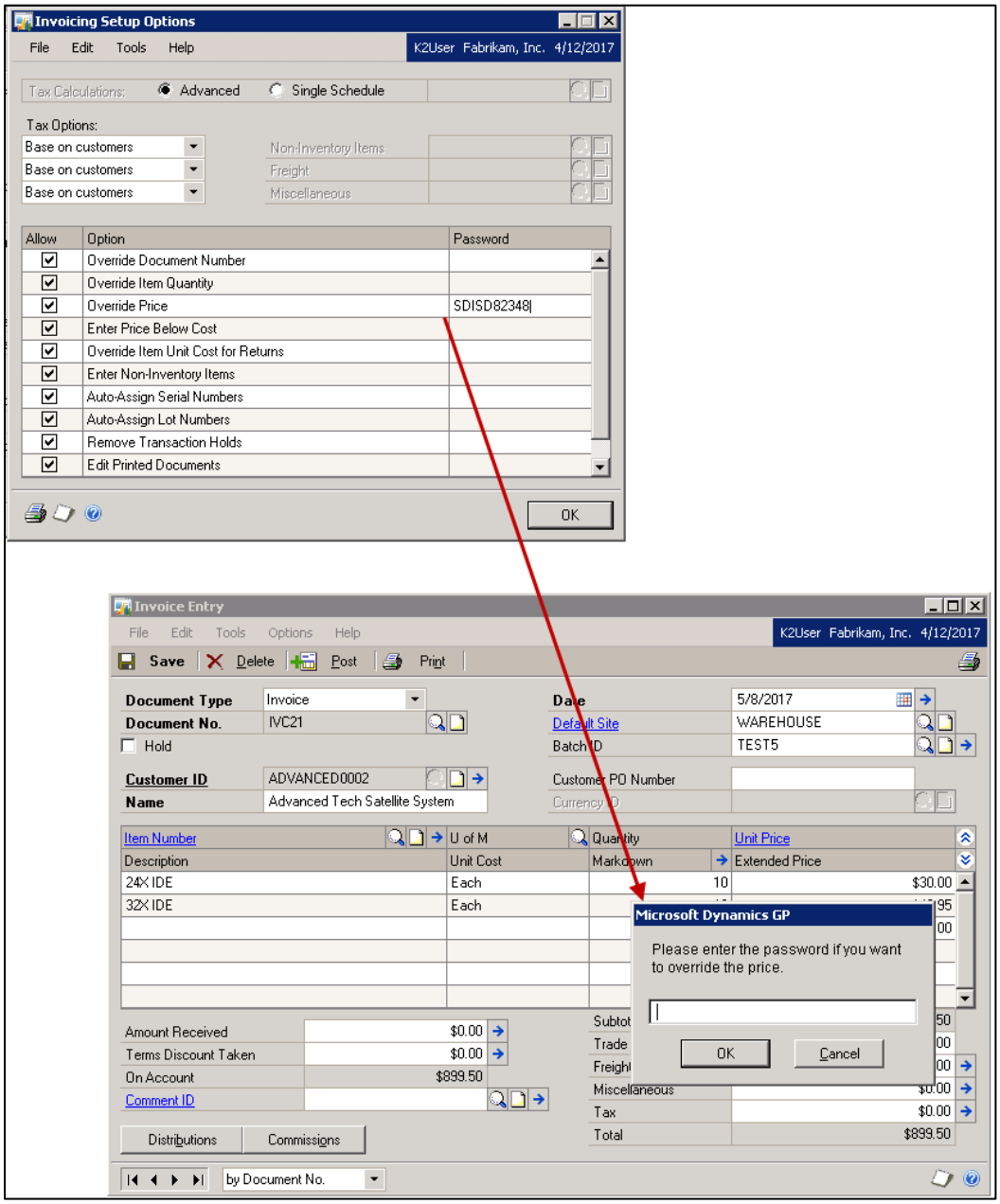


Figure 58 - Implementing Password Controls over Selling Prices

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Approval of Customer Credit Limits

One area that can present an internal control challenge – particularly in small businesses – is customers accumulating large amounts of debt that the creditor subsequently writes off. Of course, the primary control to prevent this is establishing credit limits that non-authorized users cannot override. One practical approach to implementing this control is using an automated workflow and approval process, such as those available in Microsoft Dynamics 365 and QuickBooks Online Advanced. You can also utilize Robotic Process Automation tools such as Microsoft Power Automate to create custom workflow procedures that integrate with the accounting application.

Consider the case of a customer requesting an increase in their credit limit. Perhaps the organization has a written policy that indicates the Chief Financial Officer must approve these requests. Using Dynamics 365 automated approval workflows, you can mandate these approvals in the application.

You can create a new customer-related workflow by clicking **Customers** from the Ribbon's **Home tab**. Then click **Create Approval Workflow** in the **Actions** tab on the Ribbon. Enter the requested data, including the criteria that the workflow starts whenever a team member increases the customer's credit limit, as shown in **Figure 59**.

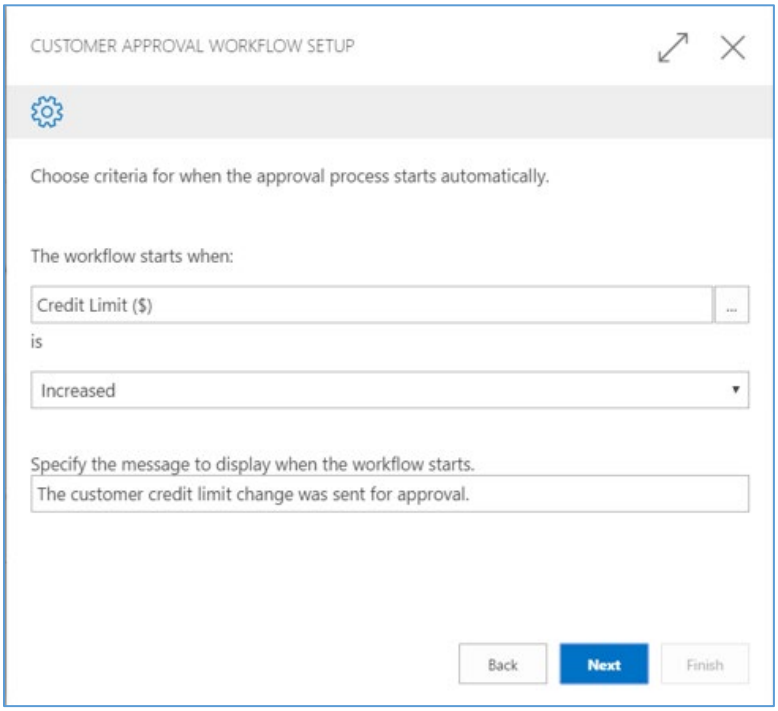


Figure 59 – Creating a Customer Approval Workflow for Increased Credit Limits

Upon clicking through the remainder of the screens and choosing **Finish**, the workflow will be in place, mandating approval from a designated manager before increasing a customer's credit limit. Of course, these approvals require managers who have the right to approve these requests

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

to check routinely to see if any outstanding requests exist. Further, managers can delegate authorizations to other team members when they may be away from the office for extended periods, such as when on vacation.

Revenue Control Procedure Checklist

For those more comfortable with a checklist approach to internal controls, the checklist presented in **Table 4** provides an alternate means of assessing the internal control structure's adequacy.

Revenue Control Procedure Checklist	*Yes*	*No*	*N/A*	*Comment*
1. Is customer credit approved by the owner or a designated credit manager?				
2. Are credit files maintained on a current basis?				
3. Are commission rates set or approved by the owner?				
4. Are sales orders or work orders approved by the owner or a responsible employee for price, terms, and credit?				
5. Are prenumbered documents used for sales orders, work orders, shipping documents, sales invoices, and credit memos? Are all prenumbered documents accounted for?				
6. Are shipping documents prepared for all shipments and based only on approved sales orders and matched with sales invoices? Are these documents processed promptly?				
7. Are all sales invoices prepared accurately and promptly for all sales orders?				

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Revenue Control Procedure Checklist	*Yes*	*No*	*N/A*	*Comment*
8. Are all credit memos controlled, approved by a designated party, and recorded promptly?				
9. Are monthly customer statements prepared, reviewed by the owner, and mailed by someone other than the preparer?				
10. Is an accounts receivable aging prepared each month and reviewed by the owner or credit manager? Are any write-offs or other adjustments initiated by the owner or credit manager?				
11. Is there an appropriate cutoff of sales at the end of the accounting period, and are all accounts receivable subsidiary records balanced to the general ledger?				
12. Is there appropriate segregation of mail opening responsibilities? Immediately upon receipt, are all checks restrictively endorsed?				
13. Are cash receipts recorded and posted promptly and deposited daily?				
14. Are cash discounts taken by customers checked for compliance with management's policies?				

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Revenue Control Procedure Checklist	*Yes*	*No*	*N/A*	*Comment*
15. Are cash sales adequately controlled through the use of cash registers and prenumbered cash receipts?				
16. Are cash registers appropriately controlled, and are register receipts appropriately reconciled to register tapes?				

Table 4 - Revenue Control Procedure Checklist

Purchasing Payable and Payroll Controls

Controlling purchasing, payables, and payroll offers unique challenges to establishing and maintaining an effective internal control structure in a small business. Not the least of these challenges is that most occupational fraud occurs in these areas, as described previously in this material. Accordingly, exercise great care when designing and evaluating internal controls over purchasing, payables, and payroll.

Like all other transactions, purchasing, payable, and payroll transactions should carry management's general and specific authorization. The purchasing function interacts with inventory control procedures and can materially affect the financial statements. Additionally, because of the sensitive nature of the information related to payroll, exercise great care when establishing procedures over these areas of the accounting system.

Application Control Procedures for Purchasing/Payables

Approval Levels

Some applications also allow users to specify options related to authorizing specific transactions. For example, supervisors must expressly authorize purchase orders over $500. To illustrate, consider the Microsoft Dynamics GP example depicted in **Figure 60**. In this example, LESSONUSER 1 can approve purchase orders up to $500; Dynamics GP automatically escalates purchase orders over $500 to LESSONUSER2.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

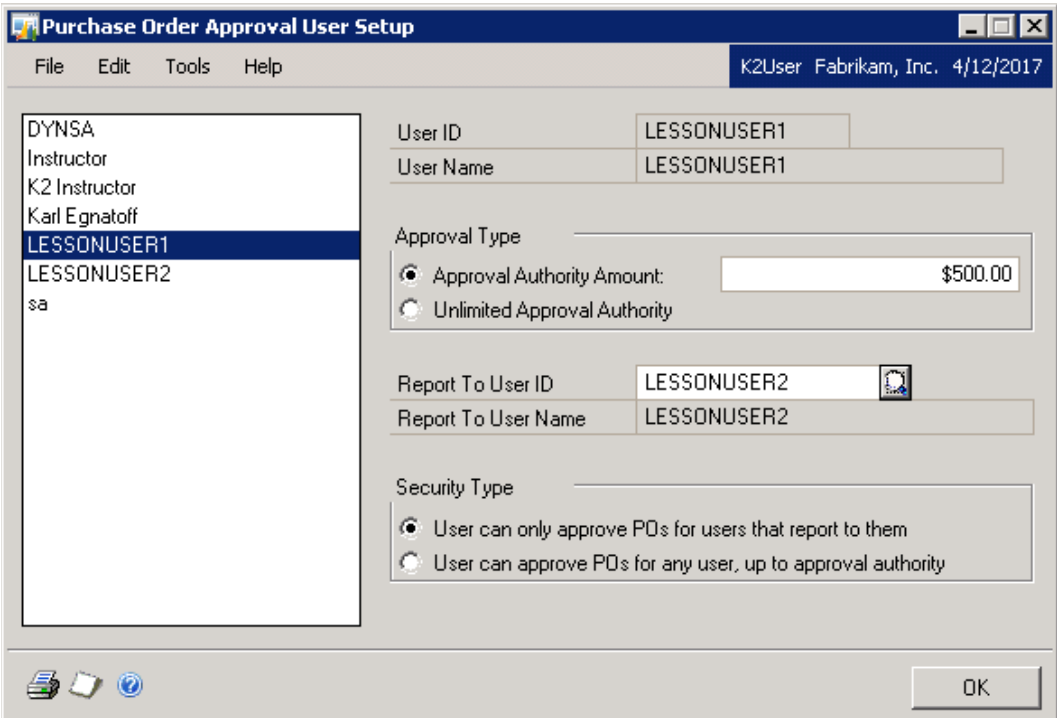


Figure 60 - Configuring Dynamics GP for Purchase Order Approval

You could configure Sage 100 to force entering a password if the vendor's invoice exceeded the amount on the purchase order, as shown in **Figure 61**.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

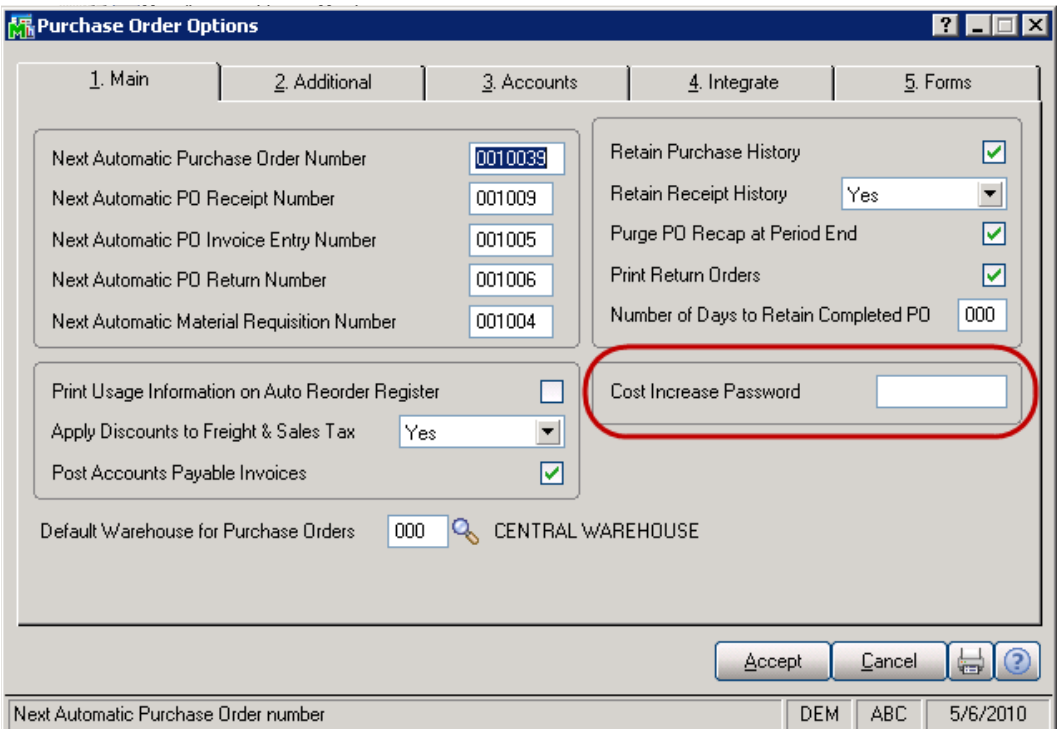


Figure 61 - Cost Increase Password in Sage 100

Again, by utilizing such options, business owners and managers can increase internal control over authorization.

You can control approval levels through workflow tools, such as those incorporated into SAP Business One. For example, in **Figure 62**, a workflow message was automatically sent to a manager requesting a purchase order approval. The application sent the message because the purchase order's originator did not have sufficient approval authority based on the purchase order amount. You can establish workflow rules such as this in many applications today to control the flow of a document pending approval by management – yet another example of using embedded tools in accounting software applications as effective internal control procedures.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

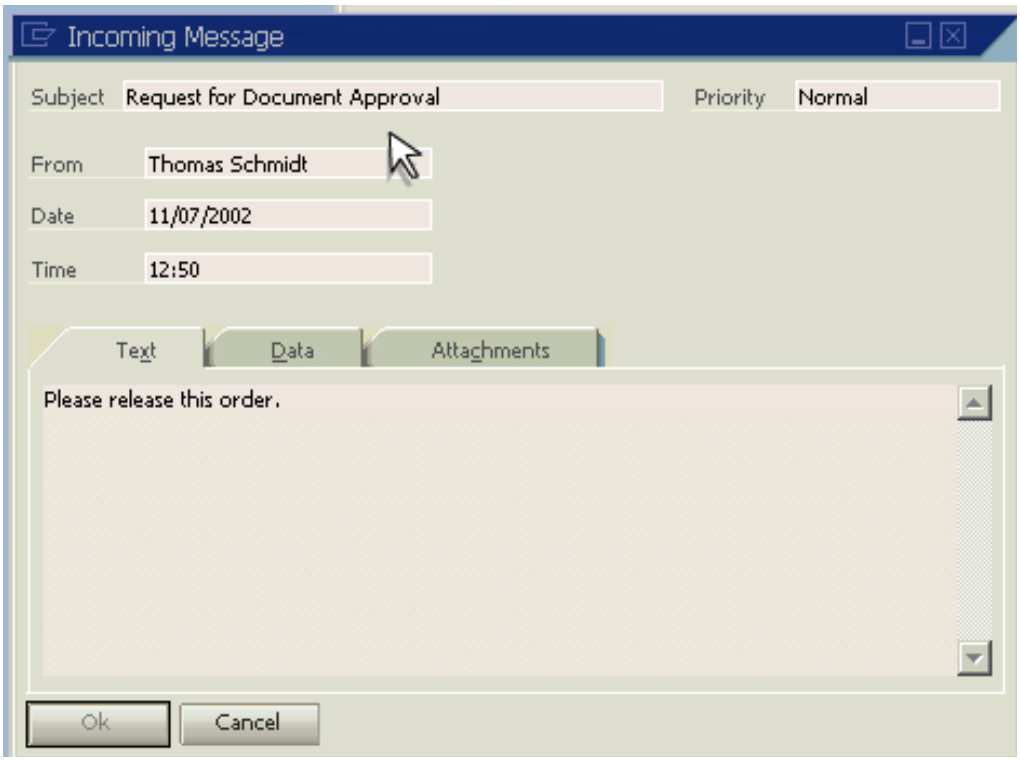


Figure 62 - Workflow Message in SAP Business One

Preventing and Detecting Duplicated Transactions

As with the revenue cycle, the focus on developing application controls over the expenditure cycle should ensure the completeness and accuracy of transactions. For example, edits on transaction number fields can reduce the risk of duplicate entries of transactions such as purchase orders. Again, in QuickBooks, this is a function of establishing a preference. We see this in the screens presented in **Figure 63** and **Figure 64.**

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

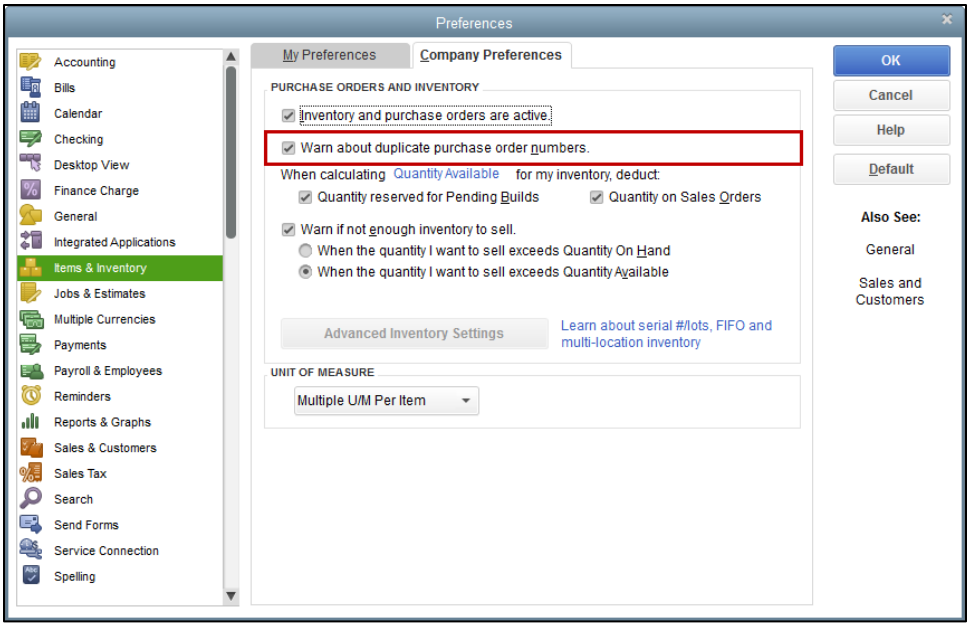


Figure 63 - Editing for Duplicate Purchase Order and Bill Numbers in QuickBooks

To prevent the duplicate entry of a vendor invoice, you can activate a similar warning control in QuickBooks.

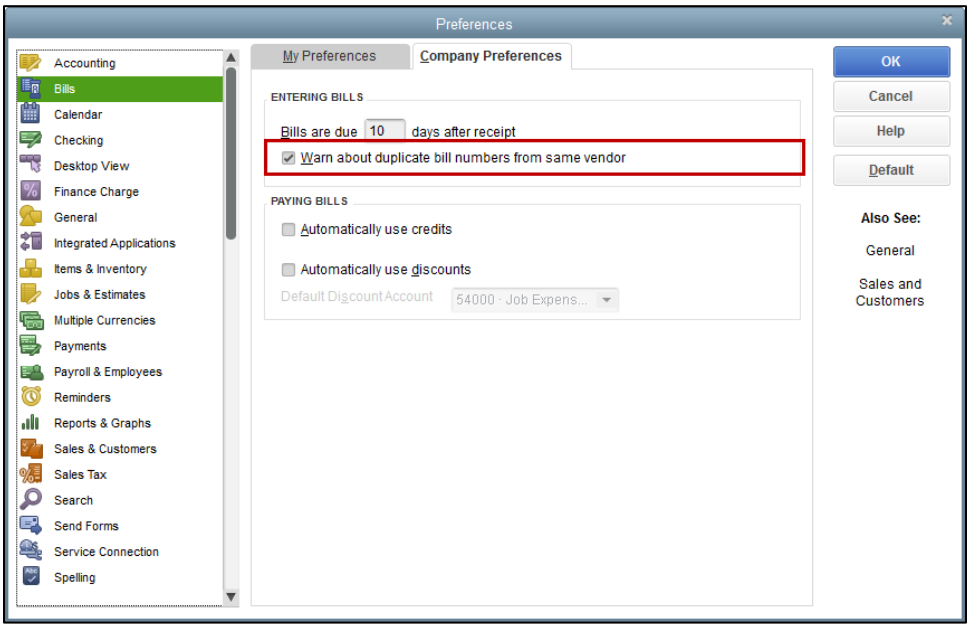


Figure 64 - Editing for Duplicate Invoice Numbers in QuickBooks

In both the examples previously presented, QuickBooks provides “soft” warnings; this contrasts with Sage 50, which gives a “hard” error when a user attempts to enter the same vendor invoice number multiple times. **Figure 65** presents the Sage 50 error screen.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

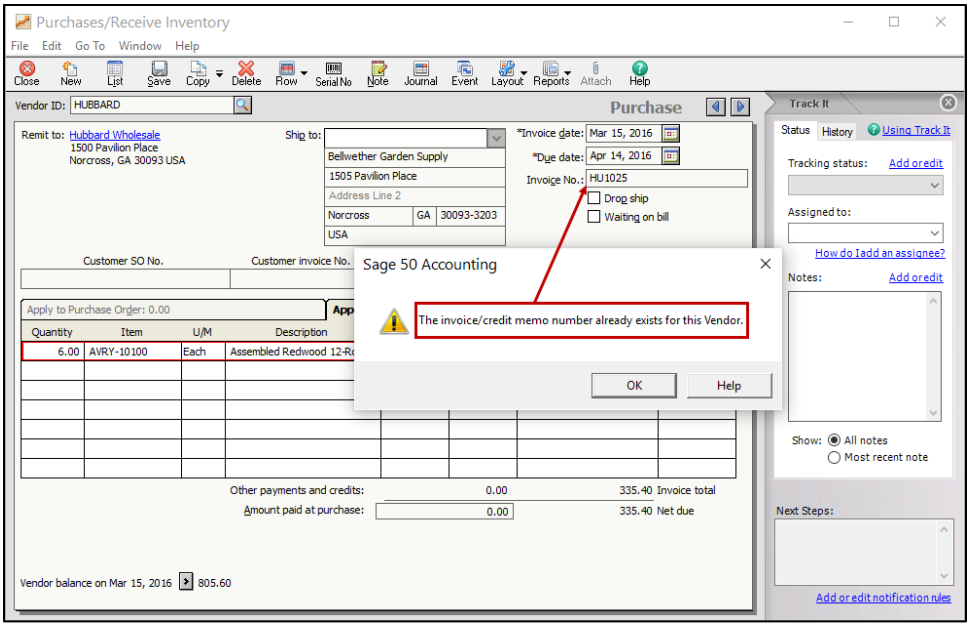


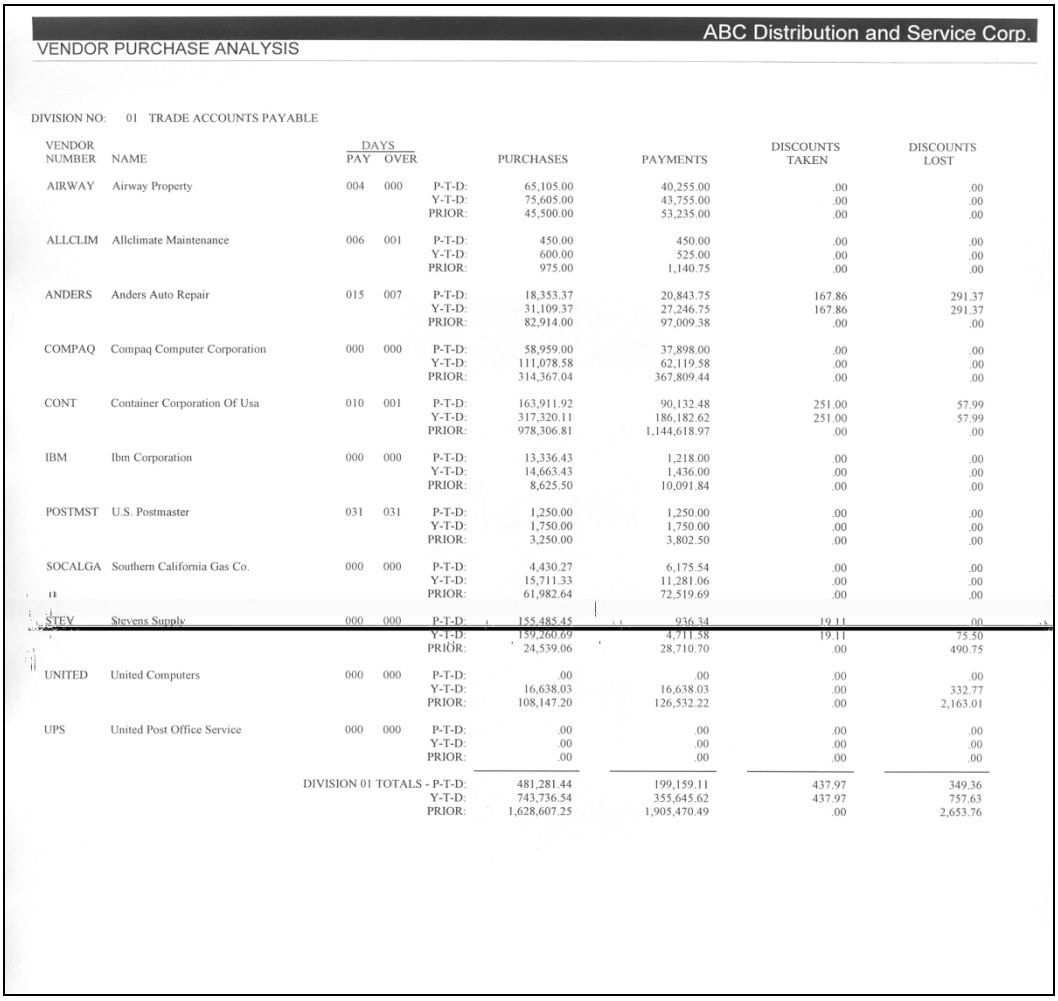
Figure 65 - Editing for Duplicate Transaction Number in Sage 50

As you can see, it is not possible in Sage 50 to enter the same invoice number for the same vendor twice; therefore, this reduces the likelihood that a company pays an invoice more than once.

Using Reports for Controlling Payables

Accounts payable reports can also provide critical controls in the expenditure cycle. For instance, the vendor analysis report produced by Sage 100 and shown in **Figure 66** offers small business owners and managers key details regarding purchases, payments, and discounts for the current period, year-to-date, and prior year, sorted by vendor. This report could help identify undesirable purchasing or payment patterns.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.



ABC Distribution and Service Corp.

VENDOR PURCHASE ANALYSIS

DIVISION NO: 01 TRADE ACCOUNTS PAYABLE

VENDOR NUMBER	NAME	DAYS PAY	DAYS OVER		PURCHASES	PAYMENTS	DISCOUNTS TAKEN	DISCOUNTS LOST
AIRWAY	Airway Property	004	000	P-T-D:	65,105.00	40,255.00	.00	.00
				Y-T-D:	75,605.00	43,755.00	.00	.00
				PRIOR:	45,500.00	53,235.00	.00	.00
ALLCLIM	Allclimate Maintenance	006	001	P-T-D:	450.00	450.00	.00	.00
				Y-T-D:	600.00	525.00	.00	.00
				PRIOR:	975.00	1,140.75	.00	.00
ANDERS	Anders Auto Repair	015	007	P-T-D:	18,353.37	20,843.75	167.86	291.37
				Y-T-D:	31,109.37	27,246.75	167.86	291.37
				PRIOR:	82,914.00	97,009.38	.00	.00
COMPAQ	Compaq Computer Corporation	000	000	P-T-D:	58,959.00	37,898.00	.00	.00
				Y-T-D:	111,078.58	62,119.58	.00	.00
				PRIOR:	314,367.04	367,809.44	.00	.00
CONT	Container Corporation Of Usa	010	001	P-T-D:	163,911.92	90,132.48	251.00	57.99
				Y-T-D:	317,320.11	186,182.62	251.00	57.99
				PRIOR:	978,306.81	1,144,618.97	.00	.00
IBM	Ibm Corporation	000	000	P-T-D:	13,336.43	1,218.00	.00	.00
				Y-T-D:	14,663.43	1,436.00	.00	.00
				PRIOR:	8,625.50	10,091.84	.00	.00
POSTMST	U.S. Postmaster	031	031	P-T-D:	1,250.00	1,250.00	.00	.00
				Y-T-D:	1,750.00	1,750.00	.00	.00
				PRIOR:	3,250.00	3,802.50	.00	.00
SOCALGA	Southern California Gas Co.	000	000	P-T-D:	4,430.27	6,175.54	.00	.00
				Y-T-D:	15,711.33	11,281.06	.00	.00
				PRIOR:	61,982.64	72,519.69	.00	.00
STEV	Stevens Supply	000	000	P-T-D:	155,485.45	936.34	19.11	.00
				Y-T-D:	159,260.69	4,711.58	19.11	75.50
				PRIOR:	24,539.06	28,710.70	.00	490.75
UNITED	United Computers	000	000	P-T-D:	.00	.00	.00	.00
				Y-T-D:	16,638.03	16,638.03	.00	332.77
				PRIOR:	108,147.20	126,532.22	.00	2,163.01
UPS	United Post Office Service	000	000	P-T-D:	.00	.00	.00	.00
				Y-T-D:	.00	.00	.00	.00
				PRIOR:	.00	.00	.00	.00
	DIVISION 01 TOTALS			P-T-D:	481,281.44	199,159.11	437.97	349.36
				Y-T-D:	743,736.54	355,645.62	437.97	757.63
				PRIOR:	1,628,607.25	1,905,470.49	.00	2,653.76

Figure 66 – Sage 100 Vendor Purchase Analysis Report



An interesting option for enhancing internal control over employee expense reports is **Zoho Expense** (www.zoho.com/expense), Zoho's online expense reporting service. With this service, small businesses can link credit card accounts to employee expense reports and embed workflow rules into employee expense reporting processes. Additionally, to improve efficiency and reduce the likelihood of data entry errors, users can import expense information in Zoho Expense into some popular small business accounting software tools, including Zoho Books and QuickBooks Online.

Control Procedures for Payroll

Many small businesses find payroll transactions challenging to control, given the data's sensitivity, the complex legal requirements surrounding payroll taxes and withholdings, and the transaction frequency, volume, and complexity involved. As a result, many small businesses

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

benefit greatly by outsourcing their payroll compliance functions to reputable third-party firms, including their local CPA firm. For those small businesses that keep payroll in-house, internal control begins by automating as much of the process as possible. This process typically requires subscribing to a payroll tax "service," "subscription," or "tax table" offered by the company's accounting software publisher.

Using Reports, Dashboards, and Alerts to Ensure Timely Processing and Notifications

For example, QuickBooks provides a "dashboard" report – the **Payroll Center**, pictured in **Figure 67** – to alert users to all upcoming payroll events, including due dates on tax returns. Assuming the payroll feature is set up correctly in the company data file, any user accessing the Payroll Center can readily see all payroll items' status.

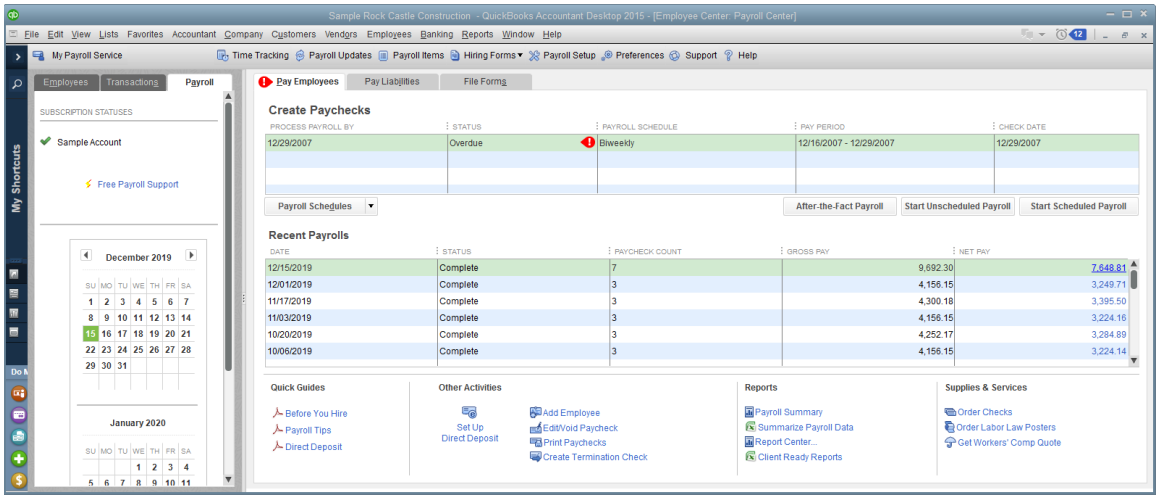


Figure 67 - Payroll Center in QuickBooks

Likewise, in QuickBooks, the **Employee Center** provides easy access to an overview of all payroll transactions, including Liability Adjustments, as shown in **Figure 68**. Users can monitor all payroll transactions, including potentially fraudulent liability adjustments from this center.

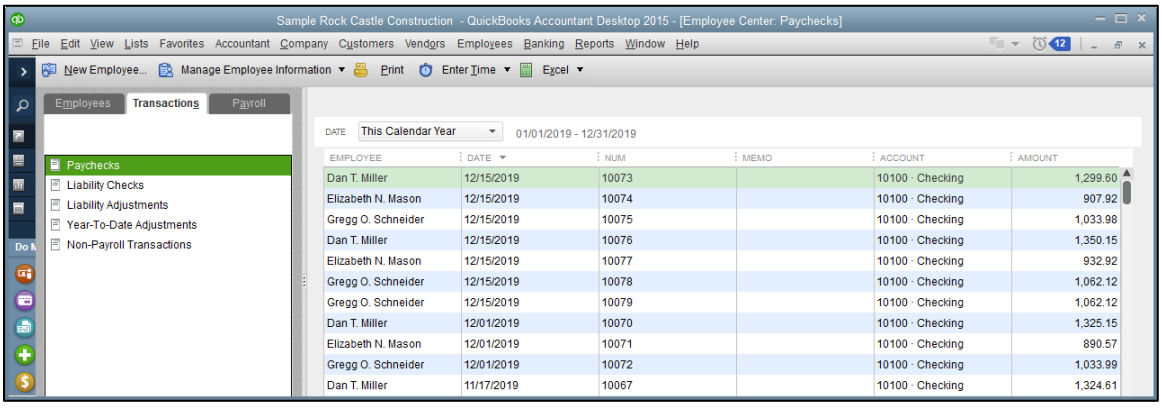


Figure 68 - Employee Center in QuickBooks

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Sage 50 offers an automated reporting mechanism that "pushes" critical data to those who need to know. For example, the **Company Alerts** feature depicted in **Figure 69** can send automatic email or text message alerts to appropriate recipients when event triggers – such as overtime – are met. By "pushing" this data, rather than relying on users to "pull" it from reports, notifications typically occur more quickly.

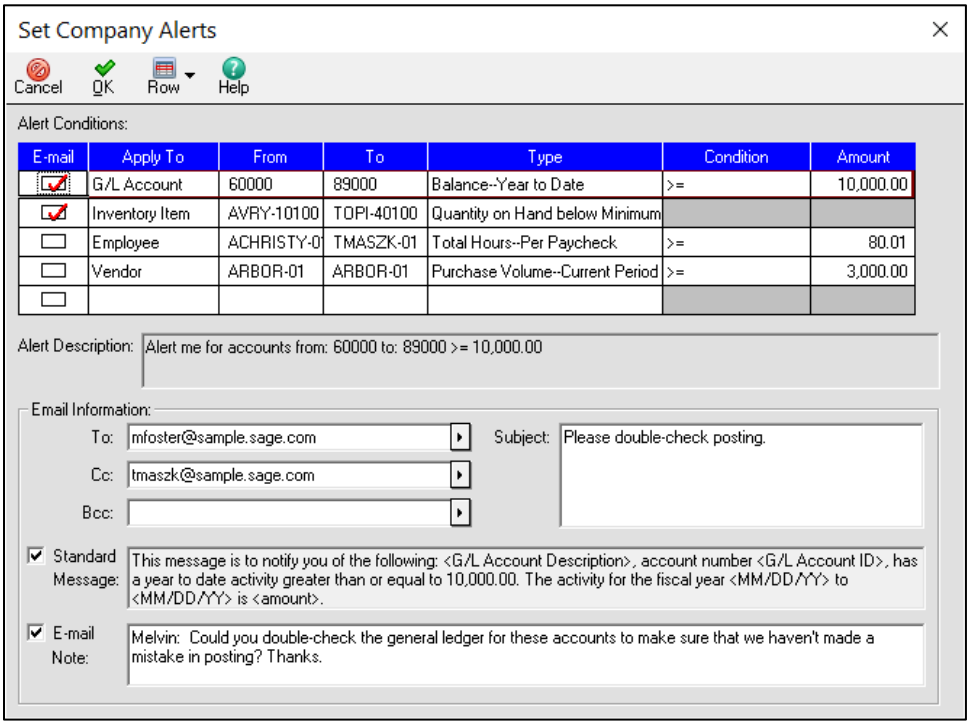


Figure 69 – Sage 50 Company Alerts Feature Established to Send Notifications of Overtime

Purchasing, Payables, and Payroll Control Procedure Checklist

Table 5 provides an alternate means of assessing the internal control structure's adequacy for those more comfortable with a checklist approach to internal controls.

Purchasing, Payables, and Payroll Control Procedure Checklist	*Yes*	*No*	*N/A*	*Comments*
1. Does a responsible party other than the bookkeeper purchase routinely used goods and services? Are non-routine items subject to approval by the owner or other designated person?				

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Purchasing, Payables, and Payroll Control Procedure Checklist	*Yes*	*No*	*N/A*	*Comments*
2. Are escalating levels of approval required before executing a purchasing transaction?				
3. Are prenumbered purchase orders used, and are they matched to receiving reports and invoices before payment of invoices?				
4. Is a record maintained of all open purchase orders? Are all prenumbered forms accounted for?				
5. Are prenumbered receiving reports used to control the receipt of inventory? Are these forms prenumbered and controlled?				
6. Are vendor invoices checked for accuracy before payment, and are invoices with available discounts processed expeditiously? Are paid invoices permanently altered to prevent duplicate payment?				
7. Are employee expense accounts used when appropriate? If so, are expenses submitted promptly, adequately supported, and approved before payment?				
8. Are all employees hired by the owner or other designated party?				

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Purchasing, Payables, and Payroll Control Procedure Checklist	*Yes*	*No*	*N/A*	*Comments*
9. Are individual personnel files detailing critical data for each employee maintained and updated as appropriate?				
10. Are wages, salaries, commissions, and other items approved by the owner or other designated party?				
11. Are proper authorizations obtained for all payroll deductions? Are all payroll taxes and other deductions remitted on a timely basis to appropriate parties?				
12. Is there adequate control over the time cards or other records for employees paid hourly?				
13. Does the owner or other designated party approve, sign, and distribute payroll checks and compare the payroll register to deposits into the payroll checking account? Does the owner or other designated party maintain control over unclaimed payroll checks?				
14. Are all disbursements (except petty cash) made by check, and are all checks pre-numbered and accounted for? Are unused checks adequately safeguarded? Are all voided checks retained and mutilated?				

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Purchasing, Payables, and Payroll Control Procedure Checklist	*Yes*	*No*	*N/A*	*Comments*
15. Are all checks signed by the owner or other designated party/parties?				
16. Are supporting documents presented with checks and reviewed by the person to sign the check before signing the check?				
17. Are checks payable to "cash" prohibited/restricted?				
18. Are signed checks mailed by an independent party?				
19. Are bank statements and paid checks received and reviewed by the owner or other designated party other than the bookkeeper?				
20. Are bank reconciliations prepared for all accounts by someone other than the cashier or persons authorized to sign checks?				
21. Are disbursements from petty cash limited and supported by appropriate documentation and approval?				

Table 5 - Purchasing, Payables, and Payroll Control Procedure Checklist

Inventory, Production, and Fixed Asset Control Procedures

Transactions involving inventory, production, and fixed assets should be accurately recorded, accumulated, and classified in detail and control accounts to (1) permit preparing statements that comply with GAAP or other applicable criteria and (2) maintain accountability for assets.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

A thorough understanding of the policies, procedures, and systems involved is necessary when evaluating the objectives and risks relative to inventory, production, and fixed assets. The practitioner can consider items like those listed below to obtain this understanding.

- The types of documents used to maintain accountability over inventory
- The nature of the inventory and fixed asset investment (for example, are the items readily salable?)
- The frequency of inventory reconciliations and comparisons
- The responsibilities of personnel involved with inventory and fixed asset accounting

Application Control Procedures for Inventory, Production, and Fixed Assets

One general issue affecting the production cycle is that many small business accounting software packages are not well-equipped to handle inventory applications other than relatively simple tasks. For instance, many small business accounting software applications do not track inventory quantities by warehouse. Nonetheless, taking advantage of the embedded internal control features over inventory, production, and fixed assets and supplementing these controls with robust administrative and alternative control procedures can lead to a very effective control structure.

Using Automatic Reorder Functions to Optimize Stocking Levels

Prerecorded data is also helpful in the purchasing function. To illustrate how prerecorded data can improve internal controls, users can specify a reorder point and desired minimum quantity on hand in Sage 100, as shown in **Figure 70**.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

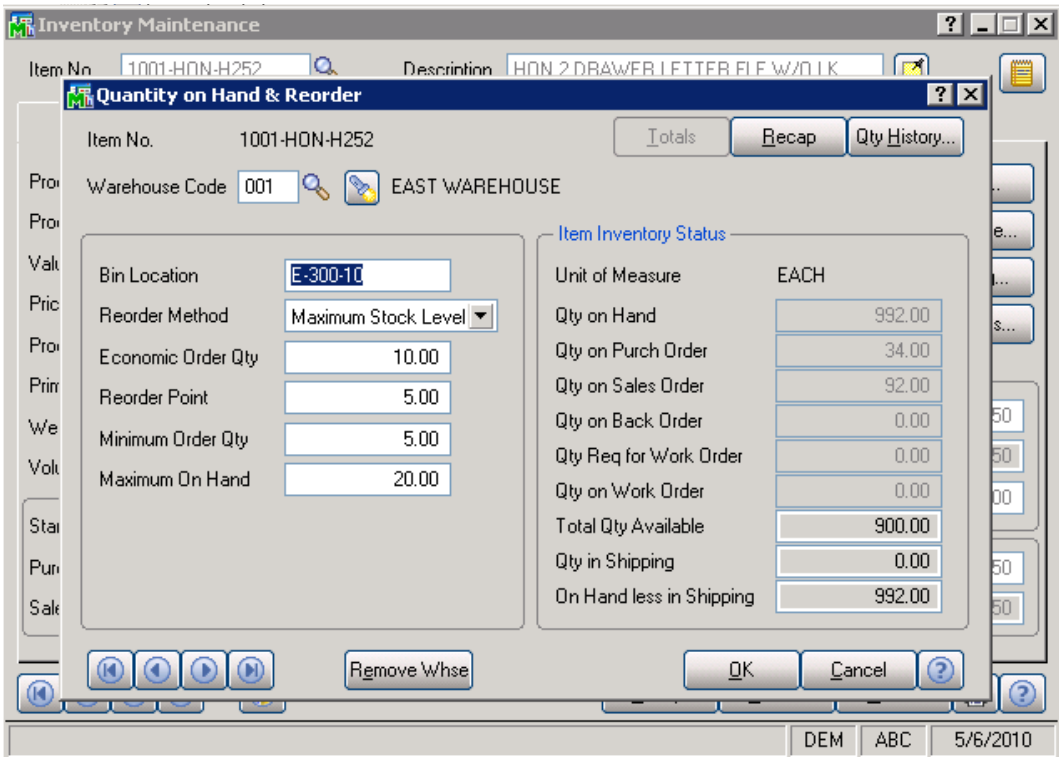


Figure 70 - Prerecorded Data in Sage 100 for Reorder Point and Minimum Quantity on Hand

Using the Automatic Reorder Selection process pictured in **Figure 71**, team members can automatically generate purchase orders for items where the quantity on hand is below the reorder point or minimum amounts specified. Using this function, business owners and managers can help ensure that inventory stocking levels remain at authorized quantities.

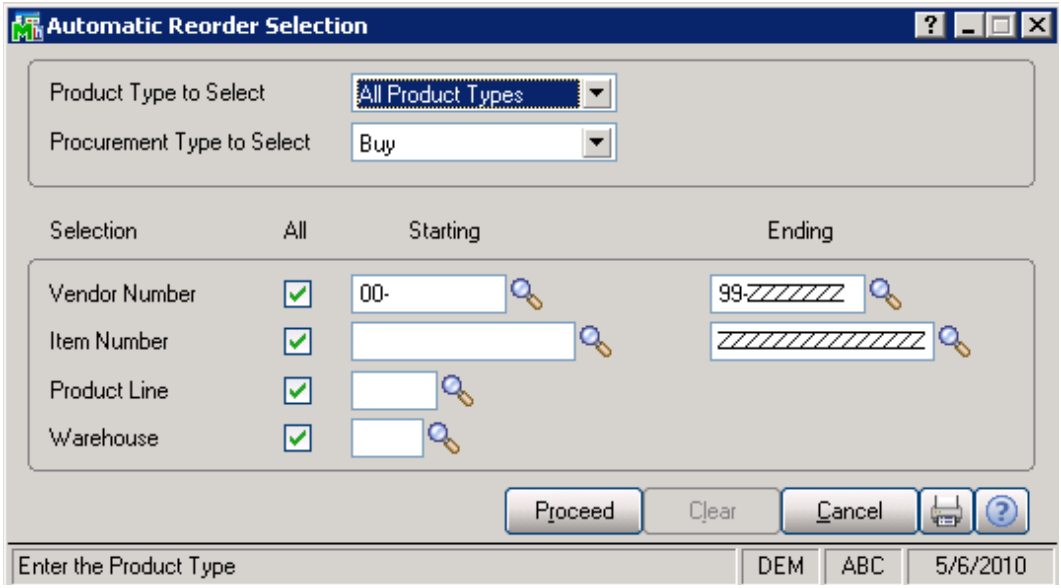


Figure 71 - Automatic Reorder of Inventory in Sage 100

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Conducting Physical Inventory Counts

One standard control procedure most small businesses utilize with inventory is a physical count of the inventory on hand. Team members should conduct this count periodically, and adjustments should be entered, as necessary, into the perpetual records. Again, virtually all packages support this function; the example in **Figure 72** presents a physical inventory list from Sage 50 software.

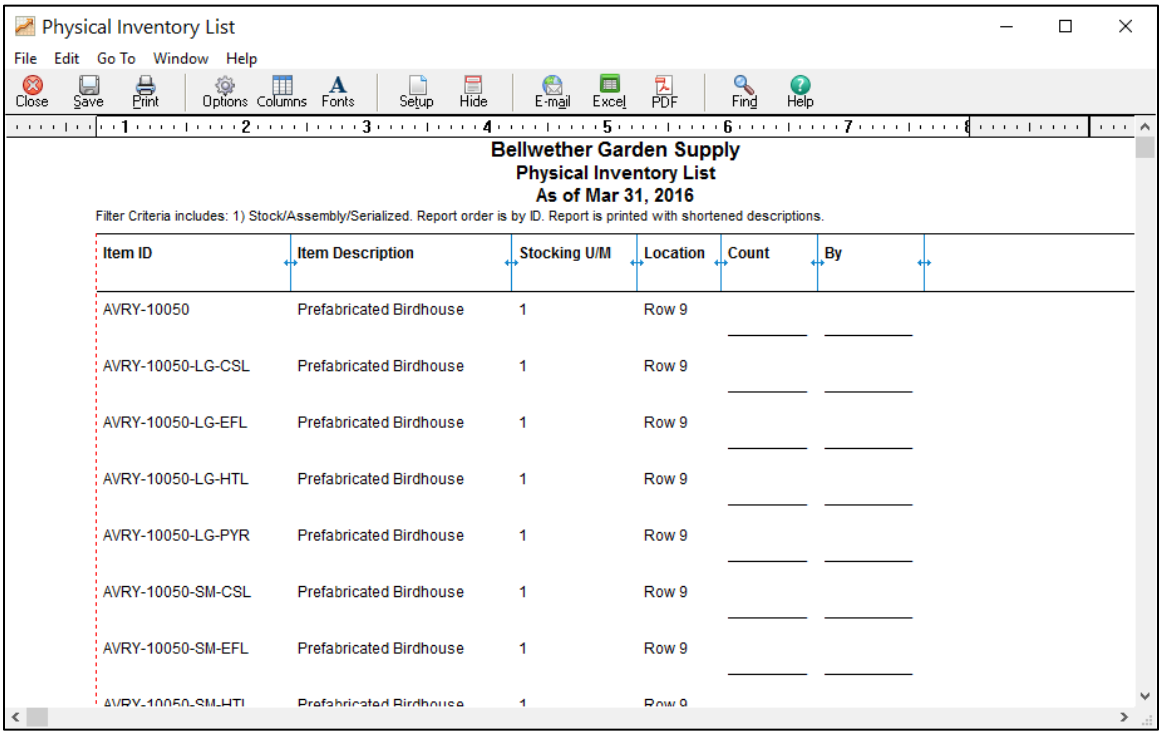


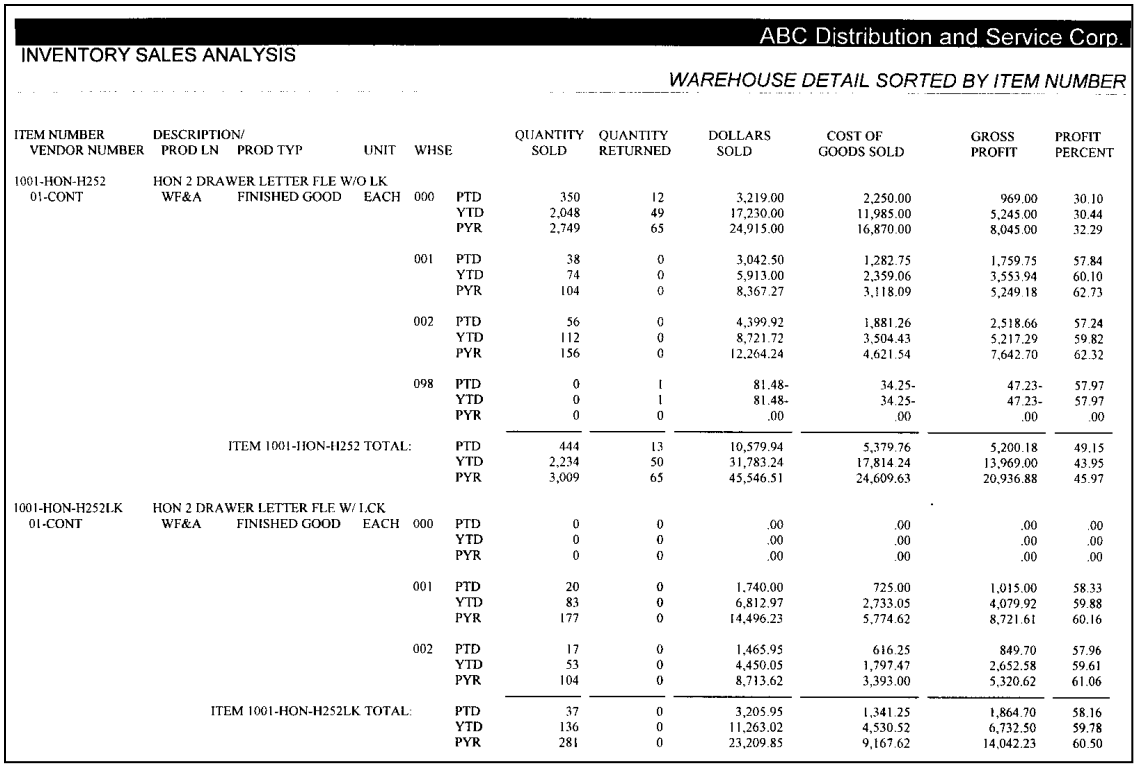
Figure 72 - Physical Inventory Worksheet in Sage 50 Accounting Software

Upon completing the physical count, adjustments are often necessary to correct the periodic records to correspond to the physical count. Organizations should consider which employees can access the inventory adjustment screens; otherwise, an employee could easily steal inventory and cover the theft by adjusting the accounting records.

Reports as Inventory Controls

Most accounting applications provide reports that can be useful in inventory control. For example, reports showing profitability by item and turnover by item help determine that items generate desired profitability. The following two – Inventory Sales Analysis (**Figure 73**) and Inventory Turnover Report (**Figure 74)** – are excerpted from Sage 100.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.



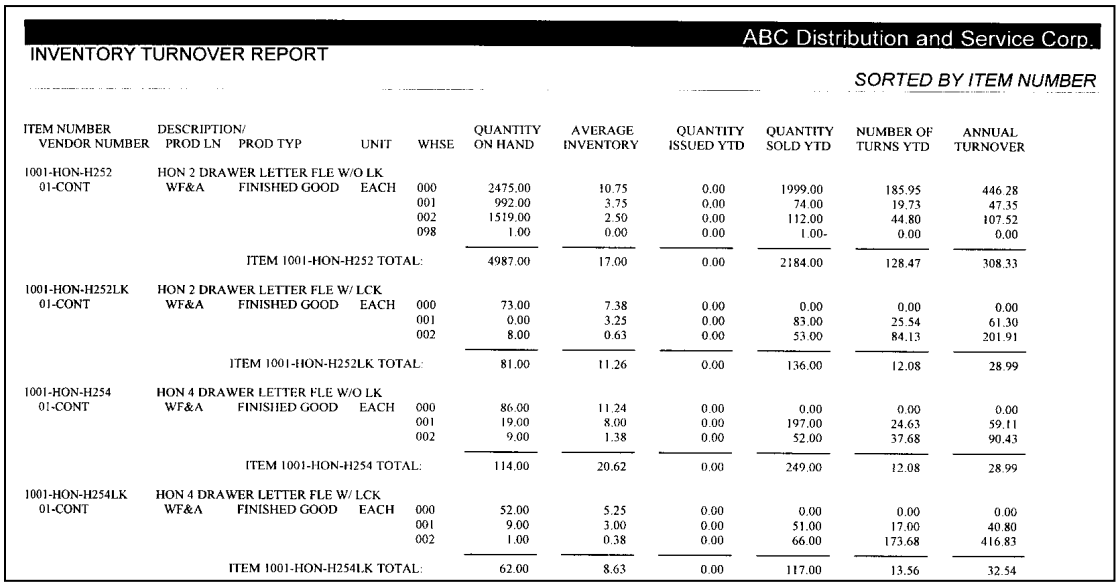
ABC Distribution and Service Corp.

INVENTORY SALES ANALYSIS

WAREHOUSE DETAIL SORTED BY ITEM NUMBER

ITEM NUMBER / VENDOR NUMBER	DESCRIPTION/ PROD LN	PROD TYP	UNIT	WHSE		QUANTITY SOLD	QUANTITY RETURNED	DOLLARS SOLD	COST OF GOODS SOLD	GROSS PROFIT	PROFIT PERCENT
1001-HON-H252	HON 2 DRAWER LETTER FLE W/O LK										
01-CONT	WF&A	FINISHED GOOD	EACH	000	PTD	350	12	3,219.00	2,250.00	969.00	30.10
					YTD	2,048	49	17,230.00	11,985.00	5,245.00	30.44
					PYR	2,749	65	24,915.00	16,870.00	8,045.00	32.29
				001	PTD	38	0	3,042.50	1,282.75	1,759.75	57.84
					YTD	74	0	5,913.00	2,359.06	3,553.94	60.10
					PYR	104	0	8,367.27	3,118.09	5,249.18	62.73
				002	PTD	56	0	4,399.92	1,881.26	2,518.66	57.24
					YTD	112	0	8,721.72	3,504.43	5,217.29	59.82
					PYR	156	0	12,264.24	4,621.54	7,642.70	62.32
				098	PTD	0	1	81.48-	34.25-	47.23-	57.97
					YTD	0	1	81.48-	34.25-	47.23-	57.97
					PYR	0	0	.00	.00	.00	.00
	ITEM 1001-HON-H252 TOTAL:				PTD	444	13	10,579.94	5,379.76	5,200.18	49.15
					YTD	2,234	50	31,783.24	17,814.24	13,969.00	43.95
					PYR	3,009	65	45,546.51	24,609.63	20,936.88	45.97
1001-HON-H252LK	HON 2 DRAWER LETTER FLE W/ LCK										
01-CONT	WF&A	FINISHED GOOD	EACH	000	PTD	0	0	.00	.00	.00	.00
					YTD	0	0	.00	.00	.00	.00
					PYR	0	0	.00	.00	.00	.00
				001	PTD	20	0	1,740.00	725.00	1,015.00	58.33
					YTD	83	0	6,812.97	2,733.05	4,079.92	59.88
					PYR	177	0	14,496.23	5,774.62	8,721.61	60.16
				002	PTD	17	0	1,465.95	616.25	849.70	57.96
					YTD	53	0	4,450.05	1,797.47	2,652.58	59.61
					PYR	104	0	8,713.62	3,393.00	5,320.62	61.06
	ITEM 1001-HON-H252LK TOTAL:				PTD	37	0	3,205.95	1,341.25	1,864.70	58.16
					YTD	136	0	11,263.02	4,530.52	6,732.50	59.78
					PYR	281	0	23,209.85	9,167.62	14,042.23	60.50

Figure 73 - Inventory Sales Analysis Report in Sage 100



ABC Distribution and Service Corp.

INVENTORY TURNOVER REPORT

SORTED BY ITEM NUMBER

ITEM NUMBER / VENDOR NUMBER	DESCRIPTION/ PROD LN	PROD TYP	UNIT	WHSE	QUANTITY ON HAND	AVERAGE INVENTORY	QUANTITY ISSUED YTD	QUANTITY SOLD YTD	NUMBER OF TURNS YTD	ANNUAL TURNOVER
1001-HON-H252	HON 2 DRAWER LETTER FLE W/O LK									
01-CONT	WF&A	FINISHED GOOD	EACH	000	2475.00	10.75	0.00	1999.00	185.95	446.28
				001	992.00	3.75	0.00	74.00	19.73	47.35
				002	1519.00	2.50	0.00	112.00	44.80	107.52
				098	1.00	0.00	0.00	1.00-	0.00	0.00
	ITEM 1001-HON-H252 TOTAL:				4987.00	17.00	0.00	2184.00	128.47	308.33
1001-HON-H252LK	HON 2 DRAWER LETTER FLE W/ LCK									
01-CONT	WF&A	FINISHED GOOD	EACH	000	73.00	7.38	0.00	0.00	0.00	0.00
				001	0.00	3.25	0.00	83.00	25.54	61.30
				002	8.00	0.63	0.00	53.00	84.13	201.91
	ITEM 1001-HON-H252LK TOTAL:				81.00	11.26	0.00	136.00	12.08	28.99
1001-HON-H254	HON 4 DRAWER LETTER FLE W/O LK									
01-CONT	WF&A	FINISHED GOOD	EACH	000	86.00	11.24	0.00	0.00	0.00	0.00
				001	19.00	8.00	0.00	197.00	24.63	59.11
				002	9.00	1.38	0.00	52.00	37.68	90.43
	ITEM 1001-HON-H254 TOTAL:				114.00	20.62	0.00	249.00	12.08	28.99
1001-HON-H254LK	HON 4 DRAWER LETTER FLE W/ LCK									
01-CONT	WF&A	FINISHED GOOD	EACH	000	52.00	5.25	0.00	0.00	0.00	0.00
				001	9.00	3.00	0.00	51.00	17.00	40.80
				002	1.00	0.38	0.00	66.00	173.68	416.83
	ITEM 1001-HON-H254LK TOTAL:				62.00	8.63	0.00	117.00	13.56	32.54

Figure 74 - Inventory Turnover Report in Sage 100

Reports depicting inventory carrying value relative to market value can provide insight into the potential need to record adjustments that reflect an item's lower of cost or market value. These same reports can also help identify risks associated with a concentration of investment by inventory item.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Inventory, Production, and Fixed Asset Control Procedure Checklist

For those more comfortable with a checklist approach to internal controls, the checklist presented in **Table 6** provides an alternate means of assessing the internal control structure's adequacy.

Inventory, Production, and Fixed Asset Control Procedure Checklist	***Yes***	***No***	***N/A***	***Comments***
1. Are inventory procedures and policies adequately documented and maintained?				
2. Are physical counts of all inventories made at least annually and compared to the underlying accounting records? Are discrepancies reconciled or adjusted?				
3. Are inventories adequately safeguarded from theft, spoilage, and other losses? Are inventories adequately insured?				
4. Do the accounting records provide for proper accumulation and classification of the costs of raw materials, direct labor, and overhead?				
5. Do the accounting records accumulate quantities or units of finished products sold and units of raw materials used in production in sufficient detail and with proper cutoff to provide adequate determination of cost of goods sold and cost of inventories?				
6. Is the cost accounting system reconciled to the general ledger?				

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Inventory, Production, and Fixed Asset Control Procedure Checklist	*Yes*	*No*	*N/A*	*Comments*
7. Are prenumbered requisitions required for releasing all materials from storerooms? Are all requisitions accounted for?				
8. Are all fixed asset additions, retirements, and dispositions approved by the owner or other designated party?				
9. Are detailed asset and depreciation records maintained and periodically compared to the general ledger?				
10. Are periodic physical inventories of fixed assets conducted?				
11. Are depreciable lives periodically reviewed for adequacy and reasonableness in relation to unanticipated use or obsolescence based on experience? Does the owner or other designated party understand and approve estimated lives?				

Table 6 - Inventory, Production, and Fixed Asset Control Procedure Checklist

Controls for Cash

The high risk associated with cash necessitates an additional discussion on mitigating the risk of losing cash through fraudulent disbursement schemes. Organizations of all sizes now use "positive pay" bank accounts to minimize the threat of check tampering fraud. Many accounting software/business management products incorporate functionality to interact with banks' positive pay services. The application will, natively or via an add-in, create the bank's positive pay file for analysis.

Banks offer positive pay accounts to enhance internal controls and reduce fraud losses. Positive pay accounts provide automated check matching, allowing banking customers to monitor checks

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

processed for payment against their accounts and reject unauthorized transactions before losses occur. With positive pay, a company transmits data such as check numbers and amounts to its bank when it issues checks. Subsequently, when checks appear for payment, the bank matches the company-provided details to those on the documents presented for payment. If all details match, the bank honors and pays the check. If inconsistencies exist, the bank provides exception notifications to the company to decide whether to honor the item. **Figure 75** presents a simplified example of the positive pay process. As you can see, if someone alters a check after its issuance or creates a bogus check drawn on the company's bank account, the bank notifies the company *before* it clears the account. Because of this early notification process, the company can reject the check before a loss occurs.

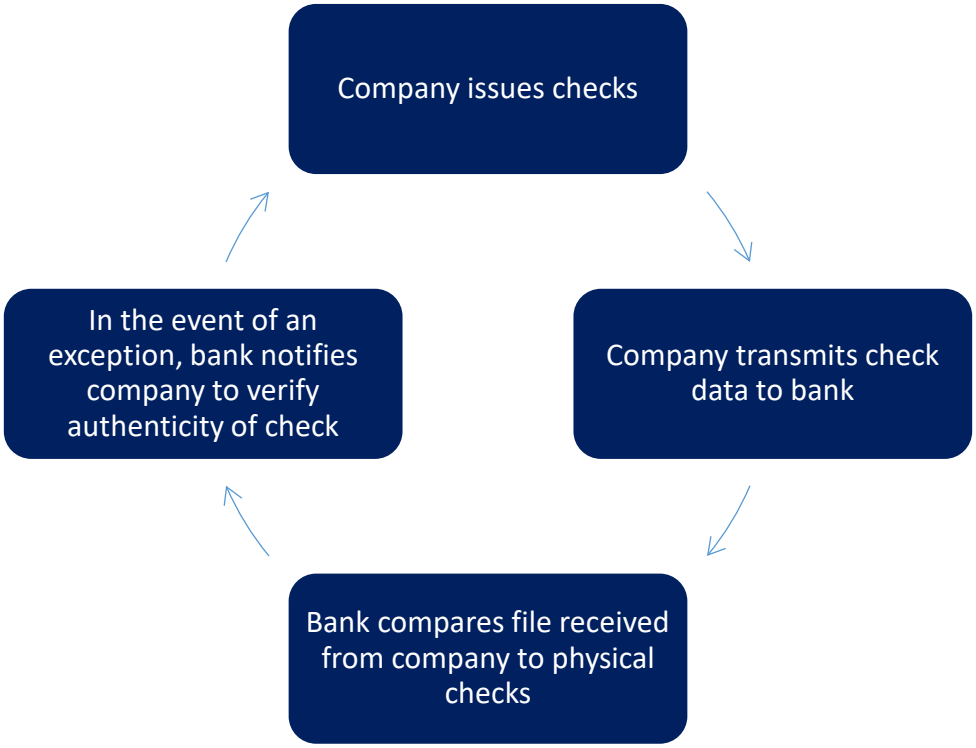


Figure 75 - Positive Pay Process

Other examples of cash controls include the following.

- **Payee Positive Pay** accounts, in which the bank verifies that the payee on a check presented for payment is the same as the payee on the check as supplied by the company
- **ACH Debit Authorization**, in which the company notifies the bank in advance of those organizations authorized to debit the company's bank account
- **ACH Debit Blocks**, in which the bank is explicitly instructed not to process any ACH debits against specific bank accounts
- **Post No Checks** bank accounts allow for deposits only; the bank rejects checks or debits presented for payment.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Segregation Of Duties

Appendix

A

The charts on the following pages depict the proper segregation of duties in organizations, where the number of team members and their education and training permit. We adapted this information from the second edition of the Handbook of Internal Accounting Controls by Wanda J. Wallace.

In many small businesses, proper segregation of duties will be impossible, as displayed in these charts. Nevertheless, the information in this appendix can be valuable in designing and implementing internal controls in small businesses.

Key points that become obvious upon studying the charts include those listed below.

- Within each departmental function, authorization, custody, and recordkeeping are identifiable.

- Someone independent of the preparer of a transactional document should review and approve the transaction.

- A team member who does not originate or approve transactions should execute overview, testing, and follow-up responsibilities.

The following tables describe the division of responsibilities associated with revenue and expenditures.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

AUTHORIZATION	CUSTODY	RECORDKEEPING
ORDER ENTRY	ORDER ENTRY	ORDER ENTRY
<u>Marketing & Sales</u> Accept orders based on the company's established procedures, including irregular sales Set price and terms of orders; review and approve sales orders <u>Treasury</u> Document approval of write-offs of bad debts and confirm the charge-offs two to three months later <u>Credit Department</u> Establish credit limits for new customers to be applied until a thorough credit check can be performed Formally approve all accounts for credit, based on company experience and independent credit check; retain a copy of approved sales orders; investigate and follow up on overdue and unusual accounts receivables, per aging schedules and exception reports	<u>Shipping</u> Prepare a prenumbered bill of lading based on approved sales order and prenumbered shipping form Review and approve shipping form; forward copies to sales and accounts receivable Ship goods to customers as instructed	<u>Accounts Receivable</u> Account for the sequences of prenumbered customer order forms to detect unbilled shipments Generate prenumbered invoices, matching them to approved customer orders and shipping documentation Review and approve billing package for distribution, checking prices, terms, extensions, and footings; accounting for sequence of sales invoices; comparing data on invoices to order entry forms and shipping documents Maintain subsidiary accounts receivable ledger; prepare an aging schedule of accounts receivable, forwarding a copy to the credit department; periodically prepare a report on write-offs and recoveries for approval by the Treasurer; maintain listing of write-offs for subsequent follow-up Mail monthly statements to customers

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

AUTHORIZATION	CUSTODY	RECORDKEEPING
		<u>General Ledger</u> Maintain the controls accounts; review exception reports based on reasonableness or limit checks of sales and credit granted as well as reports of credit balances Review and approve journal entries; reconcile subsidiary with general ledger; reconcile daily billings totals with total receivables postings; compare production and inventory records with shipping and billing documentation; match shipping advices from independent shippers to internal documentation; review open and unmatched files and unaccounted for documents

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

AUTHORIZATION	CUSTODY	RECORDKEEPING
ADJUSTMENTS TO SALES	ADJUSTMENTS TO SALES	ADJUSTMENTS TO SALES
<u>Marketing & Sales</u> Investigate customers' complaints; authorize adjustments to sales-related balances; issue prenumbered credit memo requests; initiate prenumbered forms for replacement goods Review and approve credit memo requests as well as new shipping instructions Approve any credit implications of new shipping instructions, retaining a copy of the approved documents	<u>Receiving</u> Prepare a receiving report of returned goods, including inspection of returned items Review and approve receiving report; forward copies to marketing and accounts receivable Forward goods to warehousing and storeroom <u>Shipping</u> Prepare bill of lading on approved shipping instructions and prenumbered shipping form; obtain receipts for any freight expenditures and forward copy to accounting Review and approve shipping form; forward copies to sales and accounts receivable Ship goods to customers as instructed; secure customer's signature on bill of lading	<u>Accounts Receivable</u> Account for the sequence of prenumbered credit memo requests; match them to receiving reports where applicable; generate prenumbered credit memos to customers Review and approve credit package for distribution, checking support, extensions, sequence, and agreement of credit memos to requests to receiving information Maintain the subsidiary accounts receivable ledger <u>General Ledger</u> Maintain the control accounts Review and approve journal entries; reconcile subsidiary with general ledger; reconcile daily credit requests to credit memos to total receivables postings
INVESTMENTS	INVESTMENTS	INVESTMENTS
<u>Investment/Treasurer's Department</u> Authorize purchases and sales of securities	<u>Treasurer's Department – Asset Control</u> Maintain dual control over securities under adequate safeguard conditions,	<u>General Ledger</u> Prepare necessary journal entries to reclassify and/or revalue recorded securities;

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

AUTHORIZATION	CUSTODY	RECORDKEEPING
Review and approve authorization	bonding individuals charged with control; ensure securities are held in name of company	reconcile brokers' statements to general ledger Review and approve journal entries; reconcile investment ledger to general ledger; review reconciliation of brokers' statements to general ledger <u>Investment Ledger</u> Maintain record of certificate numbers, descriptive details, cost, market value, and physical location of securities; receive investment advice and monthly statements and record activity; propose reclassification of investments
CASH RECEIPTS	CASH RECEIPTS	CASH RECEIPTS
<u>Treasury</u> Prohibit the cashing of checks out of cash receipts Instruct bank not to cash checks payable to the Company or Cash	<u>Receptionist/Mail Opener</u> Open mail; restrictively endorse all checks; prepare a listing of checks and cash received, sending copies to cashier and accounting while retaining one copy <u>Cashier</u> Control receipts through proper registration devices and use of prenumbered receipt forms; safeguard	<u>Accounts Receivable</u> Update cash receipts journal daily to reflect receipts; account for sequence of receipt forms and remittance advices and for agreement of registration devices' records and cash receipts per mail opener and cashier Maintain the subsidiary accounts receivable ledger

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

AUTHORIZATION	CUSTODY	RECORDKEEPING
	receipts; control lockboxes used for customer payments <u>Cash Receipts</u> Prepare bank deposit slip, reconciling to mail opener's listing of checks and to reported totals from cash registers or similar devices; make daily deposit Approve deposit slip, checking reconciliations made by the preparer of the slip; assure cash from grants or similar sources are supported as required by law (e.g., separate bank accounts if so required)	<u>General Ledger</u> Maintain the control accounts Review and approve journal entries; reconcile subsidiary ledger with general ledger; reconcile total receipts with total accounts receivable postings and accounts receivable balances to the accounts receivable aging schedule Compare authenticated deposit ticket to record of incoming remittances, cash book, and postings to other accounting records; investigate deposits or collection items charged back by bank; prepare bank reconciliation
PURCHASES OF INVENTORY, SERVICES, AND NON-CAPITAL ASSETS	PURCHASES OF INVENTORY, SERVICES, AND NON-CAPITAL ASSETS	PURCHASES OF INVENTORY, SERVICES, AND NON-CAPITAL ASSETS
<u>Purchasing</u> Approve purchase requisition from the operating department or from the Board of Directors initiating purchase activity Prepare Purchase Order based on requisition Review and approve Purchase Order; send copy to party making request	<u>Receiving</u> Prepare receiving report Review and approve receiving report; forward copies to purchasing and accounting Forward goods to warehouse/storeroom	<u>Accounts Payable</u> Prepare voucher, comparing purchase order, receiving report, and invoice Review and approve voucher for payment Prepare check and forward voucher package for payment

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

AUTHORIZATION	CUSTODY	RECORDKEEPING
and to accounting; retain copy for records; mail copy to vendor Investigate complaints and correspond with vendors		Maintain the Voucher Register and files of open Purchase Orders, Unmatched Receiving Reports, Unmatched Invoices, and Unmatched Records of Returns and Claims Maintain the subsidiary accounts payable ledger <u>General Ledger</u> Maintain the control accounts Review and approve journal entries; reconcile subsidiary ledger with general ledger; reconcile vendor statements; review open and unmatched files and documents unaccounted for
PAYMENT OF PURCHASE OBLIGATIONS	PAYMENT OF PURCHASE OBLIGATIONS	PAYMENT OF PURCHASE OBLIGATIONS
<u>Treasury</u> Check signer; review voucher package before signing Countersignature; review voucher package before signing	<u>Cash Disbursements</u> Distribute checks to payees Maintain check register and custody of unissued checks and debit memos Cancel voucher and supporting documents and return them to accounting, noting check numbers issued	<u>Accounts Payable</u> Update voucher register to reflect vouchers paid Maintain the subsidiary accounts payable ledger <u>Purchase & Expense Ledger</u> Maintain detailed expense ledger, including prepaid expense items for which

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

AUTHORIZATION	CUSTODY	RECORDKEEPING
		check requisitions were properly authorized <u>General Ledger</u> Maintain the control accounts Review and approve journal entries; reconcile subsidiary ledger with general ledger and vendor statements, and account for the usage of checks and debit memos Prepare bank reconciliations
EXPENDITURES - PAYROLL	EXPENDITURES - PAYROLL	EXPENDITURES - PAYROLL
<u>Personnel</u> Maintain employee master file; approve additions, deletions, or changes to payroll master file with consensus from Human Resources and operating departments <u>Timekeeping</u> Maintain time cards with approval of hours worked	<u>Cash Disbursements</u> Deposit net payroll amount in payroll imprest bank account based on voucher Distribute checks, returning unclaimed checks to a cash disbursements employee with no other cash responsibilities	<u>Payroll Preparation</u> Prepare payroll, reconciling job time tickets to time clock cards; record labor distribution Prepare payroll checks Sign payroll checks Maintain employee records <u>Accounts Payable</u> Review payroll, checking extensions and propriety; prepare voucher Review and approve voucher for payroll

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

AUTHORIZATION	CUSTODY	RECORDKEEPING
Treasury Control signature plate/stamp for checks		General Ledger Maintain the control accounts; review exception reports based on reasonableness and limit checks Review and approve journal entries; reconcile payroll journal to general ledger
PETTY CASH	PETTY CASH	PETTY CASH
Treasury Verify imprest basis of petty cash fund, approving voucher for reimbursement Check signer reviews voucher package before signing, cancels petty cash vouchers and supporting documentation, and notes the check number issued. Countersignature reviews voucher package before signing, checks for cancellation, and returns voucher package to accounting.	Petty Cash Custodian Responsible for petty cash fund, including the cashing of reimbursement checks Countersignature on petty cash vouchers	Accounts Payable Reviews petty cash vouchers for propriety and prepares voucher for reimbursement Prepare check payable to custodian and forward voucher package for payment Purchase & Expense Ledger Update purchase and expense ledger for petty cash disbursements General Ledger Maintain the control accounts Approve journal entries and adjustments Prepare bank reconciliation

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.