K2's Case Studies In Fraud And Technology Controls

Copyright 2023, K2 Enterprises, LLC

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

Follow me on Twitter: @TommyStephens

Copyright 2023, K2 Enterprises, LLC

Learning Objectives

Upon completing this session, 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

Copyright 2023, K2 Enterprises, LLC

Copyright © 2023, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises' training event is prohibited.

FRAUD – THE CURRENT STATE OF AFFAIRS

Copyright 2023, K2 Enterprises, LLC

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?

Copyright 2023, K2 Enterprises, LLC

Copyright © 2023, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises' training event is prohibited.

Primary Types Of 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*

Copyright 2023, K2 Enterprises, LLC

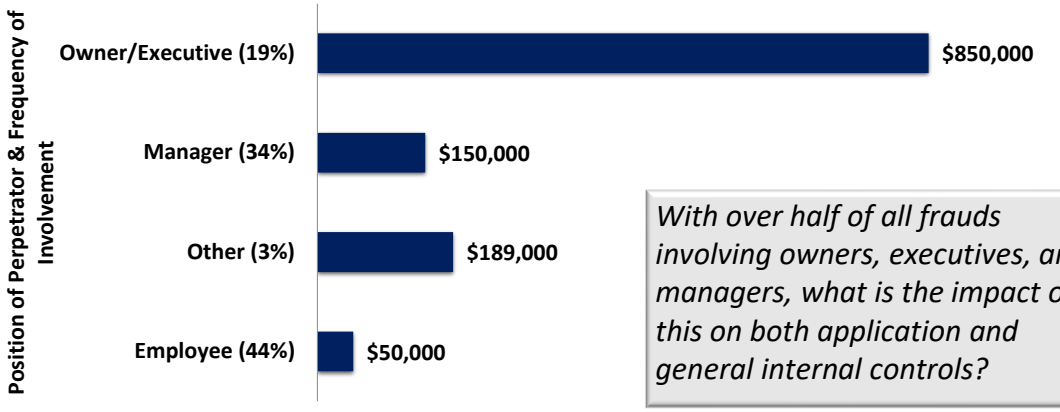
Findings From ACFE

- The following numbers are from the **Report to the Nations on Occupational Fraud and Abuse**
- Fraud consumes 5% of all business revenues
- Annual occupational fraud losses approximately $4 trillion worldwide and $929 billion in the United States
- On a per-employee basis, fraud costs on average $7,369 per full time worker, per year in the U.S. and $5,138 per full time worker, per year in Canada

Copyright 2023, K2 Enterprises, LLC

Copyright © 2023, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises' training event is prohibited.

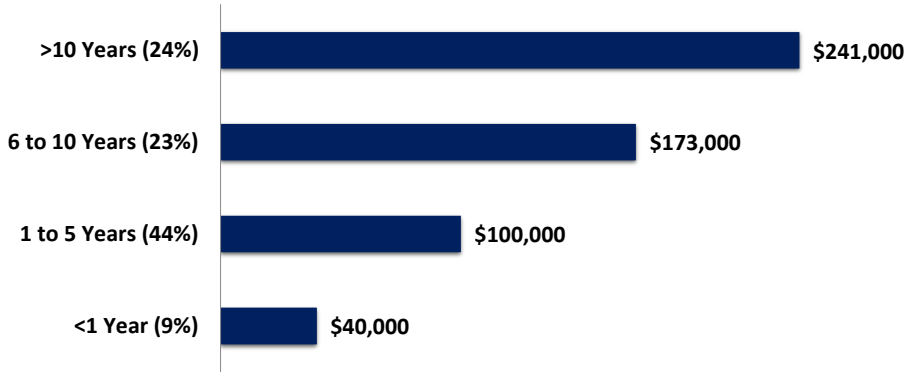
Perpetrator Position



With over half of all frauds involving owners, executives, and managers, what is the impact of this on both application and general internal controls?

Copyright 2023, K2 Enterprises, LLC

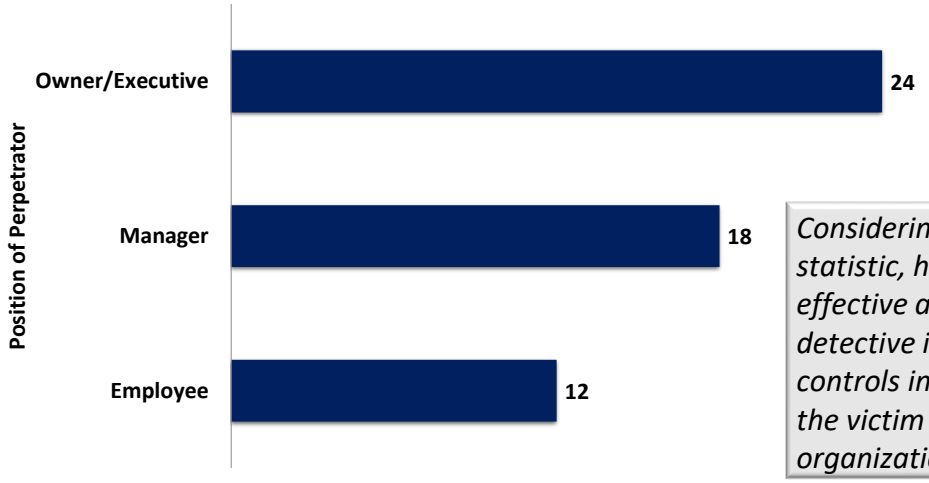
Effect Of Perpetrator's Tenure



Copyright 2023, K2 Enterprises, LLC

Copyright © 2023, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises' training event is prohibited.

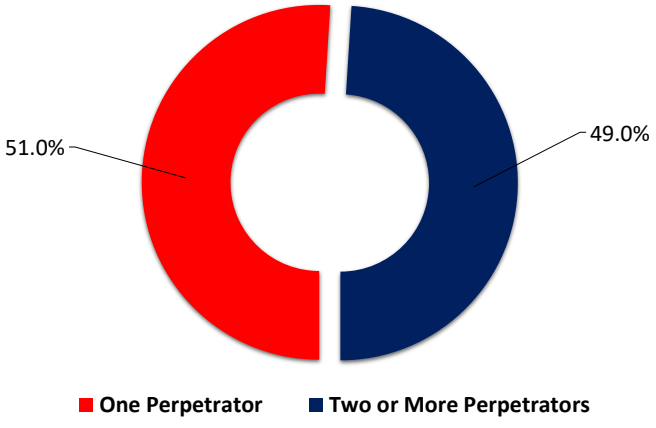
Months To Detect Fraud, By Position



Considering this statistic, how effective are the detective internal controls in many of the victim organizations?

Copyright 2023, K2 Enterprises, LLC

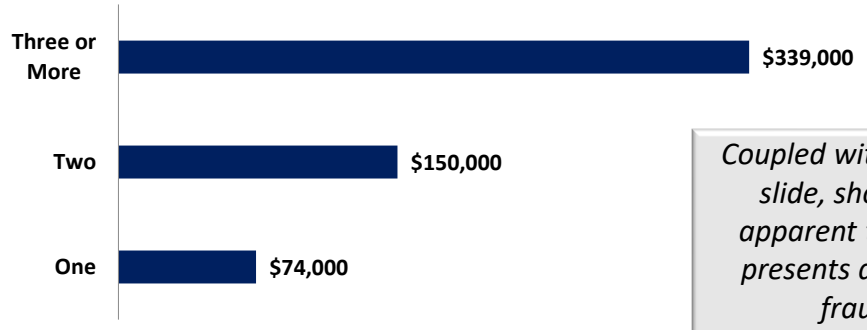
Frauds Involving Collusion



Copyright 2023, K2 Enterprises, LLC

Copyright © 2023, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises' training event is prohibited.

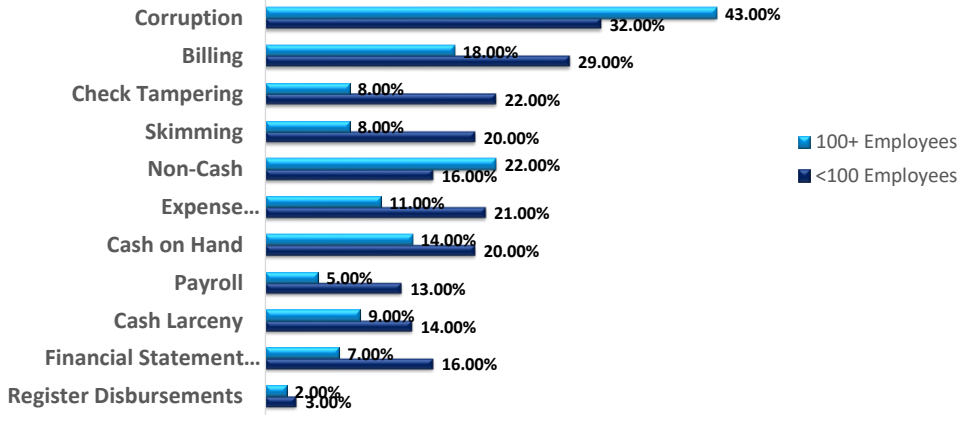
Impact Of Collusion On Losses



Coupled with the previous slide, shouldn't it be apparent that collusion presents a tremendous fraud risk?

Copyright 2023, K2 Enterprises, LLC

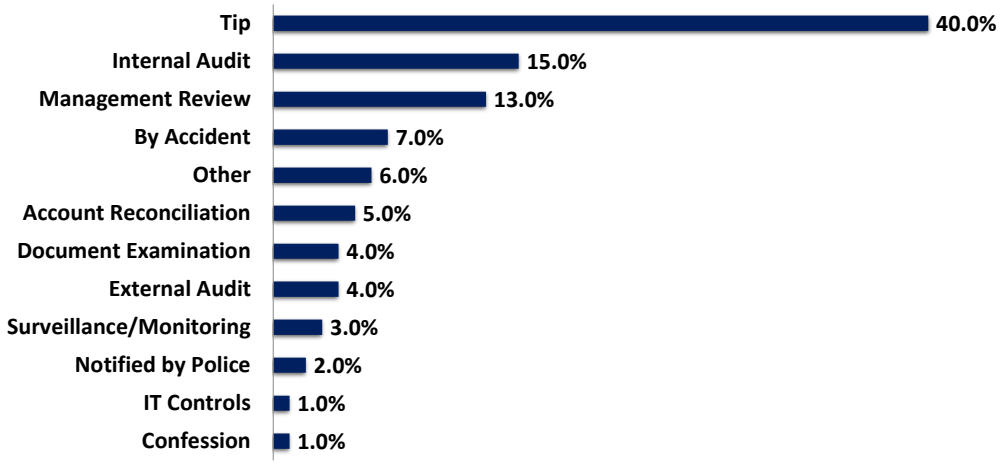
Small Businesses Fraud Risks



Copyright 2023, K2 Enterprises, LLC

Copyright © 2023, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises' training event is prohibited.

How Frauds Are Detected



Copyright 2023, K2 Enterprises, LLC

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 no single method or technology will be effective by itself…as always, a good 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 stated organizational objectives

Copyright 2023, K2 Enterprises, LLC

Copyright © 2023, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises' training event is prohibited.

CASE STUDIES IN FRAUD

Copyright 2023, K2 Enterprises, LLC

Mulder Steals Over $1.5 Million

- On May 15, 2017, Elizabeth "Lizzy" Mulder plead guilty to stealing over $1.5 million over seven years
- 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

Copyright 2023, K2 Enterprises, LLC

Copyright © 2023, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises' training event is prohibited.

Mulder Steals Over $1.5 Million

- On May 15, 2017, Elizabeth "Lizzy" Mulder plead guilty to stealing over

The kicker is that Mulder stole from friends and clients!

- 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

Copyright 2023, K2 Enterprises, LLC

Mulder Steals Over $1.5 Million

- 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 own 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 her clients

Copyright 2023, K2 Enterprises, LLC

Copyright © 2023, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises' training event is prohibited.

The Elizabeth Mulder Fraud

Copyright 2023, K2 Enterprises, LLC

Mulder Steals Over $1.5 Million

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

Copyright 2023, K2 Enterprises, LLC

Copyright © 2023, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises’ training event is prohibited.

Mulder Steals Over $1.5 Million

- In one of the more bizarre twists in this case, 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

Copyright 2023, K2 Enterprises, LLC

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

Copyright 2023, K2 Enterprises, LLC

Copyright © 2023, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises' training event is prohibited.

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

Copyright 2023, K2 Enterprises, LLC

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

Copyright 2023, K2 Enterprises, LLC

Copyright © 2023, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises' training event is prohibited.

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, etc. – common internal control weaknesses in small businesses
  - 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…

Copyright 2023, K2 Enterprises, LLC

West Melbourne Police Department Press Conference

Copyright 2023, K2 Enterprises, LLC

Copyright © 2023, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises’ training event is prohibited.

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

Copyright 2023, K2 Enterprises, LLC

CYNTHIA MILLS AND MATTHEWS INTERNATIONAL

Copyright 2023, K2 Enterprises, LLC

Copyright © 2023, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises' training event is prohibited.

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 a gambling addiction as the fraud driver

Copyright 2023, K2 Enterprises, LLC

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 criminally-derived property

Copyright 2023, K2 Enterprises, LLC

Copyright © 2023, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises' training event is prohibited.

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

Copyright 2023, K2 Enterprises, LLC

Cynthia Mills And Matthews International

Copyright 2023, K2 Enterprises, LLC

Copyright © 2023, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises' training event is prohibited.

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

Copyright 2023, K2 Enterprises, LLC

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

Copyright 2023, K2 Enterprises, LLC

Copyright © 2023, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises' training event is prohibited.

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

Copyright 2023, K2 Enterprises, LLC

PREVENTING AND DETECTING FRAUD WITH TECHNOLOGY CONTROLS

Copyright 2023, K2 Enterprises, LLC

Copyright © 2023, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises' training event is prohibited.

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."*

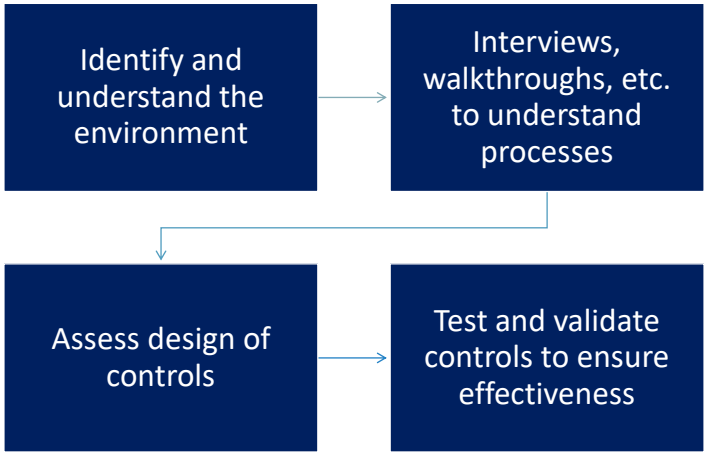
Copyright 2023, K2 Enterprises, LLC

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

Copyright 2023, K2 Enterprises, LLC

Copyright © 2023, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises' training event is prohibited.



Working With Technology Controls Is No Different Than Working With Other Controls

Copyright 2023, K2 Enterprises, LLC

IT controls are divided into two, more focused categories

IT General Controls (ITGCs)

IT Application Controls (ITACs)

Copyright 2023, K2 Enterprises, LLC

Copyright © 2023, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises' training event is prohibited.

EVALUATING INFORMATION TECHNOLOGY GENERAL CONTROLS

Copyright 2023, K2 Enterprises, LLC

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 properly 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

Copyright 2023, K2 Enterprises, LLC

Copyright © 2023, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises' training event is prohibited.

ITGCs Typically Focus On 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

Copyright 2023, K2 Enterprises, LLC

The Importance Of ITGCs

- ITGCs are the controls that should be in place to **provide reasonable** assurance with respect to 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

Copyright 2023, K2 Enterprises, LLC

Copyright © 2023, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises' training event is prohibited.

ITGCs are often broken into four groups

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

Copyright 2023, K2 Enterprises, LLC

Some Free Tools To Assist You…

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

Copyright 2023, K2 Enterprises, LLC

Copyright © 2023, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises' training event is prohibited.

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

Copyright 2023, K2 Enterprises, LLC

Examples Of How To Test 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.

Copyright 2023, K2 Enterprises, LLC

Copyright © 2023, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises' training event is prohibited.

Top 10 ITGC Deficiencies

Information Technology General Controls and Best Practices, Warren Averett, April 5, 2016

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

Copyright 2023, K2 Enterprises, LLC

Top 10 ITGC Deficiencies

Information Technology General Controls and Best Practices, Warren Averett, April 5, 2016

1. Terminated employees still active in systems and network
2. Lack of segregation of duties over development and production environments
3. Lack of critical ap… resulting in little … knowledge of vuln…
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. …d disaster recovery plans …esting completed … applications and full IT 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 2023, K2 Enterprises, LLC

Copyright © 2023, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises' training event is prohibited.

Policies – A Key Component Of Effective ITGCs

A great resource for technology control templates remains The SANS Institute's Security Policy Project (https://k2e.fyi/SANSPolicies) or https://www.sans.org/security-resources/policies/)

Copyright 2023, K2 Enterprises, LLC

EVALUATING INFORMATION TECHNOLOGY APPLICATION CONTROLS

Copyright 2023, K2 Enterprises, LLC

Copyright © 2023, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises' training event is prohibited.

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*."

Copyright 2023, K2 Enterprises, LLC

The Nature Of ITACs

- ITACs are applied at 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-on 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

Copyright 2023, K2 Enterprises, LLC

Copyright © 2023, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises' training event is prohibited.

Examples Of ITACs And Their Primary Purposes

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

Copyright 2023, K2 Enterprises, LLC

Common Examples Of Common ITACs In Use Today

- 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 field to ensure the proper type of data is being entered…for example, no text entries in a date field
- Audit trail reports to show who did what and when they did it
- Preventing price overrides on accounts payable bills or invoices issued to customers

Copyright 2023, K2 Enterprises, LLC

Copyright © 2023, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises' training event is prohibited.

ANALYZING AND EVALUATING TECHNOLOGY CONTROLS

Copyright 2023, K2 Enterprises, LLC

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**

Copyright 2023, K2 Enterprises, LLC

Copyright © 2023, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises' training event is prohibited.

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

Copyright 2023, K2 Enterprises, LLC

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 be in accordance with their 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

Copyright 2023, K2 Enterprises, LLC

Copyright © 2023, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises' training event is prohibited.

Testing Options Available

- The types of test 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

Copyright 2023, K2 Enterprises, LLC

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 are potentially logging-in using a different username and recording potentially fraudulent transactions. How could the business owner test this and what type of application control would this be?

Copyright 2023, K2 Enterprises, LLC

Copyright © 2023, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises' training event is prohibited.

Sample Test Of ITGC

A member of the IT staff wants to see if, somehow, end-users are able to install software even though they are not supposed to have Administrative rights. If end-users were able to do this, software licensing policies might be potentially violated. Or, potentially malicious software could be installed 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 members computer? What type of control would this be?

Copyright 2023, K2 Enterprises, LLC

SUMMARY

Copyright 2023, K2 Enterprises, LLC

Copyright © 2023, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises’ training event is prohibited.

To Wrap It Up

- We cannot afford to overlook fraud in our (clients') businesses today…it is a major 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 tools that are right for you and provide a positive ROI to reclaim those lost profits!

Copyright 2023, K2 Enterprises, LLC

THANKS AND BEST OF LUCK!

Copyright 2023, K2 Enterprises, LLC

Copyright © 2023, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises' training event is prohibited.