CSI for CIAs

WORKPLACE FRAUDS

How Fraud Happens (**The Fraud Triangle**)

1. **Opportunity** (to steal or incorrectly report **and not be detected**)
    A. Undeserved level of trust
    B. Lack of segregation of duties
    C. Lack of oversight and monitoring
    D. Poor control environment

2. **Motivation** or pressure experienced by the perpetrator(s)
    A. Financial problems
    B. Resentment towards employer or management
    C. Addictive behaviors
    D. Living beyond one's means

3. **Rationalization** – mental justification by the perpetrator(s)
    A. "They owe it to me"
    B. "No one gets hurt"
    C. "I am not stealing because I will repay the monies borrowed."
    D. "Everybody does it some time or another"
    E. No one told me my behavior was wrong"
    F. "Others do this and nobody has gotten caught'

How Fraud Money Is Spent (Albrecht Study)

1. Perpetrators are spenders (not savers)
2. Big fraud proceeds are usually spent on:
    A. New home
    B. Expensive automobile(s)
    C. Expensive vacations
    D. Extramarital relationship(s)
    E. Speculative investments

Who Commits Fraud?

1. People with **all three** (3) components of the **Fraud Triangle**
2. Well-trusted, long-term employees
3. No-good, “rotten-to-the-core” people
4. Nice people, with personal problems that are overwhelming
5. Regular folks (like us)

Necessary Ingredients (2)

1. **People** (anyone with a need or motivation)
    A. Employees
    B. Management or owners
    C. Vendors
    D. Customers
    E. Others
        (1) Former employees
        (2) General public

2020 Report to the Nations- 2020 Global Study on Occupational Fraud and Abuse.

1. Dollar loss and percentages from the three major categories of fraud.

	Dollar Loss	**Percentage**
A. Asset misappropriation	$100,000	86%
B. Corruption	200,000	43%
C. Financial reporting fraud	954,000	10%

2. Confidential **hot lines** and other reporting mechanisms

   A. The #1 fraud detection method is **tips (43%).**

3. Organization **type of victim** (% of cases in report, in parenthesis)

		Median Loss
	%	**Amount**
Private Company	44%	$150,000
Public Company	23	150,000
Government	27	100,000
Nonprofit	25	75,000

4. **Size of organization – # of employees**

		Median Loss
	%	**Amount**
Less than 100	26%	$150,000
100 – 999	23	120,000
1,000 – 9,999	27	100,000
10,000 +	25	140,000

5. **Background Checks**

	Yes	**No**
Performed	52%	48%
Revealed a Red Flag for Problems	13%	87%

6. **Initial detection method** – all cases (% exceed 100 because some frauds were detected by multiple means)

	Percentages
Tips	43%
Internal audit	15
Management review	12
Other	6
Accident (no specific method)	5
Account reconciliation	4
External audit	4
Document examination	3
Surveillance	3
IT Controls	2
Confession	1

7. **Sources of tips by percentage**:

Employee	50%
Customer	22
Anonymous	15
Vendor	11
Other	6
Owner	2
Competitor	2

8. **Tenure of perpetrators**

		Median Loss
	%	**Amount**
10 + years	23%	$200,000
5 – 10 years	27	190,000
1 – 5 years	46	100,000
Less than one year	9	0,000

9. **Gender** of perpetrator in the United States (% of cases in parenthesis)

		Median Loss
	%	**Amount**
Male	72%	$150,000
Female	28%	$ 85,000

10. **Education** of perpetrator

		Median Loss
	%	Amount
Postgraduate degree	15%	$200,000
Bachelor degree	49	175,000
Some college	14	150,000
High school graduate	22	80,000

11. **52% of all occupational fraud came from the following four departments.**

		%
1.	Operations	15%
2.	Accounting	14
3.	Executive/upper management	12
4.	Sales	10

12. **How do victim organizations punish fraud perpetrators and percentages?**

	Punishment	Percentage
1.	Termination	66%
2.	Perpetrator was no longer working	11
3.	Settlement agreement	11
4.	Permitted or required resignation	10
4.	Probation or suspension	9
5.	No punishment	5

13. **Why do organizations decide not to refer cases to law enforcement?**

	Reasons
1.	Fear of bad publicity
2.	Internal punishment was sufficient
3.	Too costly
4.	Private settlement

5. Lack of evidence

6. Civil suit

7. Individual disappeared

14. **Red flags for fraud**

85% of all fraudsters displayed at least one behavioral red flag while committing fraud. 52% displayed behaviors related to work and 63% displayed behaviors related to their personal life. What were some of the red flags exhibited by the perpetrators and at what percentage?

1. Living beyond one's means	42%
2. Financial difficulties	26
3. Unusually close relationship with vendors/customers	19
4. No red flag behavior	15
5. Control issues/willingness to share duties	15
6. Wheeler/dealer attitude	13
7. Divorce/family problems	12
8. Addiction problems	9
9. Complained about inadequate pay	8
10. Refusal to take vacation	7

15. **Red flags associated with work**

1. Unusually close relationships with vendors/customers
2. Control issues – unwillingness to share duties
3. Irritability, suspiciousness, or defensiveness
4. Wheeler-dealer attitude
5. Complained about inadequate pay
6. Refusal to take vacations

7. Excessive pressure from within the organization
8. Complaints about lack of authority
9. Records altered, missing or destroyed.
10. Chronic shortages of assets or records.
11. Signatures on records appear to be forgeries.
12. Employee gives inadequate answers when questions about missing supplies, assets or funds.
13. Customer or supplier complaints about shortages or discrepancies.

16. **Internal control weaknesses that contribute to occupational fraud.**

	Percentages
1. Lack of internal controls	32%
2. Overriding existing controls	18
3. Lack of management review	18
4. Poor tone at the top (culture)	10
5. Lack of competent personnel in oversight roles	6
6. Lack of independent checks/audits	5
7. Lack of fraud education	3

17. **How is fraud concealed?**

	Percentages
1. Created fraudulent physical documents	49%
2. Altered fraudulent physical documents	36
3. Altered electronic documents or files	27
4. Created fraudulent electronic documents of files	26
5. Did not involve any attempt to conceal the fraud	12

WORKPLACE FRAUDS

Types of Misappropriation Schemes (**OFA**)

1. **Billing schemes** – perpetrator submits or alters an invoice, which causes employer to **willingly issue** a check

   A. Invoicing via shell (fictitious) companies

      (1) Self-approval of invoice by perpetrator

      (2) "Rubber stamp" supervisors

      (3) Reliance on false invoice (and related documents, if any)

   B. Invoicing via non-accomplice vendors

      (1) Pay-and-return schemes – overpaying a legitimate invoice and intercepting the "refund" payment (from the vendor)

      (2) Overbilling invoices for a legitimate vendor and intercepting the excessive payments from the employer

   C. Personal purchases with company funds ("purchase" schemes)

      (1) Perpetrator authorizes payment

      (2) Falsifying documents (such as purchase orders, receiving reports, etc…)

      (3) Altering existing (legitimate) documents (either manually **or through the computer system**)

      (4) Company credit card (abuse) or personal purchases on an open vendor account

      (5) Returning merchandise for cash (or misappropriating refund checks)

2. **Skimming** – removal of cash (or checks) **before an entry** to the accounting system

    A. Sales

        (1) Not entering sale at register

        (2) Under-recording sale or using a false discount entry

    B. Receivables

        (1) Lapping

        (2) Journal entries (to write off balances)

    C. Refunds from vendors

3. **Register** disbursements – money removed from a register, based on a "false" or "fictitious" **transaction**, which **is recorded** (unlike skimming or larceny – which are not recorded transactions)

    A. False (fictitious) refunds – to customers

    B. False voids of actual sales

4. **Inventory and asset** misappropriation

    A. Abused or misused (but not stolen assets – vehicles, supplies, computers, and office equipment)

    B. Noncash larceny – supplies and inventory

        (1) False purchasing, receiving, or shipping documents

        (2) Corruption (normally collusive with an outside customer or vendor)

5. **Check tampering** – a type of fraudulent disbursement where an employee either prepares a **fraudulent check** for his own benefit **or** intercepts and **converts a legitimate check**

    A. Forged maker – signing another person's name to a check

    B. Altered payee – employee intercepts a legitimate check and alters the named payee (to facilitate conversion by the employee or an accomplice)

    C. Forged endorsement – employee intercepts a legitimate check and forges the payee's endorsement

    D. Concealed check – employee prepares a fraudulent check and submits it for approval, normally along with other legitimate checks

    E. Authorized maker – an employee with signature authority writes (authorizes) a fraudulent check for his own benefit

6. **Payroll schemes**

    A. Ghost employees – not an actual employee

    B. Falsifies hours, salary, or commissions – for actual employees

    C. False workers compensation claims (or other employee benefits)

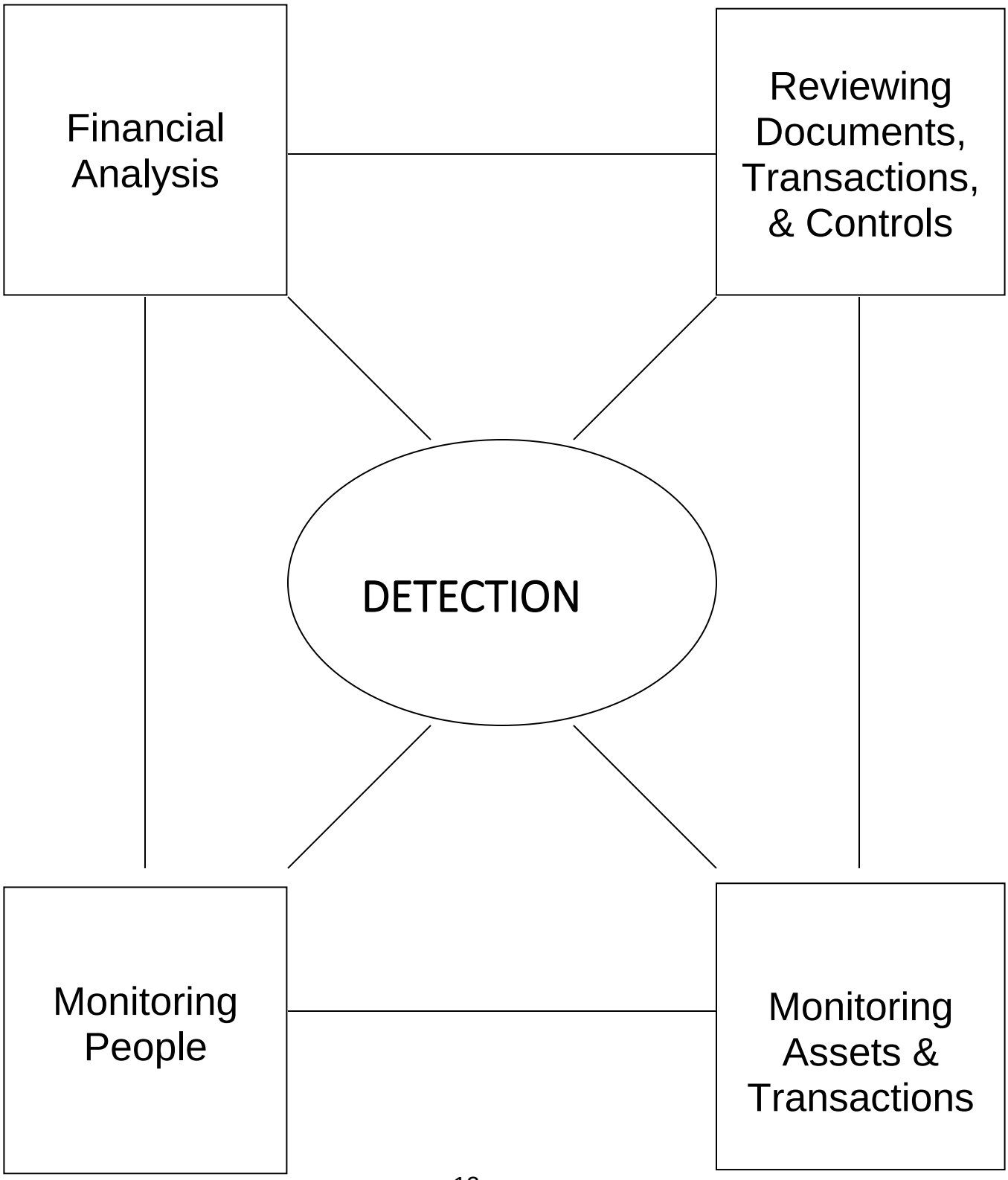
7. **Employee expense** (reimbursement) schemes – similar to payroll schemes

8. **Cash larceny** – intentional taking of employer's cash (and checks) without the consent and against the will of the employer (i.e., monies already recorded as employer assets)

RANKINGS OF ASSET MISAPPROPRIATION SCHEMES

1.	Billing schemes	20%
2.	Expense reimbursements	14
3.	Skimming	11
4.	Cash on hand	10
5.	Check tampering	10
6.	Payroll	9
7.	Cash larceny	8
8.	Register disbursements	5

DETECTION PROCEDURES
"NETWORK"



PREVENTING & DETECTING SMALL BUSINESS FRAUD

1. The following fundamentals **should not be ignored** just because "you don't have enough people (or resources) to do it" (or don't believe you have a problem)

   Outsource to qualified professionals all functions beyond the abilities of company personnel

2. Perform **periodic** internal control evaluation and fraud/theft **risk assessment** (especially when significant changes take place or when "red flags" occur)

3. Perform timely financial **trend analysis** to identify potential "red flags" (or operating inefficiencies)

4. **Segregate** (completely) incompatible functions

   Someone **not involved** in disbursements, deposits, or purchasing should receive bank statement (directly) and perform the **monthly bank reconciliation**

   Outsource if segregation is not possible

5. Perform periodic (surprise) spot checks (**monitoring**) of the high-risk areas for your company

6. Establish a **code of conduct** (including a "fraud policy") which is well communicated, understood, monitored, and enforced

7. Have a **control environment** that emphasizes **integrity** and proper internal controls (i.e., keep the other nine commandments)

8. Have proper **security** for assets, computers and technology, and high-risk transactions

9. Have adequate and appropriate bonding and **insurance**

10. Properly use an **accountability** program (ongoing education and awareness)

    A. The "number one" tool for **detecting** internal fraud is "whistle-blowing" by co-workers

    B. The "number one" **deterrent** to <u>internal</u> and <u>external</u> misappropriation is the fear of getting caught.

TOP TEN TOOLS & TECHNIQUES FOR FRAUD DETECTION

1. **Organizational commitment** to prevention & detection of occupational fraud

   A. **Executive support** (and example)

   B. Well **communicated** and **understood** by all employees (part of your "code of conduct")

   C. Managers and employees are **well-trained** to identify, report, and prevent occupational fraud

   D. Commitment should be periodically tested (monitoring)

      (1) Survey employees and managers (about fraud, abuse, & controls)

      (2) Risk assessment and evaluation by Fraud Team or outside consultant

      (3) Testing technology and other controls

2. Anonymous reporting program

   A. **Required** by Sarbanes Oxley Act

   B. **Essential** part of MAPC (Management Antifraud Programs and Controls)

      (1) The new benchmark for preventing and detecting occupational fraud

   C. The **number one tool** identified in every survey and report on fraud detection methods

3. Proper control over cash (and other "at risk" assets)

   A. **Must segregate bank reconciliation process**

   B. Use "**positive pay**" with bank depository to verify amounts, dates, and **payee**

4. Video and audio surveillance

   A. People

   B. Cash receipts

   C. Inventory and other assets

D. Satellite and cable monitoring

5. Monitor employees' e-mail, voice mail, and internet activity

6. Digital and data analysis (of transactions and information/accounting systems)

   A. Historic and contemporaneous monitoring

   B. Benford's Law

   C. Data analysis software

7. Consumer credit reports on "at-risk" or all employees

8. Proper oversight of managers and executives by:

   A. Board of directors

      (1) Required by Sarbanes Oxley Act

      (2) May outsource, to improve capabilities

      (3) Executives must submit to oversight

   B. Internal audit, audit committee, or outside consultant

9. Get transitional and / or periodic help

   A. Selling owners and management on the need for significant changes

   B. Performing certain tasks (where employees are uncomfortable or not experienced)

10. Adequate bonding and insurance

Internal Controls Modified or Implemented in Response to Fraud

1.	Increased segregation of duties	61.2%
2.	Management review of internal controls	50.6
3.	Surprise audits	22.5
4.	Fraud training for employees	16.4
5.	Fraud training for managers/executives	14.8
6	Job rotation/mandatory vacations	13.5
7.	Internal audit	12.3
8.	Anti-fraud policy	11.7
9.	Code of conduct	8.7
10.	External audit of financial statements	8.7
11.	Hotline	7.9
12.	External audit of internal controls	7.8
13.	Independent audit committee	6.0
14.	Management certification of F/S	5.9
15.	Rewards for whistleblowers	4.0
16.	Employee support program	1.8

CFEs' Ranking of Controls' Importance in Detecting or Limiting Fraud

	Control	Average Score (4.0 tops)
1.	Internal audit/fraud department	3.81
2.	Surprise audits	3.51
3.	Management review of internal controls	3.17
4.	Fraud hotline	3.03
5.	Mandatory job rotation/vacations	3.02
6.	Rewards for whistleblowers	2.86
7.	Audit of internal controls over financial reporting	2.65
8.	Audit of financial statements	2.53