Internal Controls

North Central Texas Council of Governments

Training & Development Institute
Learn. Excel. Inspire.

northtexastdi@nctcog.org

Objectives

- Produce a work environment that promotes strong internal controls
- Identify and demonstrating the internal and external risks that affect the organization
- Promote the establishment of documented and maintained internal controls
- Ensure compliance by all employees within the organization

What are Internal Controls?

- A continuous program or process of review
- It’s all about the systems
- Methods used to help ensure the achievement of an objective
  - Writing procedures, instructions, check lists, documentation to encourage compliance
- Used to ensure business units operate according to plan
  - Policies, procedures, practices and organizational design
- Affected by people
  - Every employee has a responsibility and part
- Provide reasonable assurance to the governing body
- Used to achieve objectives in overlapping categories

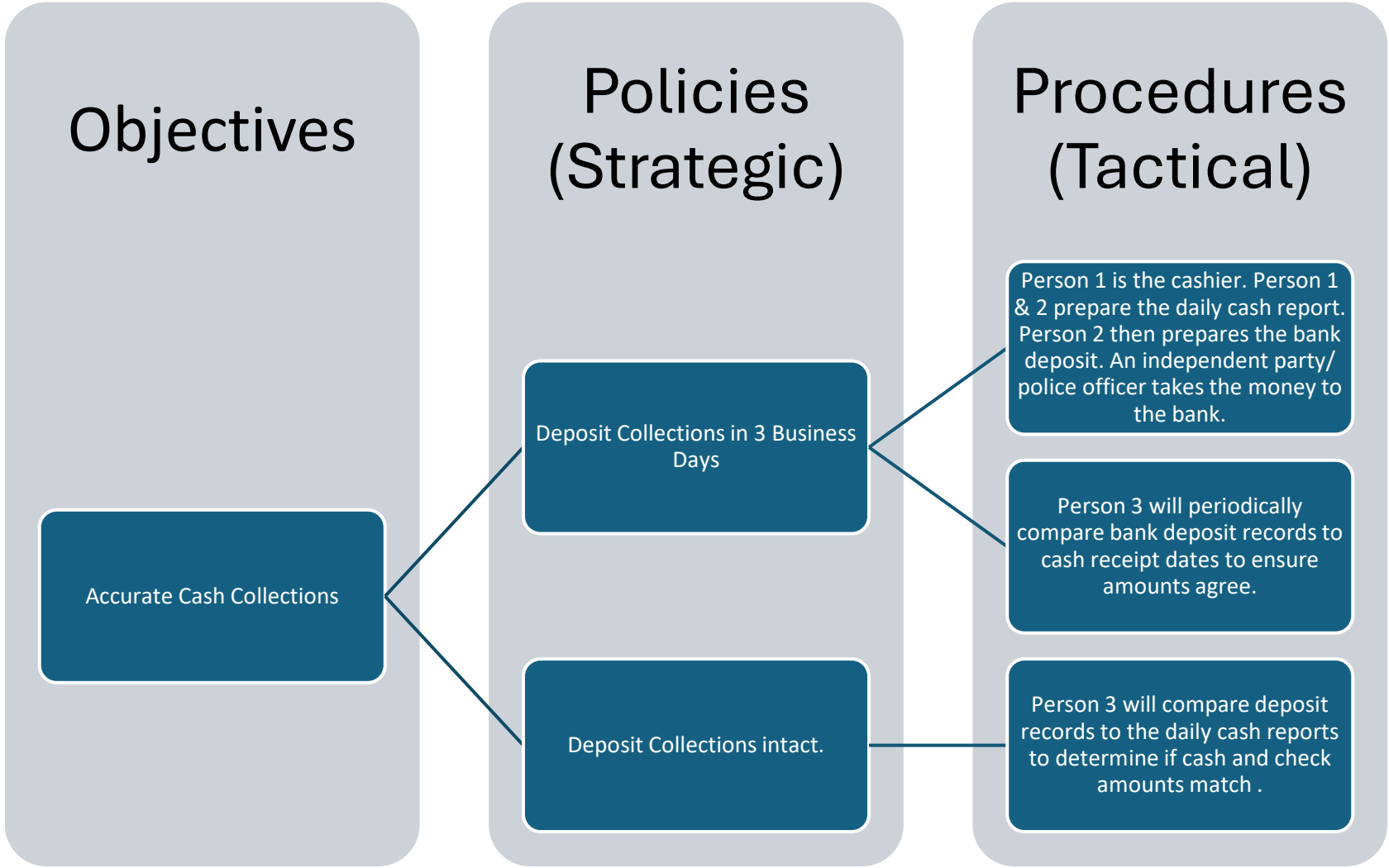
What are Internal Controls?

- An early warning for potential problems
- Measures taken for the purpose of:
  - Protecting resources against waste, theft, fraud and inefficiencies
  - Reducing potential liabilities, fines and penalties
  - Ensuring accurate and reliable accounting and operational data
  - Securing compliance with the policies
  - Evaluating the level of performance
  - Protecting employees
  - Generating accurate and reliable financial reporting
  - Maintaining effective and efficient operations
  - Complying with laws, regulations, contracts and agreements
- Annual financial Reporting (AFR) & Auditors

Purpose of Internal Controls

- Safeguarding - Protect government's assets against loss or misuse and properly authorized
  - Failure to maintain fixed assets, thereby shortening their useful life
  - Failure to avoid duplicative purchasing
  - Failure to maintain adequate cost accounting systems
  - Failure to invest available cash to best advantage and opportunities
  - Failure to avoid investments with unacceptable risk
  - Failure to take advantage of all applicable discounts on purchases
- Management – Effective, efficient and compliant use of resources
- Accountability – Reliable, accurate and timely accounting and reporting systems

Sample of Internal Controls



Actual procedures will be in greater detail, including each step and by whom it is performed through the entire cycle of the transaction.

Include the backup employee(s) in the procedure details.

Components of Internal Controls (Types)

Preventative Controls	• Proactive
Detective Controls	• Monitoring
Corrective Controls	• Remediation
Compliance	• Laws & Regulations

Control Component (Types) - Preventative

- **Preventive Internal Controls** –
  - Discourage errors or irregularities (Proactive)
    - Separation / Segregation / Effective / Efficient Duties
    - Computer Application Validity & Integrity
    - Proper Authorization
    - Checks & Balances
    - Reading and Understanding Policies
    - Adequate Documentation
    - Managerial Review & audit
    - Physical Safeguards & Security over Assets
    - Effective “Whistle Blowing” Processes
    - Keeping people honest
    - Escalation Path / Bypass

Control Components (Types) - Detective

- **Detective Internal Controls** –
  - Detect undesirable activities that have already occurred (Monitoring)
    - Exceptions Reports
    - Reviews and Reconciliations
    - Comparisons Reports
    - Managerial Review
    - Physical Inventories
    - Audits
    - Self Assessments
    - Anomalies in data

Control Components (Types) - Corrective

- **Corrective Internal Controls** –
- Corrects issues or errors that have been detected
  - Policies and procedures for reporting errors and irregularities
  - Training employees on new policies and procedures
  - Positive discipline to prevent future errors
  - Mechanisms that respond to specific circumstances
    - Software patches designed to fix known issues
    - Sprinkler systems that are activated when fire is detected
    - Systems that block access or transactions if irregular or suspicious activity is detected
  - Continuous improvement processes to adopt the latest operational techniques

Control Components - Compliance

- **Compliance Internal Controls** –
- Adherence with applicable Texas laws and regulations
  - Audit of Municipal Finances - Local Government Code 103
  - Public Funds Investment Act – Government Code Chapter 2256
  - Public Funds Collateral Act – Government Code Chapter 2257
  - Depositories for Municipal Funds – Local Government 105
  - And many others…

  - Texas Constitution and Statutes - Texas Constitution and Statutes – Home
- Federal Regulations
  - MSRB, SEC, FINRA, others…

The COSO Framework

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.

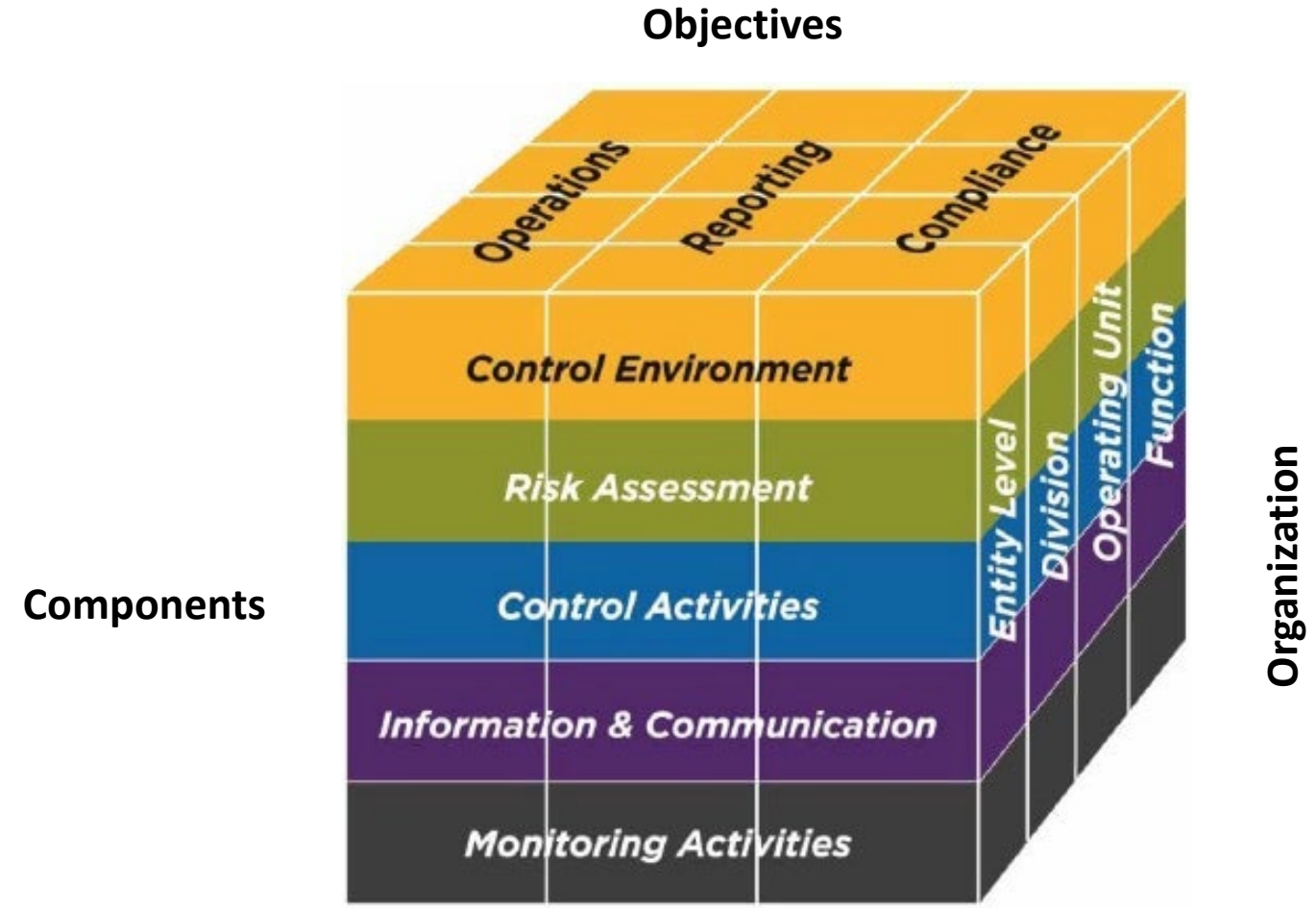
https://www.coso.org/

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 Framework 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 Components – Control Environment

- **<u>Control Environment</u>** –
  - Environment in which people conduct their activities and carry out their job functions
  - Management is responsible for setting the “Tone at the Top” including:
    - Policies and procedures
    - A code of ethics
    - Standards of conduct
    - Encouraging integrity and leadership
    - Assigning authority and responsibility
    - Commitment to staff Integrity and ethical value
    - Commitment to competence
    - Leadership example and operating style
    - Employee development and goals
    - Establishment of policies and procedures

COSO Components – Risk Assessment

- **Risk Assessment** –
  - Management must be able to identify, analyze and manage any risk that prevents them from achieving their objectives
  - Risk increases:
    - during a time of change or prior problems
    - Reliance on 3rd. Party providers
  - Ask yourself "What could go wrong and what assets do we need to do protect"
  - Risk assessments are tools to help in identification of risks as well and their potential impact on the organization
  - High – Medium – Low / Probability
  - Institutional memory and bandwidth
  - Professional judgement and experience

COSO Components – Risk Assessment

- **Risk Assessment** –
  - Both external and internal sources should be addressed
  - A precondition is establishment of objectives
  - Objectives must be identified before steps are taken to manage risk
    - Operational objective - efficiency and effectiveness of the operations
    - Financial reporting objectives – reliable published financial statements
    - Compliance objectives – laws and regulations
      - All 3 must work together
  - It is an ongoing and continuous process of identification and remediation
  - Managing change requires a constant assessment of risks and their impact on internal controls

COSO Components – Control Activities

- **Control Activities** –
  - Policies and procedures that ensure management directives are carried out
  - Occur through the organization at all levels and in all functions. Including:
    - Approvals, Authorizations
    - Verifications, Reconciliations
    - Reviews of Operational Performance
    - Security of Assets and Property
    - Segregation of Duties
  - Control Activities involve two elements:
    - **Policies** establishing what should be done
    - **Procedures** to effect and comply with the policy
  - How do we know when something has changed?
    - Periodic review

COSO Components – Control Activities

- **Control Activities** –
  - Segregation of Duties
    - Reduces the likelihood of errors and irregularities
    - Separation of (Authorization, Custody and Record Keeping)
  - Functions Rotation benefits:
    - Cross training
    - Procedure validation and accuracy
    - Fraud detection
    - Change of function & dependency empathy
    - Identification of efficiencies

COSO Components – Control Activities

- **Control Activities** –
  - Physical restrictions
    - Safeguard assets, processes and data
      - Door & cabinet locks, physical barriers, ID cards
  - Documentation and Record Retention
    - Records maintained and controlled for established retention period and proper disposal.
  - Monitoring Operations
    - Reconciliation
    - Confirmation
    - Exception Reports

COSO Components – Control Activities

- **Control Activities** –
  - Personnel –
    - Need to be competent and trustworthy
    - Established lines of authority with escalation
    - Responsibility documents in written job descriptions and procedures manuals
  - Authorized Procedures
    - Thorough review of supporting information for effective transactions

COSO Components – Info. & Communication

- **Information and Communication** –
  - General Controls
    - Controls over data center operations, software, acquisition and maintenance, access security
      - Patches and upgrades
    - Supports Application Controls
  - Application Controls
    - Help to ensure the completeness and accuracy of transaction processing, authorization and validity
  - Communication Controls
    - Must be reliable and timely and deal with internal as well as external players

COSO Components – Info. & Communication

- **Information & Communication** –
  - Relevant, reliable, and timely communications
  - Recorded, documented and communicated to management in a form and within a time frame that enables them to carry out their responsibilities
  - Operating information is also needed to determine whether the entity is achieving its compliance requirements under various laws and regulations
  - Should occur in a broad sense with information flowing down, across, and up the organization
  - Should be the normal course of business

COSO Components - Monitoring

- **Monitoring** –
  - Should be an ongoing process
  - Assesses the quality of performance over time
  - Ensures that findings are resolved promptly
  - Assists in determining proper action to be taken
  - Communication deficiencies between individuals responsible and management

The Risk Assessment

Risk Assessment – Questions to Ask

- What can go wrong?
- What assets are we protecting?
- How could we fail?
- Where are we vulnerable?
- How could someone steal or disrupt?
- What information do we rely on most?
- What is our greatest legal exposure?

Qualitative –vs- Quantitative Risk Assessment

Qualitative Risk Assessment:

- Assessing risks based on their probability of occurrence and impact on project objectives.
- Using subjective judgment and experience rather than quantitative data.
- Providing a holistic view of qualitative project risks.
- Building a theoretical model of risk without relying on numerical or mathematical analysis.
- Quantifying risk associated with a particular hazard using subjective method
- Quick but subjective.
- Relies on a person's judgment.
- Builds a theoretical model of risk.
- Less detailed.

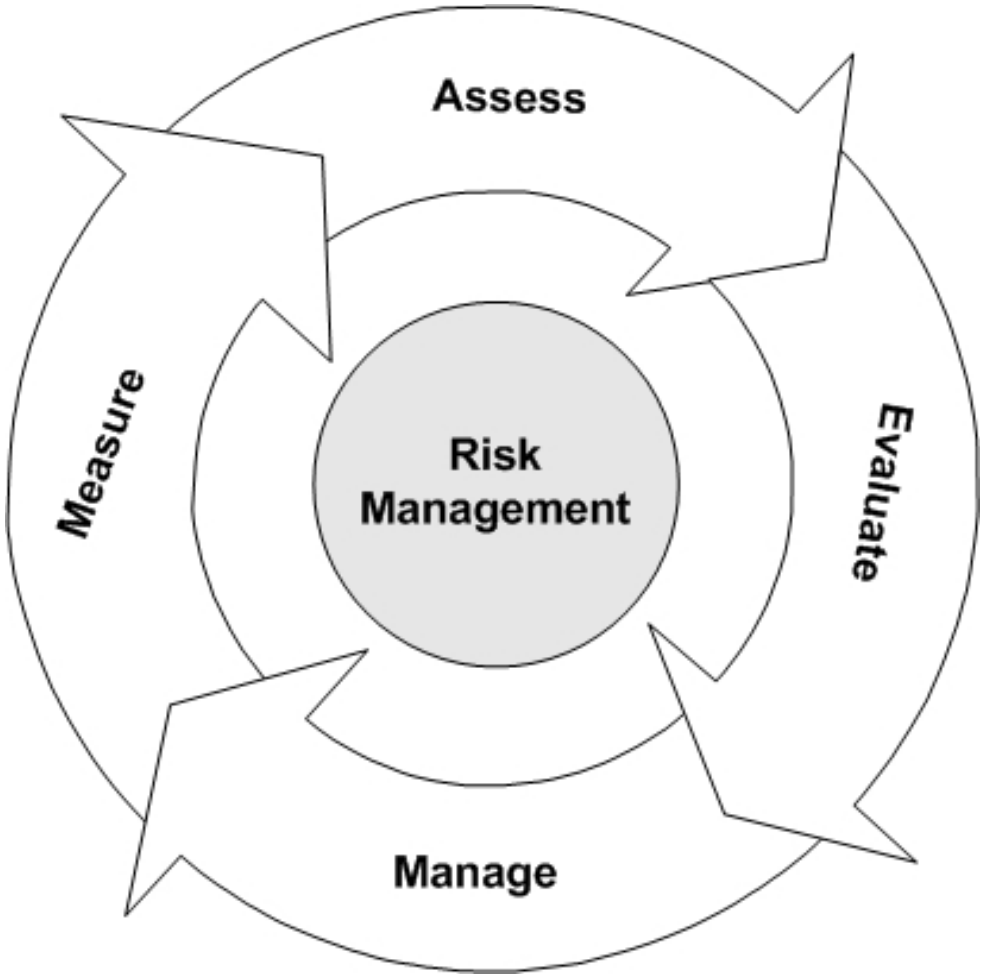
Quantitative Risk Assessment:

- Using realistic and measurable data to calculate the impact values of risks based on their probability of occurrence.
- Analyzing potential events that may result in loss.
- Assigning numerical values to risks using mathematical models and simulations.
- Calculating the possible outcomes of risks.
- Estimating how risks might impact project objectives, particularly in terms of cost and schedule.
- Objective and more detailed.
- Uses mathematical models and simulations.
- Assigns numerical values to risk.
- Requires more time and is more complex.

Risk Assessment

- **Strategic –**
  - Prevents an organization from accomplishing its objectives.
- **Regulatory –**
  - Non-compliance with laws and regulation resulting in penalties and fines.
- **Operational –**
  - Prevents efficient and effective operations.
- **Financial –**
  - Results in a negative financial impact.
- **Reputational –**
  - Result in negative publicity
- The relationship between likelihood and consequencs

Risk Assessment



Risk Assessment Matrix

	Consequence				
Likelihood	Insignificant	Minor	Moderate	Major	Critical
Rare	LOW Accept the risk Routine management	LOW Accept the risk Routine management	LOW Accept the risk Routine management	MEDIUM Specific responsibility and treatment	HIGH Quarterly senior management review
Unlikely	LOW Accept the risk Routine management	LOW Accept the risk Routine management	MEDIUM Specific responsibility and treatment	MEDIUM Specific responsibility and treatment	HIGH Quarterly senior management review
Possible	LOW Accept the risk Routine management	MEDIUM Specific responsibility and treatment	MEDIUM Specific responsibility and treatment	HIGH Quartely senior management review	HIGH Quarterly senior management review
Likely	MEDIUM Specific responsibility and treatment	MEDIUM Specific responsibility and treatment	HIGH Quarterly senior management review	HIGH Quarterly senior management review	EXTREME Monthly senior management review
Almost certain	MEDIUM Specific responsibility and treatment	MEDIUM Specific responsibility and treatment	HIGH Quarterly senior management review	EXTREME Monthly senior management review	EXTREME Monthly senior management review

The Responsibilities

Managerial/Administrative Responsibility

- Identify areas of weakness
- Strengthen practices and procedures
- Propriety & accuracy of transactions
- Reliability and integrity of information
- Compliance of policies and regulations
- Safeguarding assets & people
- Economy, efficiency and effectiveness of operations

Internal Audit Responsibility

- Provides the independent evaluation of the adequacy of Internal Controls
- Look at how the Internal Controls work together to make up the structure
- Looks at processes identifying errors, irregularities and inefficiencies
- Discussion and review with the managers
- Personnel –
  - Competent and trustworthy with clear lines of authority and responsibility defined with descriptions and procedures
  - Organizational charts
  - Periodic updates of job descriptions

Internal Audit Responsibility

- Authorization Procedures
  - Thorough review of supporting information
  - Propriety and validity of transactions
- Segregation of Duties
  - Reduces the likelihood of errors and irregularities
  - Separation of (Authorization, Custody and Record Keeping)
- Physical Restrictions
  - Protecting (Assets, Processes and Data)
    - Safe combinations changed periodically
    - Critical forms and checkbooks adequately secured
    - Alarm systems
- Documentation and Record Keeping
  - Assurance that assets are controlled, and transactions correctly recorded

Internal Audit Responsibility

- Monitoring Operations
  - Verify that the controls are operating correctly
  - Reconciliation, Confirmations, and Exceptions Reports
- Responsibility
  - Managers and supervisors execute control policies and procedures
  - Individuals are responsible for specific job responsibilities
  - IA is to examine the adequacy and effectiveness of ICs and make recommendations
  - ICs are enhanced through reviews and recommendations made by IA

4 Types of Internal Control Weakness

- Technical
  - Hardware / Software
- Operational
  - Human error
- Administrative
  - Policies and Procedures
- Architectural
  - Systems are not adequately designed
  - System implementation is not adequately monitored

What Jeopardizes Internal Controls?

- Inadequate Segregation of Duties (most common)
  - Separating custody from record keeping
- Inappropriate Access to Assets
  - Internal controls should provide safeguards for physical objects, restricted information, critical forms and application updates
- Inadequate Knowledge of Policies
  - Policies are not static
- Form Over Substance
  - They look good, but lack substance and enforcement
- Onboarding process for new employees
  - Trial by fire or structured integration?

What Jeopardizes Internal Controls?

- Control Override
  - Exceptions to established policies can pose a significant risk
- Inadequate knowledge of policies and regulations
- Inadequate access to assets
- Inadequate segregation of duties
- Inherent Limitations
  - Human errors will always be present
    - Misunderstandings, fatigue, stress, form over substance
- Internal Control Limitations
  - Staff size limitations
  - Technology limitations
  - Budget limitations

Limitations of Internal Controls

- Human error
- Manual Processes
- Technical Weakness
- Segregation of Duties
- Lack of Accurate Data
- Too Many Controls
- Inconsistent Controls
- No Sharing of Controls
- Static Controls
- Control Blind Spots
- Insufficient Resources
- Siloed Evaluation
- Collusion / Fraud
- Management Override
- Lack of Engagement
- Compromised Judgement
- Murphy’s Law
- The Unknown

How Much Do Internal Controls Cost?

- Cost should not exceed the expected benefit of the control.
  - Alarm system versus a door lock
  - Computer screen saver with passwords
  - Realignment of duties and assignments
  - A well-designed Internal Control structure incorporates people more so than systems
  - Analyzing tangible versus intangible consequences
    - Good will
    - Public Trust
    - Tone at the Top

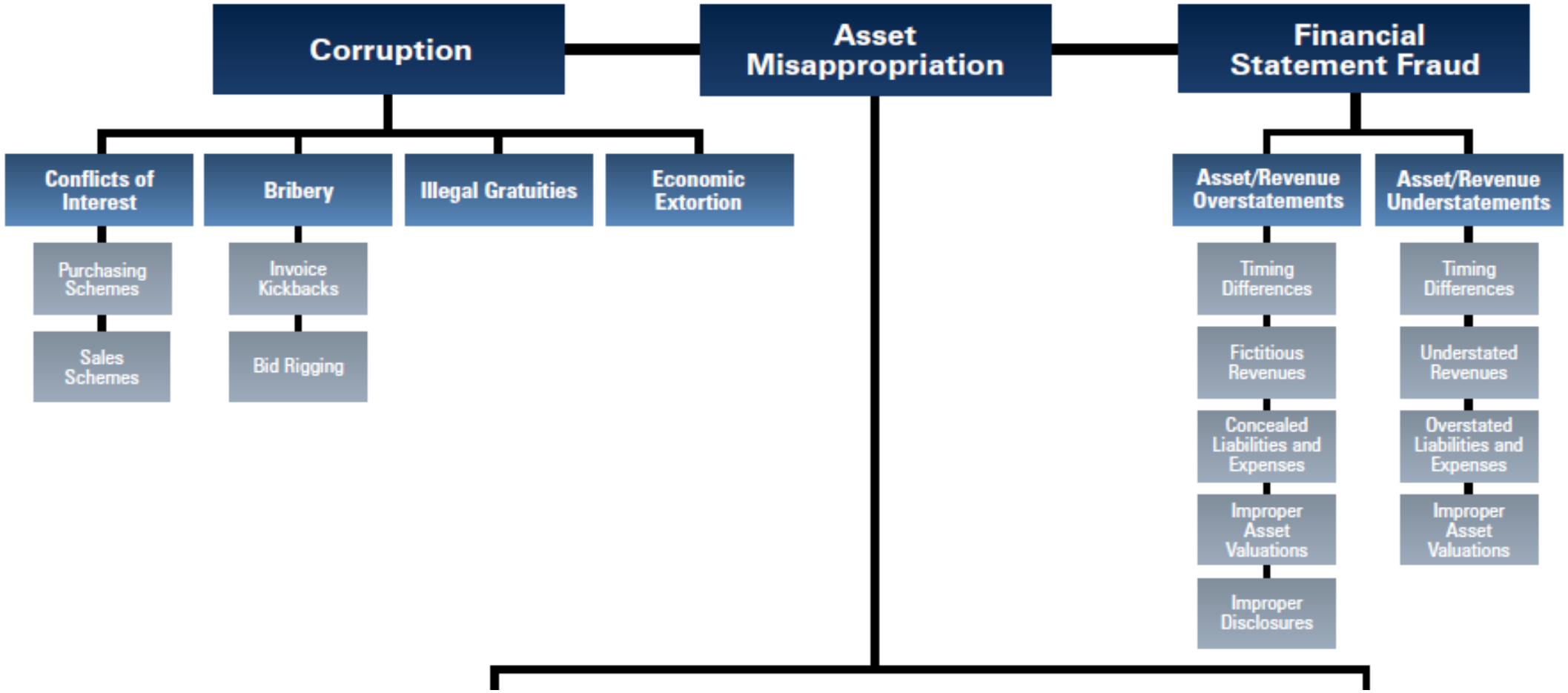
ACFE Association of Certified Fraud Examiners

acfe.com

Causes of Fraud

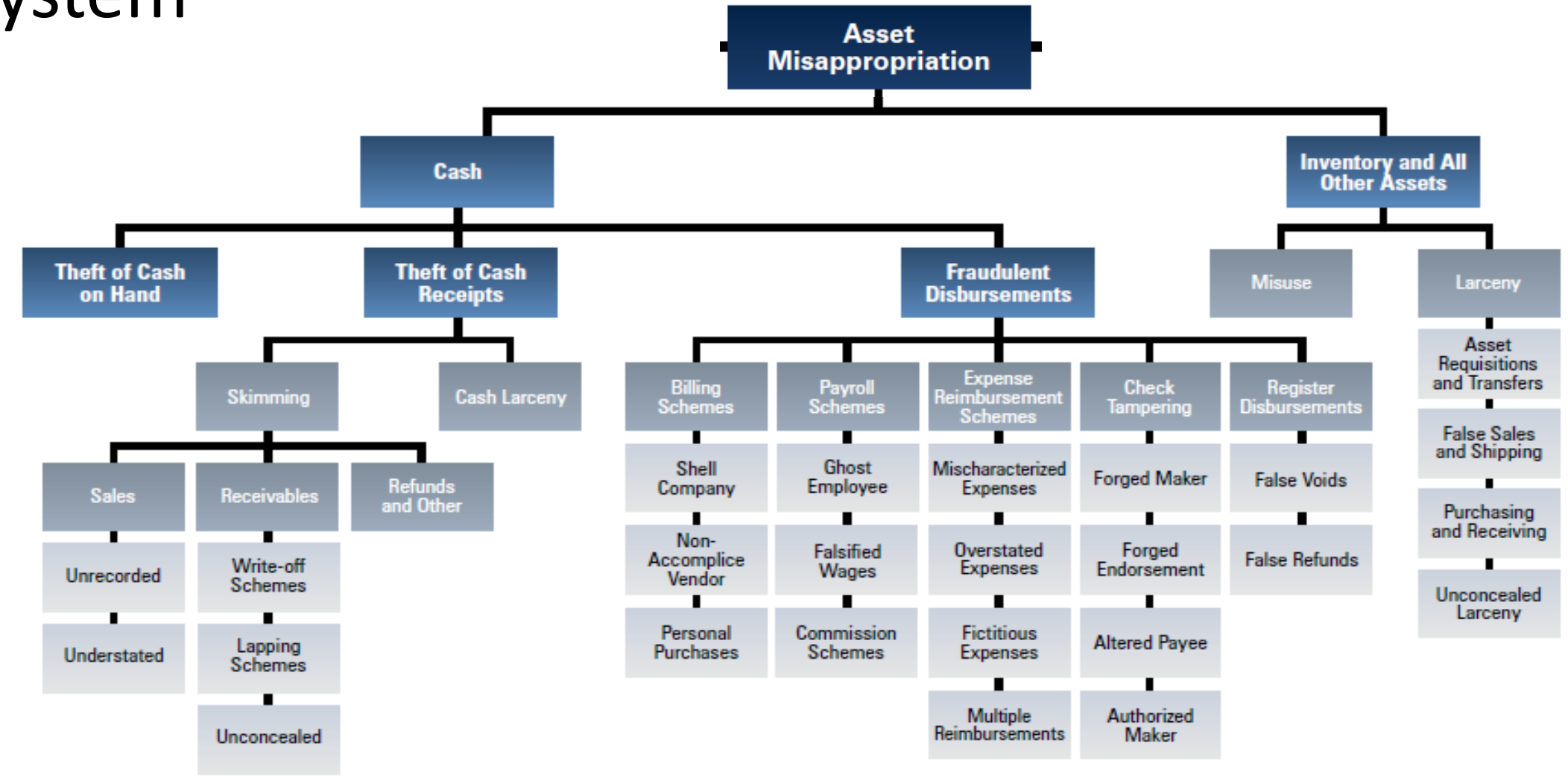
ACFE.org

Occupational Fraud and Abuse Classification System



ACFE Report to the Nations on Occupational Fraud and Abuse 2024

Occupational Fraud and Abuse Classification System



ACFE Report to the Nations on Occupational Fraud and Abuse 2024

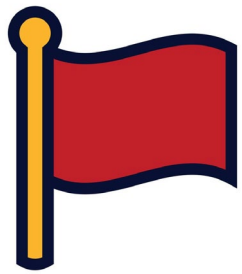
ACFE - Top 4 Internal Controls

- Below are the top four internal controls that reduce fraud losses and can improve detection:
  - **Surprise audits**
  - **Financial statement audits**
  - **Hotlines**
  - **Proactive data analysis**

  - These four anti-fraud controls were associated with a 50% or greater reduction in both fraud losses and fraud duration. Surprise audits, financial statement audits and proactive data analysis are all mechanisms that can be used to actively look for fraud, so their correlation with reduced fraud losses and duration stands to reason. In contrast, hotlines are less directly tied to fraud detection, but likely help increase the perception of detection and form the foundation for a holistic anti-fraud culture.

ACFE - acfe.com

Red Flags, Checklists and Recommendations



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
- Bookkeeping / 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.

Internal Control Checklist

Segregation of Duties	Yes	No	NA
Responsibilities for initiating, evaluating and approving transactions segregated from detailed accounting, G/L entries and other functions?			
Transaction initiating segregated from final approvals?			
Investment market valuations and performance segregated from investment acquisition?			
Maintaining detailed accounting records segregated from G/L entry?			
Custodial responsibilities and ownership segregated from accounting duties?			
For electronic record keeping systems, do processing activities require layered approvals?			

Assoc. of Public Treasurers

Internal Control Checklist

Procedural Controls	Yes	No	NA
Procedures adequate to ensure only investments allows by law and the local policy are acquired?			
Investment Policy guidelines established and formally reviewed?			
Investment Policy been approved or reaffirmed within the past year?			
Investment program integrated into the cash management program and expenditure requirements?			
Authority and responsibility been established and defined for investment evaluation and purchase?			

Assoc. of Public Treasurers

Internal Control Checklist

Procedural Controls	Yes	No	NA
Procedures for restrictions or legal limitations on pooling, disposition of investments and/or use of income proceeds?			
Is the performance of the portfolio periodically evaluated by persons independent of investment activities?			
Are formal procedures established governing the level and nature of approvals required to purchase/sell investments?			
Are competitive bids or quotes sought for investment purchases?			
Is the competitive bid process defined in the Investment Policy?			

Assoc. of Public Treasurers

Internal Control Checklist

Custody Controls – Custody Procedures	Yes	No	NA
Do physical safeguards exist for legal documents and agreements?			
Purchased securities are delivered DVP?			
Banking system requires a minimum of 2 signatures for approvals?			
All securities/collateral registered in the name of the entity?			
Safekeeping agents and holdings are periodically inspected / confirmed?			
Accounting records are timely and accurate from safekeeping custodian / bank / pool?			
Individuals with access to securities / investments insured or bonded?			

Assoc. of Public Treasurers

Internal Control Checklist

Custody Controls – Accounting Controls	Yes	No	NA
Detailed accounting records maintained?			
Cash invested with accordance to laws and regulations?			
Detailed accounting records separate from G/L functions?			
Procedures in place for proper investment calculations such as income and amortization entries?			
Controls exist to confirm investment earnings are credited to the proper funds?			
Periodic confirmation that income received closely matches calculations from security purchase terms?			
Are transactions recorded on a timely basis?			

Assoc. of Public Treasurers

Internal Control Checklist

General Ledger Controls	Yes	No	NA
Procedures exist for reconciling the detailed accounting records with the G/L controls?			
Are investment results monitored for compliance with the laws and local policies?			
Are investments maintained by trained and accountable personnel?			
Is the G/L system backed-up per local policies and confirmed via restoration periodically?			

Assoc. of Public Treasurers

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

Ways to Identify Accounts Payable Fraud

- Duplicate Payments
- Benford's Law
- Rounded Amount Invoices
- Invoices Just Below Approval Amounts
- Check Theft Search
- 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
- Validate Payment Instructions Against Existing Records / Documentation

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 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
- Close relationships between an employee and vendor
- Tips or complaints from employees, customers or vendors
- Invoices in numerical or accounting sequence
- Invoices/documentation 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 / employee address

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

GFOA Best Practices

https://www.gfoa.org/best-practices

Theft of Funds (Fraud) – In Texas

- Texas Penal Code, Title 7, Chapter 31
- 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/

Strong Tenets of Fraud Prevention

Establish Ethics and a Code of Conduct

Segregation of Duties

Implementing Internal Controls

Regular Assessments

Whistleblower Protection

Training Programs

Monitoring Systems

External & Surprise Audits

- Compliance with Laws and Regulations
- Never Underestimate
- Never Replace Diligence with Automation
- Observe, Listening and Question
- Beware of Subterfuge, Decoys and Obfuscation
- Occam’s Razor

Summary

- Know the priority
- Build a program of compliance and effective internal controls
- Spend time on strong policies and procedures
- Protect your assets and identify your liabilities
- Understand all functions in your department
- Establish objectives and performance measures
- Design & Application / Training & Awareness
- Monitor and track performance
- Be willing to adapt and change if needed