



# Governmental Auditing

## *Tools and Techniques*

# Tommy Stephens



---

CPA from Woodstock, Georgia

---

Partner, K2 Enterprises

---

Thirty-eight years public accounting & private industry experience

---

BSBA (Accounting) Auburn University

---

MS (Finance) Georgia State University

---

Please contact me: [tommy@k2e.com](mailto:tommy@k2e.com)

---

Follow me on Twitter: [@TommyStephens](https://twitter.com/TommyStephens)

## A Lot To Cover Today & Tomorrow!



Governmental Fraud Update



Excel Tips And Techniques



AI As An Auditing Tool



Designing And Testing Controls



*The news continues to be bad...*

## **GOVERNMENTAL FRAUD UPDATE**



*Occupational Fraud 2024: A Report To The Nations*

## **INFO FROM THE ASSOCIATION OF CERTIFIED FRAUD EXAMINERS**

# The Fraud News Is Still Really Bad!



## The Current State Of Affairs



- Fraud plagues US businesses as never before, and virtually every survey and study conducted on the subject bears this out
- KPMG reported:  
*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.*

# Findings From The Association Of Certified Fraud Examiners (ACFE)



- Occupational fraud consumes 5% of all business revenues
- Annual occupational fraud losses are approximately **\$5 trillion** worldwide
- Average loss per case was \$1,662,000
- A typical fraud causes losses of \$12,000 per month and continues for twelve months before discovery
- The median loss for occupational fraud is \$145,000



*We encourage you to download the report...*

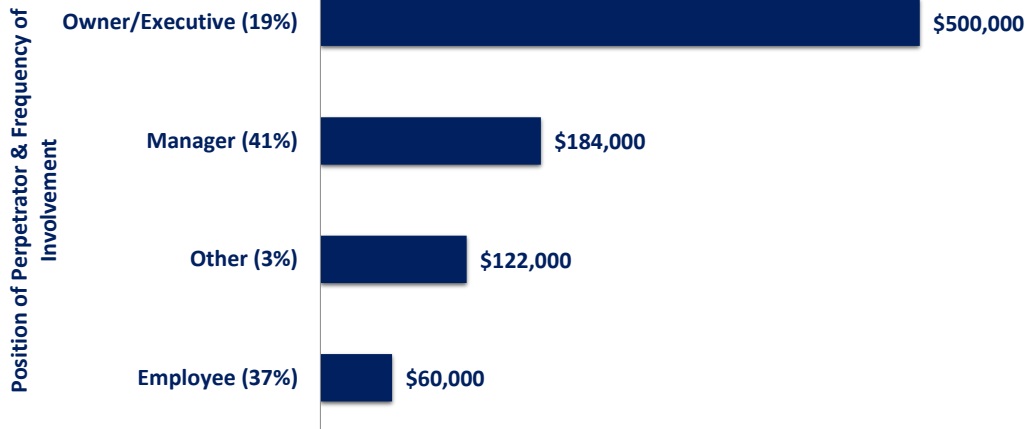
[HTTPS://LEGACY.ACFE.COM/REPORT-TO-THE-NATIONS/2024/](https://legacy.acfe.com/report-to-the-nations/2024/)

# Fraud On An International Level



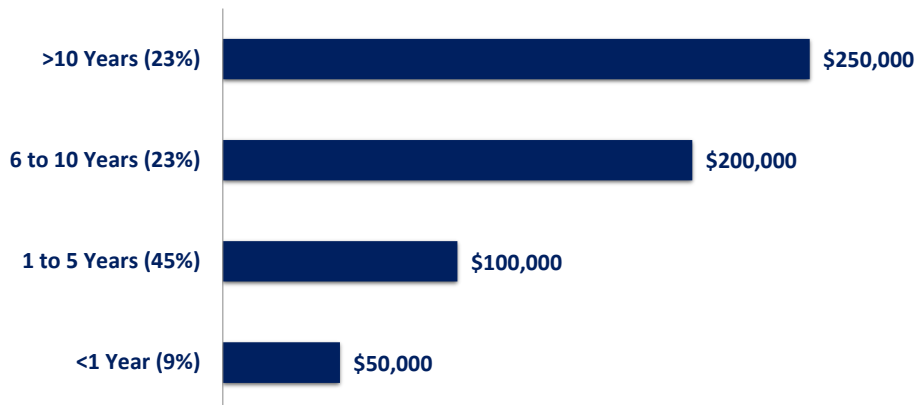
- Fraud transcends borders and is not limited to just the United States
- Selected median fraud losses by region
  - Asia-Pacific: \$200,000
  - Eastern Europe & Western/Central Asia: \$200,000
  - Latin America & The Caribbean: \$250,000
  - Middle East & North Africa: \$163,000
  - Southern Asia: \$100,000
  - Sub-Saharan Africa: \$128,000
  - United States & Canada: \$120,000
  - Western Europe: \$181,000

## Position Of Fraud Perpetrator In The United States And Canada





## Perpetrator's Tenure Median Loss And Frequency

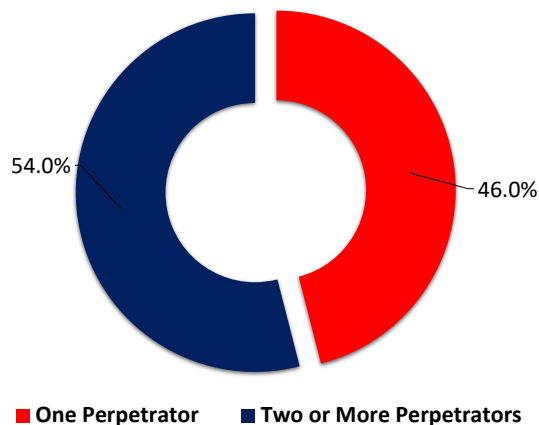


## Number Of Months To Detect Fraud, By Position

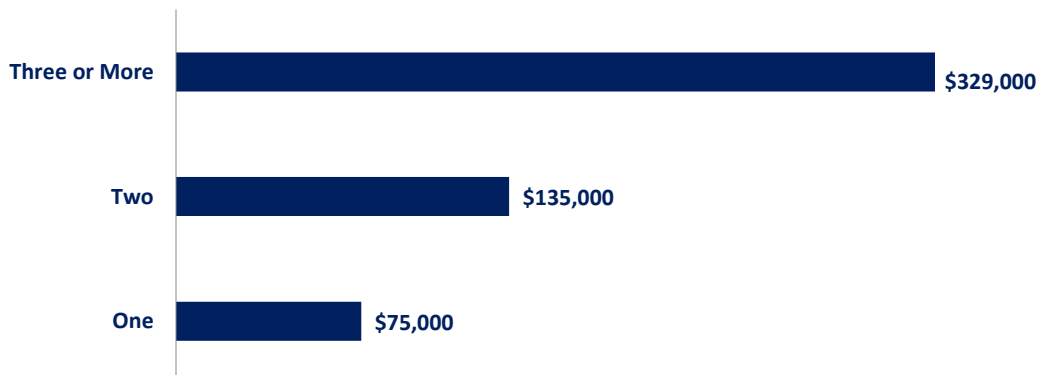




## Collusion Is Involved In Over Half Of Reported Fraud Cases



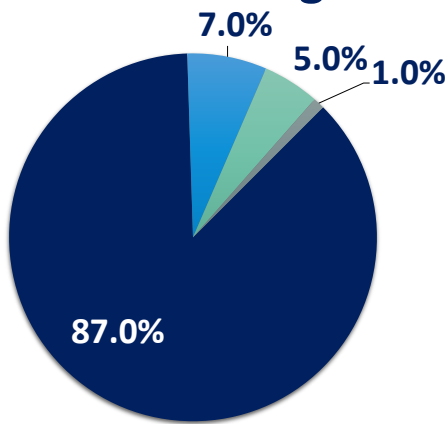
## Fraud Losses Are Higher With Multiple Perpetrators







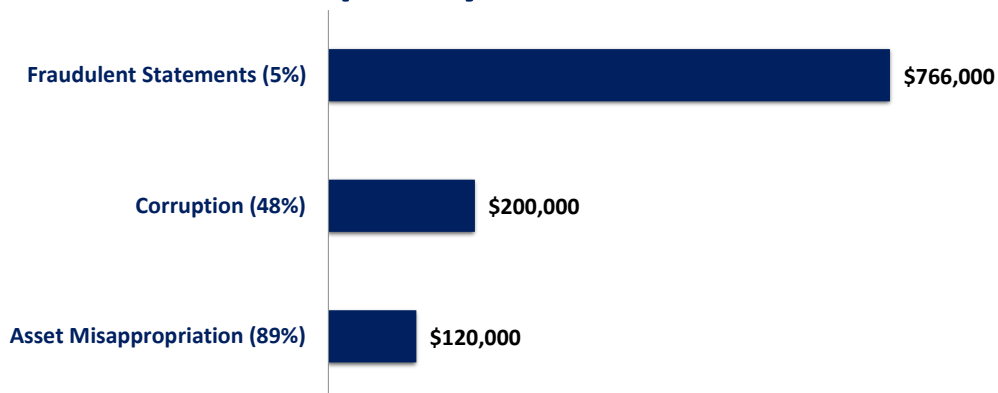
## Who Is Committing Fraud?



■ Never Charged or Convicted ■ Charged, But Not Convicted ■ Prior Convictions ■ Other

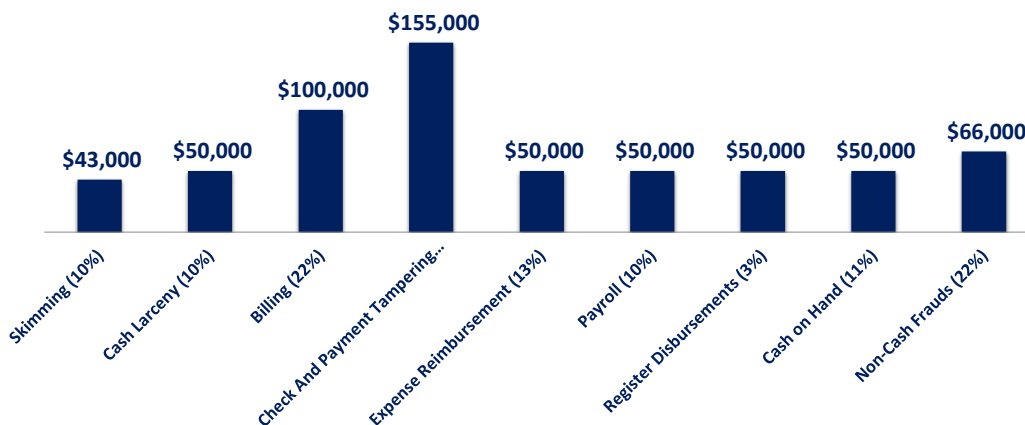


## Types Of Frauds Committed, Frequency And Losses

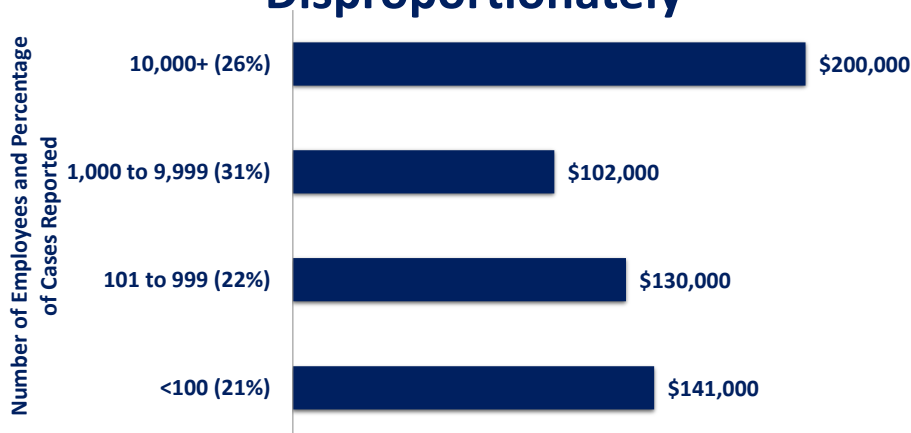




## Relative Risks Of Asset Misappropriation Frauds

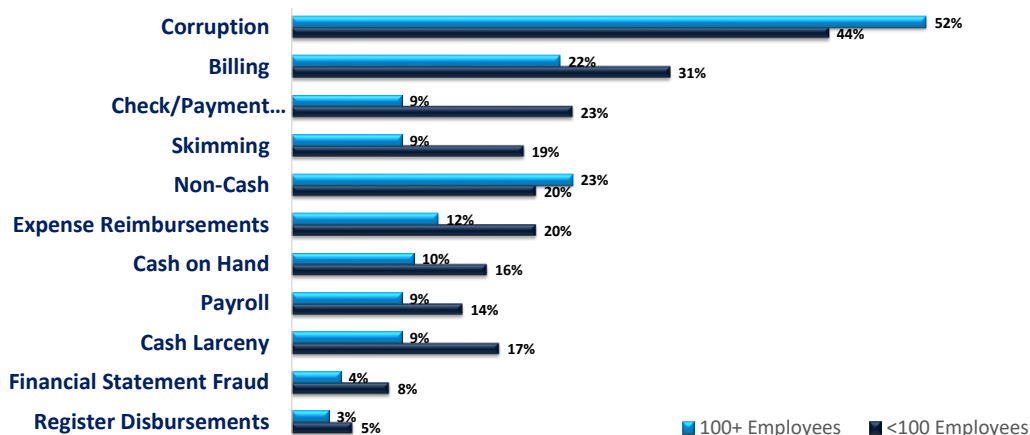


## Fraud Impacts Smaller Organizations Disproportionately

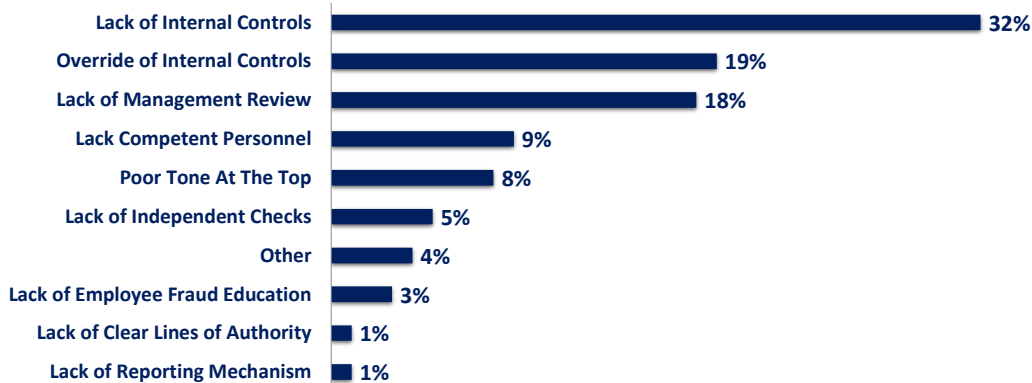




## Smaller Organizations Face Different Fraud Risks

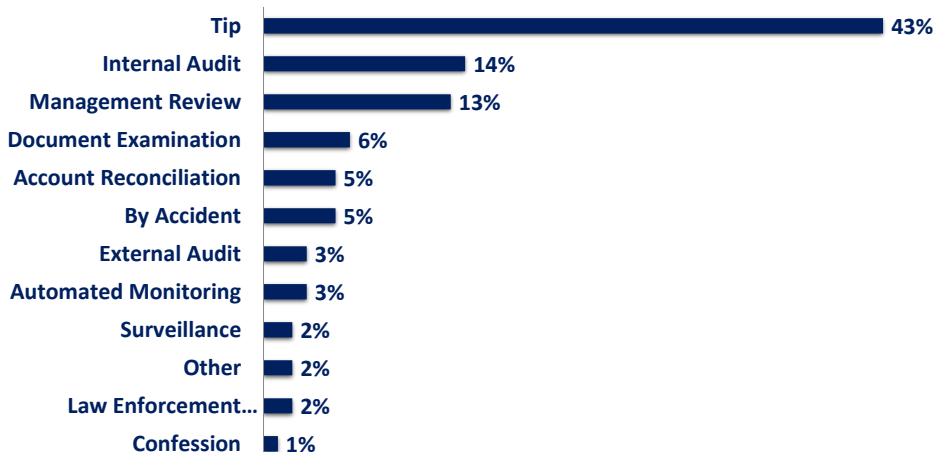


## Internal Control Weaknesses That Contribute To Occupational Fraud

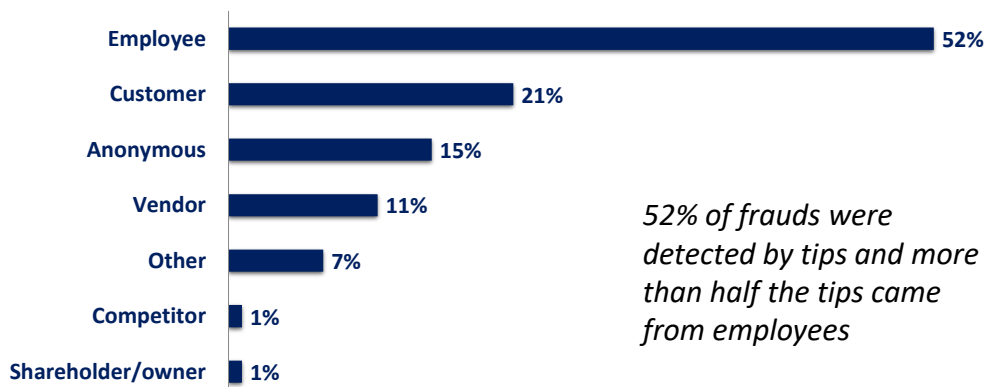




## How Frauds Are Detected



## Sources Of Tips For Occupational Fraud



*52% of frauds were detected by tips and more than half the tips came from employees*

# The Role Of Accountants And Auditors



- Clearly, occupational and organizational fraud is an international economic epidemic, the effects of which are only now being fully understood and quantified
- It is necessary to understand that fraud is not new
  - Headlines involving fraud might cause one to assume that fraud is a relatively new phenomenon
- Accountants and auditors must be equipped with more than just professional standards to prevent and detect fraud
  - We have the responsibility for preventing and detecting fraud, recovering lost profits, and restoring faith and confidence in the financial reporting system



## FRAUD IN GOVERNMENTAL ENTITIES

## Key Stats In Governmental Frauds



Median Loss

\$150,000

Mean Loss

\$2,306,000

Duration

12 months

## Governmental Fraud Perpetrators



Executive

\$313,000

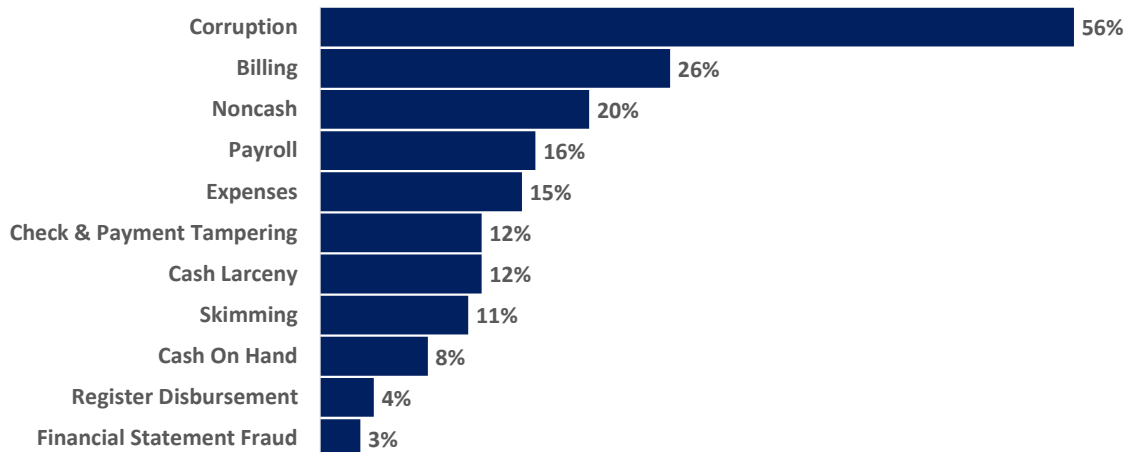
Manager

\$224,000

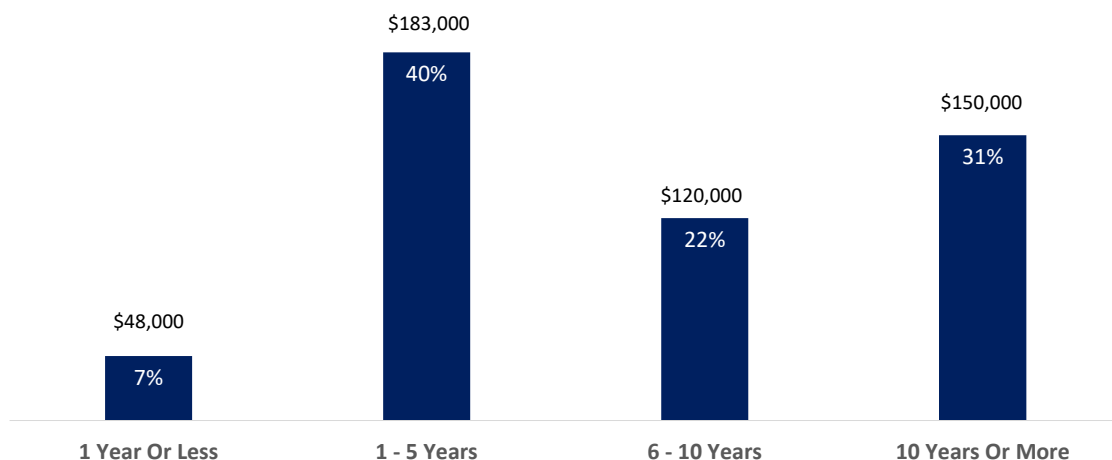
Employee

\$50,000

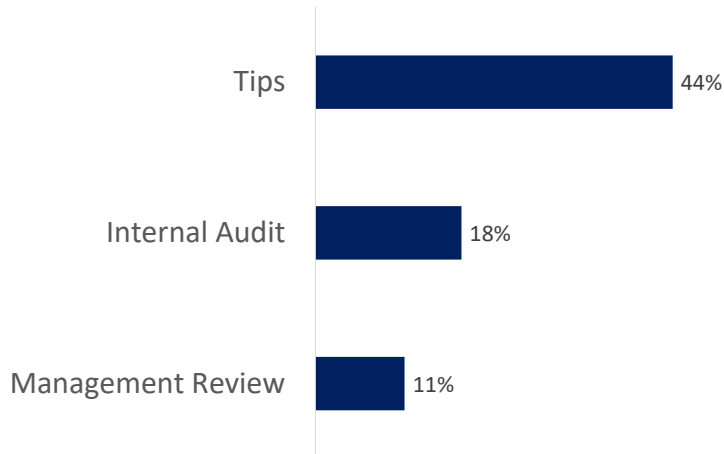
# Governmental Fraud Schemes



# Comparing Tenure To Fraud In Governmental Frauds



# Top Three Governmental Fraud Detection Techniques



## So, What Are The Key Takeaways?



- ***Fraud is alive and well!***
- No organization and no department is immune
- Governmental frauds are particularly problematic (and embarrassing!) because they often involve taxpayer funds or assets purchased from taxpayer funds
- All organizations should be on the lookout for fraud, and auditors have an elevated responsibility!



## Consider These Four Cases



United States vs.  
Carl Zaglin, Also  
Marchena, and  
Francisco Cosenza

Lifecore  
Biomedical, Inc.

HealthSun Health  
Plans, Inc.

COVID-19 Fraud  
Enforcement Task  
Force

## US vs. Zaglin, Marchena, & Cosenza



- This fraud involved a scheme to pay and conceal bribes to Honduran government officials
- In return for the bribes, the defendants gained favor when securing contracts to provide uniforms the Honduran National Police
- The defendants were charged with money laundering, engaging in transactions in criminally derived property, and acts that violated the Foreign Corrupt Practices Act (FCPA)
- \$10 million in contracts and \$160k in bribes were involved

## Lifecore Biomedical



- This fraud also involved bribery and violations of the FCPA
- From May 2018 to August 2019, employees of Yucatan Foods, L.P., paid bribes to Mexican governmental officials to secure a wastewater discharge permit
  - Yucatan Foods was Lifecore's US subsidiary

## HealthSun Health Plans, Inc.



- HealthSun disclosed a scheme to submit false and fraudulent information to US Centers for Medicare and Medicaid Services
- This false information led to an increase in payments to HealthSun of \$53 million
- The fraud covered the five-year span of 2015 until 2020

# COVID-19 Fraud Enforcement Task Force



- This task force is responsible for identifying fraud related to COVID-19 funds
- To date, the task force has charged over 3500 defendants
- Further, the task force has seized/recovered \$1.4 billion in COVID-19 relief funds
- In California, the COVID-19 fraud loss is estimated to be **\$20 billion!**

## Key Provisions Of The FCPA



Anti-Bribery  
Provisions

Accounting  
Provisions

Jurisdiction

Entities  
Covered

# Anti-Bribery Provisions



- Those subject to the FCPA are prevented from offering or giving money to foreign officials, foreign political parties, or political candidates
- Additionally, they may not provide gifts, reimbursement of travel expenses, or other goods or services in an effort to obtain or retain business

# Accounting Provisions



- Publicly-traded companies must maintain adequate records
- They must also establish and maintain strong systems of internal control
  - Proper authorization of transactions
  - Appropriate recordkeeping
  - Segregation of duties

# Jurisdiction



- The FCPA applies to all U.S. persons
- It also applies to foreign issuers of securities
- As amended in 1998, the FCPA also applies to foreign firms and persons who cause or contribute to an act that results in a corrupt payment taking place in the United States



*A “Classic” 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”





## ***CASE STUDY: WHAT COULD HAVE, SHOULD HAVE WILSON'S EMPLOYER DONE TO PREVENT/DETECT THIS?***

### **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

# 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

## The Rita Crundwell Story



## 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

## 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



## ***CASE STUDY: 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.”*

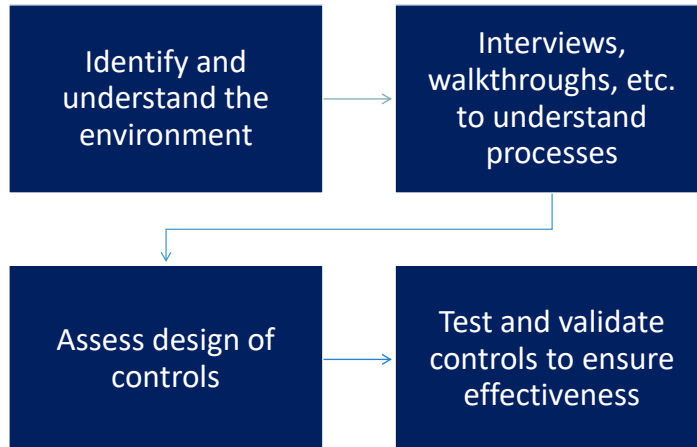
## Technology Controls, In General



- **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 ITGCs 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

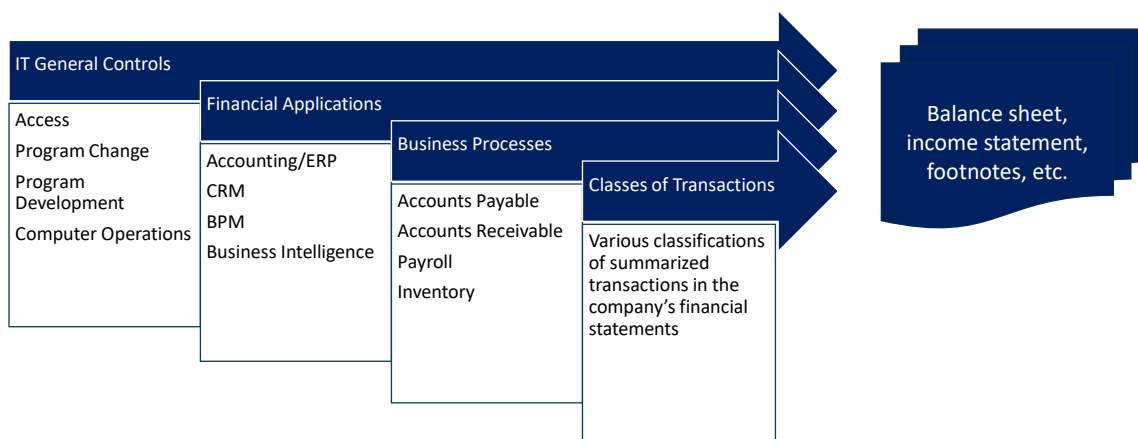
Program  
Changes

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](http://www.somarsoft.com)
- Belarc
  - [www.belarc.com](http://www.belarc.com)
- Wireshark
  - [www.wireshark.com](http://www.wireshark.com)
- Gibson Research Corporation
  - [www.grc.com](http://www.grc.com)

## Access To Programs And Data



### Objectives

Access to programs and data should be restricted to authorized individuals only, based on specific job requirements

### Risks

Unauthorized access to programs or data may lead to improper changes, destruction of data, and/or disclosure to unauthorized parties

### Sample Controls

- Usernames and passwords for logical access
- Review of audit logs

# Sample Tests Of Access Controls



## Sample Control

A formal mechanism exists for providing new users with access to a system, including formally approving the user and establishing specific rights.

Whenever a team member leaves the organization, a formal process exists for immediately disabling access by the user into their account.

The company has a strong password policy in place and all user accounts are in compliance.

## Potential Testing/Validation Option

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.

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.

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	<ul style="list-style-type: none"><li>• Design, authorization, development, testing, and approval controls</li><li>• Configuration change controls</li><li>• Data migration</li></ul>

## 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

Computing assets are available and functioning as intended

## Risk

Computing assets are not available or not performing as intended

## Sample Controls

- Monitoring
- Backup and recovery procedures
- Patch management controls

# Computer Operations Controls Tests



## Sample Control

Jobs and applications are monitored to ensure successful completion.

All critical data is backed up contemporaneously and stored in an appropriate medium and location.

A process exists for identifying, escalating, and resolving end-user technology-related problems that could affect accuracy and efficiency of efforts.

## Potential Testing/Validation Option

Review job and application logs for indications of failed jobs and for follow-up and corrective actions where failed jobs were noted.

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.

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

*40% of these are associated  
with access risk*

## 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

# Common Control Policies



- 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





# ***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

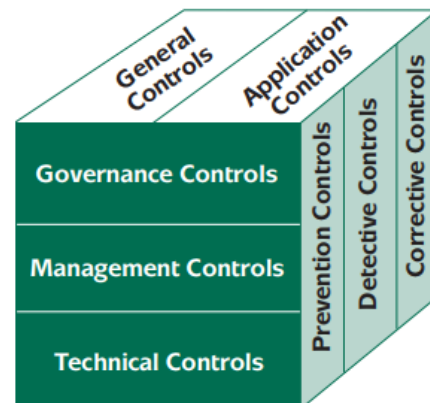


- ITACs are applied to the specific ***user, application, or business process level***
  - Contrasted to ITGCs, which are applied at a much higher level, such as at the network level
- To illustrate, an **ITGC might be applied to allow a user to sign in to a network and may even control which apps the 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, payroll, 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



<b>Process Name/Description</b>	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.
<b>Objective</b>	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.
<b>Risk</b>	Very high. Terminated employees may be emotional and have malicious intentions with respect to Company-owned systems and data.
<b>Control Description</b>	IT decommissions user access immediately for all terminated team members so as to prevent improper – and potentially – malicious access to Company systems and data.
<b>Control Category</b>	Access to programs and data
<b>Type of Control</b>	Preventive
<b>Frequency Performed</b>	On-Demand

# Catalog Of Controls



<b>Process Name/Description</b>	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.
<b>Objective</b>	Only authorized users should have access to Company-owned systems and data. Inactive employees are not allowed to access Company-owned systems or data.
<b>Risk</b>	Very high. Terminated employees may be emotional and have malicious intentions with respect to Company-owned systems and data.
<b>Control Description</b>	This test is performed to confirm that no terminated employees maintain access to the Company's information technology assets.
<b>Control Category</b>	Access to programs and data
<b>Type of Control</b>	Detective
<b>Frequency Performed</b>	Monthly

# Catalog Of Controls



<b>Process Name/Description</b>	Compare user rights in the accounting application to each team member's job description to help ensure proper authorization of transactions in the system.
<b>Objective</b>	User rights in the accounting application should align with each user's assigned job responsibilities.
<b>Risk</b>	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.
<b>Control Description</b>	This test is performed to confirm that each user has the appropriate rights in the accounting application, commensurate with their job responsibilities.
<b>Control Category</b>	Access to programs and data, authorization of transactions
<b>Type of Control</b>	Detective, preventive
<b>Frequency Performed</b>	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

- 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

### Tests of Effectiveness

- 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**

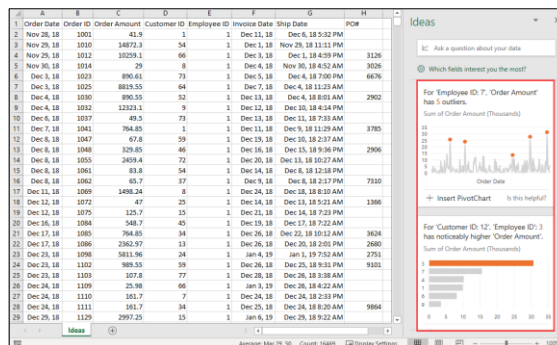
# You May Have Access To Some AI Tools Now



- **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





*A reminder...*

## **FIVE COMMON GOVERNMENT AUDIT FINDINGS**

## **Five Common Findings**

*CohnReznick Study*



Timekeeping



Subcontractors



Meals and  
Entertainment



Air Travel



Proof of  
Payment



# Timekeeping Issues



- Time records, both electronic and manual, should have evidence of approval by employee/contractor and supervisor
- If circumstances exist that prevent timely approval by the supervisor and someone else signs instead, the manager should re-sign the records as soon as possible after initial approval
- Also, time records should provide sufficient description of the work performed to ascertain were the hour reasonable

# Subcontractors



- Work performed by subcontractors is generally subject to the same rules as if the prime contractor performed the work on a project
- Common audit findings in this area center around a lack of documentation substantiating the need for using subcontractors, the work performed by subcontractors, and the rates charged by subcontractors

# Meal And Entertainment Costs



- Like in the private sector, M&E expenses can be problematic in governmental environments too
- Itemized receipts should be obtained and submitted by those seeking reimbursement to substantiate that the expenditures were, in fact, reasonable and necessary
- Further, IRS-required documentation must be maintained for tax-compliance purposes

# Air Travel



- Generally accepted practices (including FAR) prohibit airfare costs more than the lowest priced airfare available during normal business hours, except in cases of extraordinary circumstances faced by the traveler
  - Excessive layovers, circuitous routing, travel during unreasonable hours, etc.
- Fly America Act requires federal travelers to use United States-based air carrier services for all travel funded by US government

## Proof Of Payment



- Adequate documentation must exist to support payments made to vendors, contractors, and even employees
- Controls should be in place to ensure that payments are not made based on canceled purchase orders
- Further, vendor invoices and similar documentation should be corroborated by cancelled checks, banks statements, EFT confirmations, and similar documents

## Where Is Segregation Of Duties?



- Shouldn't proper segregation of duties help curtail these frauds and ensure organizational objectives are met?
- **OF COURSE, IT SHOULD!!!**
- OK, so how do we achieve proper segregation of duties?



# What's The Common Element?



## The Common Element

- Notice that documentation – more specifically, ***lack of documentation*** – is the common element across all five categories of these findings
- This condition will likely be the case in many of the audits, reviews, and investigations you work on
- Always be on the lookout for adequate and appropriately authorized contemporaneous, valid documentation
- In the absence of this documentation, you may have a finding that must be documented and addressed



## EXCEL AS AN AUDITING TOOL



*As promised, we've covered a lot of information!*

## WRAPPING UP



tommy@k2e.com

**I THANK YOU VERY MUCH!**