Internal Controls: Fraud Prevention

University of North Texas
Center for Public Management

Patrick Shinkle
University of North Texas
Center for Public Management
https://cpm.hps.unt.edu/

Objectives

- Discussion of COSO and Framework
- Review of ACFE Fraud Classifications and Examples
- Discuss Fraud Elements
- Discuss Fraud Examples
- Discuss Cash Controls

What is COSO?

https://www.coso.org/

COSO is a committee composed of representatives from five organizations:

- American Accounting Association
- American Institute of Certified Public Accountants
- Financial Executives International
- Institute of Management Accountants
- Institute of Internal Auditors

Together, the COSO board develops guidance documents that help organizations with risk assessment, internal controls and fraud prevention.

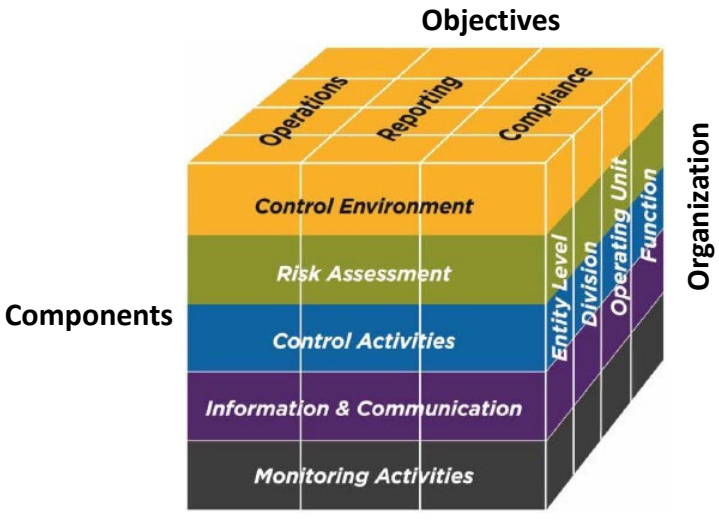
https://i-sight.com/resources/coso-framework-what-it-is-and-how-to-use-it/

What is COSO?

The columns are the three objective categories(operations, reporting and compliance).

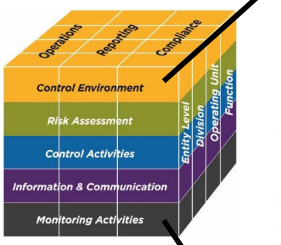
The rows consist of the five components.

Your organizational structure fits into the third dimension of the cube.



https://www.coso.org/Pages/default.aspx

COSO 17 Principle Components



Control Environment	1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability
Risk Assessment	6. Specifies suitable objectives 7. Identifies and analyzes risk 8. Assesses fraud risk 9. Identifies and analyzes significant change
Control Activities	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys through policies and procedures
Information & Communication	13. Uses relevant information 14. Communicates internally 15. Communicates externally
Monitoring Activities	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies

https://www.coso.org/Pages/default.aspx

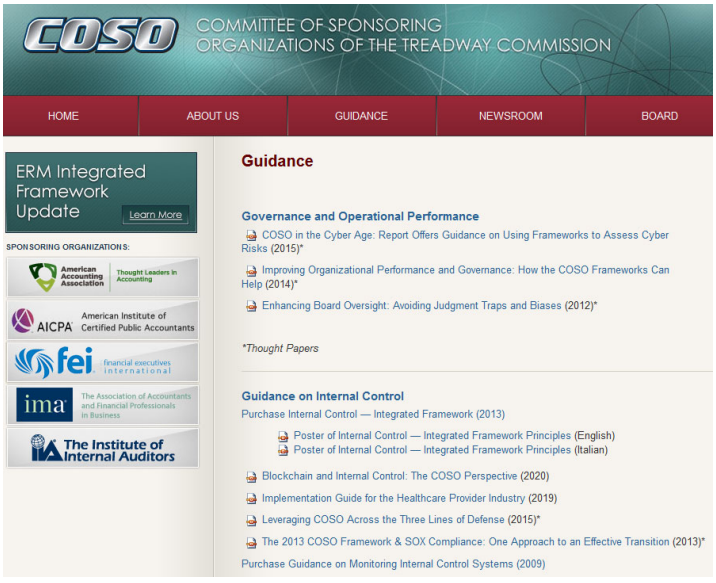
COSO Framework Approach

- **Phase 1 - Planning and Scoping**
  - Timeline, Resources, Roles & Responsibilities
  - Range of Activities
  - Tone at the Top, Buy-In
- **Phase 2 - Assessment & Documentation**
  - Reviewing Existing Controls, System Structure
  - Processes, Gaps and Reporting
  - Fraud Types, Incentives and Pressures, Opportunities
  - Attitudes and Rationalizations
  - Conducting Interviews, Process Discussions,

COSO Framework Approach

- **Phase 3 - Remediation Planning & Implementation**
  - Severity of Deficiencies, Degree of Changes, Timing and Milestones
- **Phase 4 - Design, Testing and Reporting of Controls**
  - Selection of Controls for Testing, Classification of Importance
  - Testing of Controls for Effectiveness and Anticipated Outcomes
  - Nature, Timing and Extent of Testing
  - Data Analytics, Test Scripts, Performance Measurements for Reporting
- **Phase 5 - Optimizing Effectiveness of Internal Controls**
  - Alignment of Risk and Controls with Strategy and Objectives
  - Process Control Structure – Preventative, Detective, Manual or Automated
  - Continual Monitoring, Asking "why?" Controls Fail

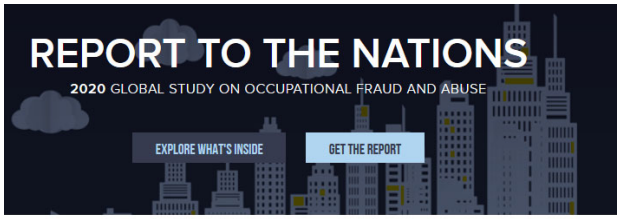
COSO - Guidance



https://www.coso.org/Pages/guidance.aspx

ACFE

- Association of Certified Fraud Examiners
  - https://www.acfe.com/report-to-the-nations/2020/



ABOUT

11th edition of the largest global study on occupational fraud

2,504 real cases of occupational fraud

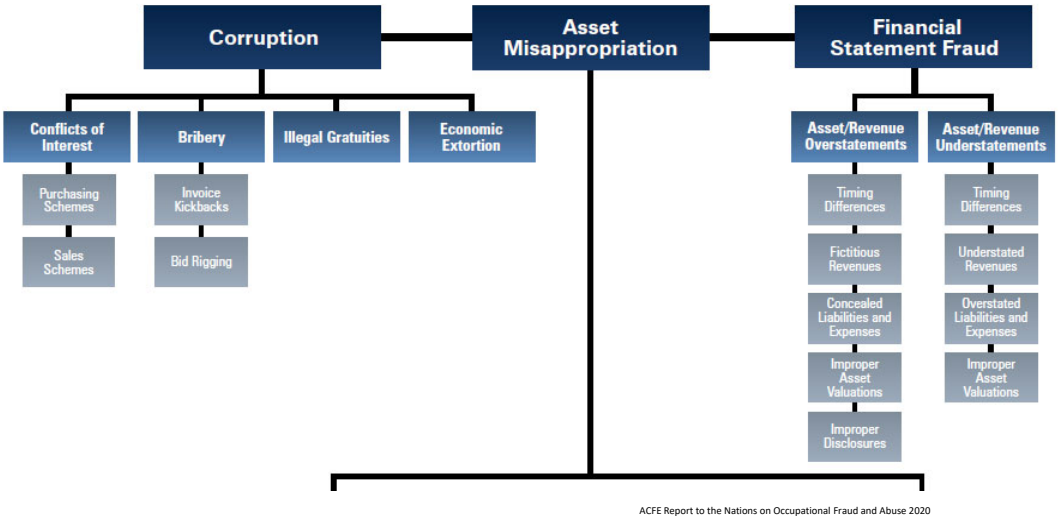
Data from **125 countries**

23 major industry categories included

Explores the **costs, schemes, victims and perpetrators** of fraud

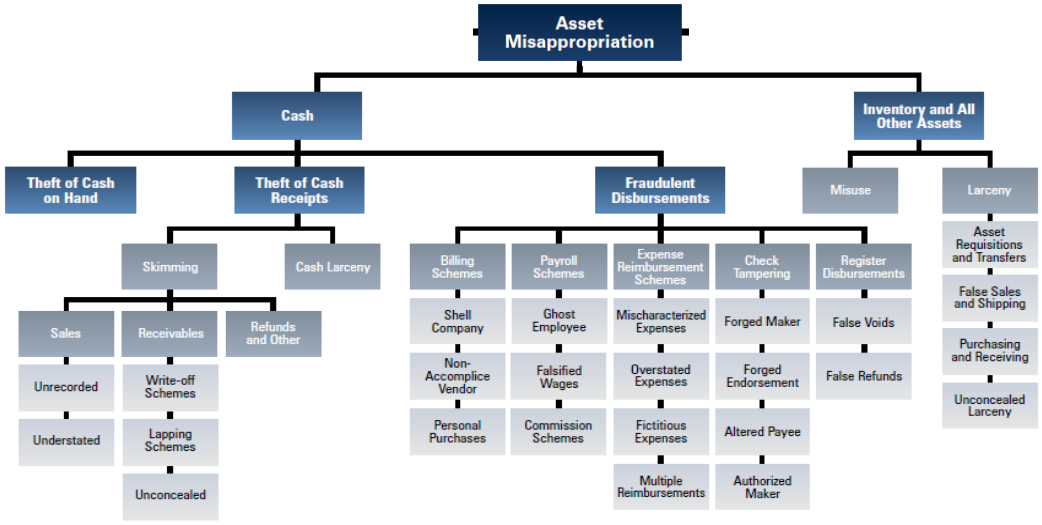
METHODOLOGY

Occupational Fraud and Abuse Classification System



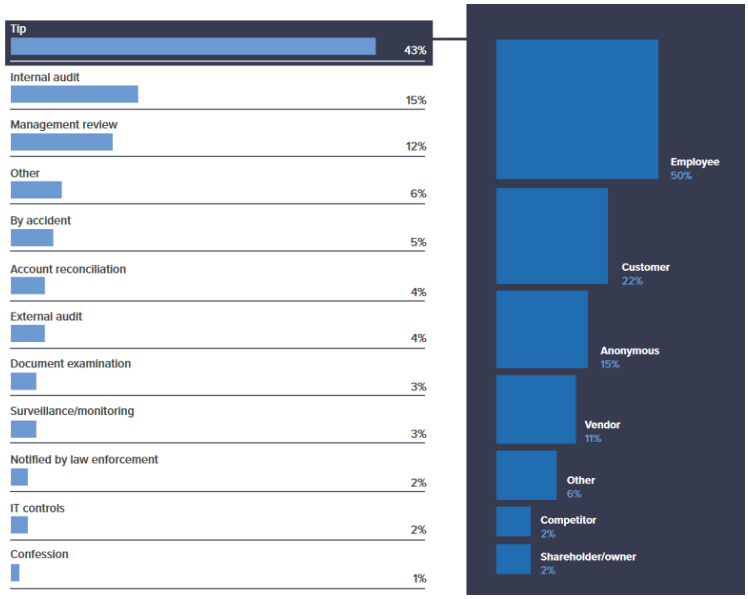
ACFE Report to the Nations on Occupational Fraud and Abuse 2020

Occupational Fraud and Abuse Classification System



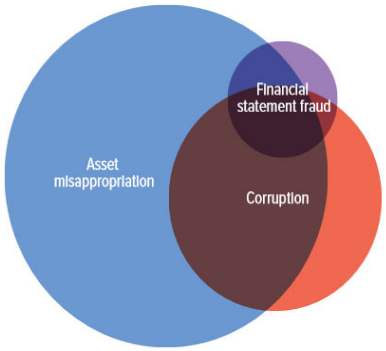
ACFE Report to the Nations on Occupational Fraud and Abuse 2020

Detection



ACFE Report to the Nations on Occupational Fraud & Abuse 2020

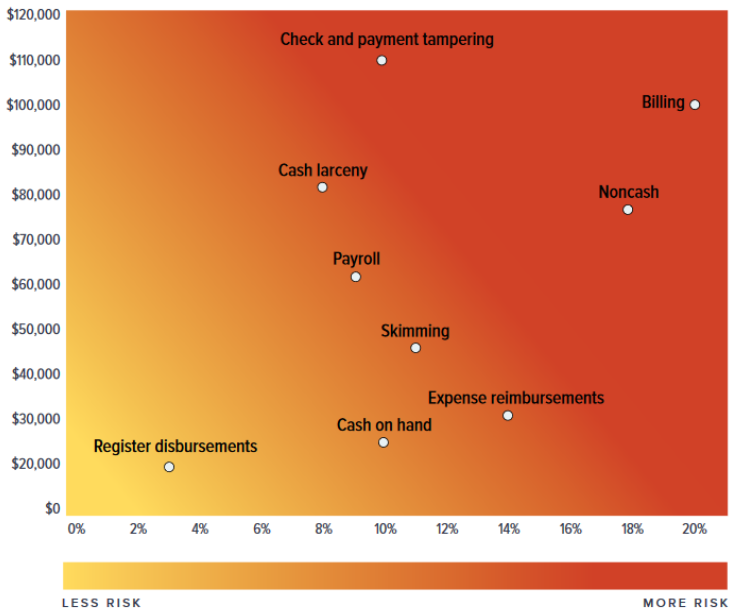
Occupational Fraud



Asset misappropriation only	53%
Asset misappropriation and corruption	26%
Corruption only	11%
Corruption, asset misappropriation, and financial statement fraud	5%
Asset misappropriation and financial statement fraud	3%
Financial statement fraud only	2%
Corruption and financial statement fraud	1%

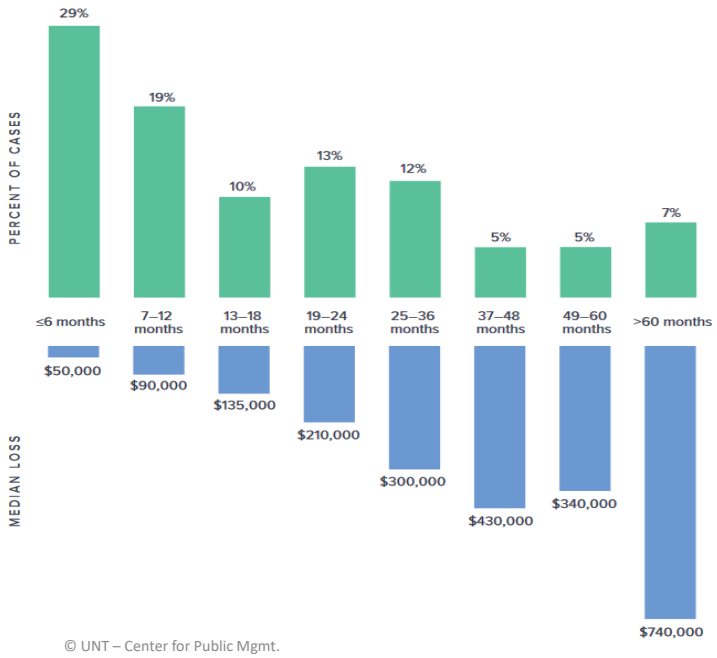
ACFE Report to the Nations on Occupational Fraud and Abuse 2020

Greatest Risk



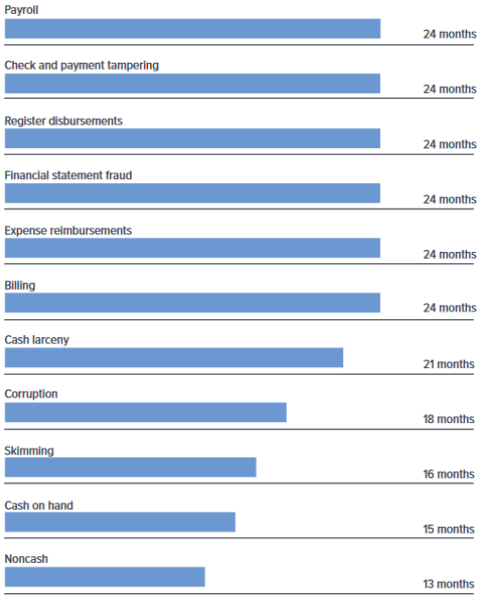
ACFE Report to the Nations on Occupational Fraud and Abuse 2020

Loss: Duration



ACFE Report to the Nations on Occupational Fraud and Abuse 2020

Type: Duration



ACFE Report to the Nations on Occupational Fraud and Abuse 2020

Fraud

GGFOA.org

Fraud Triangle - Opportunity

FACTORS	REFERS TO
Process	•Loopholes in process. Process without proper controls. Processes that are loosely defined and open to misuse.
Controls	•Loopholes in control mechanisms. Inadequate controls. Controls with manual intervention. Inadequately governed controls.
•Power	•The act of granting sweeping powers to any personnel. Powers that don't need justifications while being exercised (creating financial, reputation, regulatory, and liability for the organization). Powers exercised that aren't under the ambit of any audits. Powers granted to personnel who are either new to the organization or have risen up the hierarchy very fast.
Network	Employees having the power to influence key functions and network all functions towards a common goal.
Domain expertise	Expertise in select domains giving persons advantage over others in control positions who are not as adept.

FRAUD Magazine Apr. 2014, Vivek Krishnan, CFE

Fraud Triangle - Pressure

Monetary	The dire need for money.
Process & Rules	Employees being governed by processes and rules, the non-adherence of which would lead to the employee being reprimanded. The repercussion of non-adherence could be perceived or actual.
Ego/Vendetta	•Employees who have large egos, leading to jealousy, hatred leading to unethical behavior, internally pressurizing themselves, boosting their ego. •Employees who are excessively competitive and cut competition by unethical means. •Pressure to be the top performer. •Employees who are vengeful because they perceive harm or pressure caused to them by another employee or group of employees.
Altruistic	Employees who violate/deviate from defined processes under the pretext of "greater good of all." All could be a small group, society overall or a certain segment of society.
Sustenance	Employees who violate processes to protect "the self" from harm — physically, mentally or on financial grounds. The race for existence and to survive.

FRAUD Magazine Apr. 2014, Vivek Krishnan, CFE

Fraud Triangle - Rationalizing

Upbringing & family	Family and inner circle immediately around the employee. Typically, a function of the aspirations of the near and loved ones, which guides and influences the way a person thinks and acts.
Culture & background	These refer to societal expectations. Interactions with the society, the immediate circle of influence, benefits vs. duties defined by societal circles.
Persona	Value systems of the employees. Definition of ethics would differ from person to person. This difference itself would determine the ease of rationalization.
Belief systems	The person's beliefs: emotional, religious perceptions.
Preferences	Individual preferences, learning and past experiences.

FRAUD Magazine Apr. 2014, Vivek Krishnan, CFE

Red Flags

- Financial Duress
  - Borrowing money from co-workers.
  - Creditors or collectors appearing at the workplace.
  - Gambling beyond means
- Unusual Behavioral Changes
  - Excessive personal habits or lifestyle changes.
  - Attitude, quickly and easily annoyed at reasonable questions
- No vacations or days off, Overtime issues
- Spending Habits
  - Significant new purchases
  - Carrying large amounts of cash
- Vendor Relationships, Conflicts of Interest
- Office Issues
  - Rewriting records and documents under the guise of neatness
  - High Turnover / Low Morale
- Book Keeping Accounting Issues
  - No supporting documentation for adjusting entries or out-of-balance issues
  - Stale, Incomplete or untimely bank reconciliations
  - Excessive Voids / Refunds / Credit Memos
- Missing or Altered Documents
- Increased Customer Complaints
- Write-offs of inventory shortages with no attempt to determine the cause
- Post Office Boxes as Shipping Addresses
- Duplicate Invoices or Payments
- Un-reconciled accounts, Dormant accounts
- Failure to deactivate or terminate access after employees have separated from a position.

Fraud

- How do we protect against accusations of fraud?
- How do we handle the transfer of cash within the organization?
- How often and when do we count our cash and till deposits?
- How do we protect the funds, organization, and personal reputation?

- <u>Fiduciary Responsibility</u>
  - A fiduciary is a person who holds a legal or ethical relationship of trust with one or more other parties. Typically, a fiduciary prudently takes care of money or other asset for another person.
  - A fiduciary relationship encompasses the idea of faith and confidence and is generally established only when the confidence given by one person is actually accepted by the other person (TRUST).

High Security Check Features

- Thermochromatic Ink (Temperature sensitive)
- Toner Fusion / Toner Anchorage (permanently bonds the ink/toner to the paper)
- Bleeding Seals / Ink & Dye (Black ink turns red and runs)
- Microprinting (legible line with wording under magnification)
- Overprinting / Ultra-Violet or Fluorescent Fibers
- Laid Lines or Anti-splicing Lines (Deter cut-and-paste alterations)
- Watermark / Dual-tone Paper
- Warning Bands
- Chemical Reactive Ink
- Void Pantograph
- High Resolution Intricate Border

http://www.checksnforms.com/Articles.asp?ID=242

Types of Credit Card Fraud

- Application Fraud
- Manual / Electronic Credit Card Imprints
- Card-Not-Present (CNP) – [CVC number must also be known].
- Counterfeit Card
- Lost / Stolen Card
- Card ID Theft
- Mail Non-Received Card
- Assumed Identity
- Doctored / Fake Cards
- Account Takeover

Cash Handling Fraud Examples

- Discount Scam on Cash Transactions (Sweethearting)
  - Employee rings up more discounts than the others.
    - Compare discount charges versus peers.
- Line Item Void
  - Almost every POS system provides the ability to do a pre-check line item void in case the cashier rings up the wrong item, but this function is also used to steal money from the cash register.
- No Sales
  - The No Sale function can be locked down in many systems. The cashier can leave the cash drawer open slightly so they may work from an open drawer allowing them to pick and choose certain cash transactions in which they can pocket the entire amount of the check.

Cash Handling Fraud Examples

- Penny Trick
  - Cashier places a penny, paper clip, or other item on the register each time they don't ring in a transaction. The cashier multiply the price of the theft by the number of pennies to know how much to pull from the drawer.
- Manipulating Voids & Refunds
  - The employee issues fictitious refunds or voids a legitimate transaction and then pockets the money.
- Floating Receipts
  - Reusing receipts from transactions to steal money from future transactions.
- Phony Walkouts
  - Accepting payment then saying "The customer walked out without paying."

Cash Handling Fraud Examples

- Multiple Transactions for Less Than $1.00
  - Employees ring up cheaper items, but then give away more expensive items to someone they know or in many cases to earn a bigger tip from the customer.
- Reprint Check Function
  - Cashiers will use the reprint check feature to steal the cash when there is a duplicate transaction.
- Total Due $ 0
  - Indicates a total check void, a credit or a refund, which is an open door for fraudulent activity.

Cash Handling Fraud Examples

- Till Tapping (Customer Theft)
  - One distracts the cashier and the other "taps" the till (steals the money) while the cashier is distracted. It often starts with a customer who waits until a cashier is in the middle of a transaction and then asks the cashier to make change.
    - Train cashiers to watch for customers who not only ask for change and who holds up an article of clothing or positions himself in a way that keeps nearby customers from witnessing the attempted theft.
- Shortchanging and Change-raising
  - The cashier shorts the customers for part of the change they are due.
    - Watch for cashiers who hand over change in a lump sum instead of counting it out. Another warning sign is bills out of place in the cash drawer.

Cash Handling Fraud Examples

- Change Raising (Customer Theft)
  - involves a customer who makes several confusing change requests that result in the cashier giving back more change than the person is entitled to.
    - Usually involves a low-priced item for which a customer pays with a large bill. After receiving the correct change, the customer then begins the scam by asking to trade the change for a larger bill.
- Technology Scams (Cashier or Customer Theft)
  - Many retailers purchase POS devices that come complete with operating software. Criminal can seek Wi-Fi networks and passwords. The objective is to find unsecured network IP addresses that are serving as the IP address for a retailer's POS system.
    - Anyone with inside knowledge of payments can easily hack a POS system. "They use tools to crack a Windows remote desktop - defaults at port 3389 – and attempt to compromise the program's password.

Theft of Cash

- Skimming –
  - Any Scheme in which cash is stolen from an organization <u>before</u> it is recorded on the organization's books and records.
    - Employee accepts cash payment from a customer but does not record the sale and instead pockets the money.
- Cash Larceny –
  - Any scheme in which cash is stolen from an organization <u>after</u> it has been recorded on the organization's books and records.
    - Employee steals cash and checks from the daily receipts before they can be deposited in the bank.

ACFE Report to the Nations on Occupational Fraud and Abuse 2012

Types of Check Fraud

- Forgery
  - An employee issues a check without proper authorization. Criminals steal a check, endorse it and present for payment.
- Counterfeiting
  - Fabricating a check or duplicating a check with advanced color photocopiers.
- Alteration
  - Remove or modify handwriting and information on the check. Removing all the information is called check washing.
- Paperhanging
  - Writing and/or ordering new checks on closed accounts.
- Check Kiting
  - Opening accounts at two or more institutions and using "the float time" of available funds to create fraudulent balances.

Signs of Possible Fraudulent or “Bad” Checks

- The check lacks perforations.
- The check number is either missing or does not change.
- The check number is low (like 101 up to 400) on personal checks or (like 1001 up to 1500) on business checks. (90% of bad checks are written on accounts less than one year old.)
- The type of font used to print the customer's name looks visibly different from the font used to print the address.
- Additions to the check (i.e. phone numbers) have been written by hand.
- The customer's address is missing.
- The address of the bank is missing.
- There are stains or discolorations on the check possibly caused by erasures or alterations.

http://www.ckfraud.org/ckfraud.html

Signs of Possible Fraudulent or "Bad" Checks

- The numbers printed along the bottoms of the check (called Magnetic Ink Character Recognition, or MICR, coding) are shiny. Real magnetic ink is dull and non glossy in appearance.
- The MICR encoding at the bottom of the check does not match the check number.
- The MICR numbers are missing.
- The MICR coding does not match the bank district and the routing symbol in the upper right-hand corner of the check (if shown).
- The name of the payee appears to have been printed by a typewriter. Most payroll, expenses, and dividend checks are printed via computer.
- The word VOID appears across the check.
- Notations appear in the memo section listing "load," "payroll," or "dividends." Most legitimate companies have separate accounts for these functions, eliminating a need for such notations.
- The check lacks an authorized signature.

http://www.ckfraud.org/ckfraud.html

Theft of Funds (Fraud) – In Texas

- If found guilty of embezzlement, the penalties are dependent on the amount of money or value of goods taken.

Value of Offense	Possible Charge
0 to $1,500	Misdemeanor Charge, up to 1 year in jail
$1,500 to $20,000	State Jail Felony, up to 2 years in state jail
$20,000 to $100,000	3rd Degree Felony, 2 to 10 years in prison
$100,000 to $200,000	2nd Degree Felony, 2 to 20 years in state prison
More than $200,000	1st Degree Felony, 5 to 99 years in state prison

- If you are considered a "public servant" in your capacity as an employee when the situation happened, the charge you face will be enhanced. You will face the next higher category of offense.

http://www.mytexasdefenselawyer.com/texas-criminal-laws-penalties/embezzlement/

Cash Controls Quick Reference Guide

Quick Reference Guide

- Departments, employees, may not maintain bank accounts on behalf of the entity.
- "Cash" refers to currency/coin, checks, bank drafts, Automatic Clearing House (ACH) transactions, Electronic Funds Transfers (EFTs), money orders, traveler's checks, cashier's checks, or credit/debit card transactions.
- Only authorized employees may handle cash on behalf of the entity.
- Cash Control Training must be attended annually.
- Each department that handles cash must develop written procedures for separation of duties.

Quick Reference Guide

- Separation of duties must be 3 people deep.
  - Collecting Cash
  - Maintaining Documentation
  - Preparing Deposits
  - Reconciling Records
- Cash must be kept in a secured location, meaning a safe attached to a fixture.
- Checks must (Confirm the points of negotiability):
  - Be made payable to the entity
  - Be endorsed upon receipt
  - Have current date
  - Have written line and number amount match
  - Be signed

Quick Reference Guide

- Deposits must:
  - Be made within 3 business days
  - Be transported in either a lock bag or tamper evident bag which is inside of another bag (tote, back pack, purse, etc.).
- Cash on hand and cash deposited must equal actual receipts at all times.
- Receipts:
  - Regular sales = must issue receipt every payment
  - Occasional sales = must issue receipt with every payment OR keep sufficient transaction detail

Quick Reference Guide

- Counterfeit – check paper, portrait, watermark, and security strip. Counterfeit pen is encouraged.
- Overages/Shortages must:
  - Be reported to supervisor at end of daily closing.
  - Be investigated if in a single incident or in aggregate during one -month period in the amount of $25 under the control of a single employee or student.
  - Have maintained written documentation.
- Fraud or theft must be reported to Internal Audit and local law enforcement on the day of occurrence.

Quick Reference Guide

- Petty Cash/Change Fund must:
  - Be kept in safe, not locked drawer.
  - Be reconciled at end of day funds are used.
  - Have maintained written documentation.
  - Be balanced at all times.
- Refunds:
  - Do not issue refunds from petty cash or change fund.
  - Ensure refunds are charges back to the appropriate account or fund.

Recommended Internal Controls

- Conduct periodic surprise audits and annual reviews of procedures.
- Provide for the physical security of all checks.
  - Maintain check images in preference to paper copies.
  - Keep check stock in a locked and secure location with a formal inventory listing maintained.
    - Secure check stock daily.
    - Remove continuous check stock from printers.
    - Lock and secure check specific printers.
    - Consider the use of blank or unprinted check stock with inventory control numbers. The actual check number may be generated through the financial accounting system.

http://www.gfoa.org/bank-account-fraud-prevention

Recommended Internal Controls

- Provide for the physical security of all checks.
  - Physically void returned checks and check copies
  - Retain in a locked and secure location or destroy on a schedule.
  - Provide for the temporary physical security of electronically deposited checks, including:
    - Storage in a secure facility,
    - Timely destruction such as secure shredding. (The depositing government is liable for any fraudulent usage of these checks.)

http://www.gfoa.org/bank-account-fraud-prevention

Recommended Internal Controls

- Ensure appropriate security over signature plates, cards, and software.
- Require additional review process for all checks over a specified amount.
- Consider using a Controlled Disbursement account, to the extent permitted by law, for all payroll and Accounts Payable disbursements to provide additional control. It is preferable to make payments via batch ACH (direct deposit) for both Payroll and Accounts Payable as opposed to checks to reduce fraud potential and payment expenses.
- Require two party authorizations (initiation and release) on all wires and ACH files.
- Require daily staff reconciliation of wires and ACH releases.

http://www.gfoa.org/bank-account-fraud-prevention

Recommended Internal Controls

- Ensure proper segregation of duties among staff initiating, authorizing, preparing, signing, and mailing payments and reconciling bank statements.
- Review signature cards and authority levels whenever any changes occur and annually at a minimum. Remove individuals from bank transaction authority immediately upon resignation or termination.
- Review all bank accounts at least annually. Consolidate or eliminate bank accounts that are not frequently utilized.
- Depending on the complexity, size and volume, consider segregating cash inflow and outflow in separate accounts to allow for placement of appropriate fraud prevention practices and products. When appropriate (i.e. if no restrictions exist) these types of separate accounts should be maintained as Zero Balance Accounts (ZBAs) that are swept into the governmental entity's concentration account.

http://www.gfoa.org/bank-account-fraud-prevention

Recommended Internal Controls

- Ensure that controls exist for the storage and destruction of all documents that contain account and other related information.
- Determine that appropriate controls are present if employees access the government's financial and banking systems from remote sites (i.e., restrict the sharing of files).
- On at least an annual basis, request the government's legal counsel to research changes in laws that shift liability for fraudulent transactions to the government.

http://www.gfoa.org/bank-account-fraud-prevention

Depository Institution Controls Review

- Implement positive pay, or preferably payee positive pay, on all disbursement bank accounts and reconcile exceptions daily. Positive pay is the single best fraud prevention tool available. If a government's bank offers a positive pay service and the government chooses not to utilize it, then the government (not the bank) will be liable for fraudulent transactions.
  - Instruct the bank to return all non-conforming positive pay items as the default instruction.
  - Ensure that a clear policy exists to separate responsibilities between staff approving positive pay exceptions and staff initially requesting and/or preparing the check.
  - Avoid reverse positive pay because with this service the liability remains with the government.

http://www.gfoa.org/bank-account-fraud-prevention

Depository Institution Controls Review

- Direct the bank to reject or block any and all withdrawals not initiated by the government from accounts that only accept deposits.
- Place ACH filters and/or blocks on all accounts.
- Place total or selective ACH blocks on all disbursement accounts. Selective ACH blocks, also known as ACH filters, allow electronic debits to occur only for pre-designated transactions.
- Develop a formal plan to review ACH blocks/filters. This should be done on an annual basis, at a minimum.
- Consider the use of Universal Payments Identification Codes (UPIC) for all receivables accounts.

http://www.gfoa.org/bank-account-fraud-prevention

Depository Institution Controls Review

- Ensure that your financial institutions provides for multi-factor identification for on-line banking services involving transactions and administrative functions. Ensure separation of duties (initiation and release/approved) for financial transactions and administration of the on-line system. Multi-factor identification may include numerous passwords and/or utilization of user specific tokens.
- Ensure that your financial institution provides a quarterly listing, by account, of all approved signers and access-only individuals.
- Utilize bank reconciliation services to reduce time on reconciliation and focus on exception items.
- Discuss enhanced or new account security features with your financial institution on at least an annual basis.

http://www.gfoa.org/bank-account-fraud-prevention

10 ways to Identify Accounts Payable Fraud

- Duplicate Payments
- Benford's Law
- Rounded Amount Invoices
- Invoices Just Below Approval Amounts
- Check Theft Search

https://www.auditnet.org

10 ways to Identify Accounts Payable Fraud

- Abnormal Invoice Volume Activity
- Vendors with Cancelled or Returned Checks
- Above Average Payments per Vendor
- Vendor / Employee Cross-Check
- Vendors with a Mail Drop as an Address

https://www.auditnet.org

AP Fraud Red Flags

- Expedited or urgent instruction requests
- Untimely instruction changes
- Only electronic communications
- Poor documentation
- Deviation from protocol and/or procedures
- Unusual or unapproved Vendors
- Increased payments to particular vendors without corresponding increases in goods or services
- Very large payments to one vendor
- Unusually large purchases on an employee's company-issued credit card

https://i-sight.com/resources/accounts-payable-fraud/

AP Fraud Red Flags

- Invoices in numerical or accounting sequence
- Invoices that look unprofessional, photocopied or edited
- Invoices that are missing key details, such as address, phone number, authorizing information
- A vendor's email address that uses a free provider, such as Gmail
- Multiple invoices paid together or on the same date
- Vendor addresses that are the same as an employee address
- Vendor address that look to be residential addresses

https://i-sight.com/resources/accounts-payable-fraud/

AP Fraud Red Flags

- Vendors with similar names
- Large entertainment, gift or expense charges
- Incomplete documentation or copies instead of originals
- Vendor's prices that seem unusually low or high
- Close relationships between an employee and vendor
- Repeated purchases from a vendor with a record of poor quality goods or services
- Tips or complaints from employees, customers or vendors

https://i-sight.com/resources/accounts-payable-fraud/

Dixon, Illinois

- Dixon, Illinois
  - Population <16,000 (declining)
  - Annual Budget <$10 million
  - Total Assets $100 million
  - Cash and Investments <$2 million
- Longtime Controller
  - Started with high school work study
  - 20+ years
- Elaborate (aka expensive) horse breeding operation.
- Two independent accounting firms.
- Annual audits and reviews by state regulators.

"Rita Crundwell is a big asset to the City. She looks after every tax dollar as if it were her own."

- Former Commissioner of Finance

Dixon, Illinois – What Happened?

- **Largest Municipal Fraud in U.S. History**
  - **$54 million embezzlement over two decades**
- Opened a secret bank account as the only signatory.
  - RSCDA – Reserve Fund (Reserve Sewer Capital Development Account)
- Began transferring funds from other city accounts into the secret account. Initial transfer was $181,000.
- She created 159 fictitious invoices purported to be from the state of Illinois to show the city's auditors that the funds she was fraudulently depositing into the RSCDA account were being used for legitimate purposes.
- Built trust within the city and the community.
- Blamed shortfalls on late state of IL payments to the city.

Dixon, Illinois – Hindsight Prevention Controls

- Segregation of duties
- Multiple signatures for new account establishment
- Reconciliation verification and oversight
- Multiple receivers of statements and confirmations
- Lifestyle review (Annual salary of approximately $80,000)
- Over-reliance on key employees
- Surprise audits
- Denial culture of "Don't rock the boat".
- Who was the "back-up" in the event of an emergency?
- Mandatory Vacations with function/duties transfer

Strong Tenets of Fraud Prevention

- Never Underestimate
  - Periodically update, revise and review your processes and procedures.
- Never Replace Diligence with Automation
  - You can not replace common sense, intuition and effective oversight.
- Master the Arts of Observation, Listening and Questioning
  - Know what controls are in place and ensure their compliance.
- Beware of Subterfuge, Decoys and Obfuscation
  - Distractions, overload and emotions are part of the fraud process.
- Occam's Razor
  - Getting unnecessary information out of the way is the fastest way to the truth or best explanation.

Questions?

Thank you!