

The background features abstract green geometric shapes. On the left, a solid green trapezoid points towards the center. On the right, a complex arrangement of overlapping translucent green triangles and polygons creates a layered, architectural effect. The text is centered in a clean, green, sans-serif font.

Understanding & Implementing Internal Controls

Internal Controls????



Presentation Objectives

- ▶ Provide an understanding of internal controls and demonstrate how they can protect you and your staff and add value to your work
- ▶ Identify what types of work environments invite fraud and poor work performance
- ▶ Provide some practical ideas on how to implement internal controls at your entity

Things to look forward to: survey, jokes, PowerPoint slide transitions, and fraud case studies

Kahoot Survey

- ▶ Take out your electronic device
- ▶ Type kahoot.it into your browser. Exact website is <https://kahoot.it/#/>
- ▶ Enter the “game pin” that will be given to you
- ▶ Enter a “nickname” for yourself
- ▶ Click “enter”

<https://create.kahoot.it/login>

Internal Control Definition

► Internal control:

“a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations;
- Reliability of financial reporting; and
- Compliance with applicable laws and regulations” (Council of Sponsoring Organizations - COSO)

► Internal controls we use in our personal lives: lock your car, review bills and credit card statements before paying them, keep blank checks safeguarded, tie your shoes, etc.

► Internal controls are procedures or practices that you put in place that make you an effective manager in accomplishing those three objectives.

- Only management can ensure these procedures and practices are followed on a daily basis, as such management is charged with implementation of internal control.
- You get all the glory or blame!

Control Environment - “tone at the top”

- ▶ Control environment determines how well internal controls function
- ▶ “...it is difficult to exaggerate the importance of a good internal control environment for the effectiveness of internal control.” (GAAFR pg. 737)
- ▶ Characteristics of a good control environment:
 - Management has an understanding of internal controls and why they are needed
 - Management is committed to design, implement, and maintain internal controls
 - Management communicates that commitment and helps others understand the “why” of internal control
- ▶ What a good control environment looks like in practice:
 - Management understands their entity’s operations and its compliance and reporting requirements. They have obtained this understanding by asking questions and researching answers. They are not always the experts but have gained sufficient understanding from the experts to create necessary controls
 - Management evaluates their current practices and procedures and ensures they cover the entity’s needs and requirements
 - Management is organized enough to follow-up on current practices and procedures and frequently communicates their importance.
- ▶ Examples of a bad control environment:
 - When accountability for internal controls is questioned, everyone is pointing their finger to someone else
 - You get a blank stare
 - Parenting 101 - Never let your kids think they are in control!

Why do I need to be worried about internal controls? How do they benefit me?

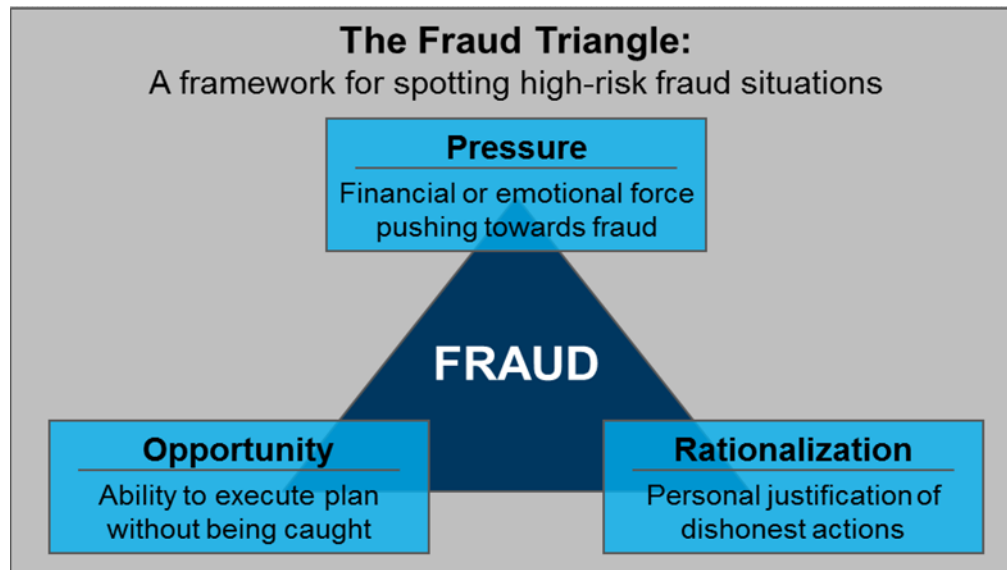
- ▶ Internal controls are implemented to mitigate or eliminate the manager's exposure to risk. What risks do managers need to mitigate or eliminate?
 - Operational Risk
 - ❖ Poor customer service caused by slow payment processing
 - ❖ Employee or customer theft of government assets (cash handling, p-card, equipment)
 - ❖ One employee's abuse can lead to other employees following suit (PTO policies, lunch/scheduled breaks, etc.)
 - Financial Reporting Risk
 - ❖ Cashiers record payments incorrectly due to cashier applying the payment to wrong GL account
 - ❖ Your department is consistently reprimanded for accounting errors
 - ❖ The entity's financial reports are not accurate because transactions are processed inconsistently and are not corrected through reviews
 - Compliance Risk
 - ❖ Bond payment is missed because the wire transfer to the bond fund account was never set up
 - ❖ Checks were not deposited within a three business day period
- ▶ Internal controls improve the accuracy and consistency of your operations
 - Bountiful's balance sheet and income statement reconciliations
 - Monthly reconciliations that speed up yearend reconciliations
- ▶ Internal controls can keep the entity compliant with entity policies, Utah or Federal laws, and binding agreements or contracts
- ▶ Internal controls can prevent theft and fraud from ever happening

Theft & Fraud Overview

- ▶ **Fraud Definition:** wrongful or criminal deception intended to result in financial or personal gain
 - Whenever there is theft by an employee there is some type of fraud covering up the theft. Sometimes fraud indicators are the only clues left behind to identify the theft
- ▶ **Fraud Ramifications:**
 - Reputation of government entity - the media loves theft and fraud stories
 - Termination of employee and potentially supervisors clear up to management level
 - Disruption of department operations and added burden on employees and management
 - Potential withholding of tax money and other grants
- ▶ James Ratley, the President of the Association of Certified Fraud Examiners, said: “We now live in a world where virtually all business and government organizations understand that fraud is a threat they must deal with.”



Theft & Fraud - The Fraud Triangle



- ▶ **Pressure** is what motivates the fraud in the first place. The individual may have financial problems, addictions like gambling, shopping or drugs, or pressure to show good performance or results.
- ▶ **Rationalization** is when an individual thinks they are justified because they are underpaid, or it's for their family, or they need it now but they'll pay it back before anyone notices. The individual justifies the crime in a way that makes it an acceptable or justifiable act.
- ▶ **Opportunity** is created when there are weaknesses in controls. Individuals think they won't get caught because nobody is reviewing their work.

Fraud = “bad people doing bad things” right????



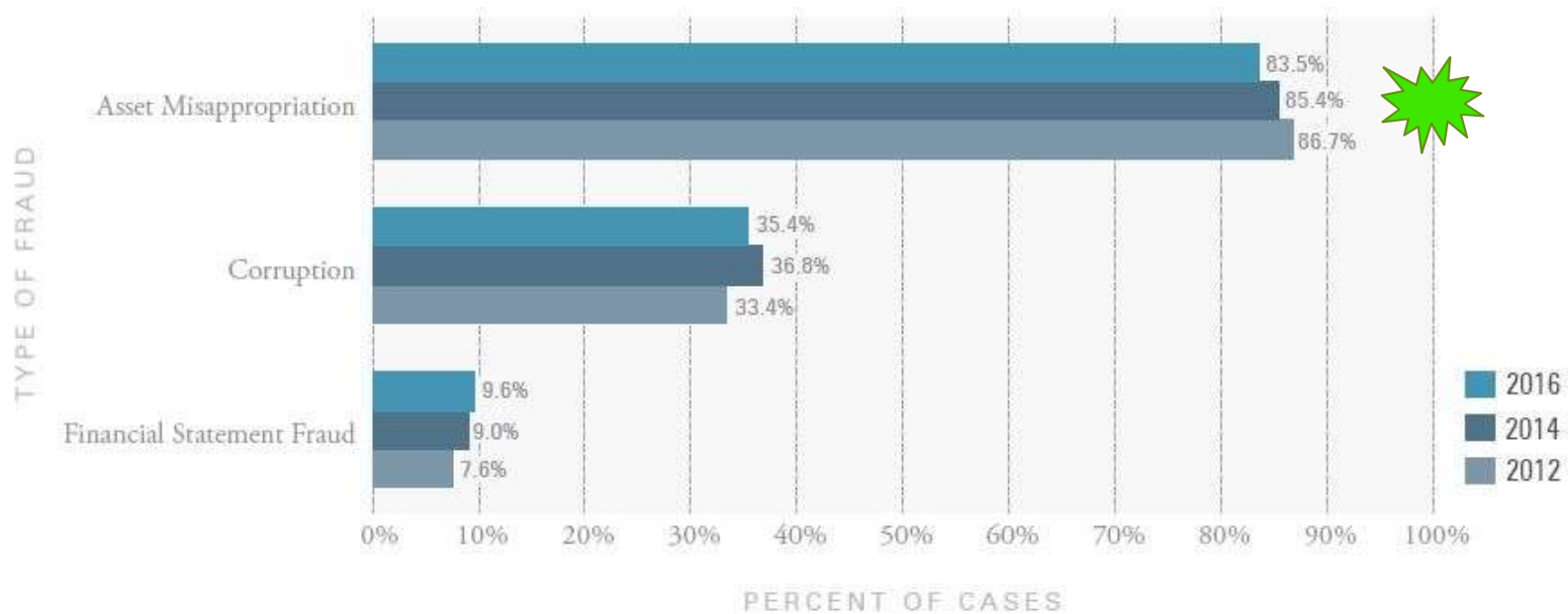
© Scott Adams, Inc./Dist. by UFS, Inc.

Association of Certified Fraud Examiner's (ACFE) - 2016 Report on Occupational Fraud and Abuse

- ▶ Details of the ACFE 2016 report:
 - ▶ This report contains an analysis of 2,410 cases of occupational fraud that were investigated by fraud examiners between January 2014 and October 2015.
 - ▶ The 2,410 cases happened in 114 different countries with 1,038 coming from the US (due to the majority of the associations members being US citizens)
 - ▶ The total loss caused by the 2,410 cases of occupational fraud in the study exceeded \$6.3 billion
- ▶ This study helps us understand general ideas about the types of fraud, how fraud is found, areas most susceptible to fraud, and the role internal controls play in mitigating fraud
- ▶ Understanding how fraud is perpetrated helps us design fraud prevention and detection internal controls

Fraud Facts & Figures - ACFE 2016-2012 global fraud studies

Types of Fraud



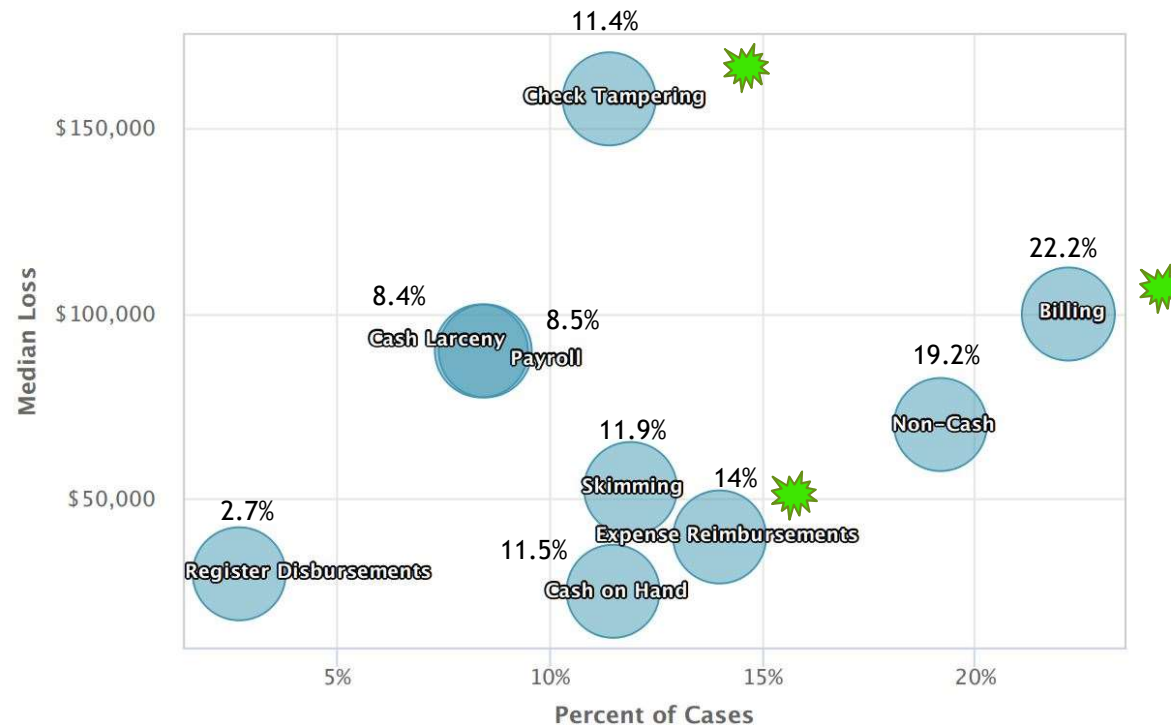
Asset Misappropriation: employee steals or misuses the entity's cash, inventory, or assets/equipment

Corruption: employee uses their influence in a business transaction in order to gain personal benefit

Financial Statement Fraud: employee intentionally misstates or omits information from financial reports

Fraud Facts & Figures - ACFE 2016 global fraud studies

Frequency and Median Loss of Asset Misappropriation



Billing (accounts payable process): employee submits invoices for payment for fictitious goods or services or personal purchases (e.g. p-cards misuse)

Check Tampering (accounts payable process): employee steals outgoing checks or electronic payments

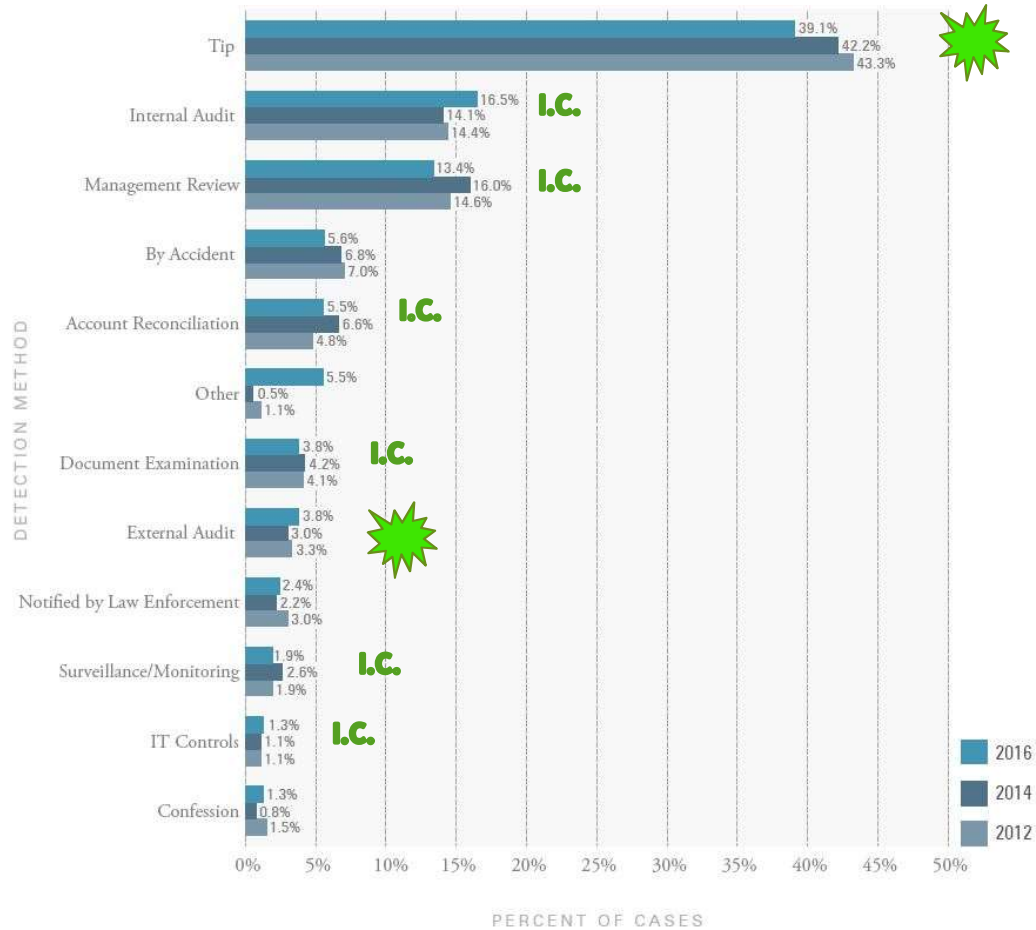
Skimming (receipting process): employee steals an incoming payment before it is recorded in the entity's books or records

Cash Larceny (receipting process): employee steals an incoming payment after it is recorded in the entity's books or records

Note: the accounts payable process makes up 47.6% of all asset misappropriation fraud cases while the cash receipting/handling makes up 34.5%

Fraud Facts & Figures - ACFE 2016-2012 global fraud studies

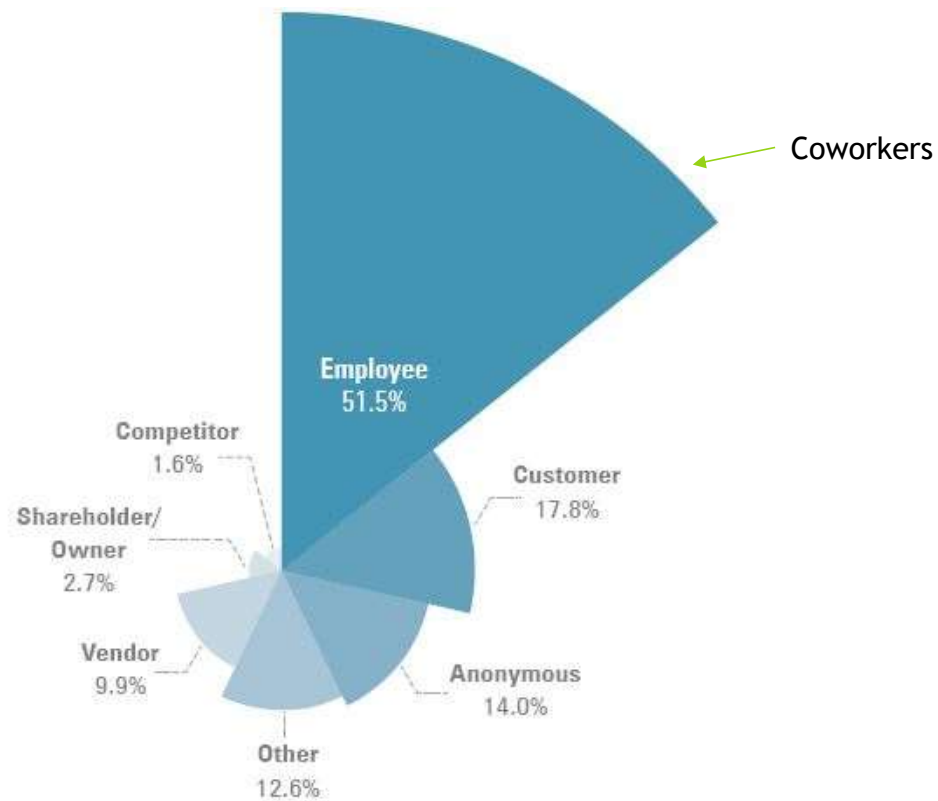
Fraud Detection



I.C. = 42.4%

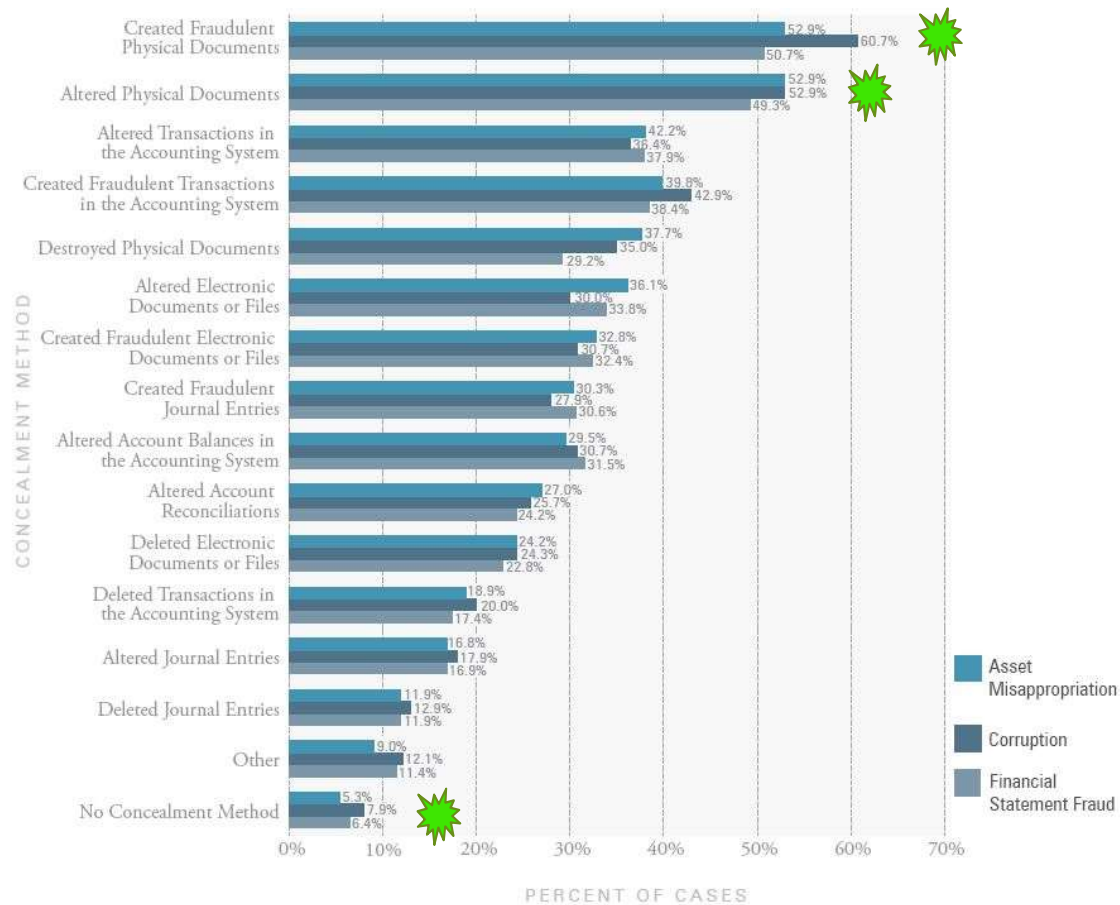
Fraud Facts & Figures - ACFE 2016-2012 global fraud studies

Fraud Detection-Source of Tips



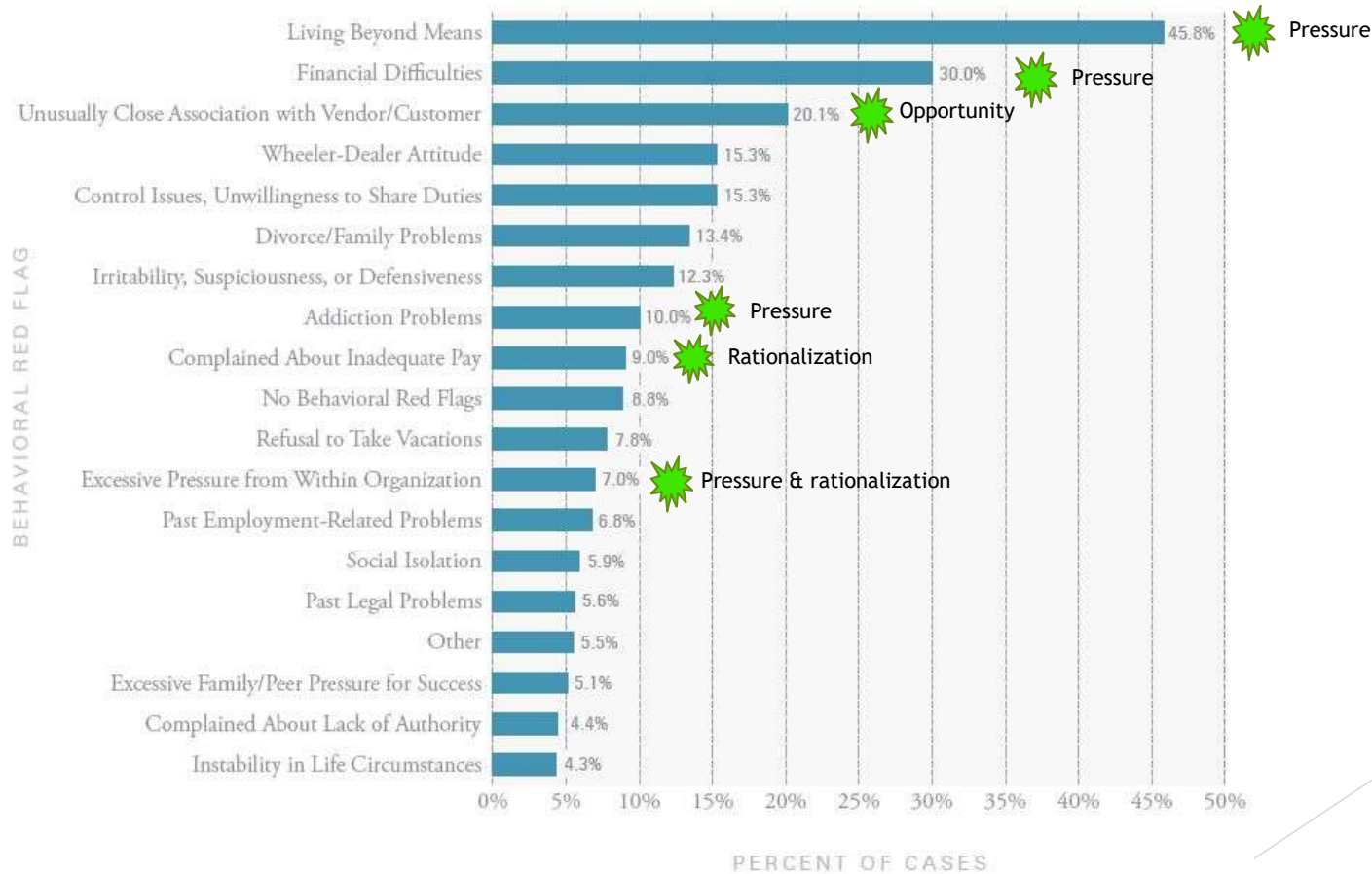
Fraud Facts & Figures - ACFE 2016-2012 global fraud studies

Methods Used to Conceal The Fraud



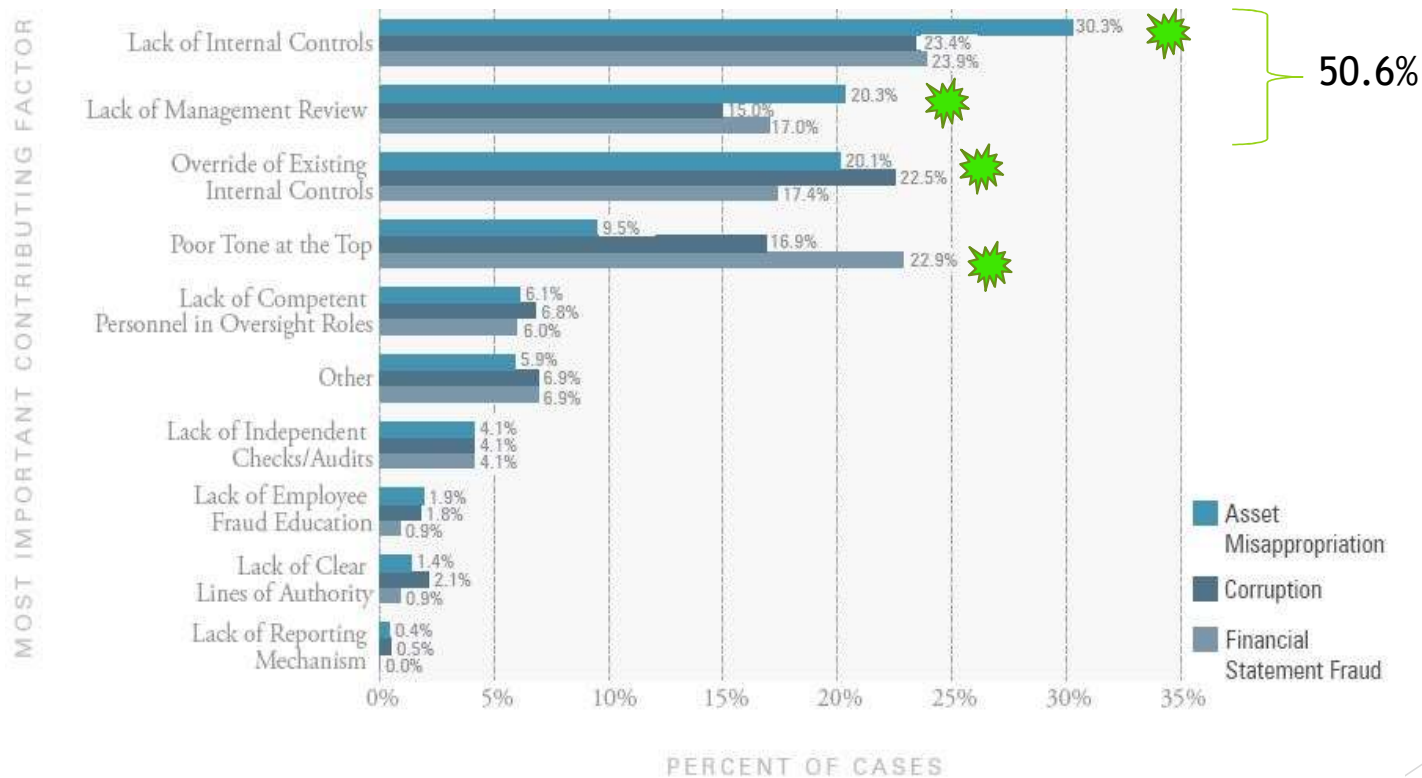
Fraud Facts & Figures - ACFE 2016-2012 global fraud studies

Behavioral Red Flags



Fraud Facts & Figures - ACFE 2016 global fraud studies

Fraud's Most Important Contributing Factors



Case Study - Kane County Treasurer

Kane County (Kanab, Mt. Carmel, Orderville, etc.) - Office of the Utah State Auditor (OSA) reported that over a 3 year period (1/1/2013-1/31/2016) the Kane County Treasurer committed theft of ~\$92,000.

- ▶ Found 46 wire transfers, totaling \$34,600, to personal accounts held by the Treasurer (transferred from three different bank accounts)
- ▶ Found one online payment for \$1,612.67 from a County bank account for a personal cell phone bill of the Treasurer. The Treasurer was already receiving a \$110 monthly stipend for cell phone use
- ▶ Found cash receipts of \$56,182 (nearly all cash) that were not deposited into the County's bank accounts
- ▶ Found adjustments (abatements, write offs, etc.) to property tax accounts totaling \$648,301 and voided more than \$1 million worth of receipts after the tax payments were recorded into the County records and deposited into the bank. "Most of these adjustments were likely for legitimate purposes"

Kane County Treasurer & The Fraud Triangle - Which of the three elements were present?

► Opportunity

- Treasurer was able to authorize bank transfers without secondary authorization
- Treasurer had access to the cash/checks, was in charge of recording the accounting into their software, had access to make accounting and property tax adjustments, and performed the monthly bank reconciliations (i.e. no separation of duties)
- The County Auditor (position within the County not the independent auditor) provided no oversight as a compensating control for the Treasurer performing all of these duties

► Pressure

- According to Utah State Court records, a debt collection complaint was filed against the Treasurer in August 2011 showing there was financial difficulty near the time the fraud began

► Rationalization?

- In July 2014 Treasurer paid a \$20,913 judgment and resolved the case, which was right in the middle of the theft. Treasurer could have possibly said they would borrow those funds and pay them back when the case was resolved

Are you or any of your staff in a similar opportunity, pressure, or rationalization situation? Protect you and your staff with internal controls



Case Study - Utah Communications Authority (UCA)

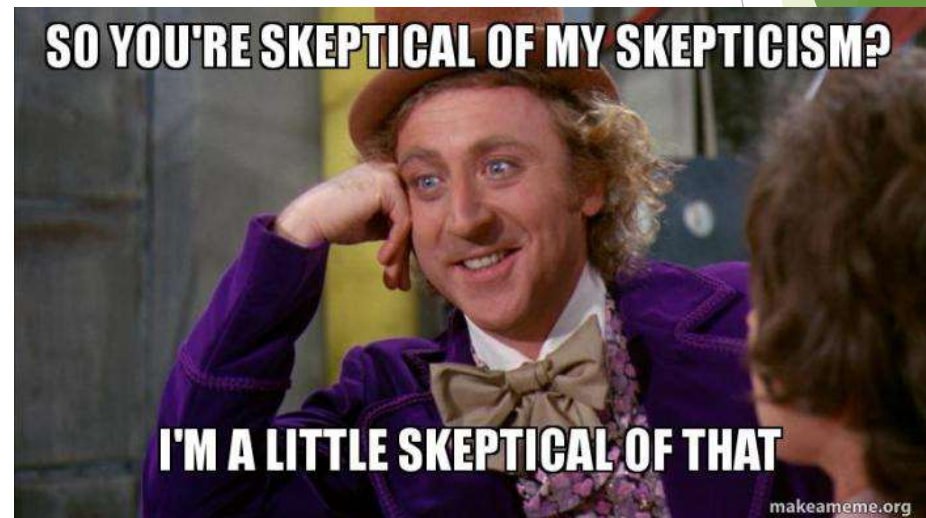
State agency over emergency communications including 911 - Office of the Utah State Auditor (OSA) reported that over a 10 year period (2006-2016) the UCA Administrative Assistant committed theft of over \$800,000

- ▶ The Amin. Assistant had access to a UCA credit card, a UCA unassigned credit card, and a UCA travel card. The assistant used those cards to purchase personal items for herself and her daughter
- ▶ This assistant had the responsibility to collect receipts and backup, reconcile them to the credit card statements, and submit them for review by the CFO. The original credit card statements were sent directly to the assistant and only she was authorized to access the online account
- ▶ The assistant concealed her theft by altering the statements electronically, printing the altered statement, and then submitting the altered statement with her approval for review
 - Example alteration was changing a charge from the state liquor store into a Codale Electric purchase. She concealed payments for a trip to the Bahamas, retail, home improvement, etc.
- ▶ The assistant either did not include backup for the statement's fake expense or fabricated receipts to substantiate that expense
- ▶ Throughout this fraud UCA was being audited. From 2006-2012 they were audited by the Utah State Auditors Office (SAO). From 2013-2015 they were audited by an independent CPA firm. In 2010 the SAO gave a finding for credit card statements with missing backup, but the fraud was never discovered
- ▶ Fraud was discovered by another UCA employee who happened to see the original credit card statement left on the printer and noticed some suspicious charges
- ▶ KSL reported that the assistant was sentenced on May 4, 2017 by a US District Judge to pay \$1.2 million in restitution and will serve 27 months in prison

UCA Fraud - Lessons Learned

- ▶ There was no separation of duties
 - Admin. Assistant was the only person with access to the original credit card statements, had access to many UCA credit cards, had sole responsibility to reconcile the statements and provide backup for the purchases, and authorized those purchases
- ▶ UCA had procurement policies that should have prevented this but the policy was not implemented properly.
 - There was a CFO review of the credit card statements to compensate for lack of segregation of duties; however, it was either not properly implemented or not properly designed to catch this theft and fraud
- ▶ Not only did the Admin. Assistant lose their job and get prosecuted, but the UCA Executive Director resigned his position. Both had been with UCA for 17 years
- ▶ UCA itself had repercussions
 - “Legislative leaders last week put a hold on \$17 million earmarked for the agency until it could show it had cleaned up its act in the wake of a \$1 million embezzlement and other problems cited in an audit.” (KSL)
- ▶ Independent audits did not detect the fraud. External audits are focused on GAAP not detecting fraud
- ▶ “[the administrative assistant] was the last person in the world we would have expected to commit fraud”

Theft & Fraud - Where is your department susceptible?



“Professional skepticism” & “Trust but verify”

Theft & Fraud - Where is your department susceptible?

- ▶ Potential areas employees can steal/commit fraud:
 - Theft of cash (petty cash, cash receipting, opening of checks that come in the mail)
 - Theft of equipment
 - Fraudulent purchases on purchase cards or charge cards (Home Depot, Lowe's, etc.)
 - Over purchasing of office supplies or operational inventory
 - Payroll tampering
 - Financial statements (debt covenants, bond ratings, resident outrage, etc.)
 - Theft of time (fraudulent time cards, abuse of sick time, etc.)
 - Travel & training expenses (submitting personal expenses, fraudulent receipts, etc.)
- ▶ Ask yourself a couple of questions:
 - Internal controls aim at taking away opportunity for errors and fraud, so where do I foresee opportunity?
 - Do I have any employees in my department over high risk areas (cash handling, equipment/inventory access, purchase/charge card, etc.) that have little or no supervision?
 - Does my department have an environment where employees are held accountable and know they will be monitored in their responsibilities?
 - ❖ Perception of detection is one of the biggest deterrents to fraud

So how do I design effective and efficient internal controls?



Steps:

1. Risk assessment/process reviews
 - Understand what internal controls you need
 - Identify where the weakness/risk is
2. Use knowledge gained in risk assessment/process review to determine what type of internal control could be used

Designing Internal Controls

- ▶ Properly designing internal controls is very important
 - Internal controls are very entity and individual employee specific
 - Understand the purpose behind the internal control. Could CFO catch UCA fraud if they understood why they did the review?
 - Kane County Treasurer was performing bank reconciliations throughout the fraud. Bank reconciliations could have caught the wire transfers and missing cash but unfortunately it was being performed by the individual perpetrating the fraud. This made the design of the control ineffective
- ▶ Internal controls can be detective or preventative in design. Detective controls are relatively easy to implement and usually involve just one person, but they are limited. Preventative controls are more involved but are the ideal.
 - Detective in nature - fire alarm
 - ❖ Bank reconciliations or GL account reconciliations
 - ❖ Budget to actual comparisons
 - Preventative in nature - sprinkler system
 - ❖ Training on entity policies
 - ❖ Accounts payable invoice approvals
 - ❖ Requiring cashiers to give a receipt with every transaction
 - Depending upon the complexity of the transaction you might need both aspects for the control to be effective
- ▶ Not all internal controls are created equal. To be effective, internal controls must:
 - Address the heart of the risk
 - Function consistently
 - Leave an audit trail (i.e. documented so there is proof that the control is functioning)
 - Win the benefit vs. cost battle

Designing Internal Controls

- ▶ Internal controls can be looked at in various categories:
 - Separation of duties - “one-man-band” vs. orchestra
 - Physical/Access controls - locks, video recording, PO’s, check request
 - Directive controls - policies, budgets, resolutions
 - Automated (IT) controls - accounting system permissions, passwords, budget limit, debits = credits
 - Monitoring controls - account reconciliations, secondary cash drawer reviews, budget to actual comparisons, financial statement reviews
- ▶ According to GAGAS, an internal control weakness “exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis.”
 - If mistakes are only caught by external auditors then there is a weakness
 - External audits are not an internal control
 - County that relied on auditors for yearend adjustments

Implementing Internal Controls

- ▶ It is management's responsibility to implement internal controls
 - You are the expert in cash handling and payment processing for your entity. Help offsite departments
 - You can be held responsible for lack of internal controls. In the UCA fraud both the Administrative Assistant and Executive Director lost their jobs
- ▶ Assuming that the procedures and policies you inherited adequately fulfill your objectives as a manager is very risky
 - Impact fee refund due to not understanding State code and implementing a control to ensure compliance
 - Reevaluating existing policies and procedures also allows you to find current practices that waste time
- ▶ Internal controls can be properly designed but if they are not implemented and being monitored, the entity and employees are still at risk
 - UCA policy that credit-card statements should be reviewed by CFO



So how do I implement internal controls?



Steps:

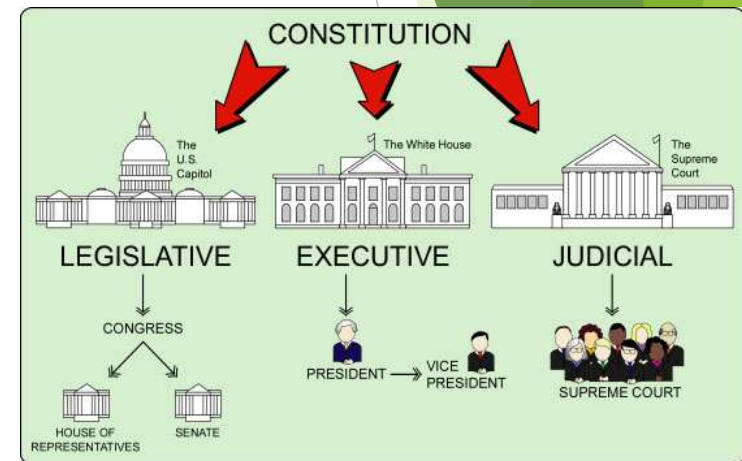
1. Use knowledge gained in your process review and internal control design stages to define what the objective of the internal control should be
 - “Keep dirty thieves from stealing the City’s inventory”
2. Then create the process/procedure that will best fulfill the objective of the control
 - “We will place inventory within the City’s 10 foot wall, create an alarm system with motion activated tasers, and install a camera system so we can watch with joy as the dirty thieves get tazed”

The following slides cover some ideas of internal control objectives and potential internal control procedures to fulfill those objectives. NOT ALL-INCLUSIVE!

Internal Control Objectives - Segregation of Duties

- ▶ The objective of this type of internal control is to separate as much as possible the following employee duties:
 - Authorization (AP invoice or p-card statement approval, sign checks, approve write-off's, Policy making ability, etc.)
 - Custody of assets (access to cash/check stock, p-card, equipment, inventory)
 - Record keeping responsibilities (GL input, customer account adj., spreadsheet tracking)
 - Reconciliation responsibilities (bank account, balance sheet, significant expense accounts)
- ▶ When these responsibilities are separated it creates accountability throughout any process, which improves accuracy and safeguards assets
- ▶ Probably the best internal control available against theft and fraud as it prevents one individual to both commit and conceal their fraudulent acts
- ▶ Bountiful's accounts payable process

When in doubt, separate it out!



Internal Control Examples - Segregation of Duties

- ▶ Good rules of thumb:
 - Eliminate the ability for one person to process a cash disbursement or cash receipt transaction from start to finish without a secondary review
 - ❖ UCA & Kane County
 - ❖ Non-profits, fund raisers, etc. Whenever they are a component unit of the entity or are performed by the entity, try and have the payments flow through your regular cash receipting process
 - If an employee performs a cash receipting and GL recording/adjusting function, they should not be allowed to also reconcile the bank account
 - Cashiers that also record payments should not have access to adjust or write-off customer accounts (utilities, customer deposits, etc.) without some type of secondary review of the adjustment or write-off
 - Ensure the individual creating the billings does not also handle the payments
 - Take a look at any position and see if they have most or all of the outlined (authorization, custody, recording, & reconciling) responsibilities. Those positions need oversight!
- ▶ When segregation of duties is not possible, due to lack of staff and inability to hire more, you must find some other compensating control:
 - Get other people involved with regular independent reviews (stay clear of any area of potential accusations, even honest mistakes)
 - ❖ Monthly checks of bank reconciliation
 - ❖ Random but consistent spot checks (cash counts, register closeout, etc.)
 - ❖ Vouching accounting information to source documents (bank statements, check copy)
 - ❖ Make sure the reviewer has the proper skill to perform the review
 - Outsource specific management functions (monthly reconciliations, journal entry reviews, yearend prep, etc.)
 - ❖ CPA firms love to do consulting work and it can be cheaper than hiring additional staff (Just don't hire your current auditors! They can't audit what they create)

Internal Control Objectives - Payment Receipting

Payment Receipting = cash, card, check, EFT

- ▶ Payments are appropriately safeguarded
 - Safe from theft, misplacement, etc.
- ▶ Payments are valid and processed only once
- ▶ Payments are recorded into the proper accounting period and GL account
- ▶ All payments received are recorded
- ▶ Payment amounts are accurately recorded

Note: in a process where hundreds of payments are processed each week there is a high likelihood of input error. Internal controls help prevent and/or detect those errors so they can be avoided or corrected



Internal Control Examples - Payment Receipting

► Cashiering

- Instruct cashiers to give a receipt with every transaction and post a sign in plain view of the public stating that policy
- Have a supervisor review the cashier's register reconciliation to the closeout report
- Have a camera recording the cashiering station
- Ensure the individual performing the bank reconciliation does not have cash receipting or deposit handling responsibilities. If they do, implement a detailed secondary review of the bank reconciliation
- Have an accounting system username and password for each cashier and do not allow others to receipt in payments under a different username
- Give each cashier a separate cash drawer that they are responsible to closeout
- Minimize the number of people who handle cash and checks and who have access to the safe
- Create a good closeout form that documents totals of each type of receipts, cashier, performance of receipt reconciliation to GL report, and signatures of cashier and supervisor

► Mailed payments

- Ensure the individual opening the mail where payments are received is also not entering those payments into the accounting system
 - ❖ When possible apply payments off of a check log or check copies
 - ❖ Be especially careful with unexpected payments that are not part of the regular billing cycle (cell tower, State restitution, sale of scrap or equipment)

► Ensure a detailed bank reconciliation is performed each month

Internal Control Objectives - Customer Billing

Customer Billing = utilities, property tax and other assessments, business licenses, court fines

- ▶ Revenues and receivables are properly recorded
 - Correct period, year, & dollar amount
 - Accurate GL account
- ▶ Only valid billing adjustments are recorded to the customer accounts
- ▶ Customer accounts are only written off through proper approval
 - Segregation of duties findings for court clerks, utility billing cashiers, and county clerks



Internal Control Examples - Customer Billing

▶ Customer Accounts

- All account adjustments (write-off, voids, credits, dismissals, etc.) are performed by a supervisor rather than the requesting cashier. Best case scenario would be to limit the cashier's software permissions to payment processing only
- Maintain backup (physical or electronic) for account adjustments.
- When the cashier also performs the account adjustments, ensure adjustment backup is maintained and periodically reviewed by supervisor
 - ❖ Accounting software reports showing all customer account adjustments
 - ❖ Bountiful's finding
- Delinquent receivables are reviewed by management regularly

▶ Accurate Billings

- Supervisor reviews billings created before they are sent

▶ Financial Reports

- Regular revenue financial reports are prepared and reviewed by management & governance
 - ❖ The greater the detail of the review the stronger the control

Internal Control Objectives - Cash Disbursements

Cash Disbursements = AP check, p-card, charge account, EFT

- ▶ Disbursements are processed only for the entity's goods and services received
- ▶ Disbursements are only processed once
- ▶ Disbursements are recorded into the proper accounting period and GL account
- ▶ All disbursements made are recorded
- ▶ Disbursements are accurately recorded

Note: in a process where hundreds of invoices are hand input for payment each week, there are bound to be mistakes. Additionally, the cash disbursement process was the area where the most fraud was discovered in the ACFE 2016 report



Internal Controls Examples - Cash Disbursements

► Proper Authorization

- Invoices are reviewed and approved by the associated department before being paid
- P-card or credit card statements are only paid after completion of a secondary review

► Accounts Payable (AP) Processing

- Purchase order, receiving document, and vendor invoice are matched up before payment is made
- Weekly AP batch is reviewed by AP Clerk supervisor before checks are cut

► Automatic/IT Controls

- System rejects any duplicate invoice numbers from the same vendor
- AP Clerk does not have ability to alter (inquiry only) the vendor file

► Physical/Access Controls

- Checks are not given back to AP Clerk after they are cut (risk of check tampering)
- P-cards or credit cards are only issued on an “as needed basis”

► Budget-to-actual reports are created monthly and reviewed by management and governing board

- This helps correct expense miscoding and could detect accounts payable fraud

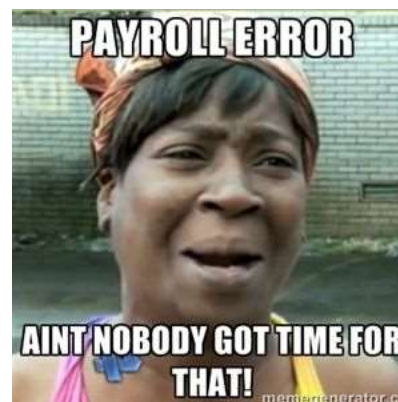
► Wire transfers

- Use bank controls to not allow the same individual to initiate and authorize a transfer
- If the same individual must perform both functions ensure all wire transfers are reviewed by management or governance

Internal Control Objectives - Payroll

- Payroll disbursements (i.e. checks, EFT, or retirement payments) are issued to the proper employee
 - 401k Fraud
- Time cards are appropriately authorized and represent time worked
- Salary and wage changes are appropriately authorized
- Payroll is accurately calculated
- PTO policies are properly followed
- Payroll and associated disbursements are only processed once
- Payroll is recorded into the proper accounting period and GL account

Note: in a process where hundreds of time sheets are hand input for payment, there are bound to be mistakes.



Internal Controls Examples - Payroll

► Proper Authorization

- Time cards & wage changes are reviewed and approved by the associated department
- Retirement contributions meet policy and changes are only processed after governing approval

► Segregate the payroll duties of:

- Initiating and authorizing electronic payroll disbursements
- Preparing and signing payroll checks
- Ability to enter and process payroll from ability to edit the employee master file

► IT Controls

- Access to payroll module is appropriately restricted
- Software performs significant payroll calculations (taxes, PTO balances, etc.)
- Payroll Clerk does not have ability to alter (inquiry only) the employee file

► Physical Controls

- Physical checks are not given back to Payroll Clerk after they are cut (risk of check tampering)

► Monitoring Controls

- Budget-to-actual and financial reports are created monthly and reviewed by management and governing board
 - ❖ This helps correct expense miscoding and could detect payroll fraud
- Software change log showing any changes to payroll information is reviewed by management
- Payroll registers are reviewed for accuracy against source documents before the final payroll is processed
- Payroll batch is reviewed by payroll supervisor before being processed

Final Take Away

- ▶ Internal controls are procedures used to improve operations, reporting, and compliance
 - Internal controls are used more to improve processes than they are to detect and prevent fraud. Use them to make you look good!
- ▶ Take the time to identify risky areas or areas of poor performance and design internal controls to address those areas
- ▶ Remember that internal controls keep honest people honest and protect both the entity and the employees





Internal Controls!!!