Responding to Fraud in the Work Place

Accounting Day 2019
May 13, 2019

Jenny Dominguez, Signing Director
CPA/CFF, CFE

Michael Schulstad, Director
CPA/CFF/CGMA/FBI(ret)

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor
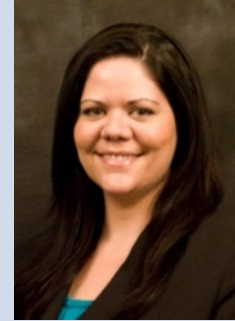
Create Opportunities

Introduction

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

2

Speaker Introduction

Signing Director
CLA's Forensic Practice

Over 18 years of experience leading fraud investigations, forensic accounting projects, and internal control reviews for large government organizations, education institutions, and commercial businesses.

Jenny Dominguez

CPA/CFF, CFE

Speaker Introduction

Director, *CLA's Forensic Practice*

Over 28 years of professional law enforcement experience performing forensic examinations and analysis of contract, health care, bank, business, bankruptcy, government and procurement fraud, as well as bank failure, money laundering and asset forfeiture. Former FBI Special Agent.

Michael Schulstad

CPA, CFF, Ex FBI

Role of the Outside Forensic Accountant in Financial Fraud Investigations

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Objectives

1. Identify when outside Forensic Accountants / Financial Investigators should be called upon – "Predication"

2. List of various "Scopes of Work" to be conducted by outside Forensic Accountants / Financial Investigators

3. Describe "Investigative Techniques" utilized by Forensic Accountants / Financial Investigators

4. Contrast between Law Enforcement vs. private sector investigative techniques

"Predication"

When and Why we are called upon to conduct a Financial Fraud Investigation

Predication

"…the totality of circumstances that would lead a reasonable, professionally trained, and prudent individual to believe a fraud has occurred, is occurring, or will occur. Predication is the basis upon which a fraud examination/investigation is commenced. Fraud examinations should not be conducted without proper predication."

(Source: Association of Certified Fraud Examiners – ACFE)

Some Examples of Predication

1. Complaint from a "Whistleblower" – or other "Tips"
2. Internal Audit Findings
3. External Audit Findings
4. Difficulties in Financial Reporting/Information/Disclosure
5. Issues involving Customers or Vendors
6. Potential "Conflict of Interest" concerns
7. Foreign Corrupt Practice Act (FCPA)
8. Responding to Regulatory Action
9. Unusual journal entries, transactions or trends
10. Others?

Are These Sufficient Predications?

1. Employee John Doe seems to be living beyond his means…

2. Employee Mary Doe is a trouble maker and we want her fired…

3. Our insurance expense costs seem to have increased significantly but yet our business model hasn't changed…

4. A new CFO has been hired and she wants to clean house…

5. The Board wants to get rid of the Superintendent so take a look at all payments to him and find us some dirt…

Create Opportunities

"Scope"

Goals and Objectives of our Investigations

Some Goals and Objectives

- "Administrative" – Human Resource Issues – Possible termination
- "Insurance" – Proof of Loss – Get Reimbursed!
- "Civil Litigation" – Suit against fraudster for recovery of fraudulent funds
- "Criminal Referral" – See that "Justice" is done
- "Internal Controls" – Implement ICs so fraud doesn't happen again
- Forensic Accounting / Data Analytic Projects
- Other?

What Do You Do When the CEO Wants to Personally Arrest the Fraudster?

What Do You Tell The CEO?

- Two trusted employees colluded to embezzle $5.6 Million over a 10 year period.

- The CEO is extremely angry at his external CPA's as they did not detect the fraud.

- He wants to sue them ASAP!

- CEO asked your opinion.

- What do you tell the CEO?

Responsibility of External Auditor

AU-C Section 240

- The Auditor is responsible for the detection of fraud that "would have a direct and material effect" on the financial statements.

- The primary responsibility for the prevention and detection of fraud rests with both those charged with governance of the entity and management.

Responsibility of External Auditor

Frauds your External Auditor Probably will not detect:

- Majority of Embezzlements
- Theft of Cash Receipts "Skimming of Cash"
- Fraudulent Disbursements
- Corruption/Bribery
- Conflict of Interest

"Investigative Techniques"

Utilized in our Investigations

Overt/Covert Investigative Techniques

- Data Analytics of financial records
- Search warrants
- Interviews
- Undercover agents
- Cooperating witnesses/sources
- Title IIIs
- Surveillance
- Database checks

- Computer Forensics
- Consensual monitoring
- Mail cover
- Trash cover
- Polygraph
- Liaison with counterparts
- Toll register

How Would You Handle This?

- A Whistleblower says he has valuable information concerning an ongoing major fraud in your organization.

- He is ready to speak to someone about this.

- How do you handle this?

Contrast between Law Enforcement

vs.

Private Sector Investigative Techniques

Some Key Differences

Criminal Prosecution

- "Justice is served"

- Not required to advise the victim organization of internal control weakness and recommendations to improve internal controls

- Not required to ensure the victim organization gets all their monies back

- Not required to keep the victim organization "in the loop" as to the progress and findings of the criminal investigation

- All legal investigative techniques at their disposal

- The financial ability of the victim organization to pay for the criminal prosecution is not a factor

Some Key Differences

Private Sector Fraud Examinations/Investigations

- Purpose: Depends on your "Scope"

- If requested by victim organization (client) we will advise them of internal control weaknesses and recommendation to improve internal controls

- Not required to ensure the victim organization gets all their monies back – but attempt to identify magnitude of loss

- Yes – required to keep the victim organization "in the loop" as to the progress and findings of our investigation

- Not all legal investigative techniques are at our disposal

- The financial ability of the victim organization to pay for the fraud examination/investigation is a major factor on work we can perform

Use of Computer Forensics and Data Recovery in an Investigation

Computer Forensics in an Investigation

- Preserve relevant evidence

- Gather relevant evidence

- Identify electronic evidence relevant to the investigation

- Consider impact of electronic evidence on investigation

Preserve Relevant Electronic Evidence

- Through consultation with legal counsel, determine whether employee should be put on administrative leave during investigation

- Identify and preserve sources of electronic evidence (company owned & issued):
  - Computer (desktop, laptop)
    ◊ Ensure all portable devices are turned in immediately
    ◊ Do not power on or shut down
    ◊ If necessary, move device to a secure location (IT, HR, locked office)
    ◊ Do not wipe or re-issue device
  - Mobile device and/or tablet
    ◊ Ensure all mobile devices are turned in immediately
    ◊ Do not power on or shut down
    ◊ Obtain passcodes from employee
    ◊ Do not wipe or re-issue devices; store in a secure location

Create Opportunities

Preserve Relevant Electronic Evidence (cont.)

- Identify and preserve sources of electronic evidence (company owned & issued) - continued:
  - Company email
    - ◊ Immediately remove employee's access to email account
    - ◊ Discuss with IT ability to preserve emails, including "deleted" folders
    - ◊ Do not allow other employees to access/search emails of employee
  - Access to accounting system, servers, etc.
    - ◊ Immediately remove employee's access to all company systems/servers
    - ◊ Do not give employee's log-in credentials to other employees to "fill in"
    - ◊ Discuss with IT ability to access and preserve any user folders/files used by employee
  - Building access
    - ◊ Immediately remove employee's access to building

Create Opportunities

Gather Relevant Electronic Evidence

- Through consultation with legal counsel, determine whether organization can legally obtain and review electronic evidence as part of investigation

- Computer hard-drives:
  - Obtain forensic image of hard-drives for computer devices used by employee
  - Use licensed professional (Certified Digital Forensic Examiner)
  - Forensic image = read only

- Mobile devices:
  - Generally, cannot be forensically imaged
  - Use licensed professional (Certified Digital Forensic Examiner)
  - Can make a back-up of the data on a mobile device to search and review

Gather Relevant Electronic Evidence (cont.)

- Company email:
  - Licensed digital forensics professional will work with internal IT to extract employee's email from email server/system
  - Ensure that inbox, sent files, and all other folders (including deleted) are obtained
  - If possible, obtain employee's electronic calendar (depending on nature of investigation)

- Server data:
  - A copy of all relevant server data (user folder) can be obtained through internal IT
  - Assess whether departmental files stored on server should be gathered and reviewed

- Accounting data:
  - Generally obtained by request from the accounting department (general ledger, disbursement register, etc.)

Gather Relevant Electronic Evidence (cont.)

- Building access:
  - Assess whether building access logs could provide relevant evidence
  - Obtain access logs through IT
  - Reports generally can be provided in Excel or PDF print report

Identify Relevant Electronic Evidence

Once you have gathered all of the relevant electronic evidence:

- Index data

- Search data (using key words, date parameters, etc.)

- Review results of relevant searches
  - Third-party online review tools
  - Extract files to server folder or external drive

Impact of Electronic Evidence on Investigation

- School District:
  - Principal negotiated a contract with a third-party to use the high school's parking lot for evening/weekend events at a cost of $2,500 per event/day
  - Principal represented to district that the amount collected was $10 per car and average number of cars was 30-60 per event/day ($300-$600)
  - Principal's emails revealed that he was sending invoices to the third-party for $2,500 per event/day
  - Funds were being deposited into a bank account opened by principal in school's name and funds were being paid to his personal business and other inappropriate expenses

- County Office:
  - Allegation that employee was secretly recording conversations with other employees
  - Image of laptop hard-drive revealed a recording application with various recordings of conversations/meetings

Impact of Electronic Evidence on Investigation

- School District (misrepresentation of facts):
  - Principal negotiated a contract with a third-party to use the high school's parking lot for evening/weekend events at a cost of $2,500 per event/day
  - Principal represented to district that the amount collected was $10 per car and average number of cars was 30-60 per event/day ($300-$600)
  - Principal's emails revealed that he was sending invoices to the third-party for $2,500 per event/day
  - Funds were being deposited into a bank account opened by principal in school's name and funds were being paid to his personal business and other inappropriate expenses

- County Office (illegal acts):
  - Allegation that employee was secretly recording conversations with other employees
  - Image of laptop hard-drive revealed a recording application with various recordings of conversations/meetings

Impact of Electronic Evidence on Investigation

- School District (knowledge):
  - School officials gave construction work to a contractor without going out for a public bid (over $100k)
  - One official interviewed claimed no knowledge of the requirement to bid
  - Several emails between the official and facilities indicated that the official had knowledge of the public bidding dollar thresholds

Questions?

Anti-Fraud & Data Analytics Methodology

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Objectives

1. Describe the importance of proactive fraud auditing

2. List current statistics and trends with respect to proactive fraud auditing

3. Identify and describe common fraud indicators

4. List and describe the 5 phases of the data analysis methodology

5. Identify commonly requested data sets and the key elements of a data request list

Objectives

6. Identify the 5 types of data analytic tests

7. List and describe common data analytic tests

8. Describe key considerations for implementing data analytics

Forensic Thinking

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

38

Six Elements of Fraud

- A representation
- About a material point
- Which if false
- And intentionally or recklessly made
- Which is relied upon
- Victim suffers damage
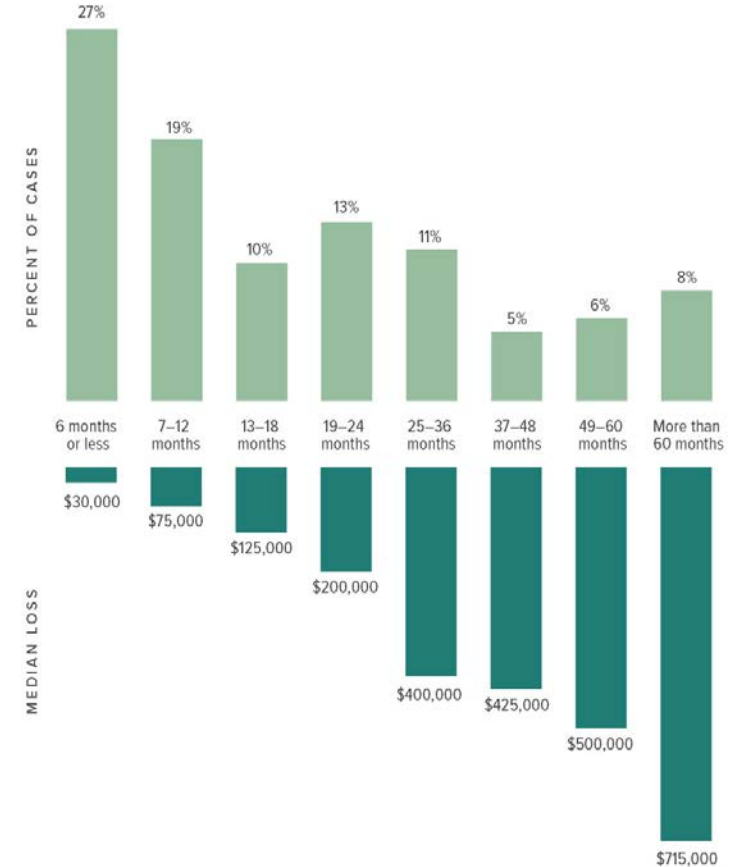
DECEPTION!

Frequency and Cost of Fraud

- The typical organization loses 5% of annual revenue to fraud.

The longer the duration of a scheme, the higher the median loss.

FIG. 7 How does the duration of a fraud relate to median loss?

Active Detection Methods Reduce Fraud Loss

FIG. 11 How does detection method relate to fraud duration and loss?

- Active detection method
- Potentially active or passive detection method
- Passive detection method

MEDIAN MONTHS TO DETECTION

$39,000 — 5 months — IT controls
$50,000 — 6 months — Surveillance/monitoring
$52,000 — 11 months — Account reconciliation
$108,000 — 12 months — Internal audit
$110,000 — 14 months — Management review
$130,000 — 18 months — Document examination
$126,000 — 18 months — Tip
$250,000 — 23 months — External audit
$150,000 — 24 months — By accident
$186,000 — 24 months — Confession
$935,000 — 24 months — Notified by police

Maintaining Skepticism

- Acknowledge that fraud risk exists
- Encourage open and candid discussion
  - If I were to try to commit fraud, how would I do it?
- Continuously assess the risk of management and control override
- Openly display your skepticism to set the tone at the top and spread awareness
- Take swift action when fraud event occurs and make the event of action (not the details) known internally

Weaknesses That Contribute to Fraud

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Lack of internal controls 30%

Override of existing controls 19%

Lack of management review 18%

Poor tone at the top 10%

Lack of competent personnel in oversight roles 8%

Other 6%

Lack of independent checks/audits 4%

Lack of employee fraud education 2%

Lack of clear lines of authority 2%

Lack of reporting mechanism <1%

FIG. 23 How do internal control weaknesses vary by scheme type?
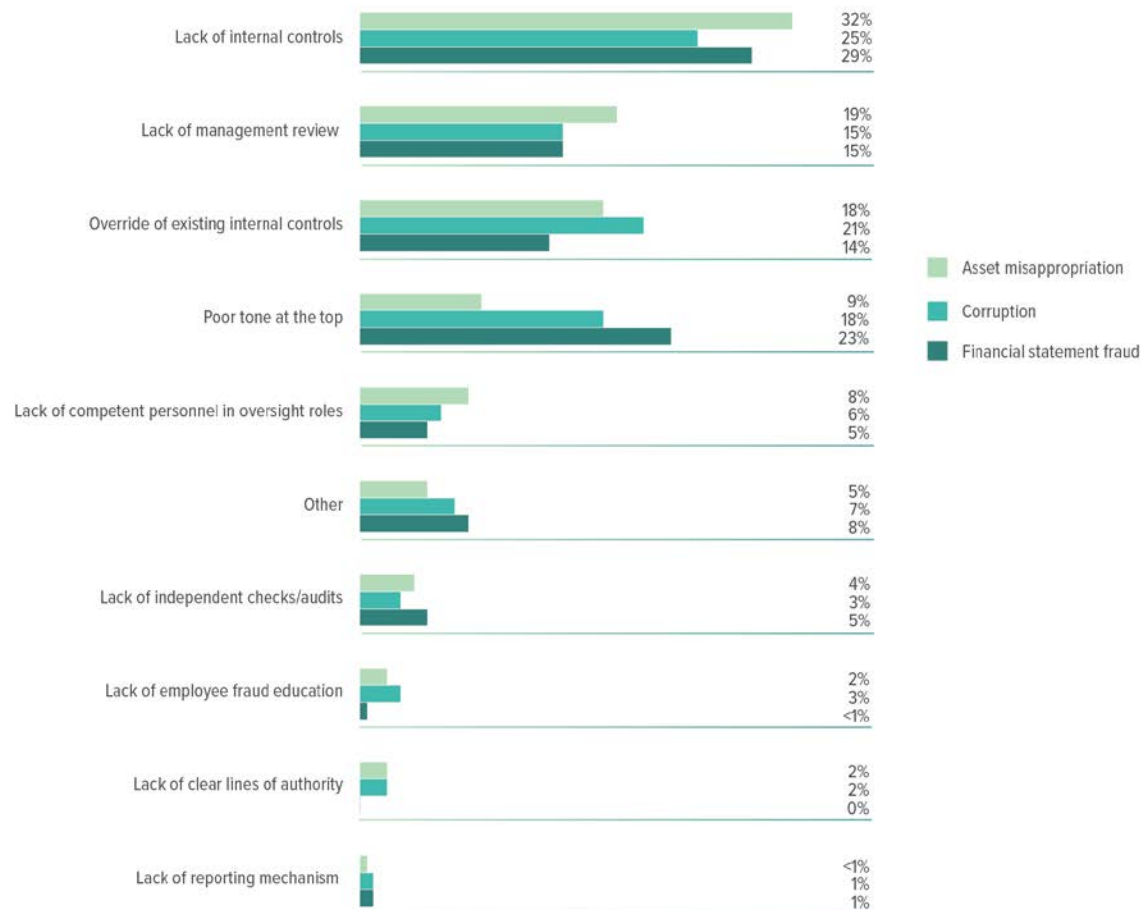
Lack of internal controls: 32%, 25%, 29%

Lack of management review: 19%, 15%, 15%

Override of existing internal controls: 18%, 21%, 14%

Poor tone at the top: 9%, 18%, 23%

Lack of competent personnel in oversight roles: 8%, 6%, 5%

Other: 5%, 7%, 8%

Lack of independent checks/audits: 4%, 3%, 5%

Lack of employee fraud education: 2%, 3%, <1%

Lack of clear lines of authority: 2%, 2%, 0%

Lack of reporting mechanism: <1%, 1%, 1%

Asset misappropriation
Corruption
Financial statement fraud

Create Opportunities

Fraud Types

The Fraud Tree

FIG. 4 Occupational Fraud and Abuse Classification System (the Fraud Tree)
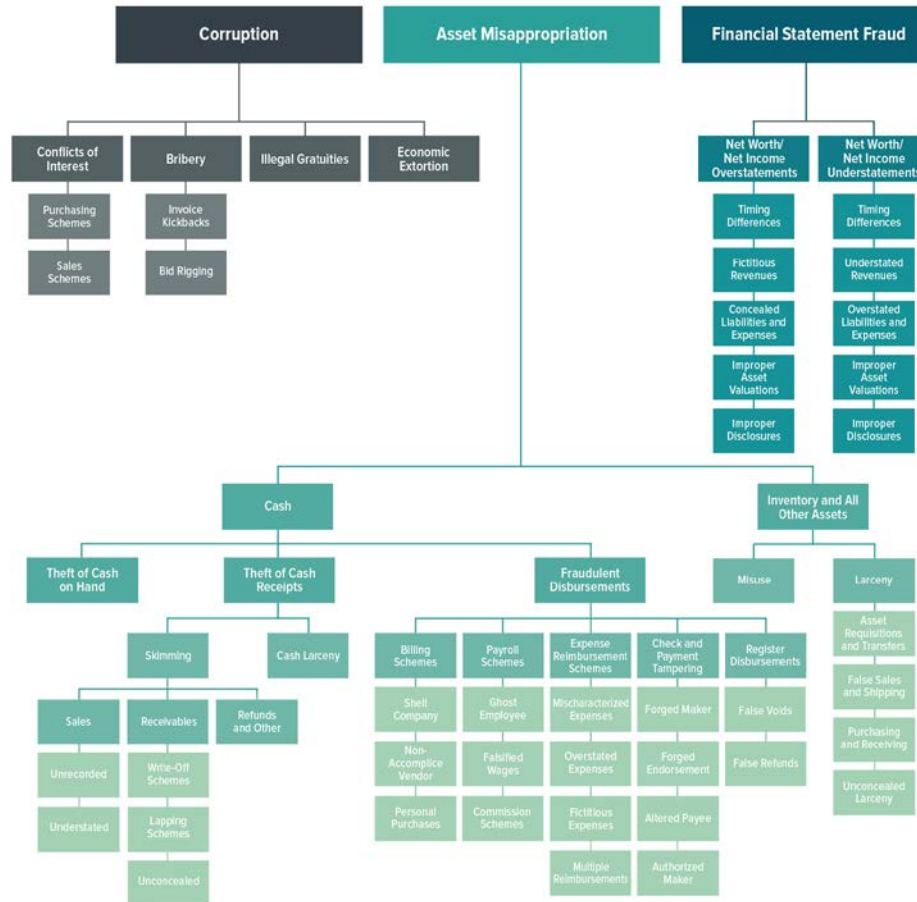
Internal Audit

The Impact of Internal Audit

FIG. 11 **How does detection method relate to fraud duration and loss?**
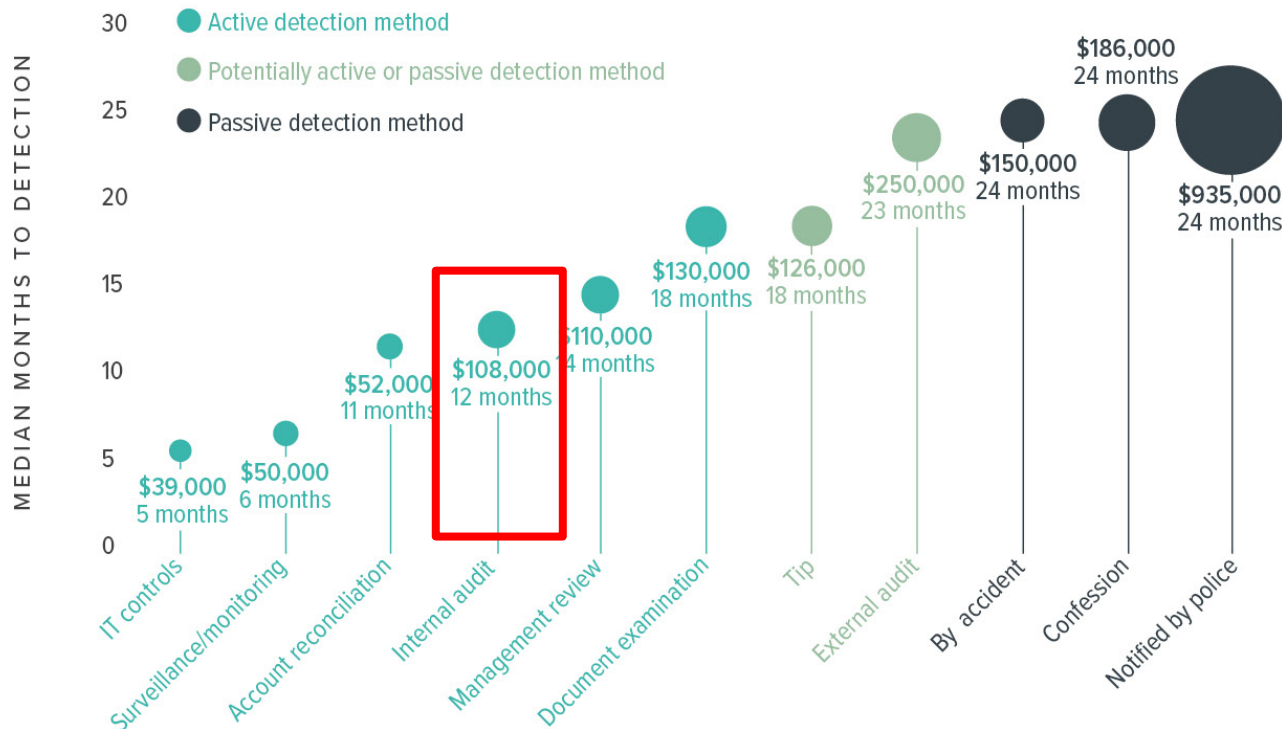
Internal Audit and Your Organization

- How does management view internal audit and their purpose?

- Does management understand the purpose of an internal audit department?

- Does management understand the benefits of having an internal audit department in your organization?

Deloitte's 2018 Global Chief Audit Executive Survey
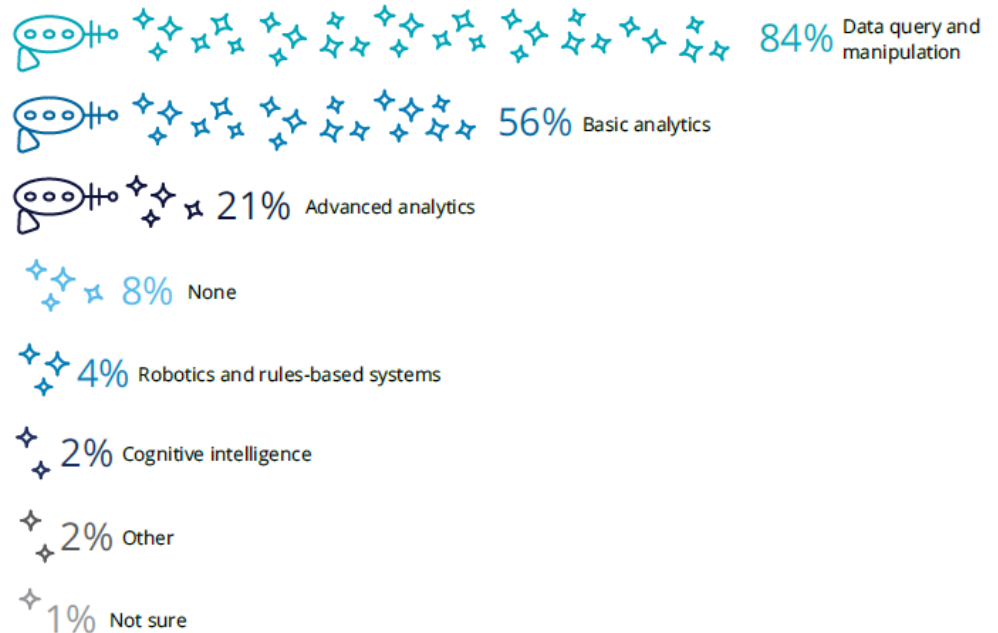
- 21% of Internal Audit groups are using advanced data analytics
- Up from 7% in 2016

Types of analytics used

Types of analytics techniques 'typically' in use within the Internal Audit function

84% Data query and manipulation

56% Basic analytics

21% Advanced analytics

8% None

4% Robotics and rules-based systems

2% Cognitive intelligence

2% Other

1% Not sure

2019 North American Pulse of Internal Audit

Deployment of analytics by the Internal Audit function

During fieldwork	**65%**
As part of audit scoping	**46%**
As part of the annual audit planning process	**31%**
For continuous auditing	**26%**
To provide assurance over operational effectiveness of internal controls	**23%**
To develop reporting	**18%**
For continuous risk assessment	**18%**
Do not currently use analytics	**14%**
Other	**3%**
Not sure	**1%**
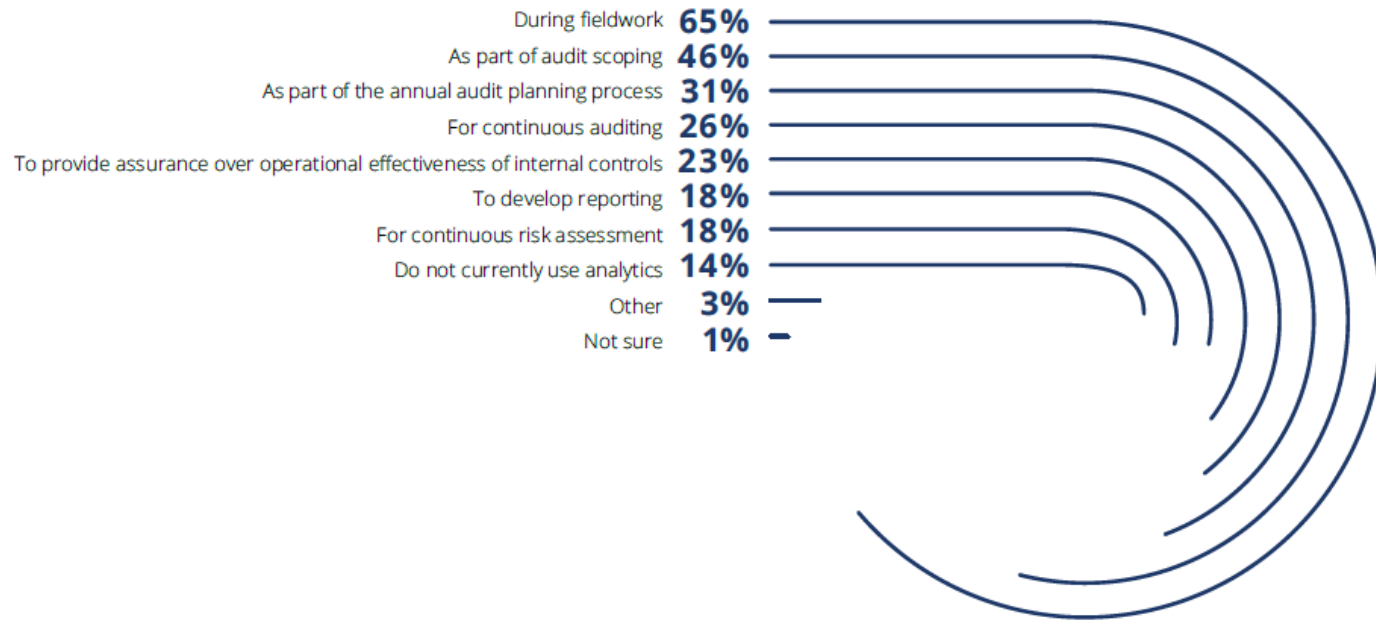
Quick Poll

- How well is your team utilizing *Computer Assisted Audit Techniques* (CAAT)?
- What tools are being used for data analysis?
- What is keeping us from performing *better* data analysis?

> **It is difficult to explain what data analysis is, but you know it when you see it.**

Excel

Data

IDEA / ACL
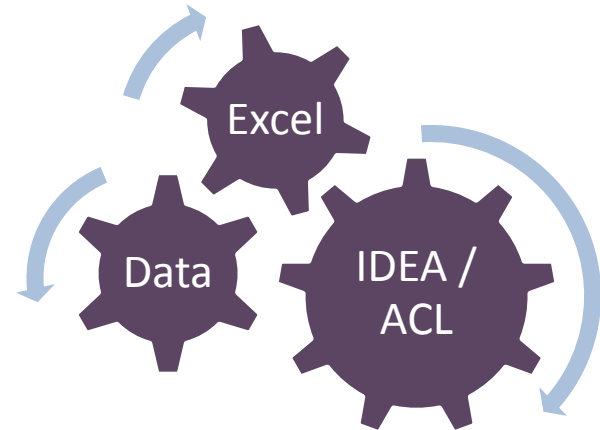
CLA's Robust Data Analysis Methodology

Value of Data Analytics

Data analytics can improve the effectiveness and efficiency of your engagement by:

- Focusing attention on areas of high risk

- Identifying previously unknown risks

- Providing greater insight and interpretive value

- Improving compliance with professional standards

- Enhancing capabilities by leveraging available technology to work smarter and more comprehensively

Risk Based Approach to Analytics

- Systematically identify greatest risk areas specific to the organization

- Tailor analytics to assess and better understand those areas

- Readily analyze 100% of the data rather than extrapolating from samples

- Compare results across time, by location, by supervisor, etc.

Use Effective Planning and Risk Assessment to Direct Analytics
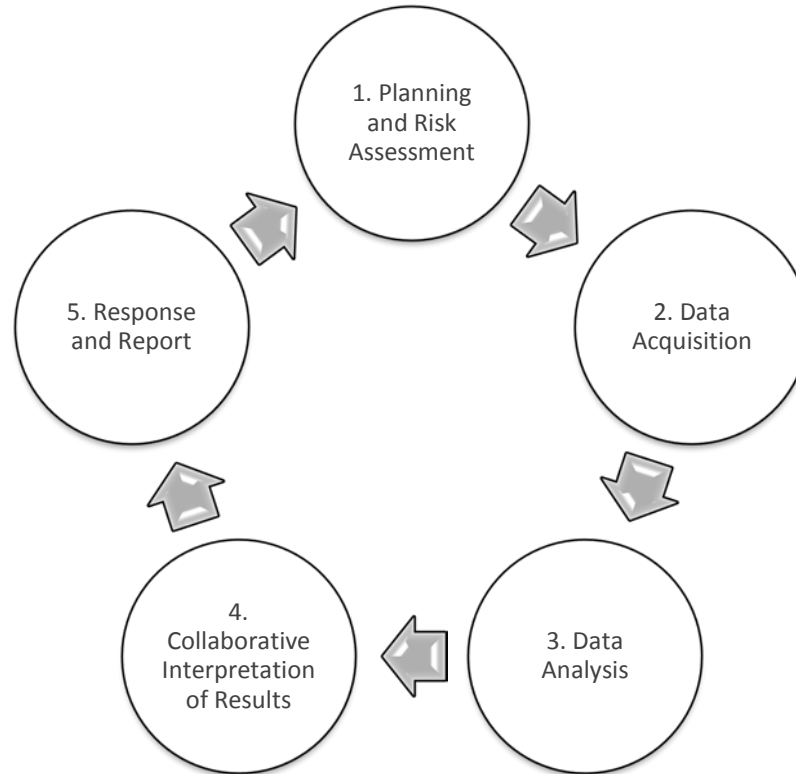
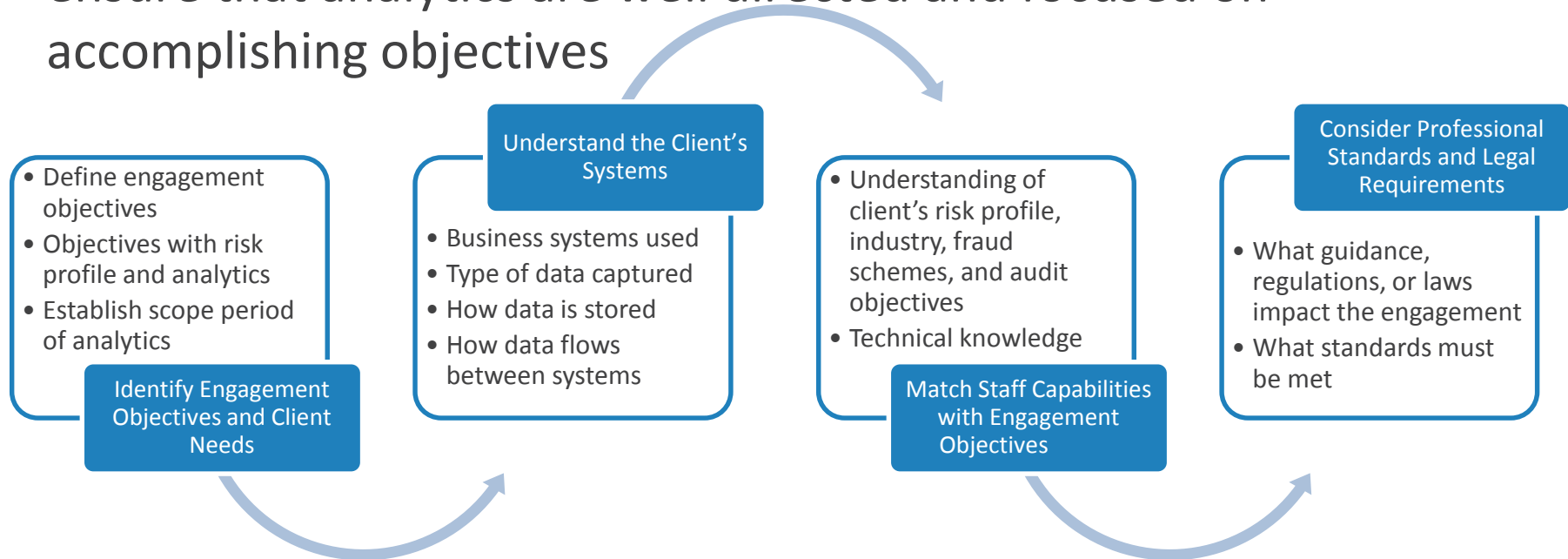WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

57

Data Analysis Methodology – 5 Phases

1. Planning and Risk Assessment

2. Data Acquisition

3. Data Analysis

4. Collaborative Interpretation of Results

5. Response and Report

Planning

Planning is a team effort, staff to principal should contribute to ensure that analytics are well directed and focused on accomplishing objectives

- Define engagement objectives
- Objectives with risk profile and analytics
- Establish scope period of analytics

Identify Engagement Objectives and Client Needs

Understand the Client's Systems

- Business systems used
- Type of data captured
- How data is stored
- How data flows between systems

- Understanding of client's risk profile, industry, fraud schemes, and audit objectives
- Technical knowledge

Match Staff Capabilities with Engagement Objectives

Consider Professional Standards and Legal Requirements

- What guidance, regulations, or laws impact the engagement
- What standards must be met

Brainstorming to Identify High Risk Areas for Analytic Testing

1. **Assess known risks (impact and likelihood) facing the client**
   - Economic
   - Industry
   - Client specific

2. **Consider the three basic types of fraud and <u>what fraud would look like in the data</u>**
   - Financial statement fraud
   - Asset misappropriation
   - Corruption

Brainstorming to Identify High Risk Areas for Analytic Testing

3. **Understand the fraud triangle**
    –   Pressure – motivation for committing act
    –   Opportunity – method by which act can be committed
    –   Rationalization – justification making act acceptable
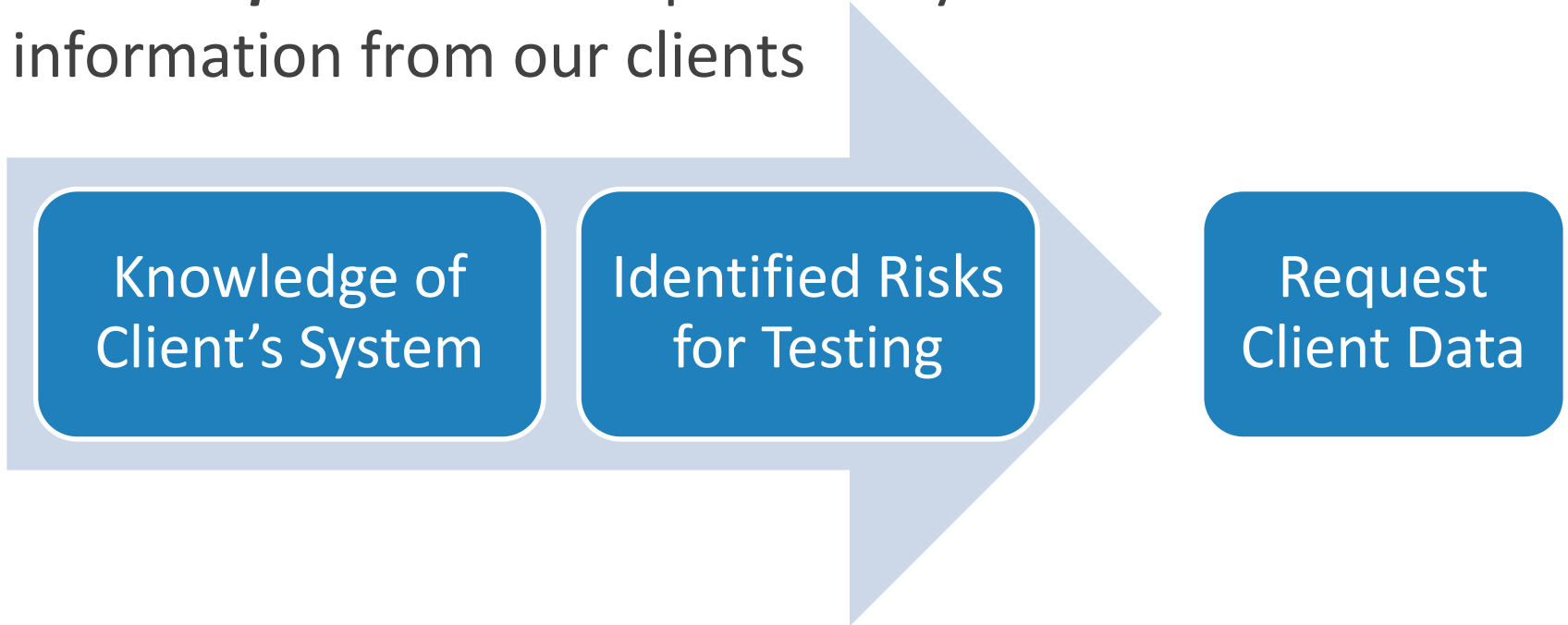4. **Understand the who, where, and why of likely fraud perpetrators**
    –   Role/position/tenure
    –   Departments/business area
    –   Age/gender
    –   Education level

Rationalization

Pressures   **Opportunity**
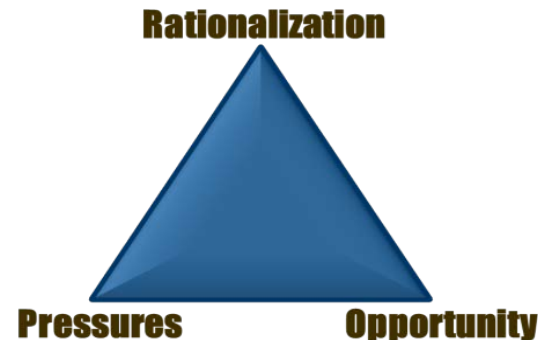
Data Acquisition

Data acquisition is the process by which we obtain information from our clients

Knowledge of Client's System	Identified Risks for Testing	Request Client Data

Commonly Requested Information

- Accounting, General Ledger
- Accounts Receivable
- Accounts Payable
- Inventory Manufacturing
- Sales
- Cash Disbursements
- Procurement
- Payroll
- Entity Credit Cards
- Travel and Entertainment Expenses
- Activity logs

- Along with the aforementioned data sets, the following information is usually needed to adequately interpret the data files:
  - Chart of Accounts
  - Data Dictionary
  - File Source Listing – indicating from which systems and locations the data was extracted
  - Vendor Master File (A/P, A/R, Sales)
  - Employee Master File (Payroll, Travel and Entertainment, Credit Cards)

Technical Data Analysis

Technical data analysis requires the combination of technical capability and analytical knowledge.

- <u>Technical capability </u>is one's proficiency using the available tools.

- <u>Analytical knowledge </u>comprises understanding of the client's risk profile, industry, and engagement and is required to apply the tools to accomplish the engagement objectives.

Fundamental Skills

Fundamental skills that are common across data analysis software packages:

- Project organization/data management
- Importing
- Normalizing
- Calculated/modified fields
- Appending/merging
- Joining/connecting

- Indexing/sorting
- Filtering/extracting
- Summarizing
- Stratification
- Aging
- Benford's Law
- Duplicate testing
- Gap testing
- Sampling

- Cross tabulation/pivot table
- Searching
- Statistical analysis
- Charting
- Exporting

Ensure Complete and Accurate Data

It is <u>critical</u> for effective analytics to ensure that the data from the client is both complete and accurate

- **Proper Importation** – verify that the imported data accurately reflects the files provided by the client

  - Verify field type definitions (character, numeric, date/time)

- **Completeness** – verify that the information provided by the client reflects all transactions or data expected

  - Compare data to another source (e.g., recalculate account balances from general ledger detail and compare to trial balance report)

Prepare Data for Analytic Tests

Once verified as complete, data must be normalized or prepared for analysis

- **Reformatting**
  - Convert fields imported as one field type into another (e.g., dates as character fields)
  - Merging or separating fields (e.g., to segregate or join fund and account codes)
- **Extracting only necessary information**
  - Transactions out of the scope period or extraneous fields can be extracted to streamline testing
- **Joining data**
  - Linking information from supplemental files or disparate sources

Example Areas of Focus and Analyses that may be Considered

Types of Risks and Areas of Analysis

Accounts Payable

- Fictitious vendors
- Fictitious, inflated and / or duplicate invoices
- Structured payments
- Conflicts of interest
- Kickbacks
- Bid-rigging

Purchase Cards

- Duplicate purchasing and reimbursement schemes
- Unauthorized and/or improper purchases
- Unauthorized users
- Unauthorized SIC codes

Payroll

- Ghost employees
- Improper supplemental payments
- Improper bonus or incentive compensation payments
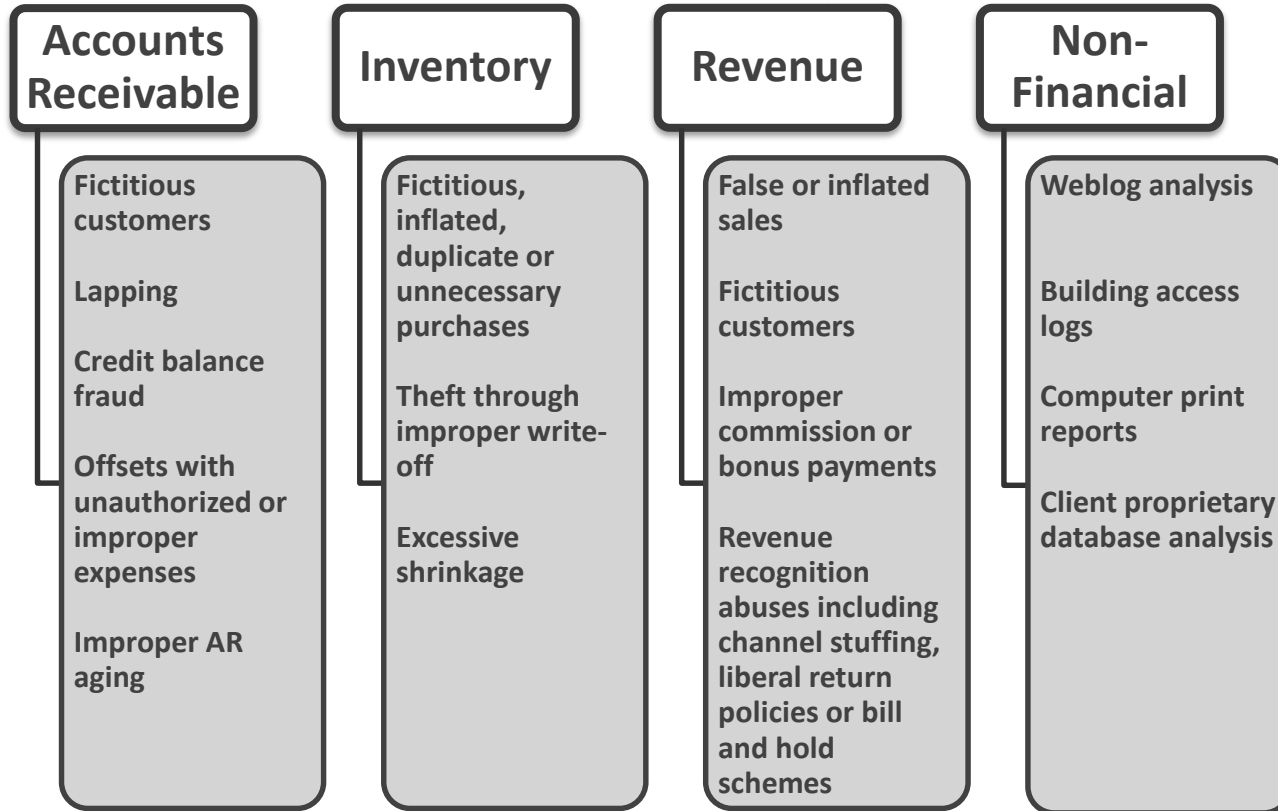- Inflated salaries
- Inflated hours

Travel and Entertainment Expense

- False or inflated reimbursement submissions
- Improper use of corporate credit card
- Purchase for personal use
- Duplicate purchasing and reimbursement schemes
- Foreign Corrupt Practices Act

Journal Entries

- Unbalanced journal entries
- Improper management override
- Improper expense capitalization
- Improper revenue recognition
- Entries to unusual or seldom used accounts
- Improper or unauthorized user activity
- Entries during non-business hours

Types of Risk and Areas of Analysis

Accounts Receivable

Fictitious customers

Lapping

Credit balance fraud

Offsets with unauthorized or improper expenses

Improper AR aging

Inventory

Fictitious, inflated, duplicate or unnecessary purchases

Theft through improper write-off

Excessive shrinkage

Revenue

False or inflated sales

Fictitious customers

Improper commission or bonus payments

Revenue recognition abuses including channel stuffing, liberal return policies or bill and hold schemes

Non-Financial

Weblog analysis

Building access logs

Computer print reports

Client proprietary database analysis

General Ledger

- Ensure reconciliation and completeness of systems and subledgers flowing in the trial balance
- Assess and review the activity of subledgers, understand manual vs. automated
- Identify user access, user threshold level controls and consistency of access and control across the organization
- Trend results over time, such as monthly:
  - Account level results
  - Business unit level results
  - Geography based results
  - Relevant Revenue and Expense groupings
- Identify suspicious entries such has transactions to suspense accounts, reversals, or entries occurring with strange timing

Cash Disbursements

- Understand vendor relationships:
  - Identify key vendors
  - Identify new/unapproved vendors
  - Identify related party vendors
  - Identify vendors receiving suspicious recurring or one-time payments
- Reconcile Inter-company and Inter-branch transactions
- Identify duplicate payments
- Identify payments that were structured to evade threshold level controls

Cash Disbursements

- Identify unapproved disbursements

- Understand out of sequence payments

- Understand compliance with threshold level controls

- Analyze disbursements by vendor type, review for reasonableness

- Trend vendor level disbursements by time period to identify increasing or strange trends

Payroll

- Ensure all paid employees are on the appropriate approved lists
- Ensure paid employees are receiving correct salary and hourly rates
- Analyze and understand overtime payments
- Identify payments made before hire date over after term date
- Understand bonus, commission and other non-standard payments
- Analyze pay and pay rates by:
  - Business Unit
  - Geography
  - Job Function

Payroll

- Understand headcount by functional area

- Identify manual adjustments to payroll

- Ensure hours logged in timekeeping software is reasonable, identify employees with excessive overtime

- Review employee master file for:

  - Unusual updates and changes

  - Multiple employees that share contact information and/or bank accounts

  - Missing or unusual personal information

  - Assess Active and Inactive employees for reasonableness

Travel and Expense Reimbursement

- Group payments by meaningful classifications, such as hotel, airfare, meals, mileage, transportation, etc.
- Group payments by meaningful classifications, such as administrative, sales, production, etc.
- Group payments by employee
- Identify duplicate submissions. This can be run on invoice number, amount, employee, month, or description.
- Conduct digital frequency testing. Often, transactions that occur more often than expected are a result of subjective or created amounts. Look for evasion of approval limits, irregular amounts and number invention.
- Identify payments made outside of understood business hours

Travel and Expense Reimbursement

- Organizations commonly use credit cards for business expenses. Each credit card transaction will include a Standard Industry Code (SIC), which classifies the expense by meaningful type, such as airfare, lodging, dining, etc. These codes can be used to analyze expenses.

- Identify gifts and charitable donations

- Identify Multiple Gifts to the same person

- Identify instances where the submitter is the same as the approver

- Identify excessive cash reimbursements

- Understand excessive mileage

- Identify abuse and non-compliance with policies

Customer Account Maintenance

- Identify instances were employees update/change information to their own or their families' accounts

- Identify dormant accounts, where account information was changed, then financial transactions occurred

- Identify significant changes to accounts, such as PIN changes, contact names changes, and the methods of such changes

- Review number of changes to accounts for reasonableness

- Identify accounts held by significant others' of employees

- Identify multiple accounts that owned by the same person or group of people

- Review nature of access to account maintenance, via online, phone, branch visit, other, etc.

Loan Portfolio Analysis

- Analyze loans by type of security, risk profile, amount, etc. Break down results by geography, branch, date of inceptions, etc.
- Analyze loans by individual, business, etc.
- Identify loans to employees and related party
- Identify loans with unusual updates to terms
- Identify loans with unusual and/or inconsistent terms and interest rates
- Isolate and extract loans that are delinquent
  - Break down by type of security, risk profile, etc.
- Analyze and understand write-off activity
- Understand loans by accounts receivable and inventory
- Analyze portfolio by branch, type, officer, etc.

Suspicious Customer Account Activity

- Isolate and review transactions to employee and related deposit and other accounts (related to maintenance)

- Review dormant accounts, where transactions then occurred
  - Often Certificate of Deposit Accounts (or similar) are targeted because transactions are sporadic, create a query for withdrawals greater than 50% (or other amount) of balance after a certain amount of time
  - Identify accounts as dormant by looking at balances and transactions dates and compare listing with accounts that show up on "dormant" reports, are there accounts that are not reported? Why?
  - Understand "dormant" threshold (100 days) and review transactions occurring just below that threshold

- Trend results after accounts is opened, does activity and dollar amounts increase unexpectedly after then first few months?

- Review accounts with related transactions and assess for reasonableness

- Identify accounts that should have generated services charges, but did not, why?

Applying Forensic Techniques to Design Analytics that Address Risk

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Skepticism and Forensic Thinking

Add value through application of "forensic thinking":

- An investigative <u>mindset</u> - more than skeptical

- An <u>understanding of fraud schemes</u> and indicia of fraud

- <u>Experience</u> in dealing with fraud, risk and compliance issues

- <u>Knowledge</u> of certain investigative, analytical and technology-based techniques

- <u>Knowledge of legal process</u> (pitfalls, ramifications, etc. on engagements that may be subject to litigation)

Design and Perform Tests

Design a well rounded and comprehensive set of tests. Give specific consideration to learned insight. Assess known risk, collaborate to identify unknown risk.
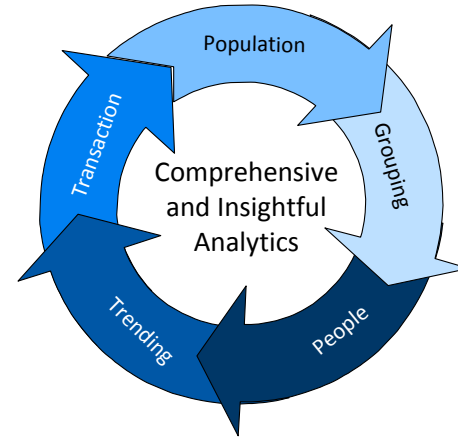
Analytic tests selected from the following five categories will provide insight into the areas being examined.

1. **Population Analytics** – Conducted to gain an understanding of the entire population.
2. **Grouping Analytics** – Summarize transactions into meaningful groups.
3. **People Analytics** – Designed to provide insight into who benefits from a transaction and who is responsible for the transaction.
4. **Trending Analytics** – Provide interpretive value by showing data results over time.
5. **Transaction Analytics** – Isolate transactions exhibiting particular traits or have a certain "DNA".

The Fraud Triangle

Pressure/Incentive

Opportunity

Rationalization/Concealment
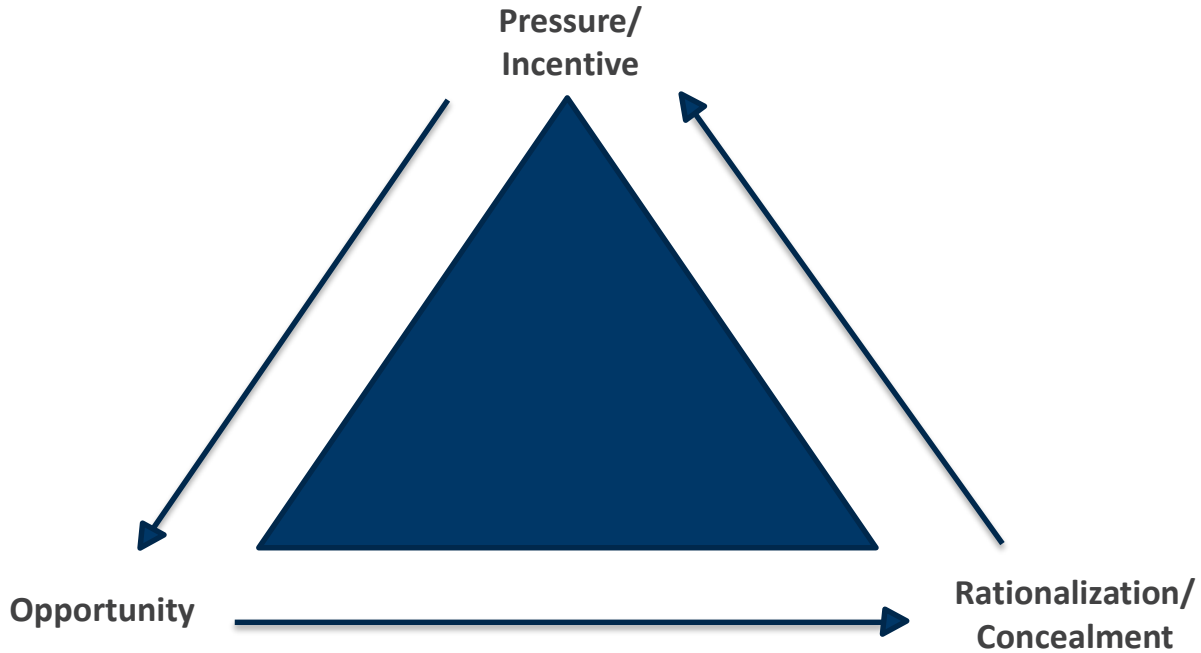
The Fraud Triangle & Data Analysis

- Comparison of company financial data vs. analysts' estimates
- Budgets and forecasts
- Business line or departmental goals
- Analysis of bonus payments
- Benford's analysis
- Identification of round dollar transactions
- Analysis of journal entry description
- Analysis of accounts affecting goals
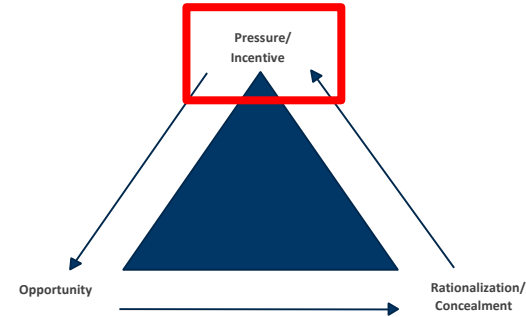
The Fraud Triangle & Data Analysis

- Manual journal entries
- Lack of internal controls
  - Journal entry approval process
  - Knowledge or lack of knowledge of those involved in the journal entry process
- Analysis of user versus approver
- Analysis of system weaknesses
  - Lack usage of certain fields
  - Lack of segregation of duties
  - Ability to open new accounts

Pressure/ Incentive

Opportunity

Rationalization/ Concealment
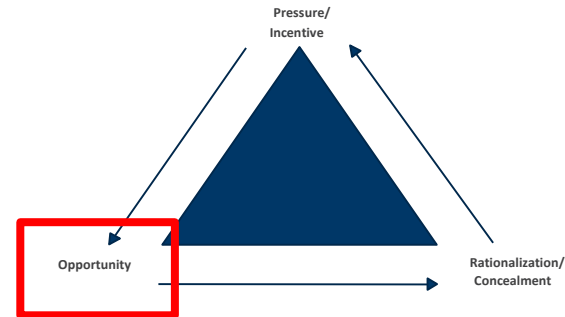
The Fraud Triangle & Data Analysis

- Anomalies identified while trending
- Transactions broken into smaller amounts
- User is the same as approver
- Related party analysis
- Analysis of individuals receiving decreasing bonuses
- Dormant accounts
- Posting entries in prior quarters
- Ghost employees
- Fictitious vendors

Pressure/ Incentive

Opportunity

Rationalization/ Concealment
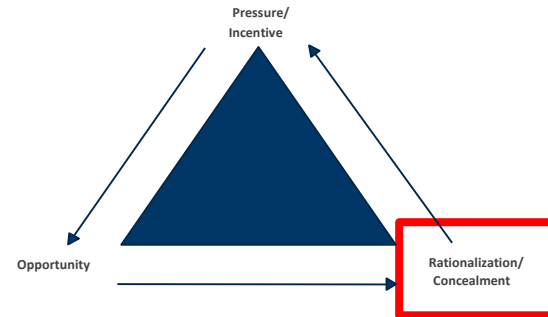
Interpret Results and Subsequent Risk Assessment

Interpretation of the results requires team collaboration to evaluate the data analysis output within the context of the entity's risk profile.

Team Effort

Together the most knowledgeable members of the engagement team should determine which results are relevant to accomplishing the engagement objectives.

Selected Tests Performed by Areas

Population Analytics:

1. Population Stats – Max, Min, Ave, No of Records, Total
2. Cash vs. Credit Card vs. P-Card
3. Expenses by Geographic region
4. Stratification of expenses by amount, understand large and small and where the data lies
5. Benford's law to identify excessive frequency
6. Benford's law to identify impact of threshold controls
7. Perform completeness checking procedures
8. Identify lack of use and or implementation of controls such as blank description fields, generic usernames
9. Identify expenses to unauthorized SIC/MCC codes

Trending Analytics:

1. Late Report Submissions
2. Transactions on holidays, weekends, and on Personal time off days
3. Flights booked in close proximity to travel days
4. Trending expenses by Organization Unit by Month
5. Trending expenses by Type (Hotel, flights, mileage, meals, etc.) by month
6. Expenses by date
7. Organizational Unit monthly results and forecasting
8. Top "X" transactions by Type by Month
9. Top "X" transactions by Expense Type by Month

Selected Tests Performed by Areas

People Analytics:

1. Headcount – total, department
2. Spend by Employee by Business Unit
3. Identify Employees whose spend is increasing at "x" rate
4. Personal and Non- business expenses by Industry code
5. Compare Number of purchases and amount of purchase over time to other with similar job tiles
6. Identify employees with more volume and large dollar value of credit transactions
7. Identify employees who approved their own expense reports
8. Identify Employees who spent large amounts by expense type (for example a hotel stay of $1,250/night, when the average was $200 for hotel in city)
9. Identify employees with excessive lack of supporting documentation
10. Expenses at Merchants that are related parties to employees

Grouping Analytics:

1. T&E Spend by Organization Unit
2. T&E Spend per Expense Type
3. Calculate totals and average per day for travel by location, identify lavish locations and trips to known locations outside of the norm
4. Spend by Merchant, review merchant names for personal use (PayPal, Apple stores, etc.)
5. Group transactions by type by time period for reasonableness (for example, 2+ parking expenses per day)
6. Group by description and search for suspicious words, such as cash, consulting fees, misc., government official

Selected Tests Performed by Areas

Specific Risks:

1. Duplicates where the Amount, Date, and Employee were the same
2. Duplicates where the Amount, Month/Quarter and Employee were the same
3. Duplicates where the same item was charged to the credit card and P-card
4. Duplicates submitted within 90 days
5. Policy non-compliance
6. Hotel stays with no corresponding flights
7. ID Payments to electronic currency vendors (PayPal, google wallet, apple pay, bitcoin, etc.)
8. ID third party CC fraud, such as stolen CC numbers
9. Excessive mileage/parking/per diem
10. Excessive submission below threshold
11. Excessive travel in "x" period of time
12. Split (or structured) transactions that are broken down into smaller amounts
13. Mileage on the same days as rental car
14. Identify instances where the employee received a credit from the airline, for example booked a first class seat, then flew coach and took the difference

Implementation Considerations

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Data Analytics is a Team Effort

1. *Planning* is required to ensure that analytics are well directed and focused on accomplishing objectives
2. *Risk identification* is necessary to focus our analytics
3. *Accessing the Data* is the process by which we obtain information from our clients
4. *Technical Analysis* of the data requires the skillful blend of knowledge and technical capability. The analysis should follow the plan established in the planning and risk identification phases.
5. *Interpreting the Results* of the data analysis is a team effort, the most knowledgeable members of the engagement team should be relied up to identify which results are relevant to accomplishing the engagement objectives
6. *Reporting* we report in compliance with our professional standards, we express results in an impactful way and we document the procedures we performed
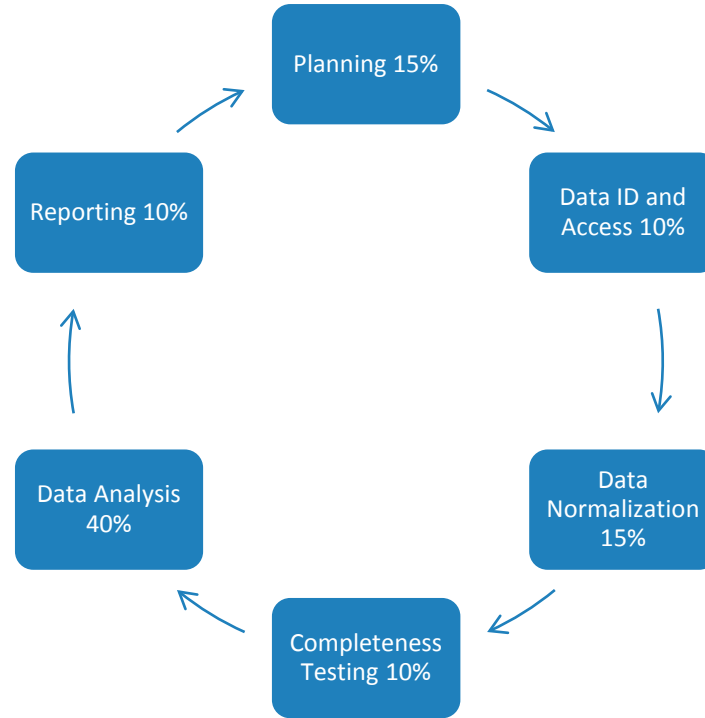
Implementation Considerations

- Generally, the data analysis should be performed at the <u>beginning stages</u> of the engagement
  - It can be utilized to focus procedures and identify areas of risk
  - It can be used as a benchmark for expectations
  - Data issues can be vetted early, while still allowing time to accomplish engagement objectives
    - ◊ Completeness Testing

Implementation Considerations

- Engagements **<u>small and large</u>** can benefit from data analytics
  - Applied on engagements with as little as 10 chargeable hours
- Well conducted data analytics makes engagements more efficient and effective
  - Better match procedures to areas of consequence and high risk
  - Automate, otherwise time consuming and less effective procedures

Budgeting Considerations

Planning 15%

Data ID and Access 10%

Data Normalization 15%

Completeness Testing 10%

Data Analysis 40%

Reporting 10%

Questions?

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Interviewing for Fraud Detection

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Objectives

1. Describe the structure of an interview and the elements necessary to conduct effective interviews

2. Identify considerations necessary to prepare for an interview

3. List methods to make interviews as productive and informative as possible

4. Explain the importance of non-verbal communication during the interview process

Effective Interviewing

1. Interviews are more important than you think!

2. How to make the most out of your interview

3. Non-verbal communication says a lot

Interview Structure

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Structure of the Interview

- Preparation
- Introduction
- Rapport Building
- Questions
- Verification
- Catch-all questions
- Departure
- Critique

Preparation

- Know the objective of your interview – Purpose
- Know your Case/Audit/Investigation – May only have one chance for interview, have your ducks in a row
- Know as much as you can about the person you are going to interview
- Know elements of Crime/Audit/Internal Controls

Be a Positive Interviewer

- Use positive language at beginning of the interview

- Be confident and professional

- Positive and confident people are respected and liked and get better results

Initial Contact/Introduction

DRESS FOR SUCCESS

- Initial contact sets the tone

- Who you are

- Who you work for

- What you want (nature of the interview) – People may not be cooperative if they don't know why you want to talk with them

  - I always say, "I need to talk to you." Doesn't give person a chance to say "no." Instead of saying, "Can I talk to you?"

Rapport Building

- The establishment of non-threatening common ground between the interviewer and interviewee. Make the interviewee feel important.
- Which can be built around biographical data, hobbies, sports, family, weather, etc. Look at photos in person's office and talk about them – family members, vacations, hobbies, etc.
- Don't feel rushed into getting in the question part of the interview. The more effective rapport you have will go a long way toward the success of the interview.

Questions

- Open

- Closed

- Indicator

Open

- "Tell me what happened"

- "Describe your activities"

- It's better when you don't know much about the case:

  - Lets the interviewee tell his story

  - Lets you observe his body language. Is he being cooperative or being evasive?

- Good way to get quiet people to talk

Closed

- Answer with "yes" or "no"

- Good way to get info quick

- Also good if the interviewee is too talkative or is trying to take control of the interview

Indicator

- "Would there be any reason someone said you took the money?"
- (Would there be a reason someone said you did not follow the ICs?)
- "What should happen to someone who took the money?"
- (What would happen if you did not follow the ICs?)
- "Why do you think a person would take the money?"
- (What do you think about a person who does not follow the ICs?)
- Watch person's body language and verbal cues – Does he hesitate, stutter, seem evasive?

3 Ways To Ask A Question

- "Did you take the money?"

- "You took the money, didn't you?"

- "You didn't take the money, did you?"

Questions To Ask

- Who?
- What?
- When?
- Where?
- How?
- Why?

Listening

- Make sure you listen to answers

- Don't get too focused on asking the next question that you

  aren't listening

Questions To Avoid

- **Leading**
  - Was the car red? Instead of: What color was the car?

- **Compound**
  - Did you notice anything unusual or did you look outside the window that night?

- **Unclear**
  - Who is responsible for internal controls? (Interviewee will not respect you if you appear to be disorganized or all over the map)

- **Loophole**
  - "Did you use any drugs?" The person answers "I used marijuana" but fails to mention any other drugs. Answer is truthful but incomplete.

Verification

- To ensure accuracy:

  - Provide opportunity to take notes or additional notes

  - Prompt further recall

  - "Let me go over this one more time with you to make sure that I have this right"

  - Did they change their story?

Catch All Questions

- "Is there anything else that I should be aware of?"

- "Is there anything else that you would like to tell me?"

Departure

- Lay the foundation for re-contact

- Leave them with a good impression

Critique

- What worked well?

- What went poorly?

- What would I do differently?

Tips For A Good Interview

- Be professional, confident, and respectful

- Limit the number of people in the room

  - Easier to talk to one person than more than one

- Give information to get information

- Make it a conversation

  - Not a list of questions

- If possible, don't have a desk or table between you and the interviewee

- Listen to what they are saying and what they are NOT saying

  - Are they hiding something?

Detection of Deception

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

FBI Story

Fugitive Investigation

- Went to mother's home to speak to mother

- Asked mother one question three times

- "Have you seen your son lately"

- Same reaction three times but different than her normal behavior

- Found son hiding in the attic

Fight Or Flight Response

- It actually is Freeze, Fight, or Flight

- Physiological responses take place when someone is being deceptive:

  - Perspiration

  - Breathing

  - Heart Rate

Two Ways A Person Can Lie

- Omission – They simply leave the information out

  - Harder to detect the lie

- Fabrication – They make up something

- Most people lie by omission – "I didn't steal the money, I wasn't there"

Two Ways A Person Can Lie

- Both the guilty and the innocent may be nervous, worried, or anxious during the interview/interrogation

- The innocent will fear the unknown, fear error (police will make mistake), and fear of involvement or testifying

- The guilty will fear the unknown, fear detection, fear punishment

Two Ways A Person Can Lie

- Determine normal verbal and non-verbal responses during beginning of interview

- Build rapport to make person comfortable and observe his verbal and non-verbal characteristics/patterns

Indicator Questions

- "Why do you think someone might have done this?"

- "What should happen to the person when caught?"

- "Any reason someone would say you were at the scene?"

- Observe closely their reactions to questions

Truth & Deception

- Lying requires the deceiver to keep facts straight, make the story believable, and withstand scrutiny

- Truthful – Convey information, make you understand

- Deceptive – Convince you and manage your perceptions

Truth & Deception

- Attention should be directed to deviations from a person's normal patterns of behavior

- Look for clusters (more than one) of deceptive behavior.

    - "One of something is nothing"

Two Basic Types Of Deceptive Indicators

- Verbal

- Non-verbal

- Verbal indicators of deception are more reliable

Verbal

- Equivocation – Lack of conviction. Such terms allow the speaker to evade the risk of commitment. The speaker is undermining his own assertion.

  - Examples – "Kind of " "Sort of" "I think" "To the best of my knowledge"

- Analyzing adverbs

  - Intensifying adverbs: "Truthfully" "Really" Honestly"

  - Did you take the money? "I really, honestly, can't remember that"

  - Minimizing adverbs: "Just" "Only" "Simply"

  - Were you with her? "I was only in the house for a few minutes"

- Other possible verbal indicators of deception: stuttering, pausing, nervous laugh, memory lapses, unclear thought lines, repetition of thoughts

- Phrases often used by liars: "I have no reason to lie to you" "Why would I lie to you?" "You probably think I did it" "I know it looks like I'm guilty"

Denials

- Innocent - "I didn't steal any money"

  "I didn't create that journal entry"

  "I didn't approve that invoice"

- Guilty – "I didn't take that $3,500" (Specific denial, maybe he only stole $3,000)

  "I'm not responsible for making journal entries" (Specific denial)

  "I don't know the company on that invoice" (Specific denial)

Blocking Statement

- "If I took the money, I would have paid bills with it"
- "Why would I do this?"
- "Nobody in their right mind would…"
- "I work at a bank, they have so much money I don't even see it anymore!"

Text Bridges

- A liar will convey truth up to the event he wants to conceal. He will then use a "text bridge" to cross over the activity he wants to hide.

  - "After that"

  - "Later on"

  - "Next"

  - "Finally"

Non-Verbal Indicators of Deception

These don't necessarily mean someone is lying. A person may only be nervous, under stress, or reacting to your question.

- Wringing hands, unfolding arms and legs, crying, picking on clothes, coughing, grooming gestures, sighing

- Some research indicates that the best non-verbal indicators of deception are:
  1. Hand(s) to the head during denial – Covering mouth as he speaks, pulling ear, touching nose
  2. Head aversion – Leaning away from the interviewer while making denial
  3. Lower half of body more truthful, especially the feet

Create Opportunities

Questions?

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Case Study #1

Flushing Money Down the Drain

Background

- Type of Fraud – Hybrid between "Sales Scheme" and "Unrecorded Sales"

  - Sales Scheme = Involves the underselling of company goods by an employee to a company in which the employee maintains a hidden interest (giving the company more goods than it paid for)

  - Unrecorded Sale = Collecting cash, keeping a portion of the cash, and underreporting the sale amount

- Total theft – $505,000

Background

- EDU: Equivalent Dwelling Unit
  - A numerical value designation where 1 EDU represents the sewage from a single family residential household
  - One-time fee assessed to connect to sewer system is based on EDUs
  - Fee is assessed and collected by the water agency and passed onto the regional wastewater authority
  - EDU purchases remain with the existing building and are not transferrable
- New construction or tenant improvements require a permit from the water district; the fee is assessed through the permitting process.

Background

- Supervisor orchestrated a "credit" to an applicant connecting to the sewer system (EDUs).

- Supervisor confirmed that the EDUs were "owned" by another business.

- The applicant purchased EDUs from this other business for $505,000.

Background

- The applicant purchased EDUs from this other business for $505,000; however:

  - There was no record (at the water agency) that this business had ever paid for EDUs.

  - There was no record (at the water agency) that these EDUs existed at the location specified.

  - If the business had paid for EDUs but never used them, it could have received a credit from the water district.

  - Generally, the policy did not allow for a "transfer" of EDUs between addresses.

Create Opportunities

Background

- Supervisor included a "credit" in the fee calculation.

- The explanation for the credit on the paperwork indicated that it was due to <u>existing</u> EDUs at the location.

CAPITAL CAPACITY REIMBURSMENT FEES:

- COMMERCIAL USE
  __130.5__ FIXTURE UNITS × __0.0741__ SEWER FACTOR = __9.67005__ Equivalent Dwelling Units [EDUs]

- INDUSTRIAL USE

  SEWER FLOW: __50,000__ gallons per day (largest average discharge based on calendar month average)

  BOD: __500__ mg/liter (largest average concentration based on calendar month average)

  TSS: __115__ mg/liter (largest average concentration based on calendar month average)

  50000 gpd / 270 gpd × [0.37 + 0.31 × (500 mg/L / 230 mg/L) + 0.32 × (115 mg/L / 220 mg/L)] = __224.29__ EDUs

- CAPITAL CAPACITY CREDIT

  The following paid and available Capital Capacity EDUs are to be applied to this Tenant Improvement project per the Building Owner's written permission submitted to the District, or by demolition of existing sewer drainage fixtures within Tenant space: EDU Credit: __119.54926__ EDUs

- TOTAL EDUs (Ord. 32-C, Exhibit A)
  __114.41079__ EDUs × __$4,909.00__ PER EDU = __$561,642.57__

How the Fraud was Detected

- The EDU credit on the applicant's paperwork was questioned by the Engineering Department at an external agency (fees were collected on their behalf).

- The credit on the paperwork indicated that the credit was due to "existing" EDUs; however, there was no record of EDUs of that magnitude having ever existed or been paid for that location.

- During an on-site visit by the Engineering Department, the applicant revealed that the "credited" EDUs had been purchased from a 3rd party (this raised suspicion).

Create Opportunities

How the Fraud was Detected

- Engineering Department knew that an audit was coming up of the EDU process, so it was referred to the Internal Audit Department – asked them to include this transaction in their sample.

- During the **audit**, the Supervisor kept telling the auditors that the documentation to support the credit was missing, but the EDUs were purchased by previous tenants. The Supervisor never mentioned that a payment was made to a 3rd party.

- The auditors called the applicant that purchased the EDUs and obtained documentation regarding who the EDUs were purchased from.

How the Fraud was Detected

- Documents provided by the applicant (and provided to water district):
  - Fictitious business name filing of the company from which they purchased the EDUs
  - Driver's License of the person that owned the business
- Personnel at the water district recognized the "owner" of the business as a grade school friend of the Supervisor
- After several requests, the Supervisor could not provide documentation to support the credit

Length of Time Until Detection

- Transaction occurred in January 2013
- Internal audit began questioning this transaction in July 2013; however, internal audit:
  - Not aware of the possible relationship between the Supervisor and the "owner" of the business that was paid for the EDUs
  - Believed it was poor documentation and/or non-compliance with policy (not allowed to transfer EDUs between addresses)

Length of Time Until Detection

- Water district became concerned after the internal audit report was released in approximately March 2015

- Investigation began in July 2015 after unsuccessful attempts at resolving the matter with the Supervisor

Investigative Techniques

- Public database searches and background checks
- Interviews:
  - Employees of the water district
  - Internal auditors at external agency
  - Engineering department at external agency (first raised concern about transaction)
  - Suspect (Supervisor)
- Analyzed available documents
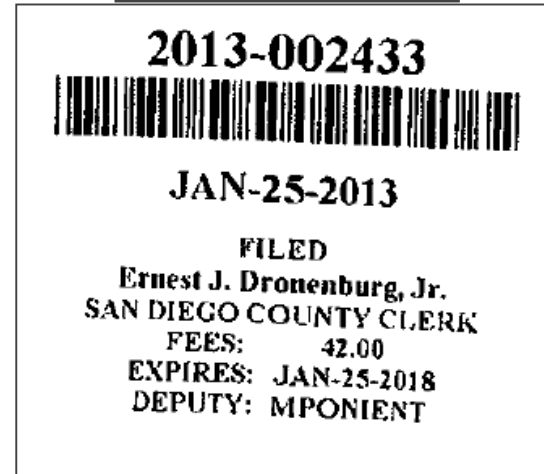- Computer hard-drive image & search; email search

Investigative Techniques

Pulled Fictitious Business Name filing and identified that the version provided by the "owner" to the applicant had been altered.

Altered Document

Actual Document

Investigative Techniques

A public record search on the "owner" of the business that was paid for the EDUs revealed that he lived in a house owned by the Supervisor at the water district (information partially redacted).


```
1576                          ESCONDIDO CA 92026-222
Summary  ]
    Owner:
        SHAWN                    [ View Person Record ]
    Purchase Date: 03/25/2015
    Assessed Value: $256,000
    Living Square Feet: 1,188
    Land Square Feet: 13,600
```

Investigative Techniques

An online search of the business address (in San Diego) revealed that the only building on the small street appeared abandoned.

Investigative Techniques

Email Review:

- In June 2012, Supervisor sent an email confirming that the address had only 11.93 EDUs

- Supervisor sent himself a template of a transfer agreement that was ultimately used and signed by the two companies in making the "transfer"

- In January 2013, Supervisor sent an email stating that the address had EDUs of 119.54926 from past tenants and occupancies

Investigative Techniques

Email Review (cont.):

- Email from 2010 in which Supervisor confirmed that he was friends with the person later listed as the "owner" of the business that sold the EDUs

- Supervisor discusses establishing a "market" for EDUs that can be sold at a discount (*believed to be his rationale*)

Profile of Suspect

- <u>Supervisor</u> – 34% of frauds are committed by a manager
- <u>Male</u> – 69% of frauds are committed by males
- <u>43 years old</u> – 19% of fraudsters are between the ages of 41 and 45 (36-40 and 41-45 were both the highest at 19%)
- <u>14 years at water district</u> – 47% of fraudsters have been with their organizations for more than 5 years
- Married with 2 children – stable family life
- No known addictions or health issues

Red Flags - Supervisor

- A lot of autonomy – lack of oversight/review
- Shared with co-workers how he made "good money" on a side job – one time thing
- Personal relationship with the "owner" of the fictitious business
- Often complained that there was not an "open market" for the sale of EDUs

Internal Control Weaknesses

- Supervisor given a lot of autonomy – lack of oversight/review
- Supervisor was the only person that calculated EDUs for this particular type of tenant improvement
- All records of existing EDUs were in paper – no database
- EDUs are not a physical asset – only exist on paper

Other Information

- When the Supervisor was questioned about the transaction during the audit and by his superiors, he could not locate supporting documentation or recall the specifics of the transaction. Everyone we spoke to said that this was unusual as he was always detailed and organized.

- The form used to calculate the assessed fee to the new tenant did not accurately describe the nature of the credit given.

Email Review

"I have achieved some professional 'stretch goals' of which you are unaware, and I think you would be surprised. I also would like to request some additional 'stretch goals' that I can demonstrate are very achievable. Please let me buy lunch. I've been anxious to share with you guys for *many* months."

Outcome

- On the same day of the interview of the Supervisor, his <u>defense counsel</u> contacted the water district and asked if the matter had been referred to law enforcement

- He ultimately resigned from his position

- Pled guilty to grand theft by false or fraudulent representation or pretense

- Water district received full restitution from the Supervisor (former employee) and the accomplice on the day the guilty plea was entered

  - Supervisor: $463,257.56
  - Accomplice ("owner" of business that sold EDUs): $65,044.44

Case Study #2

Banks are not an internal control

Background

- **Entity:** Medical insurance company
- **Type of fraud:** Cash disbursement scheme
- **Total theft:** $697,300 (207 checks)
- **Time period:** 10/20/2003 to 2/14/2018*
- No other employees involved

*Checks identified by the bank went back to only 2011; additional checks identified in investigation because client kept copies of cancelled checks

Background

- **Employee:**
  - Hired on January 20, 2003
  - During her employment she received 2 promotions; annual evaluations showed she always met or exceeded expectations
  - Duties included interacting with customers to resolve claims and related issues

- **Investigation:**
  - CLA retained March 2018
  - Worked with internal audit department

How the Fraud was Detected

- The employee's bank identified suspicious checks deposited into the personal bank account of the employee and her husband
  - Two checks deposited in December 2017 were found to be suspicious and the bank sent a letter to the suspect

- The bank then conducted internal research on the account

- Bank alerted local law enforcement of numerous suspicious checks deposited into the bank account of the suspect

- Law enforcement reviewed bank surveillance video tape and saw the suspect making the deposits

How the Fraud was Detected

- Law enforcement interviewed the employee and obtained a confession

- The employee admitted to committing the theft starting prior to 2011

- Law enforcement then notified the insurance company of the possible loss to the company and provided a listing of the checks the bank had identified as suspicious

  – All of the suspicious checks deposited were issued by the insurance company

- Employee was terminated one week later and CLA was engaged

Scope of Investigation

- Determine whether there was any additional loss to the organization besides what had been identified by the employee's bank

  - The bank could look at activity going back to only 2011, and the employee admitted to law enforcement that she had started prior to 2011

- Determine whether anyone else within the organization was involved or had knowledge

Investigative Techniques

- Public database searches and background checks
- Interviews of employees of the insurance company
  - CLA could not interview the suspect because of the ongoing criminal investigation
- Computer hard-drive image & search; email search
- Data analytics on disbursements
- Reviewed documentation for disbursements:
  - Check requests
  - Cancelled checks

Fraud Scheme

- Employee prepared fictitious Accounts Payable Check Requests made payable to various providers and individuals

- On the check request form, the employee marked the "route back" option to request that the checks be routed back to the employee

  - Check requests were completed on paper and forwarded to Accounts Payable for processing (majority of time period)

Fraud Scheme

- The "route back" option was allowed and used so that customer service employees could include a letter to the customer (generally processing customer claims)

- The check requests were manually signed by employee's supervisor (she had several different supervisors during her tenure)

  - Internal audit interviewed employee's current and former managers, who claimed that most of the approval signatures appeared to be forged

Fraud Scheme

- Electronic payment system was implemented in the last year; however, the employee simply uploaded to the system scanned copies of the paper check requests

- Payments were processed using a "one-time vendor" account
  - Did not require the payee to be established through the vendor setup process
  - Allowed manual entry of the payee name and address
  - Vendor code "1" identified on checks
  - Believe accounts payable used the one-time vendor account because the payees indicated on the check requests were not in the system

Fraud Scheme

- Payee names on checks:
  - 2003 to 2008: Employee primarily used names that appeared similar to her name or the names of family members (husband, daughter, mother)
  - 2008 to 2018: Employee primarily used names that were providers in the vendor listing
- Deposited checks:
  - 2003 to 2006: Employee deposited checks into at least 4 different bank accounts
  - 2007 to 2018: Employee deposited checks into 2 bank accounts

Fraud Scheme

- Check endorsements:
  - **Individual Names:** Forged signature of payee name; then forged husband's signature
  - **Provider Names:** Stamped "Patient Reimbursement – Pay to the Order Of"
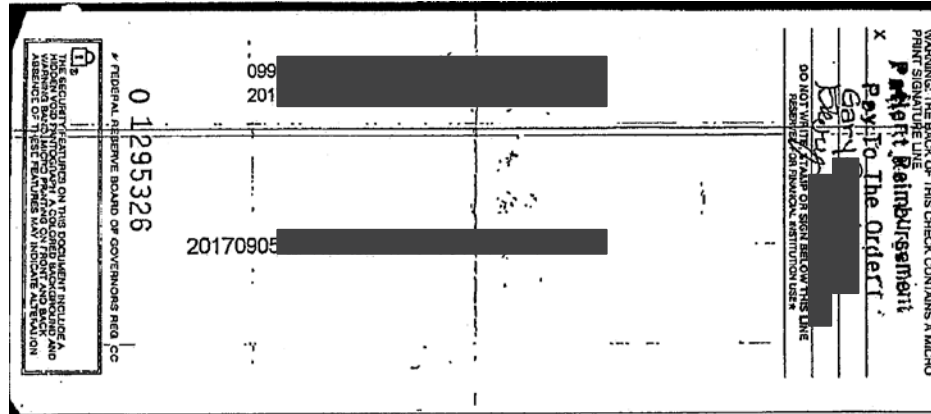
Analysis of Documents

- Check Requests:
  - Client pulled all manual (paper) check requests for 2003 to 2018 and identified any requested by the employee
  - Most check requests had no supporting documentation (even provider payments did not have invoices or statements from the providers)

- Cancelled checks:
  - 13 variations of signatures for employee, husband, daughter, and son
  - Used bank account number on back to identify many checks that did not have recognizable payee name or endorsement

Data Analytics

- Data used:
  - One-time vendor account
  - Customer accounts
  - Certain discounts processed by employee
  - Manual check request disbursements
- Analyses performed:
  - General trending
  - Round dollar amounts
 - Same/similar names and addresses
  - Benford's Law

Challenges

- Everything was documented on paper (check requests, approvals, route back)
- Identified a handful of check requests that had a different employees name and mail box number, but the check was deposited by the suspect employee
- Availability and quality of data
  - Payee name and address for one-time vendor account
  - Disbursements were grouped when recorded to customer accounts
  - Manual check listing did not have requestor name included

Create Opportunities

Results of Investigation

- 207 checks totaling $693,239.54

- Majority of this loss impacted a customer, who the insurance company was reimbursing plus interest

- No other employees were identified as involved

- As we identified additional checks the details were provided to law enforcement

Create Opportunities

Results of Investigation

Majority of checks were to payees with California addresses

Amount of Checks to Payees with California Addresses
2003-2018

California
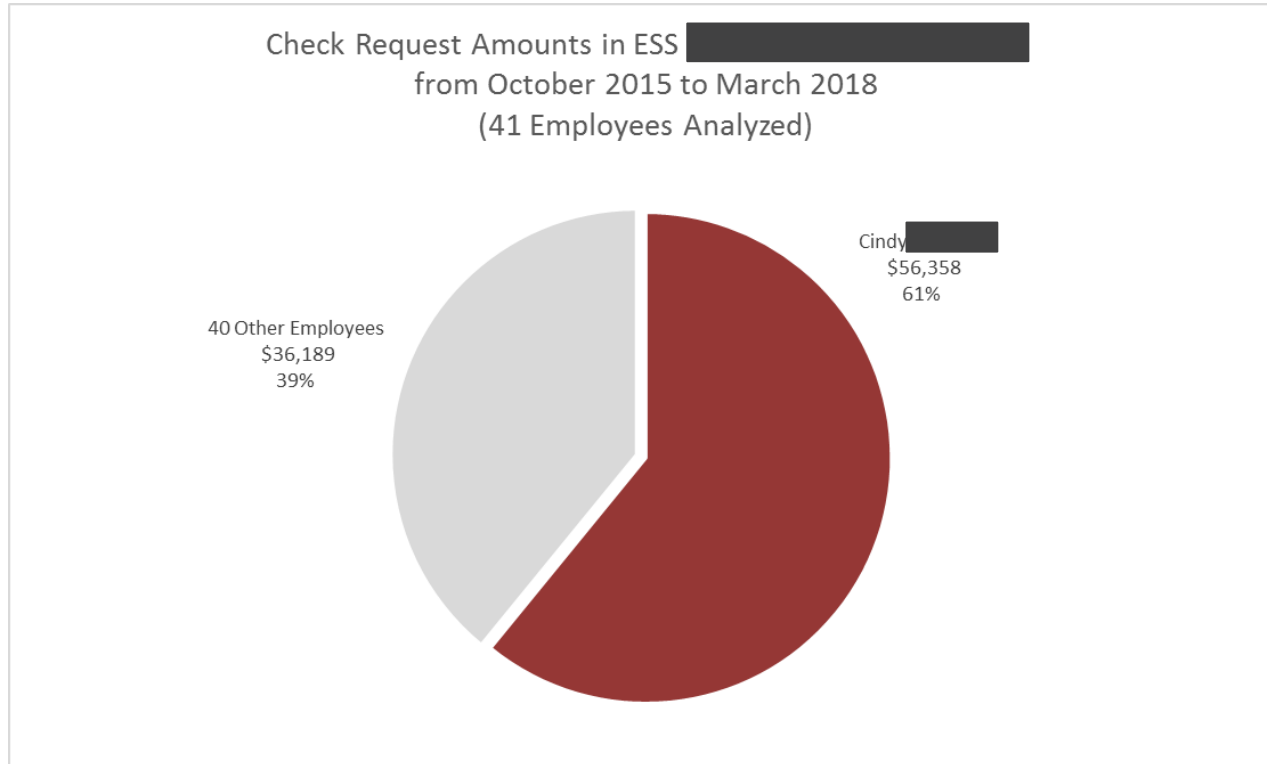$496,016
72%

Other States
$197,224
28%
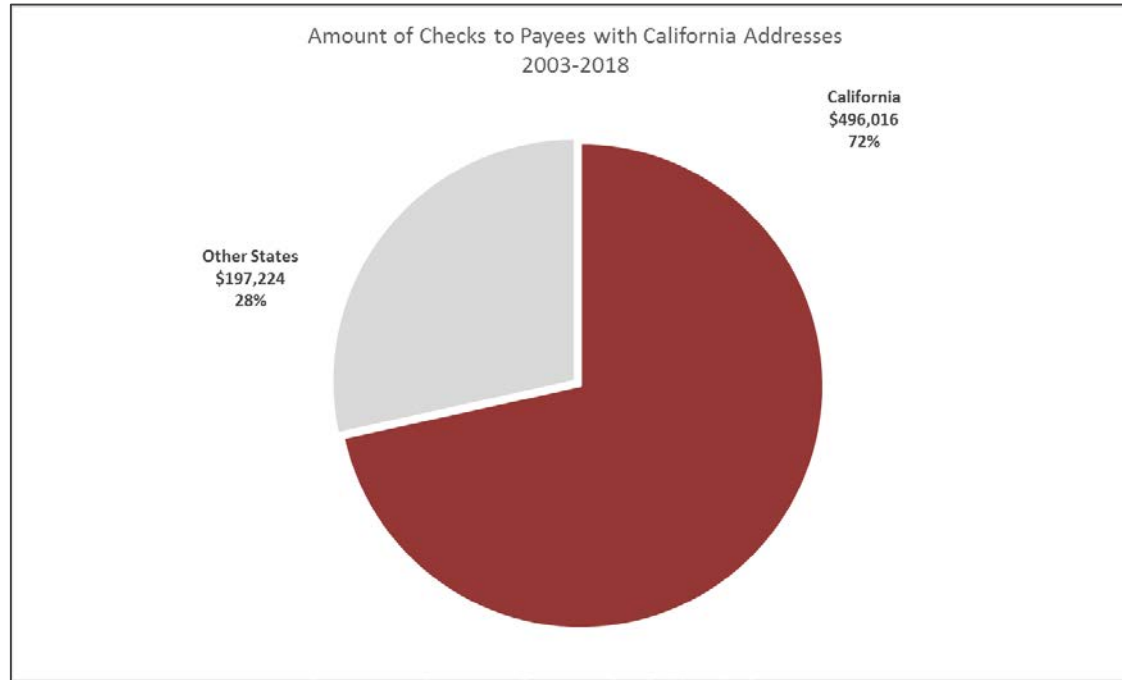
Results of Investigation

Route Back Analysis

- Manual checks were processed electronically for approximately 2.5 years

- Included only employees who worked within the same department or in similar positions as the employee (41 employees)

- Employee requested 76 manual checks (2nd highest quantity)

- Employee requested $56,358 in manual checks (highest)

  - Next highest person requested only $12,882

  - 12 of the checks were over $500 and totaled $52,875

Results of Investigation

Check Request Amounts in ESS ██████████████
from October 2015 to March 2018
(41 Employees Analyzed)

Cindy ████████
$56,358
61%

40 Other Employees
$36,189
39%

Create Opportunities

Internal Control Weaknesses

- Manual check requests were handled only on paper until very recently

- Employees could request that signed checks be routed back to them (very common occurrence)

- Inadequate supervisory review prior to approval
  - No support was attached to check requests
  - A couple of the supervisors admitted to not understanding the importance of their review and approval; trusted employee

- Frequent use of the "one-time vendor" account

Internal Control Weaknesses

- No monitoring of the "one-time vendor" account

- Accounts payable never questioned when a manual check request included a payee not in the system

- Employee forwarded the manual check requests directly to accounts payable (were not required to come from the approver)

Open Discussion and Q&A

Jenny Dominguez, CPA/CFF, CFE

Jenny.Dominguez@CLAconnect.com

Phone 626-387-8227

Michael Schulstad, CPA/CFF, CGMA, FBI (ret.)

Michael.Schulstad@CLAconnect.com

Phone 908-502-2825

Create Opportunities