K2's Case Studies In Fraud And Technology Controls

Continuing Professional Education Series

K2 Enterprises www.k2e.com

K2E Canada Inc. www.k2e.ca

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

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

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.

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

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.

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

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

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.

Learning Objectives

Upon completing this course, you should be able to:

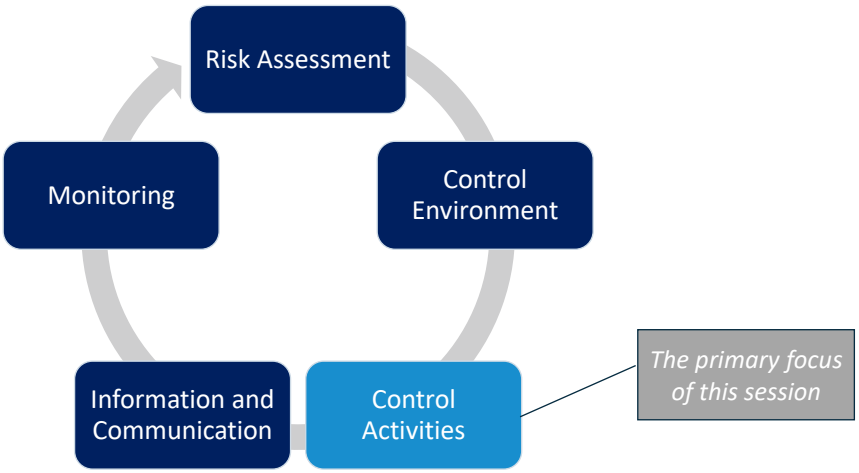
- Define information technology general controls and information technology application controls and distinguish between the two
- List examples of key information technology controls
- Recognize control failures and weaknesses that can lead to fraud
- List recommendations for improving internal controls in an organization

FRAUD – THE CURRENT STATE OF AFFAIRS

Fraud Is Rampant!

- The sad truth – and virtually every study on the topic bears this out – is that **fraud is rampant today in businesses of all sizes**
- Most **estimates peg fraud losses at 5% to 8% of total organizational revenues**
- Be aware that **distinct differences exist in the numbers and types of frauds based on the size of the victim**
- Of course, internal controls are ***supposed*** to be working to prevent/reduce fraud, but with losses that high, are internal controls as effective as they should be?

Five Internal Control Components



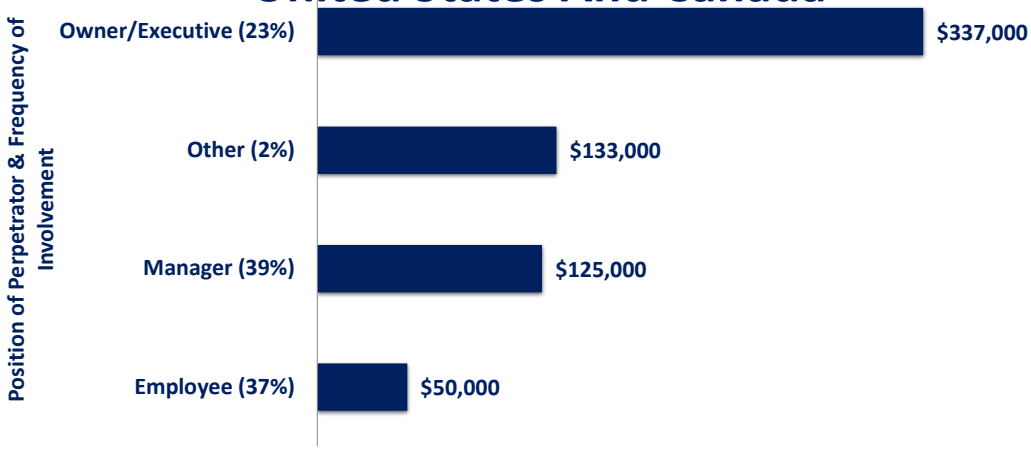
Four Primary Control Activities

Preventive controls	*Activities in which we engage attempting to prevent undesirable actions or outcomes*
Detective controls	*Measures we put in place to let us know on a timely basis that an intended result is not being achieved*
Deterrent controls	*Actions that are occurring with the intended purpose of discouraging non-desired behavior*
Compensating controls	*Undertakings for the express purpose of accounting for a known internal control weakness*

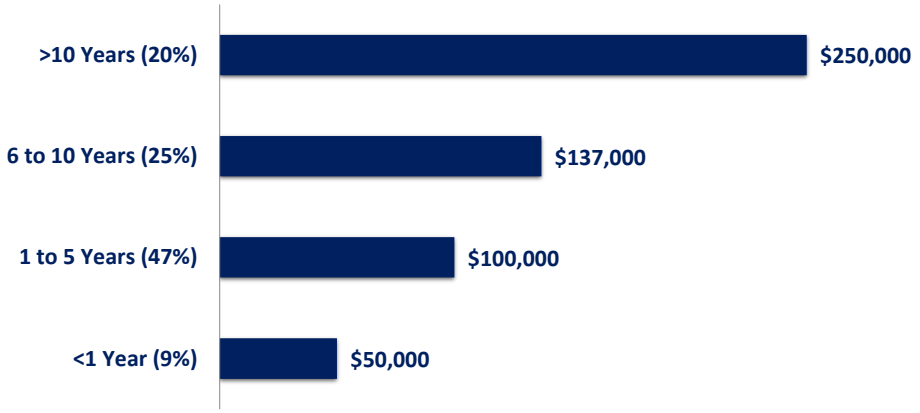
Findings From The Association Of Certified Fraud Examiners (ACFE)

- **Occupational fraud consumes 5% of all business revenues**
- Annual occupational **fraud losses approximate $4.7 trillion worldwide**
- **Average loss per case was $1,783,000**
- A **typical fraud causes losses of $8,300 per month** and continues for twelve months before discovery
- The **median loss for occupational fraud is $117,000**

Position Of Fraud Perpetrator In The United States And Canada

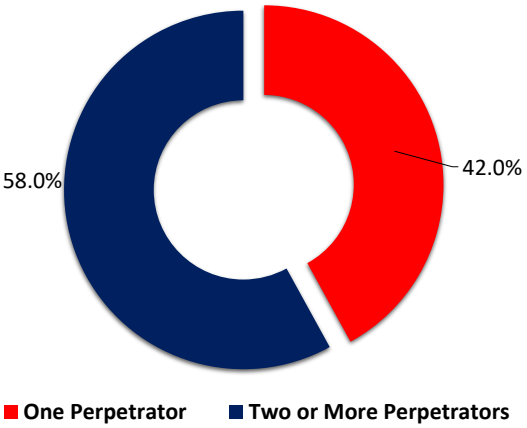


Perpetrator's Tenure Median Loss And Frequency

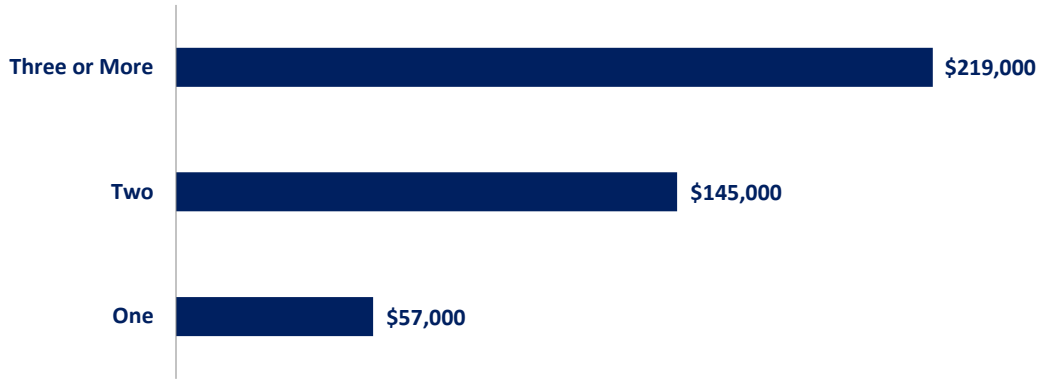


Number Of Months To Detect Fraud, By Position

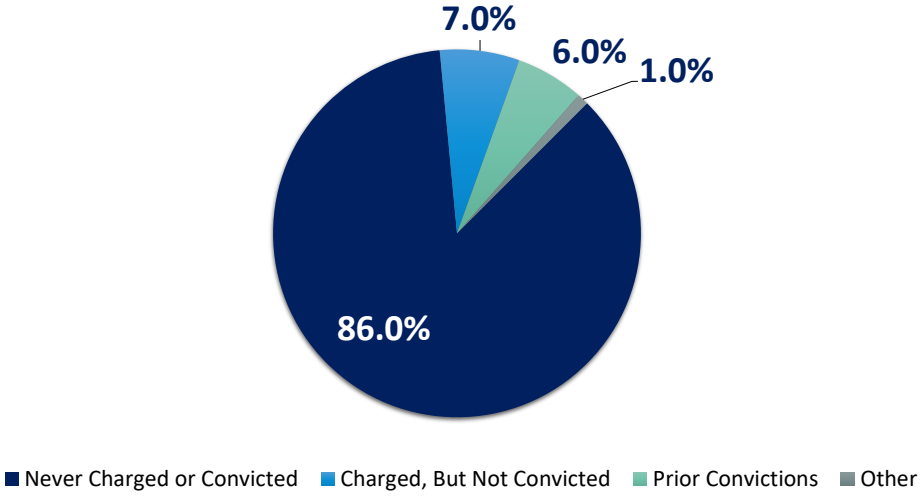
Collusion Is Involved In Over Half Of Reported Fraud Cases



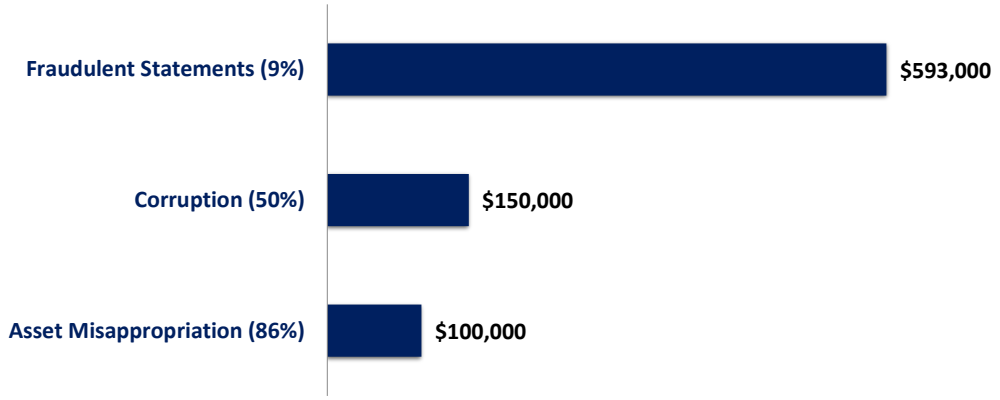
Fraud Losses Are Higher With Multiple Perpetrators



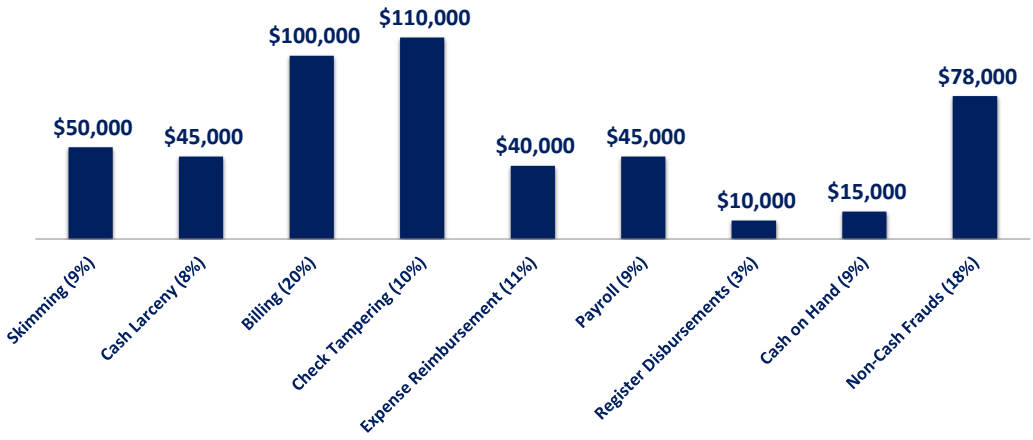
Who Is Committing Fraud?



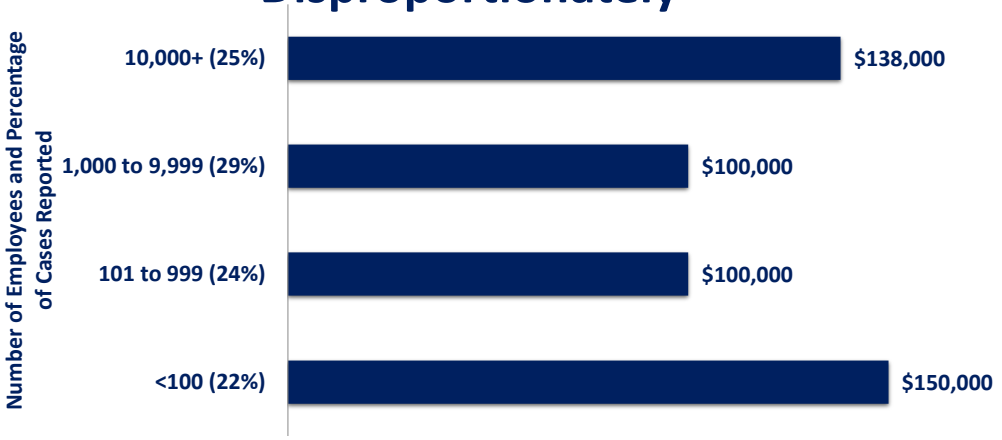
Types Of Frauds Committed, Frequency And Losses



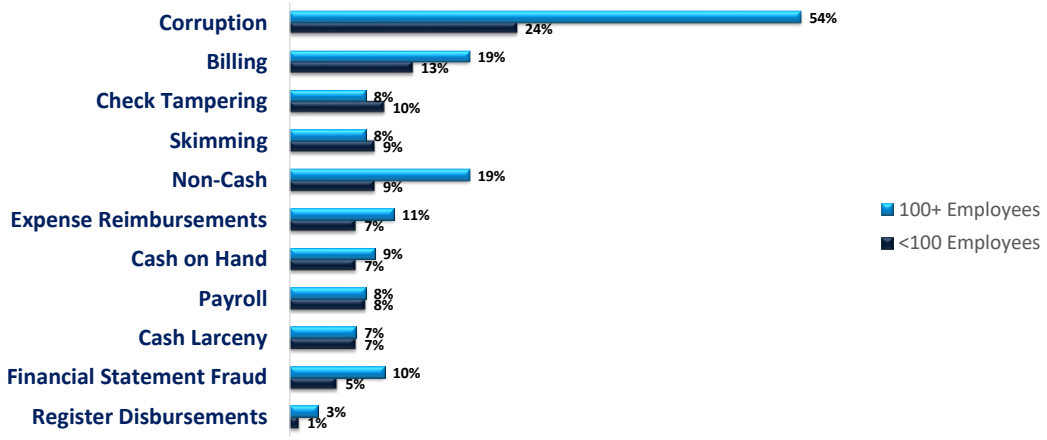
Relative Risks Of Asset Misappropriation Frauds



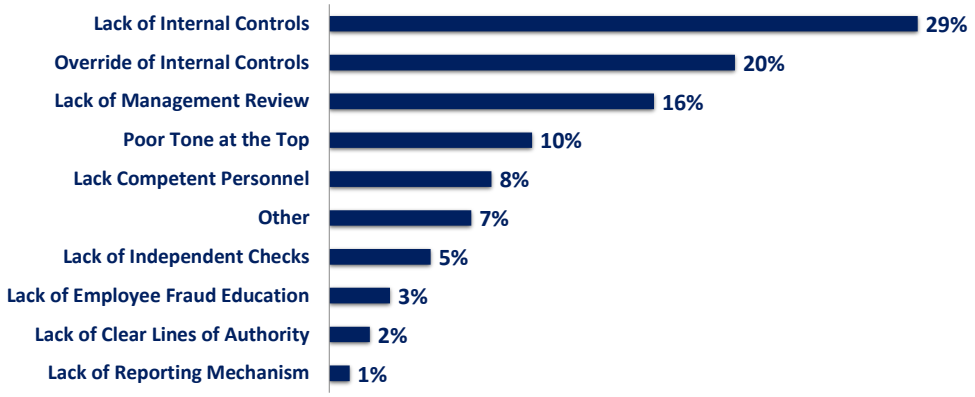
Fraud Impacts Small Businesses Disproportionately



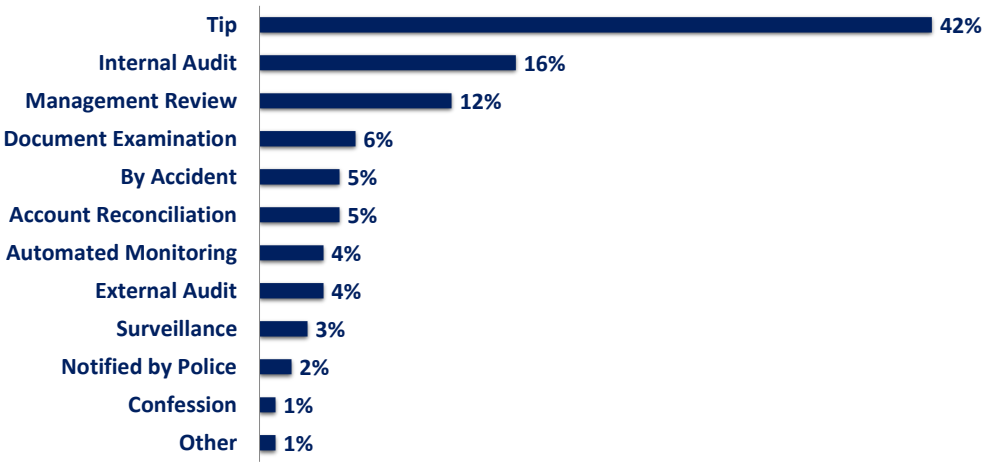
Small Businesses Face Different Fraud Risks



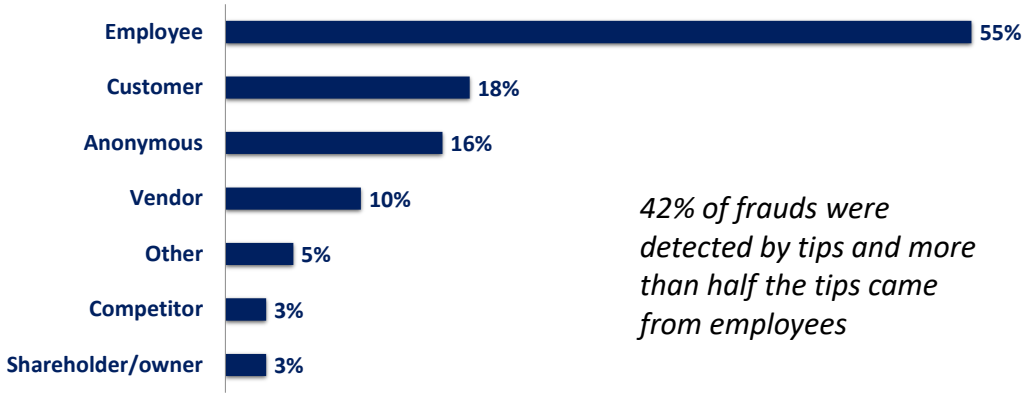
Internal Control Weaknesses That Contribute To Occupational Fraud



How Frauds Are Detected



Sources Of Tips For Occupational Fraud



42% of frauds were detected by tips and more than half the tips came from employees

There Is Some Good News

Another recent report by the ACFE – **Anti-Fraud Technology Benchmarking Report** – shows that many organizations are preparing to invest in technology to help prevent and detect fraud, as highlighted below

- 55% of respondents expect to increase their budgets for anti-fraud technology over the next two years
- The use of Artificial Intelligence as part of anti-fraud efforts is expected to triple over the next two years
- Presently, 2/3 of all respondents use exception reporting, and 1/2 use automated monitoring…those numbers are expected to grow to 72% over the next two years

There Is Some Good News

- So, what can we conclude from the conversation so far?
- First, **businesses of all sizes have recognized the problem and see technology as a potential solution**
- Second, recognize that **no single method or technology will be effective by itself**…as always, a sound system of internal controls is a balanced system of internal controls
- Third, **effective internal control structures will consist of people utilizing technology in tandem with traditional measures and controls to stem fraud losses** and achieve their stated organizational objectives

CASE STUDIES IN FRAUD

The Pink-Collar Crime Phenomenon

- According to the FBI, since 1990, the number of men embezzlers has increased by 4%, whereas the **number of women embezzlers has risen by 40%**!
- The ACFE reported in 2018 that when men are involved, the median loss is $156k, whereas when women are involved, the median loss is "only" $89k; however, **PinkCollarCrime.com** reports that **numerous studies indicate that women are involved in more embezzlements than men**, although less money is usually involved

A "Classic" Small Business Accounting Fraud

THE AMY WILSON CASE

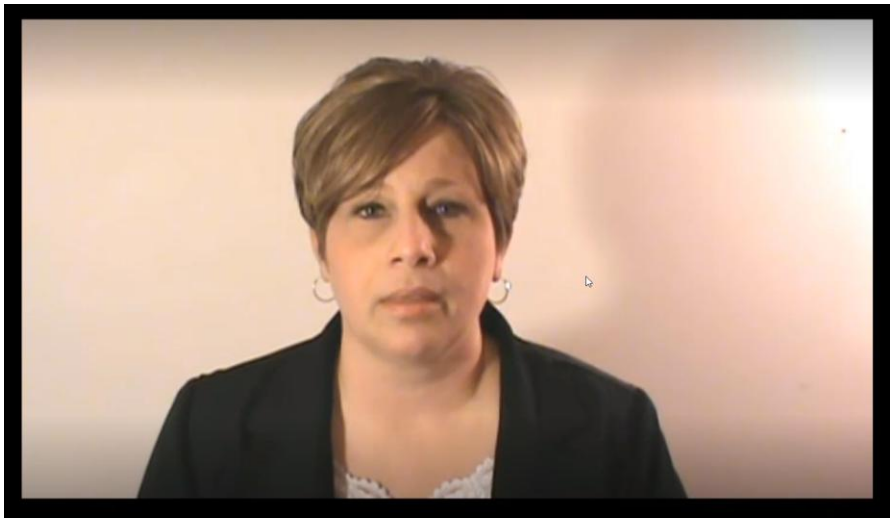
The Amy Wilson Case

- Amy Wilson embezzled approximately $340,000 from her employer, a Rockville, Indiana-based manufacturing company
- In her role as Office Manager, she began stealing from the company to pay for her son's legal troubles
- However, because it was so easy, she continued to steal, even though her son's legal troubles were behind him

How Did She Get Caught

- Capital One called the President of her company on a fraud check, investigating charges they thought suspicious
- Interestingly, the Company did not call the police immediately…
  - Instead, they allowed her to process payroll first
  - After all, bonuses had to be paid in that pay period
- Wilson plead guilty to four forgeries and four thefts, although she said she committed many more illegal acts
- Wilson was sentenced to six years in prison, where she served two years and was released on probation

Let's Hear Mrs. Wilson's Story



In Her Words…

Concealing my embezzlement was easy. My employer didn't care about internal controls. As the office manager, I had access to all computer modules and bank accounts. The only safeguard was that I was not allowed to sign checks.

In Her Words…

I hid my embezzlement in the cost of goods for the company's largest customer. If the owners had reviewed the costing reports and paid attention to other signs in the financials, they might have caught me.

In Her Words…

My credit card company's fraud audit uncovered my theft. I had been more worried about the company's outside CPA uncovering it than the president or vice president. The accountant strongly encouraged my boss, the president, to get to the bottom of the 2 percent increase in the cost of goods, but he ignored that advice, and he refused to pay for more than a compilation.

What Could Have Been Done?

Segregation of duties
Budget versus actual comparisons/investigations
Spot checks of purchases
Financial statement audits
Purchasing cards
Data analytics
Other actions?

Donald Cressey's Fraud Triangle

- **Opportunity** – the ability to do something wrong, including the ability to hide the action
- **Incentive/Motivation** – the need (perceived or real) or desire to do something wrong
- **Rationalization** – the ability to persuade oneself that the fraud is not really a fraud…"I'm just borrowing the money"

WHAT COULD HAVE, SHOULD HAVE WILSON'S EMPLOYER DONE TO PREVENT/DETECT THIS?

SIM CARD FRAUD

SIM Card Fraud Is Real And Growing

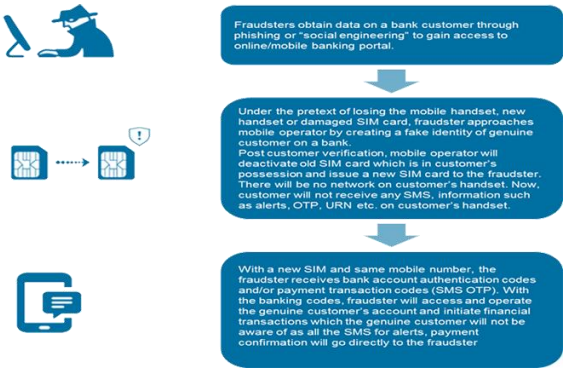
- Think, for a moment, about the SIM card in your mobile device
- Essentially, it is linking your mobile phone to your mobile device account and carrier
  - Without an active SIM card in the device, the device is useless
- Now, if those wanting to commit fraud can transfer your SIM card to a device that *they* have in *their* possession, then *that* device becomes active, and the one that you have becomes virtually useless
  - In this case, the person committing the fraud has access to almost everything on your device…think about this if you use your device in a multi-factor authentication environment…you're **TOAST**!

What Is SIM Card Fraud?

- SIM card fraud is a form of **identity theft**
- When someone commits SIM card fraud, they can steal your mobile account and the personal data attached to it
- The fraudster can do this by **taking advantage of weak authentication** you have on your account or by **colluding with someone working at a retail phone store** and having that person bypass established controls
- Either way, the crook gets access to your sensitive corporate and personal data stored on the device

Anatomy Of A SIM Card Fraud

Courtesy Of
www.gemalto.com



An Account Of SIM Card Fraud

Another SIM Fraud Case…

- Carlos Tapang sued T-Mobile in 2017, claiming the company "improperly allowed wrongdoers to access" his account, transfer it to AT&T, and then steal cryptocurrency valued at approximately $20k
- Allegedly, T-Mobile indicated before the crime that they would **add a PIN code to Tapang's account**…this did not happen
- Additionally, Tapang alleged that the hackers were able to make **repeated calls to T-Mobile representatives in attempts to gain access to customers' accounts, until they are successful in reaching a representative that was cooperative**

How To Prevent SIM Card Fraud?

Reconsider how you implement multi-factor authentication (MFA)

- If a hacker gains access to your device and you are using SMS (text)-based MFA, **they will be able to see your text messages**…thus, if they're trying to access an account – bank account, for example – that you have protected with SMS-based MFA, they will receive the text message and be able to log-in to that account
- Instead of SMS-based MFA, consider using an authentication app such as **Google Authenticator**, **Authy**, **LastPass**, **1Password**, or **OTP Manager**
- With an authenticator app, the crook would have to be able to log-in to the app on the device from which you're trying to gain access to an account to obtain the authentication code
  - Keep in mind, with SMS-based authentication, they only need to log-in to the phone

How To Prevent SIM Card Fraud?

- Add a SIM PIN to your mobile device
  - A SIM PIN is a multi-digit code that you are prompted for every time the phone restarts or if you remove the SIM card from the device
  - For **AT&T** subscribers, log-in to your account, go to **Manage Profile**, **Sign-in Info**. Then select **Account Passcode** followed by **Manage Extra Security**.
  - **Sprint** mandates these PIN codes. To change yours, log-in to your Sprint account, select **My Sprint**, **Profile**, **Security**, **Security Information**
  - If you use **T-Mobile**, dial 611 or 1-800-937-8997 to add the PIN code
  - For **Verizon** customers, log-in to your account and visit the **Change Account PIN** page, or call **1-800-922-0204**, or stop by a Verizon store
- No carrier will ever call you and ask for your PIN!!!!

GIVEN THE RISK ASSOCIATED WITH SIM-CARD FRAUD, WHAT ACTIONS SHOULD WE TAKE TO MITIGATE THAT RISK?

Mulder Steals $1.5M, ***From Friends***

- On May 15, 2017, Elizabeth "Lizzy" Mulder pleaded guilty to stealing over $1.5 million during a seven-year scam where friends were her victims
- Mulder, facing up to 23 years in prison, was sentenced to only five years after pleading guilty to felony wire fraud and subscribing to a false tax return
  - She was also to pay restitution of $1.5 million to clients she defrauded

Mulder Steals $1.5M, ***From Friends***

- Mulder passed herself off as an accountant – although she had no formal training – and solicited friends and acquaintances as clients
- Once she had gained the trust of her clients, she began to divert tax payments from clients into her bank account
- To do this, she had clients make checks payable to "Income Tax Payments"…of course, her bank account was also in the name of "Income Tax Payments"
- Once she had her clients' money, she used it for things such as cosmetic surgery, vacations, jewelry, horse rentals, and even gifts for clients

K2 Enterprises
Copyright 2026, K2 Enterprises, LLC

The Elizabeth Mulder Fraud

Mulder Steals $1.5M, ***From Friends!***

Among specific crimes, Mulder was charged with

- Diverting 77 checks allegedly for tax payment from a hair salon run by two friends
- Drafting 44 checks from a travel agency to “Income Tax Payments”
- Stealing $202,000 from a Pilates studio, including taking out loans in the name of the business
- Pocketing $200,000 from a San Clemente wine distributor
- Thefts from a copy and print company that ended up closing after 22 years of business because of the losses and tax penalties resulting from Mulder’s actions

Mulder Steals $1.5M, ***From Friends!***

- In one of the more bizarre twists, Mulder would sometimes call clients, pretending to be a vendor or a tax agency
- These calls were often made to let clients know that everything was OK and that their debts had been settled, so there was no need to worry about matters
  - In some cases, the calls were made to pressure clients into making payments, payments that ended up with Mulder, of course
- However, Mulder was the person making the call, and she used a voice-altering app on her phone to disguise her voice so that clients would not know it was her
- Mulder's case was featured on TV's "American Greed" series

WHAT COULD HAVE, SHOULD HAVE MULDER'S CLIENTS DONE TO PREVENT/DETECT THIS?

The Rodolfo Olivas Case

- In 2018, Rodolfo Olivas was arrested and accused of stealing $1.3 million from his West Melbourne, Florida employer
- The 10-month investigation revealed that Olivas allegedly stole from his employer – Hill, Inc. – through fraudulent credit card transactions and by writing company checks for personal expenditures
- Olivas allegedly racked up $1.025 million in fraudulent charges on an unauthorized American Express account and wrote approximately $291,000 in fraudulent checks
- The transactions in question dated back to 2010, although Olivas began working for his employer in 2001

The Rodolfo Olivas Case

- The fraud was discovered while Olivas was on vacation and another team member was performing Olivas' duties
- According to police reports, Olivas used the money to lead a lavish lifestyle, including
  - Paying for cruises
  - Vacationing at Disney properties
  - Buying season tickets to Tampa Bay Buccaneers football games
- Detectives also reported that Olivas had a history of substance abuse issues that had spiraled out of control

The Rodolfo Olivas Case

- Olivas was in-charge of purchasing and payables
  - In the words of the detective, “he was the sole person over all that stuff”
  - Further, “he was able to input information into the work computer under false entries that showed one thing, but it was actually checks that were written to him”
  - Stated differently, no segregation of duties, no oversight, no data analysis, no detective controls, etc.
  - Company trusted him as a “family member”
- Police said that Olivas did not make any significant purchases, but rather, because of his addiction he “spiraled out of control”
- Let’s view a portion of the press conference…

West Melbourne Police Department

WHAT COULD HAVE, SHOULD HAVE OLIVAS' EMPLOYER DONE TO PREVENT/DETECT THIS?

CINDY MILLS AND MATHEWS INTERNATIONAL

Cynthia Mills And Matthews International

- Matthews International is a publicly-held company that, among other things, serves the funeral home industry with memorialization products and services
- The company generated $365 million in revenue in Q1 2020, has approximately 11,000 employees, and is based in Pittsburgh
- Cynthia Mills worked for Matthews for 34 years…in 2016, Mills was charged with stealing $13 million from Matthews in a fraud scheme that lasted from 1999 to 2015
- Mills' attorney pointed to gambling addiction as the fraud driver

Cynthia Mills And Matthews International

- Mills' position at Matthews was Treasury Specialist, which put her in the position of receiving and stealing inbound payments from customers
  - She would subsequently alter bank statements and vendor invoices to cover her fraud
- Additionally, in 2013, Mills created a company named **Designs by Cindy** and began initiating wire transfers from Matthews to the shell company
- Mills was charged with mail fraud, wire fraud, tax evasion, and engaging in monetary transactions in the criminally derived property

Cynthia Mills And Matthews International

Among other items Mills purchased were

- Three homes
- An $800,000 yacht, plus two other boats
- At least 8 cars
- A snowmobile
- Three motorcycles
- Furs and designer handbags
- Jewelry

Cynthia Mills And Matthews International

Cynthia Mills And Matthews International

- Remarkably, in 2014, another Matthews employee pled guilty to embezzling $415,000
- In this fraud, Peter Kalemon submitted and approved bogus invoices from a West Virginia-based company he controlled
- As dispatcher of delivery, Kalemon negotiated rates and approved invoices with no oversight
- He started his crime in 2010, creating and issuing 126 fake invoices to Matthews that he approved

Cynthia Mills And Matthews International

- He deposited 81 checks into his corporation's account
- Matthews also caused an additional 39 checks to be issued after postal inspectors talked to him about the crime, ***including 14 that were issued after he was indicted***
- After his trial, he was sentenced to thirty-three months in prison and ordered to pay $415,000 in restitution

WHAT ARE THE LESSONS TO BE LEARNED FROM MILLS AND KALEMON FRAUDS AGAINST MATTHEWS INTERNATIONAL?

Rita Crundwell And Dixon, Illinois

- In one of the more remarkable occupational frauds on record, Rita Crundwell stole $53.7 million from the residents and taxpayers of Dixon, Illinois – a town of 16,000 people and the childhood home of Ronald Reagan
- Beginning in 1990, Crundwell started siphoning money out of city bank accounts into an account that appeared to be legitimate, but it was one she controlled personally
- Crundwell used the money to fund her lavish lifestyle – that could not otherwise be supported on an $80,000 annual salary – and her quarter horse farming business

Rita Crundwell And Dixon, Illinois

- Crundwell was arrested in 2012, which means that much of her fraud was committed during recessionary years
- Crundwell is serving a sentence of 235 months, of which she must complete at least 85%
- Further, she has been ordered to pay $53.7 million in restitution
- The city has recovered approximately $40 million from two accounting firms and the bank that was involved

Rita Crundwell And Dixon, Illinois

- Crundwell committed her fraud by opening a bank account entitled “RSCDA – Reserve Fund,” which was supposedly the “Reserve Sewer Capital Development Account”…of course, this was an account that she controlled, and it was NOT a city-related account despite the official-sounding name
- She would then transfer money from the city into the account
- Of course, once money was in the account, she would use it to pay for her personal and private business expenses, including horse farming operations, personal credit card payments, real estate, and vehicles

K2 Enterprises
Copyright 2026, K2 Enterprises, LLC

Rita Crundwell And Dixon, Illinois

- During budget meetings, Crundwell would explain away the shortage of city funds by blaming the recession and saying that the State of Illinois was late on its payments to the city
- To conceal the fraud, Crundwell picked up the city's mail to keep other employees from knowing about the fraudulent bank account
- The fraud was discovered while Crundwell was on vacation and another city employee requested copies of bank statements so that she could prepare a financial report
- At that time, the employee noticed the RSCDA account

Rita Crundwell And Dixon, Illinois

- Over time, Crundwell created 159 fictitious invoices to show the city's auditors that the funds she was depositing into RSCDA were being used for legitimate purposes
- For example, on September 8, 2009, Crundwell wrote a check for $350,000 from a legitimate account to the RSCDA account…later on, the same day, she wrote a check for $225,000 drawn on the RSCDA account and deposited that into her RC Quarter Horses account to cover the cost of her purchasing a horse…absent the $350,000 deposit, her $225,000 check would not have cleared the bank

WHAT ARE THE LESSONS TO BE LEARNED FROM THE CRUNDWELL FRAUD?

PREVENTING AND DETECTING FRAUD WITH TECHNOLOGY CONTROLS

So, What Are Technology Controls?

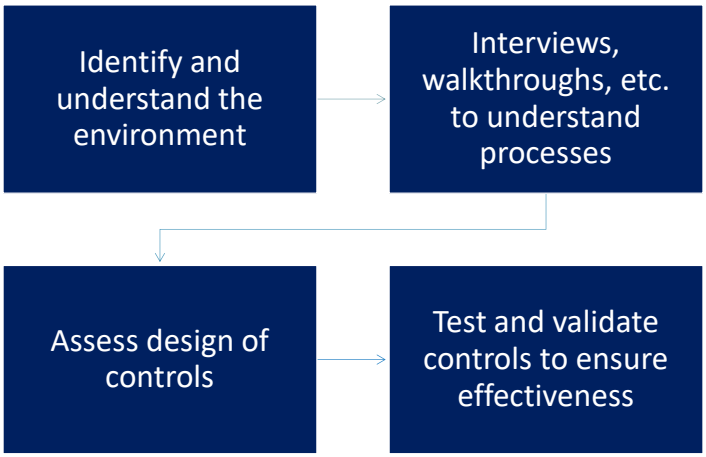
Wikipedia defines **information technology controls** as

*"Specific activities performed by persons or systems designed to ensure that business objectives are met. They are a **subset of an enterprise's internal control**. IT control objectives relate to the **confidentiality**, **integrity**, and **availability of data** and the overall management of the IT function of the business enterprise."*

Technology Controls, In General

- **Technology controls**, like all forms of internal control, exist to mitigate risk to a ***prudently acceptable level***
- A well-designed control environment will include a mixture of ***preventive***, ***detective***, ***deterrent***, and ***alternate*** controls
- Further, the extent to which controls are implemented should be based on the ***risk appetite*** and ***risk tolerance*** of the organization
  - ***Risk appetite*** is the degree risk management is willing to take
  - ***Risk tolerance*** is the acceptable level of variation relative to achieving defined organizational objectives

Technology Controls Are No Different Than Other Controls



IT controls are divided into two, more focused categories

- IT General Controls (ITGCs)
- IT Application Controls (ITACs)

EVALUATING INFORMATION TECHNOLOGY GENERAL CONTROLS

What Are IT General Controls?

- Broadly speaking, ITGCs are controls that apply ***across an organization and all its systems, components, data, computers, servers, etc***.
- The purpose of ITGCs is to help maintain the integrity of programs and data and to ensure that applications are appropriately developed and implemented
- ITGCs can be thought of as the perimeter or first line-of-defense controls, whereas ITACs (discussed later) focus on specific applications and processes

ITGCs Focus On These Ten Areas

1. Control environment
2. Change management procedures
3. Source code/document version procedures
4. Logical access policies, standards, and applications
5. Incident management policies and procedures
6. Problem management policies and procedures
7. Technical support policies and procedures
8. Hardware/software configurations, installation, testing, and management
9. Disaster recovery/business continuity
10. Physical security

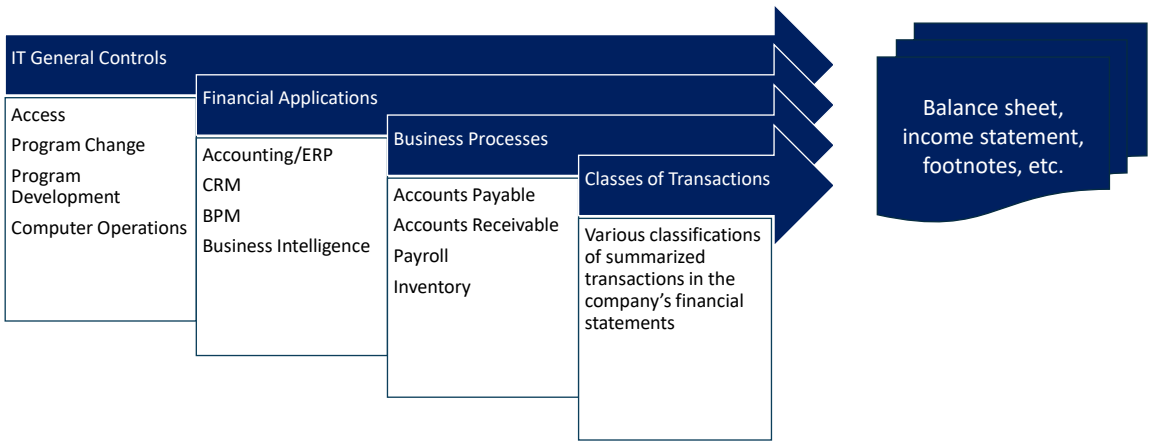
The Importance Of ITGCs

- ITGCs are the controls that should be in place to **provide reasonable** assurance concerning the **security**, **stability**, **and reliability of an organization's IT infrastructure and related personnel**, particularly as these relate to financial systems
- Poor or ineffective ITGCs or inconsistent application of ITGCs can affect the ability to rely upon ITACs and manual procedures and potentially result in no reliance on either/both
- ITGCs show up in many regulatory audits, including HIPAA assessments, SSAE 16 assessments, PCI reviews/audits, and SOX assessments

ITGCs are often broken into four groups

- Access To Programs And Data
- Program Changes
- Program Development
- Computer Operations

Where Do These Four Groups Of ITGCs Fit Into Financial Reporting?



Some Free Tools To Assist You…

- DumpSec
  - www.somarsoft.com
- Belarc
  - www.belarc.com
- Wireshark
  - www.wireshark.com
- Gibson Research Corporation
  - www.grc.com

Access To Programs And Data

Objectives	Risks	Sample Controls
Access to programs and data should be restricted to authorized individuals only, based on specific job requirements	Unauthorized access to programs or data may lead to improper changes, destruction of data, and/or disclosure to unauthorized parties	• Usernames and passwords for logical access • Review of audit logs

Sample Tests Of Access Controls

Sample Control	Potential Testing/Validation Option
A formal mechanism exists for providing new users with access to a system, including formally approving the user and establishing specific rights.	Acquire and read a copy of the policy that applies to this activity, making note of specific requirements. For a sampling of new users, validate that access was approved and that user rights aligned with job description.
Whenever a team member leaves the organization, a formal process exists for immediately disabling access by the user into their account.	Acquire a listing of former team members, including date of termination. Compare this to listing of inactive users to determine if deactivation was timely. Additionally, compare list of all current users in the system to a listing of all current team members.
The company has a strong password policy in place and all user accounts are in compliance.	Acquire a copy of the policy and compare it to mandated password strength for accessing specific applications.

Program Changes

Objectives

All changes to existing systems are authorized, tested, approved, and documented

Risks

Unauthorized, inappropriate, or error-ridden changes may result in incomplete and/or inaccurate data

Sample Controls

- Methodology surrounding change and development
- Approval prior to implementation of changes

Program Development

Objectives	Risks	Sample Controls
New systems and applications should be authorized and thoroughly tested, approved, implemented, and documented	Inappropriate system or program development or implementation may result in incomplete and/or inaccurate data	• Design, authorization, development, testing, and approval controls • Configuration change controls • Data migration

Sample Tests Of Program Change And Development Controls

Sample Control	Potential Testing/Validation Option
A formal process for initiating and managing changes to systems is in place.	Acquire and read a copy of the policy governing program changes and development. Make inquiries and observations regarding team members' compliance with this policy.
All system changes are documented and tracked.	Examine various change logs to ensure that changes were documented and tracked. Additionally, trace all changes per log back to change request documents to ensure that all changes were formally approved. Also trace all change request documents to change logs to ensure that all approved changes were effected.
New and updated applications and systems are fully tested and authorized prior to implementation.	Review results of tests, review evidence of approval that was obtained prior to implementation.

Computer Operations

Objectives	Risk	Sample Controls
Computing assets are available and functioning as intended	Computing assets are not available or not performing as intended	• Monitoring • Backup and recovery procedures • Patch management controls

Computer Operations Controls Tests

Sample Control	Potential Testing/Validation Option
Jobs and applications are monitored to ensure successful completion.	Review job and application logs for indications of failed jobs and for follow-up and corrective actions where failed jobs were noted.
All critical data is backed up contemporaneously and stored in an appropriate medium and location.	Obtain, read, and understand backup procedure policy. Compare policy requirements to backup logs. Analyze backup locations for folders containing critical data that is not being backed up. Determine if periodic tests are performed to validate the recoverability of data.
A process exists for identifying, escalating, and resolving end-user technology-related problems that could affect accuracy and efficiency of efforts.	Inquire of team members as to any on-going issues such as software or hardware malfunctions. Determine if these have been reported and the resolution status.

Top 10 ITGC Deficiencies

Information Technology General Controls and Best Practices, Warren Averett

1. Terminated employees still active in systems and network
2. Lack of segregation of duties over development and production environments
3. Lack of critical application list, resulting in little or no knowledge of vulnerabilities
4. Lack of vendor management/risk programs
5. Lack of external penetration testing and internal vulnerability scanning
6. Shared and/or generic administrator accounts without monitoring
7. Weak system password parameters
8. Outdated disaster recovery plans and no testing completed (financial applications and full IT network)
9. Lack of data backup testing
10. Lack of portable device policies and security

Top 10 ITGC Deficiencies

Information Technology General Controls and Best Practices, Warren Averett

1. Terminated employees still active in systems and network
2. Lack of segregation of duties over development and production environments
3. Lack of critical application list, resulting in little or no knowledge of vulnerabilities
4. Lack of vendor management and risk programs
5. Lack of external penetration testing and internal vulnerability scanning
6. Shared and/or generic administrator accounts without monitoring
7. Weak system password parameters
8. Outdated disaster recovery plans and no testing completed (financial applications and full network)
9. Lack of data backup testing
10. Lack of portable device policies and security

40% of these are associated with access risk

K2 Enterprises
Copyright 2026, K2 Enterprises, LLC

Common Examples Of ITGCs

- Usernames and passwords (or other forms of authentication, including multi-factor authentication) to access to a computer, a network, or a Cloud-based service or resource
- Restrictions on who signs in to their device with Administrative rights
- Network firewalls to minimize the threat of outside intrusion
- End-user security training
- Off-site, contemporaneous backups of critical data

Policies Are Key ITGC Components

- Every organization should maintain a well-documented and current set of policies governing the IT operating environment
- Not only do these provide clarity to all IT administrators as well as end-users, but they also serve as a reference point for conducting evaluations of technology controls

Control Policies You Should Have

- Acceptable use policy
- Acquisition assessment policy
- BYOD policy
- Clean desk policy
- Data breach response policy
- Disaster recovery plan policy
- Email policy
- Encryption policy
- Password policy
- Remote access policy
- Technology equipment disposal policy
- Server security policy
- Software installation policy
- Web application security policy
- Wireless communication policy
- Workstation security policy

Policies Are ITGC Key Components

A great resource for technology control templates remains The SANS Institute's Security Policy Project

(https://k2e.fyi/SANSPolicies)

or

K2 Enterprises
Copyright 2026, K2 Enterprises, LLC

EVALUATING INFORMATION TECHNOLOGY APPLICATION CONTROLS

What Are IT Application Controls (ITACs)?

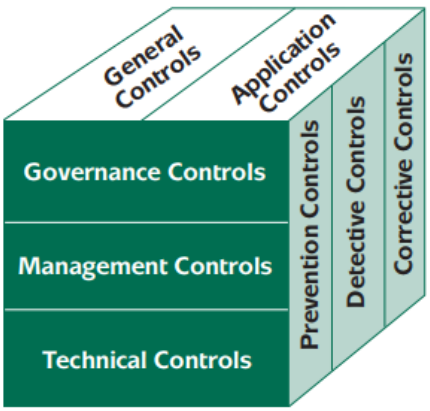
The PCI Security Standards Council defines ITACs as those controls that "*pertain to the **scope of individual business processes or application systems and include controls within an application around input, processing, and output**. Application controls also can include data edits, segregation of business functions (e.g., transaction initiation versus authorization), balancing of processing totals, transaction logging, and error reporting*."

The Nature Of ITACs

- ITACs are applied to the specific ***user***, ***application***, or ***business process level***
  - Contrasted to ITGCs, which are applied at a much higher level, such as at the network level
- To illustrate, an **ITGC might be applied to allow a user to sign in to a network and may even control which apps the user can access, but an ITAC would control that user's rights to enter transactions or access reports** in that organization's accounting application

The Nature Of ITACs

- Like ITGCs, ITACs can be ***preventive***, ***detective***, ***corrective***, or even ***deterrent***
- ITACs can also slice across the group responsible for implementing and maintaining them, such as the Board of Directors (*governance controls*), management (*management controls*), or technical team members (*technical controls*)



Examples Of ITACs

Type of Control	Purpose/Use
Authentication Controls	To validate that the person accessing the application or data is authorized to do so
Authorization Controls	To validate that the person executing the transaction is authorized to do so
Completeness Checks	To validate that all authorized transactions have been entered into the system
Forensic Controls	To detect that a potentially inappropriate transaction or event has occurred
Input Controls	To ensure that the data being entered is valid

Common Examples Of ITACs

- Usernames and passwords to access applications, such as accounting, CRM, and similar line-of-business systems
- Specific rights granted within business applications controlling what a named user can – and cannot – access
- Edits on fields to ensure the proper type of data is being entered…for example, no text entries in a date field
- Audit trail reports showing who did what and when they did it
- Preventing price overrides on accounts payable bills or invoices issued to customers

ANALYZING AND EVALUATING TECHNOLOGY CONTROLS

Analyzing Risks Relative To Controls

- When considering the need for either ITGCs or ITACs, a thorough risk analysis should be performed to determine the depth and breadth of the control measures that should be implemented
- Among the questions to be asked in this analysis are
  - Which IT assets are at risk and their value in terms of confidentiality, integrity, and availability?
  - What could happen to affect the information asset's value adversely?
  - If the asset was threatened or compromised, how bad could the impact be?
  - How often could the threat materialize?
  - What can be done to address the risk, and is it cost-effective?

A Process For Evaluating Controls

- **Step 1 Conduct a high-level risk assessment**
- **Step 2 Identify applications in use**
- **Step 3 Create a catalog of existing ITGCs and ITACs**
- **Step 4 Test**
- **Step 5 Evaluate and Report**

A Process For Evaluating Controls

- **Step 1 – Conduct a high-level risk assessment**
  - Read and evaluate any existing risk assessment documentation
  - Evaluate the current IT environment to identify critical systems and process owners
  - Determine if any forthcoming projects could impact the internal control environment
  - Ask for prior years' audit reports and feedback

A Process For Evaluating Controls

- **Step 2 – Identify all applications in use**
  - Create a listing of all significant applications that are in use
  - Document software versions, operating systems, databases, etc.
  - Determine if any significant changes are planned

A Process For Evaluating Controls

- **Step 3 – Create a catalog of existing ITGCs and ITACs**
  - Assess the relative level of risk associated with all internal controls
  - Make a preliminary assessment of whether this control would effectively mitigate the designated risk IF it and related controls are functioning properly
  - Make a preliminary assessment of the risk to the organization IF this and related controls are not functioning properly
  - Based on the perceived level of risk, determine the extent of any testing to perform on each control

Consider Different Types Of Risk When Assessing ITGC Risks

Integrity Risk

- Number of changes
- Number of application controls
- Developed in-house?
- Number of developers

Access Risk

- Number of users
- Number of administrators
- Direct access to underlying database
- Integrated or independent authentication?

Which Application Is Riskier?

Integrity Risk				
Application Name	**Number of Annual Changes/Updates**	**Number of Application Controls**	**Developed In-House**	**Number of Developers**
Application #1	2	25	No	0
Application #2	300	0	Yes	20

Access Risk				
Application Name	**Number of End Users**	**Number of Administrators**	**Direct Access to Database**	**Authentication**
Application #1	150	2	No	Independent
Application #2	100	10	Yes	Integrated

A Process For Evaluating Controls

- **Step 4 – Design tests, if necessary, of controls**
  - Consider the quantity of data to test, based on perceived risk
  - What data, logs, and information will be necessary to perform this test, and is that information readily available?
  - Should this test be done on a surprise basis?

A Process For Evaluating Controls

- **Step 5 – Evaluate and report**
  - Based on your test results, evaluate and report on your tests
  - Indicate which controls are working as expected, which are not, and which could be improved to be more effective/cost-effective

Catalog Of Controls

Process Name/Description	Deleting inactive users. Immediately upon a team member's termination, a notification is sent to IT to terminate user access to all Company IT assets and services. IT is to act upon this notification immediately.
Objective	Only authorized users should have access to Company-owned systems and data. No matter the nature of the termination, inactive employees should never be allowed to access Company-owned systems or data.
Risk	Very high. Terminated employees may be emotional and have malicious intentions with respect to Company-owned systems and data.
Control Description	IT decommissions user access immediately for all terminated team members so as to prevent improper – and potentially – malicious access to Company systems and data.
Control Category	Access to programs and data
Type of Control	Preventive
Frequency Performed	On-Demand

Catalog Of Controls

Process Name/Description	Periodically review a list of authorized users. To ensure that only authorized users have access to the Company's information technology assets and data, monthly, an IT manager should compare the listing of active employees per payroll records to the listing of active usernames to determine if any former employees still have access to the Company's information technology assets.
Objective	Only authorized users should have access to Company-owned systems and data. Inactive employees are not allowed to access Company-owned systems or data.
Risk	Very high. Terminated employees may be emotional and have malicious intentions with respect to Company-owned systems and data.
Control Description	This test is performed to confirm that no terminated employees maintain access to the Company's information technology assets.
Control Category	Access to programs and data
Type of Control	Detective
Frequency Performed	Monthly

Catalog Of Controls

Process Name/Description	Compare user rights in the accounting application to each team member's job description to help ensure proper authorization of transactions in the system.
Objective	User rights in the accounting application should align with each user's assigned job responsibilities.
Risk	Moderate. If the rights established in the accounting application are not aligned with the team member's job description, unauthorized transactions could materialize, and the team member may become privy to sensitive data. Additionally, the risk of fraudulent transactions increases.
Control Description	This test is performed to confirm that each user has the appropriate rights in the accounting application, commensurate with their job responsibilities.
Control Category	Access to programs and data, authorization of transactions
Type of Control	Detective, preventive
Frequency Performed	Annually

Testing Options Available

- The types of tests you will conduct will vary based on the control, risk, and data available for testing
- As with "traditional auditing," testing options include
  - Inquiries
  - Observations
  - Inspections
  - Corroboration
  - Physical performance

Other Testing Considerations

Tests of Design	Tests of Effectiveness
• Test of Design (TOD) tests the control for effectiveness, assuming it operates as designed • In other words, could the control prevent or detect errors or fraud	• A Test of Effectiveness (TOE) determines whether the control is operating as designed • Are assigned team members qualified to perform the control procedure? • Are team members performing it as intended and on a timely basis?

How Much Data Should Be Tested?

- There are many factors to consider when determining the volume of data that should be tested
- Among these are
  - The inherent risk that the control will not operate as intended
  - The volume of data involved
  - Will statistical sampling be used, or will non-statistical methods such as judgmental sampling be used?
    - This is an essential consideration because using non-statistical methods, auditor bias might appear when selecting items for testing, as opposed to statistical methods, in which every item has an equal chance of being selected

How Much Data Should Be Tested?

- The following table provides some level of ***broad*** guidance as to the number of transactions that should be tested

If the control is to be performed…	…and if the typical population size is…	…then a typical sample size would be
Annually	1	1
Quarterly	4	2
Monthly	12	3 to 5
Weekly	52	6 to 10
Daily	250+	25 to 50
Multiple Times Per Day	250+	30 to 60

Sample Test Of ITAC

A small business utilizes an off-the-shelf accounting application to maintain its books. The system was set up by the Company's external accountant, who set up usernames and passwords for each user. Additionally, the accountant established each user's rights within the system to restrict them to only the functions they should be performing based on their job description. However, the owner is concerned that this control may not be effective as team members routinely share passwords. Periodically, the business owner would like to review a list of transactions to determine if team members can log in using a different username and record potentially fraudulent transactions. How could the business owner test this, and what type of application control would this be?

Sample Test Of ITGC

An IT staff member wants to see if, somehow, end-users can install software even though they are not supposed to have Administrative rights. If end-users can do this, software licensing policies might be potentially violated. Or, potentially malicious software could be installed, thereby compromising the security of all data on the network. How could the IT staffer quickly create an "inventory" of all the software on a team member's computer? What type of control would this be?

ARTIFICIAL INTELLIGENCE AND FRAUD PREVENTION AND DETECTION

Much Has Been Said About AI!

- **AI is a very popular topic** today!
- Tools such as **ChatGPT** and **Bard** are allowing many to use AI to solve practical, everyday tasks
- However, AI has been in use for several years to **help prevent and detect fraud**

AI's Building Blocks

- Artificial Intelligence (AI) is the ability of a device (computer) to understand and deal with situations in essentially the same way as a person would
- Using AI, we can potentially **automate many rote and mundane tasks, including checking for potential instances of fraud**
- For example, according to Accenture, **AI has the capability of boosting productivity by nearly 40% over the next 15 years**

Five AI Building Blocks

Computer Vision	• Computers can “see” and “understand”…scanning a check on a mobile app or facial recognition to log in
Machine Learning	• Computers learn from previous experiences…junk mail filters, for example
Deep Learning	• A subset of machine learning…think of it as *advanced* machine learning
Semantic Analysis	• Computers begin to use logic to reason from design models
Natural Language Processing	• Allows computers to understand commands/requests that are not in computer “code”

Artificial Intelligence And Fraud

- One of the bright spots in preventing and detecting fraud is the use of Artificial Intelligence (AI)
- With AI-based tools, the opportunity to analyze data in real-time (or very near real-time) for anomalies is a reality **today**
- Consider, for example, credit card fraud...**a Nilson report estimates that losses could exceed $408.50 billion globally during the coming decade**
- However, **AI-based tools are now in use by many banks and processors in attempts to reduce the rate of credit card fraud**

Eno, Capital One, And AI

- **Eno** is Capital One's AI-powered virtual assistant
- On the backend, as credit card transactions are processed, **AI is used to spot transactions that are not in line with the customer's normal purchasing patterns or otherwise seem suspicious**
- Once a transaction is flagged, Eno sends a message to the customer asking if they are aware of the transaction
- Eno then analyzes the response, continuing to look for any pattern of deception

You Can Use AI For Other Tasks, Too

- You can also use AI for many other tasks related to accounting and financial functions
  - For example, the **American Productivity and Quality Center reports that 37% of businesses still manage travel and expense reports via paper and Excel spreadsheets**
  - **Further, direct labor costs account for 62% of the total cost associated with processing accounts payable**
- Both the above functions can take advantage of AI for improved efficiencies and reduced costs

AI And Employee Expense Fraud

- In the book "**Artificial Intelligence in Spend Auditing**," authors Anant Kale and Kunal Verma report that one out of every ten dollars spent on Travel and Entertainment expenses is a mistake, does not comply with company policy, or is fraudulent
- Further, **the average enterprise-class organization processes 4,500 expense reports per quarter, each expense report contains an average of 11 expenses, and 10 percent of all reports carry a high-risk factor**

AI And Employee Expense Fraud

Seven Risky Areas for Employee Expense Fraud

- Duplicate expense claims
- Out-of-policy spend
- Travel violations
- Weekend/holiday purchases
- Excessive meal/alcohol purchases
- Unnecessary upgrades
- Other fraudulent behavior

Using AppZen To Audit Employee Expenses

AI Can Reduce Expenditure Fraud

- AI allows you to **audit 100% of transactions**
- AI can help to **identify fraudulent/mistaken transactions**
- With AI, you can **audit transactions before you pay them**
- AI can often electronically **match an invoice to supporting documents**, such as purchase orders and/or receiving reports

AI Can Improve Compliance, Also

- **Identify over-the-limit expenses**
- AI can identify expense reports where **amounts don't agree with submitted receipts**
- Recognize when **personal payment cards are used instead of corporate cards**
- **Identify meal costs** over daily limits
- Recognize when **two or more employees submit the same expense**

AI Can Improve Spend Processes

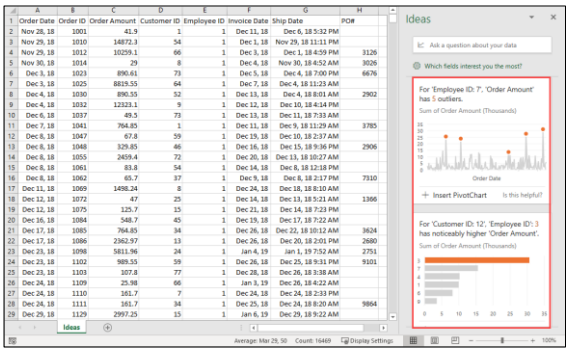
- AI can detect **duplicate payments** before they occur
- AI can scour the Internet to **make sure you are paying a competitive price for the products and services** your company is purchasing
- AI can **verify that appropriate discount terms** are being applied
- AI can help to verify that **services that you are paying for are being performed**
- AI can help to determine that you are **paying the correct amount for software licenses**

You May Have Access To Some AI Tools Now

- **AI is appearing in "everyday" applications** in subtle and not-so-subtle ways seemingly each day
- Take the ubiquitous spreadsheet, for instance
- If you are running Microsoft 365, in Excel you may have access now to **Analyze Data** (formerly known as **Ideas**), an artificial intelligence tool
- With Analyze Data, **Excel will analyze your data automatically and alert you to trends and patterns** in the data you may not have noticed

Analyze Data

As shown to the right, using Ideas in Excel, you may be able to identify patterns and relationships in your data that do not align with expectations, historical patterns, or norms



AND POWER BI MIGHT BE A USEFUL TOOL HERE ALSO

Power BI, In General

- **Power BI is a set of adaptable business intelligence reporting tools** available from Microsoft
- Power BI Desktop is free for all users and solves a large volume of reporting and analytics needs
- A subscription to a Power BI Pro account ($9.99 per month) extends the functionality to a Cloud-based environment, making it easier to share dashboards and reports with others

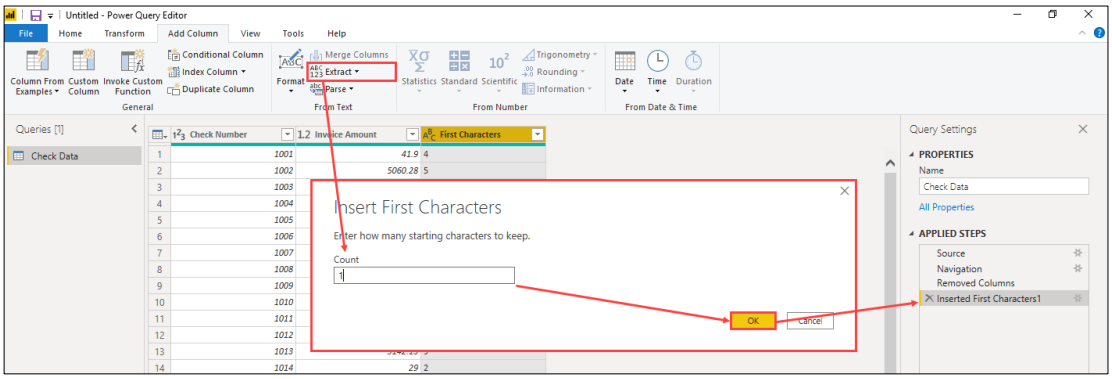
Power BI And Fraud Detection

- Because of Power BI's powerful query and transformation capabilities, **you can easily use the tool to perform such fraud tests as a Benford's Law test**
- Once you've created your report or dashboard, depending upon your license, you can potentially share it with other users so that all parties have real-real-time visibility into potential instances of fraud
- The following slides illustrate Power BI in a **Benford's Law** context, but you could easily extrapolate this to other types of fraud tests, **including accounts payable billing scheme frauds**

Connecting To & Transforming Data

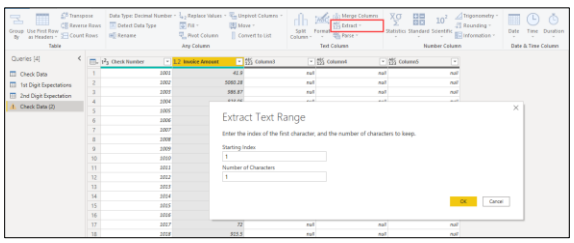
- In Power BI Desktop, choose **Get Data**, **Excel**, and select the Excel file you want to analyze
- You will need to create a **Transformation** in Power BI to extract the first character from the amount column
  - As shown on the following slide, you can use Power BI's **Extract, First Character** feature for this task
- It's important to note that building this transformation will create an **Applied Step** in Power BI that will automatically apply every time the query updates or refreshes

Benford's Law Analysis & Power BI



Connecting To & Transforming Data

- You will also need to create a transformation to extract the second character from the column of data you need to analyze
- Again, you can use **Extract** for this task, but this time choose **Range** and set the **Starting Index** value to **1** and the **Number of Characters** to **1**, as shown below



Add Two Tables In Power BI

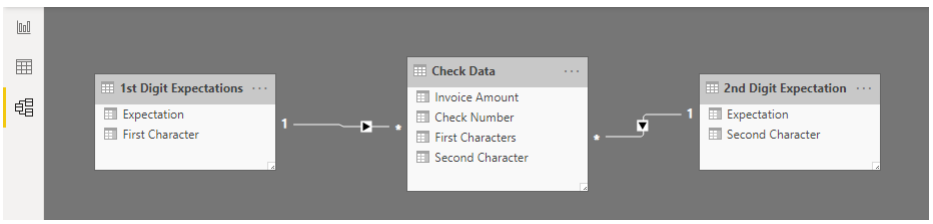
- You will need to add two user-defined tables in Power BI, in which you will store the Benford's Law expected values
- Do this by selecting **Enter Data** from the **Home** tab of Power BI's Ribbon

	First Character	Expectation
1	1	30.10%
2	2	17.61%
3	3	12.49%
4	4	9.69%
5	5	7.92%
6	6	6.69%
7	7	5.80%
8	8	5.12%
9	9	4.58%

	Second Character	Expectation
1	0	0.1197
2	1	0.1139
3	2	0.1088
4	3	0.1043
5	4	0.1003
6	5	0.0967
7	6	0.0934
8	7	0.0904
9	8	0.0876
10	9	0.085

Next, Relate The Tables In Power BI

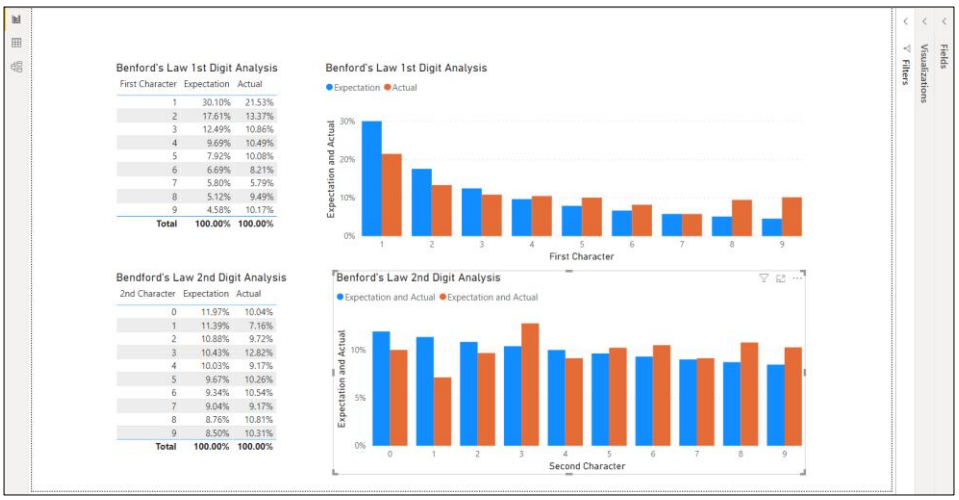
- The last step before dragging-and-dropping fields to create your Power BI visualizations is to relate the three tables in your dataset, as shown below



Now, You Can Create Your Report

- A ***page*** on a ***report*** can contain multiple ***tiles,*** and a ***report*** can contain multiple ***pages***
- For example, the report shown on the next slide contains four tiles on a single page
- Of course, you could easily add more tiles (space permitting) on that page, and you could easily add more pages to this report on which you could place other fraud detection/monitoring metrics

Sample Benford's Law Test



AICPA Audit Data Analytics Initiatives

- The AICPA has established an **Audit Data Standard** working group to develop a standardized data model that facilitates data analytics
- To date, three standards have been published – 1) **Base Standard**, 2) **General Ledger Standard**, and 3) **Order to Cash Subledger Standard**
- By creating a standardized data layout, **auditors can apply "repeatable, refreshable" processes** to data, getting us much closer to real-time data analysis, fraud detection, and audit testing

AICPA Audit Data Analytics Initiatives

- The AICPA has published "Guide to Audit Data Analytics"
- The guide is intended to encourage auditors to make more and better use of data analytics during an audit
- The AICPA believes using the guide should help auditors
  - Enhance traditional audit procedures
  - Contribute to every phase of an audit
  - Offer new ways of visualizing and analyzing results

AICPA Audit Data Analytics Initiatives

- The AICPA has published a document on how auditors can use Python, an open-source programming language, to analyze data for suspicious patterns
- For example, evidence shows that fraudulent journal entries are often entered after regular business hours, on the weekends, and/or by those who ordinarily don't enter journal entries
- You can write and run Python procedures to analyze journal entries (and other transactions) for suspicious characteristics

AICPA Audit Data Analytics Initiatives

*TRADITIONAL AUDIT PROCEDURES	INDUSTRY	AUDIT ASSERTION OR OBJECTIVE OF THE PROCEDURE	PHASE OF AUDIT
a. Examine population for missing or incomplete journal entries.	General	Completeness and accuracy	Interim and year-end
b. Examine possible duplicate account entries.	General	Completeness	Interim and year-end
c. Examine round-dollar entries.	General	Completeness and accuracy	Interim and tear-end
d. Examine post-date entries.	General	Completeness and accuracy	Interim and year-end
e. Examine entries posted on weekends.	General	Completeness and accuracy	Interim and year-end

All potential indicators of fraud.

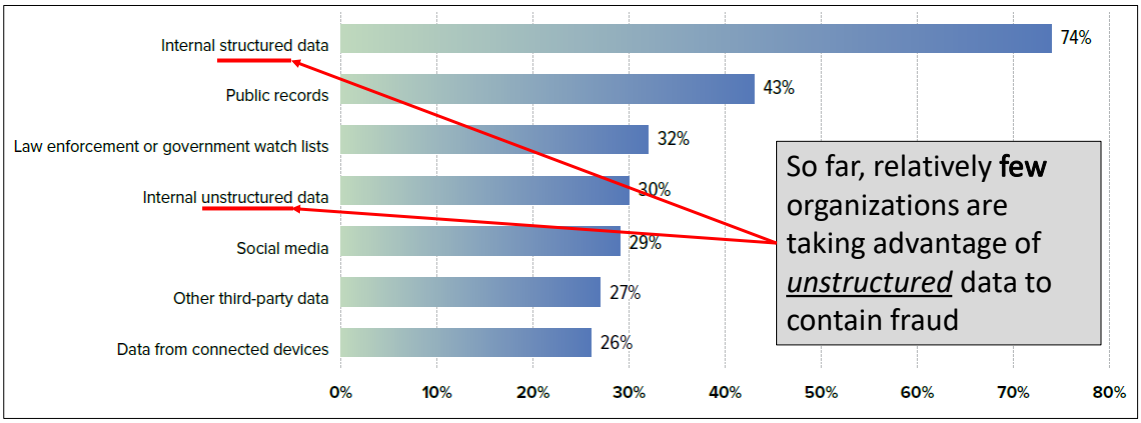
Summarizing AI And Fraud Detection

- Clearly, **yesterday's approaches are not working as well as we need them to prevent, detect, and deter fraud** in today's business climate
- We **need automated tools** that can analyze data in real-time, or very near real-time, and let us know when conditions appear suspicious
- **AI and other emerging technologies offer great promise** as fraud prevention and detection tools
- But you also have significant capabilities to develop real-time monitoring with the overused **Excel spreadsheet, Microsoft Access queries, and Power BI**

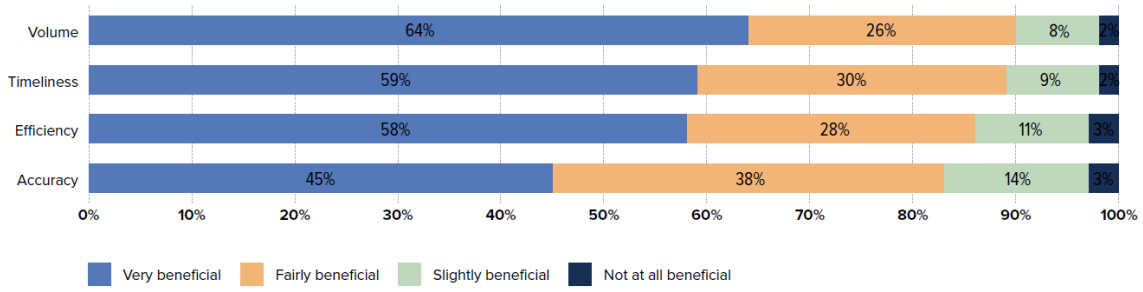
Anti-Fraud Technology Benchmarking Report

- Was published in 2019 by the **Associated of Certified Fraud Examiners in partnership with SAS**
- The Report encapsulates the responses sent to a survey of over 41,000 accounting, auditing, and forensic specialists
- The Report recognizes **that technology is a double-edged sword concerning fraud – it provides opportunities to commit fraud, but it also supplies tools to combat fraud**
- The Report seeks to identify those technologies that will help to mitigate fraud risk and provide positive ROI

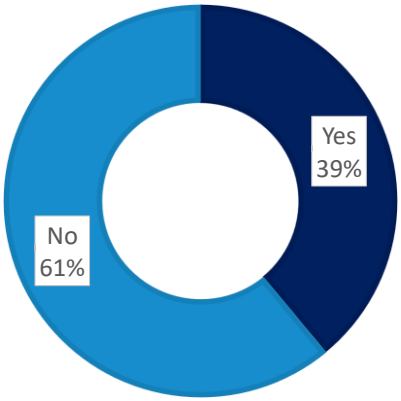
Most Organizations Are Using Data Analytics To Some Degree



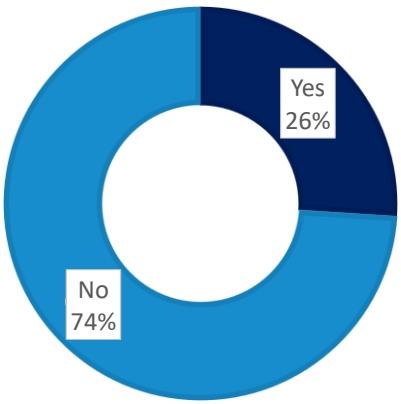
How Beneficial Have Data Analytics Been In Analyzing Data



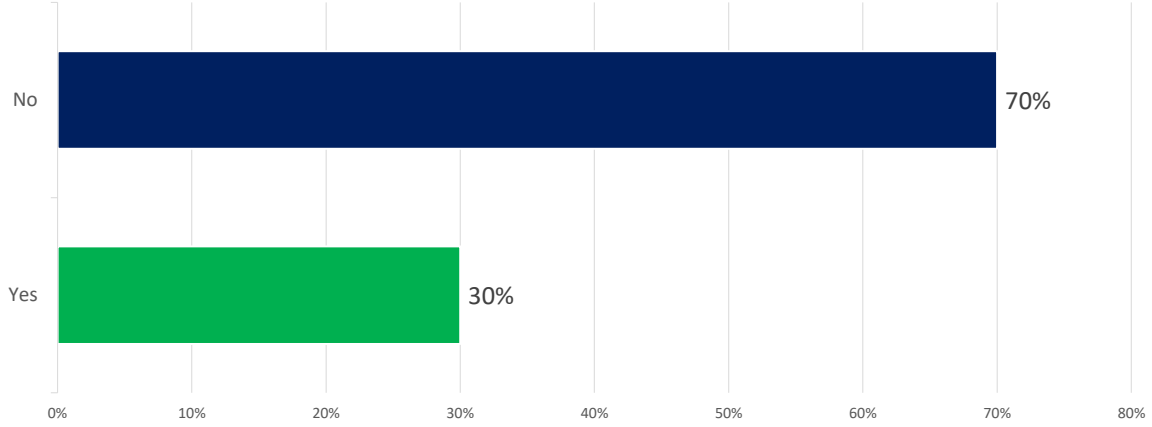
How Many Organizations Use Case Management Programs To Track Cases



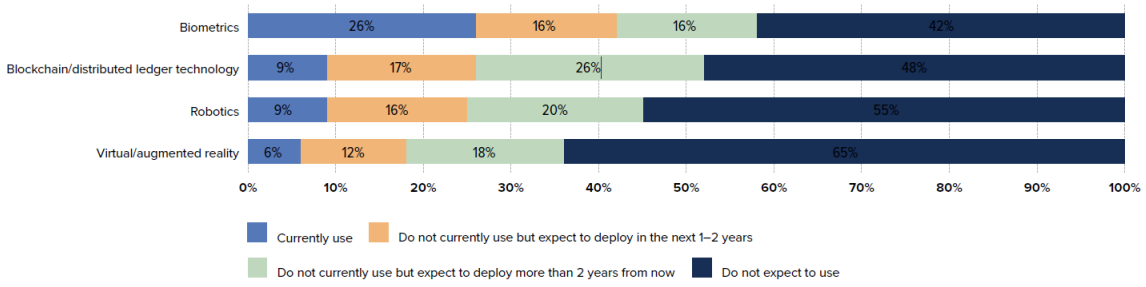
How Many Organizations Use Digital Forensics And e-Discovery Software



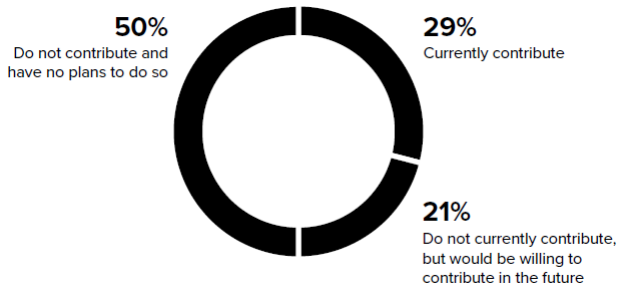
What Percentage Of Companies Use Online-Evidence Gathering Software?



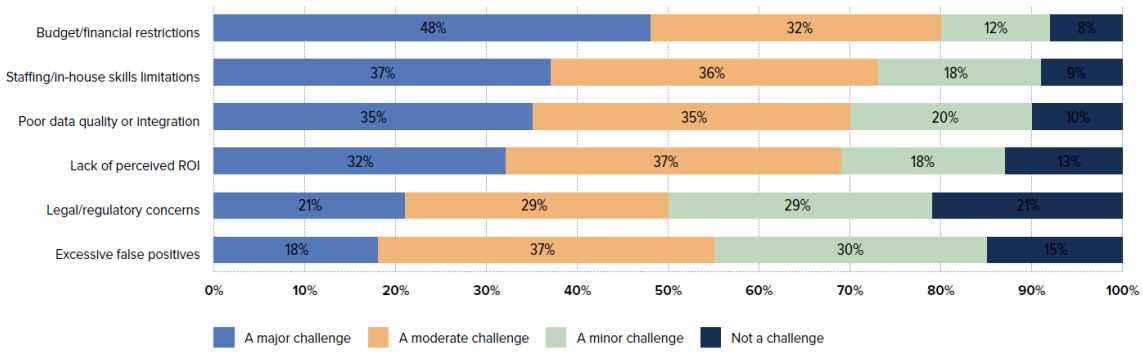
What Emerging Technologies Are Being Used To Fight Fraud?



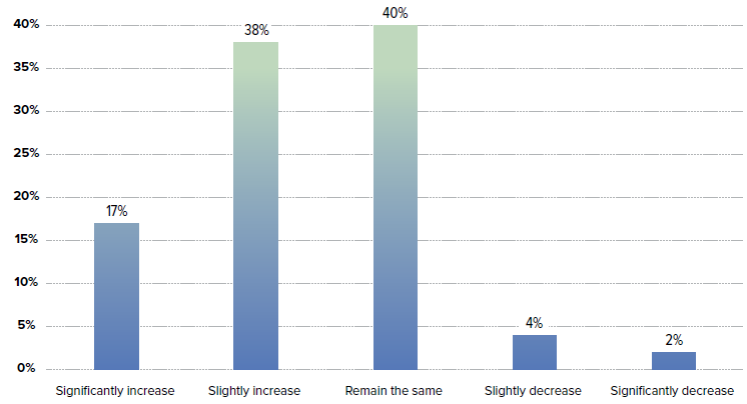
Does Your Organization Share Fraud-Related Data?



What Are Your Challenges With Anti-Fraud Technology?



What Changes Will Occur In Your Anti-Fraud Tech Budget For Next 2 Years?



SUMMARY

To Wrap It Up

- **We cannot afford to overlook fraud** in our (clients') businesses today…it is a significant drain on profit
- Unfortunately, **many frauds originate from outdated internal control structures** that fail to recognize the importance of technology on both sides of the fraud equation
- Yet, that need not be the case with so **many great technology tools available today to help us prevent, detect, and deter fraud**
- ***Take advantage of the right tools for you and provide a positive ROI to reclaim those lost profits***!

THANKS AND BEST OF LUCK!